

TOP

BURPSUITE

EXTENSIONS
USED BY
PENETRATION TESTERS



DOCUMENT BY: VIEH GROUP

Disclaimer

This document is generated by VIEH Group and if there is any contribution or credit, it's mentioned on the first page. The information provided herein is for educational purposes only and does not constitute legal or professional advice. While we have made every effort to ensure the accuracy and reliability of the information presented, VIEH Group disclaims any warranties or representations, express or implied, regarding the completeness, accuracy, or usefulness of this document. Any reliance you place on the information contained in this document is strictly at your own risk. VIEH Group shall not be liable for any damages arising from the use of or reliance on this document. also we highly appreciate the source person for this document.

Happy Learning

Note: This document is not created by a professional content writer so any mistake and error is a part of great design

Content Credit: piyush kumawat (securitycipher)

Let's begin

Burp Suite's power lies in extending its core with user-built plugins, boosting capabilities and workflow efficiency.

This sentence highlights the key points of extensions:

- They extend Burp Suite's functionality.
- They are user-built, offering customization.
- They improve efficiency and workflow.

I hope this is helpful!

let's move to next page

What is burp suite ?

Burp Suite is a powerful tool used for web application security testing. It is a comprehensive platform that includes a range of tools to help identify vulnerabilities and security flaws in web applications. The suite includes a web proxy, spider, scanner, and intruder, which can be used to intercept and modify traffic, crawl websites, identify potential vulnerabilities, and test for vulnerabilities. Burp Suite is an essential tool for any security professional or researcher looking to ensure the security of their web applications. It is also widely used in the ethical hacking community due to its versatility and effectiveness.

Top Burp Suite Extensions used by Penetration Testers

Active Scan ++

Active Scan++ is a powerful Burp Suite extension that enhances the active scanning capabilities of the popular web application testing tool. This extension utilizes advanced techniques and algorithms to identify a wide range of vulnerabilities in web applications, including cross-site scripting, SQL injection, and insecure direct object references.

Additionally, Active Scan++ can detect issues with authentication, authorization, and session management, providing comprehensive coverage for web application security testing. One of the standout features of Active Scan++ is its ability to accurately and efficiently identify potential injection points within the application, making it an invaluable tool for any web application security professional. With its advanced capabilities and seamless integration with other Burp Suite tools, Active Scan++ is a must-have extension for anyone looking to improve the effectiveness and efficiency of their web application security testing.

BApp Store

The BApp Store contains Burp extensions that have been written by users of Burp Suite, to extend Burp's capabilities.

Search... (?)

Name	Inst...	Rati...	Pop...	Last upd...	System...	Detail
.NET Beautifier	★ ★ ★	23 Jan 2...	Low			
403 Bypasser	★ ★ ★	27 Sep ...	Low	Pro exten...		
5GC API Parser	★ ★ ★	23 Sep ...	Low			
Active Scan++	★ ★ ★	24 Nov ...	Low	Pro exten...		
Add & Track Custo...	★ ★ ★	25 Feb 2...	Low	Pro exten...		
Add Custom Header	★ ★ ★	08 Jul 2...	Low			
Add to SiteMap+	★ ★ ★	28 Nov ...	Low			
Additional CSRF Ch...	★ ★ ★	14 Dec ...	Low			
Additional Scanner ...	★ ★ ★	21 Dec ...	Low	Pro exten...		
Adhoc Payload Pro...	★ ★ ★	31 Jan 2...	Low			
AES Killer, decrypt ...	★ ★ ★	13 May ...	Low			
AES Payloads	★ ★ ★	04 Feb 2...	Low	Pro exten...		
Anonymous Cloud, ...	★ ★ ★	11 Feb 2...	Low	Pro exten...		
Anti-CSRF Token Fr...	★ ★ ★	28 Feb 2...	Low			
Asset Discovery	★ ★ ★	12 Sep ...	Low	Pro exten...		
Attack Surface Dete...	★ ★ ★	16 Dec ...	Low			
Auth Analyzer	★ ★ ★	20 Dec ...	Low			
Authentication Toke...	★ ★ ★	23 Sep ...	Low			
AuthMatrix	★ ★ ★	15 Oct 2...	Low			
Authz	★ ★ ★	01 Jul 2...	Low			
Auto-Drop Requests	★ ★ ★	10 Feb 2...	Low			
AutoRepeater	★ ★ ★	10 Feb 2...	Low			
Autorize	★ ★ ★	01 Oct 2...	Low			
Autowasp	★ ★ ★	10 Feb 2...	Low	Pro exten...		
AWS Security Checks	★ ★ ★	18 Jan 2...	Medium	Pro exten...		
AWS Signer	★ ★ ★	08 Jun 2...	Low			
AWS Sigv4	★ ★ ★	16 Feb 2...	Low			
Backslash Powered...	★ ★ ★	23 Sep ...	Low	Pro exten...		
Backup Finder	★ ★ ★	04 Aug ...	Low			
Batch Scan Report ...	★ ★ ★	04 Feb 2...	Low	Pro exten...		
BeanStack - Stack-t...	★ ★ ★	04 Feb 2...	Low	Pro exten...		
Blazer	★ ★ ★	01 Feb 2...	Low			
Bookmarks	★ ★ ★	21 May ...	Low			
Bradamsa	★ ★ ★	02 Jul 2...	Low			
Brida, Burp to Frida...	★ ★ ★	04 Feb 2...	Low			

Refresh list Manual install ...

Active Scan++

ActiveScan++ extends Burp Suite's active and passive scanning capabilities. Designed to add minimal network overhead, it identifies application behaviour that may be of interest to advanced testers:

- Potential host header attacks (password reset poisoning, cache poisoning, DNS rebinding)
- Edge side includes
- XML input handling
- Suspicious input transformation (eg 7*7 => '49', '\x41\x41 => 'AA')
- Passive-scanner issues that only occur during fuzzing (install the 'Error Message Checks' extension for maximum effectiveness)

It also adds checks for the following issues:

- Blind code injection via expression language, Ruby's open() and Perl's open()
- CVE-2014-6271/CVE-2014-6278 'shellshock' and CVE-2015-2080, CVE-2017-5638, CVE-2017-12629, CVE-2018-11776

It also provides insertion points for HTTP basic authentication.

To invoke these checks, just run a normal active scan.

The host header checks tamper with the host header, which may result in requests being routed to different applications on the same host. Exercise caution when running this scanner against applications in a shared hosting environment.

This extension requires Burp Suite Professional version 1.6 or later and Jython 2.5 or later standalone.

Copyright © 2014-2022 PortSwigger Ltd.

Estimated system impact

Overall: **Low** (?)

Memory	CPU	Time	Scanner
Low	Low	Low	Low

Author: James 'albinowax' Kettle, PortSwigger
Version: 1.0.22
Source: <https://github.com/portswigger/active-scan-plus-plus>

Backslash Powered Scanner

The Backslash Powered Scanner is a powerful Burp Suite extension that helps security professionals identify vulnerabilities in web applications. This tool uses advanced techniques to search for vulnerabilities, including SQL injection, cross-site scripting (XSS), and other common exploits. It also has the ability to integrate with other Burp Suite tools, such as the Intruder and Scanner modules, to provide a comprehensive view of an application's security posture. The Backslash Powered Scanner is an essential tool for any security professional looking to ensure the security and integrity of their web applications. It is an easy-to-use, reliable, and efficient tool that will help you identify and remediate vulnerabilities quickly and efficiently.

BApp Store

The BApp Store contains Burp extensions that have been written by users of Burp Suite, to extend Burp's capabilities.

Name	Installed	Rating	Popula...	Last upd...	System i...	Detail
Backslash Powered Scanner	✓	★★★☆☆	High	23 Sep ...	Low	Pro exten...
CSTC, Modular HTTP Manipula...		★★★★☆	Medium	10 Jul 2...	Low	
Param Miner		★★★★☆	Medium	23 Sep ...	Low	
Turbo Intruder	✓	★★★★☆	Medium	23 Aug ...	Low	

Backslash Powered Scanner

This extension complements Burp's active scanner by using a novel approach capable of finding and confirming both known and unknown classes of server-side injection vulnerabilities. Evolved from classic manual techniques, this approach reaps many of the benefits of manual testing including casual WAF evasion, a tiny network footprint, and flexibility in the face of input filtering.

For more information, please refer to the whitepaper at <http://blog.portswigger.net/2016/11/backslash-powered-scanning-hunting.html>

This extension requires Burp Suite 1.7.10 or later and Java version 8.

Copyright © 2016-2022 PortSwigger Ltd.

Copyright © 2016-2022 PortSwigger Ltd.

Estimated system impact

Overall: Low

Memory	CPU	Time	Scanner
Low	Low	Low	Low

Author: James 'albinowax' Kettle, PortSwigger Web Security
Version: 1.21
Source: <https://github.com/portswigger/backslash-powered-scanner>
Updated: 23 Sep 2022

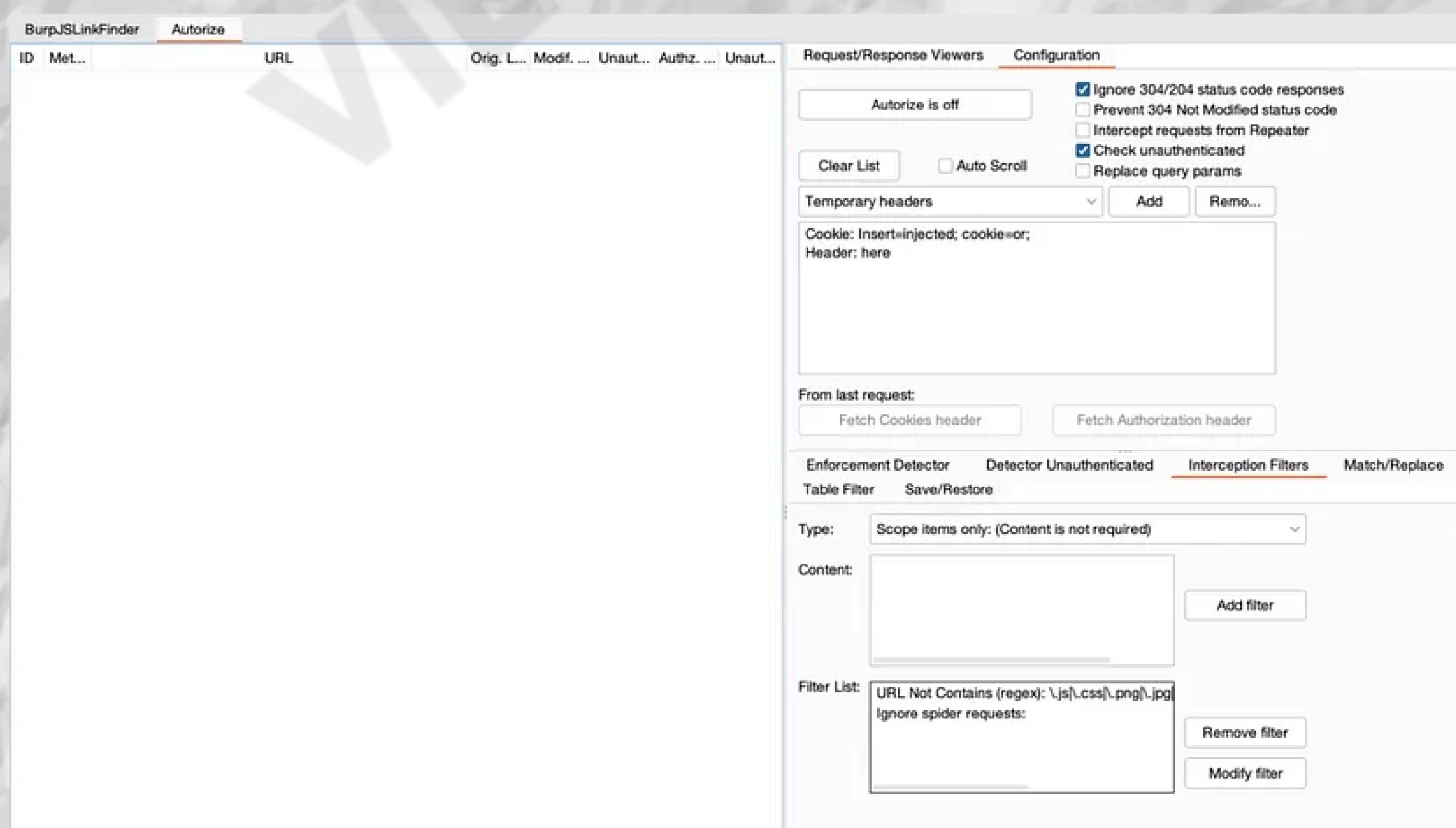
Rating: ★★★★★ [Submit rating](#)

Popularity: [View profile](#)

[Reinstall](#)

Autorize

Autorize is a Burp Suite extension that allows you to easily manage and automate the authorization process for web applications. With Autorize, you can create custom authorization rules and apply them to specific URLs or groups of URLs. This can help streamline your testing process, as you won't have to manually enter authorization credentials for each request. In addition, Autorize integrates with other Burp Suite tools, such as the Scanner and Repeater, allowing you to perform authenticated scans and tests with ease. Overall, Autorize is a valuable tool for any security professional looking to simplify and optimize their web application testing workflow.

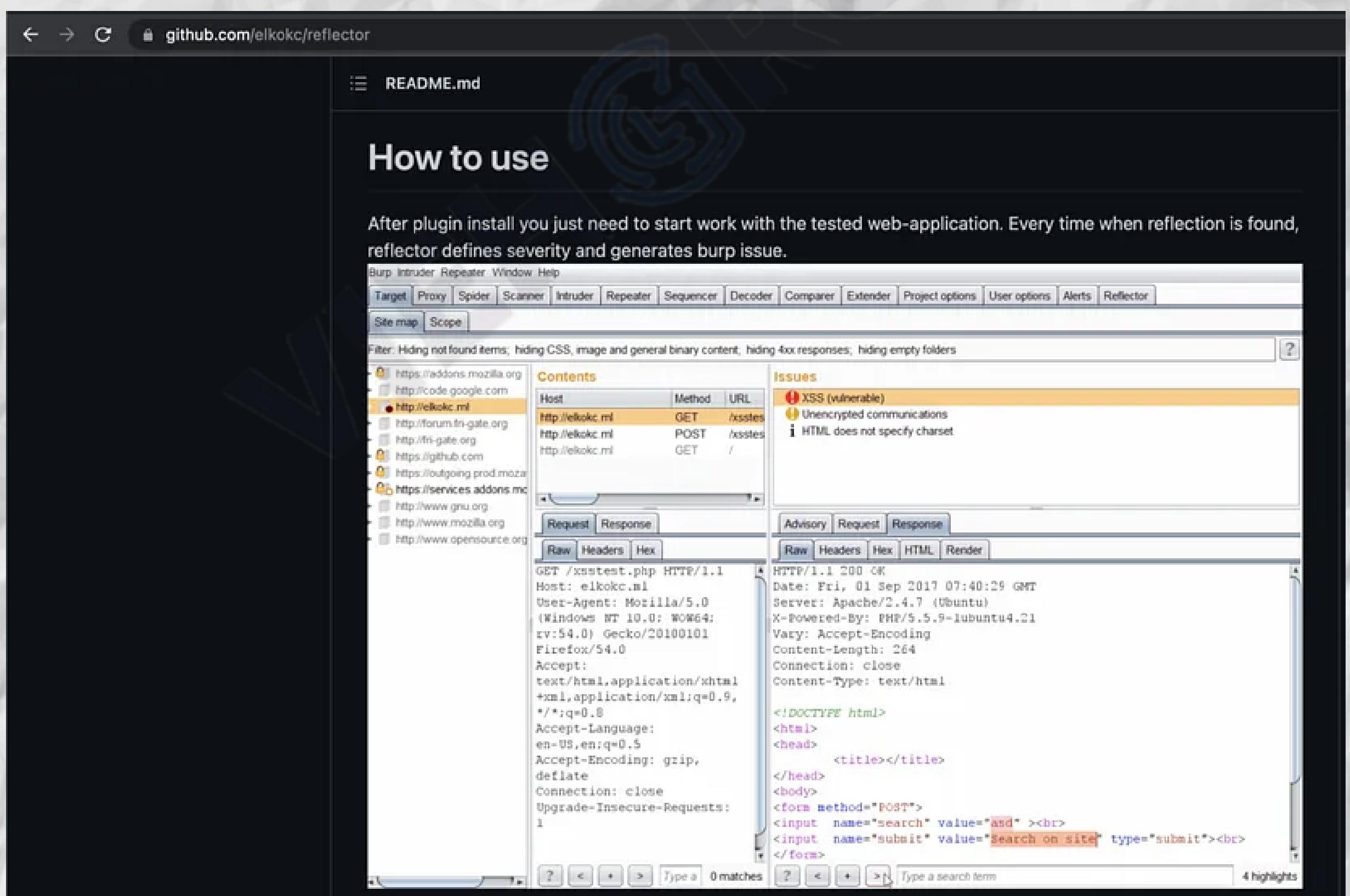


Sentinel

The Sentinel Burp Suite extension is a powerful tool for detecting and preventing security vulnerabilities in web applications. It uses advanced techniques to identify potential injection points, weak authentication and authorization measures, and issues with session management. The extension provides clear and actionable recommendations for remediation, making it easy for developers to fix vulnerabilities and improve the security of their applications. With its seamless integration into the Burp Suite framework, Sentinel is a must-have for any security professional looking to protect their web applications from threats.

Reflector

Reflector is a useful burp suite's extension for finding reflected cross-site scripting vulnerabilities on a webpage in real-time as you browse. It offers several helpful features, including highlighting reflections in the response tab, testing which symbols are allowed in the reflection, analyzing the reflection context, and a content-type whitelist. These features help you more effectively identify and mitigate potential security risks on your website.



HTTP Request Smuggler

The HTTP Request Smuggler Burp Suite extension is a powerful tool for testing the security of web applications. It allows users to perform HTTP request smuggling attacks, which can be used to bypass security controls and expose vulnerabilities in the application. With this extension, users can easily craft and send malicious requests to the target application and analyze the response to identify any potential security issues. The extension is easy to use and integrates seamlessly with other Burp Suite tools, making it a valuable addition to any security testing toolkit. Overall, the HTTP Request Smuggler extension is a must-have for anyone looking to improve the security of their web applications.

The screenshot shows the BApp Store interface. At the top, there's a search bar with the text "HTTP Request Smuggler". Below the search bar, a table lists extensions. The first row, "HTTP Request Smuggler", is highlighted with an orange background. The table columns include Name, Installed, Rating, Popularity, Last updated, System impact, and Detail. The "Detail" column for the highlighted row shows the extension's description, usage instructions, and a link to online labs. It also includes sections for estimated system impact (overall low, with low values for memory, CPU, time, and scanner), author information (James 'albinowax' Kettle, PortSwigger), version (2.14), source (https://github.com/portswigger/http-request-smuggler), update date (15 Nov 2022), rating (5 stars), popularity (high, indicated by a long orange progress bar), and a "Reinstall" button.

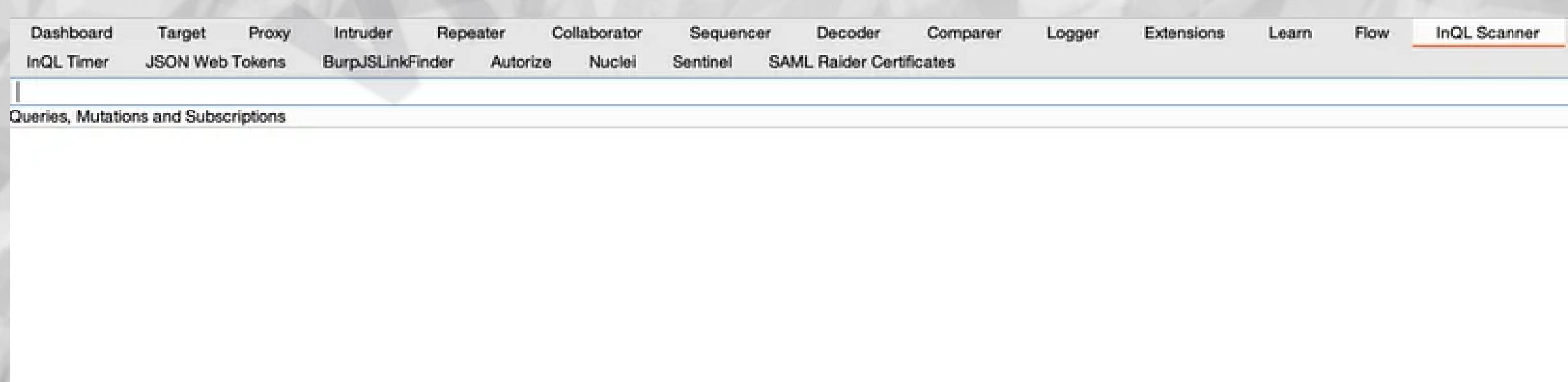
J2EEScan

J2EEScan is a powerful Burp Suite extension that is designed specifically for scanning Java EE web applications. It can detect a variety of vulnerabilities related to authentication, authorization, and session management, and provide recommendations for remediation. The extension also has the ability to identify potential injection points within the application, making it a valuable tool for security professionals. One of the key benefits of J2EEScan is its integration with other Burp Suite tools, such as the Intruder and Scanner modules, which allows for even more comprehensive testing. Overall, J2EEScan is an essential tool for any security professional working with Java EE applications.

The screenshot shows the BApp Store interface. On the left, there's a search bar with the text 'J2ee' and a table of extensions. The first row in the table is for 'J2EEScan', which is installed ('✓'), has a 5-star rating, was last updated on 25 Aug ..., and is categorized as 'High' system impact. On the right, the detailed page for 'J2EEScan' is displayed. It includes a brief description: 'The goal of this extension is to improve the test coverage during web application penetration tests on J2EE applications. J2EEScan adds more than 80+ unique security test cases and new strategies to discover different kind of J2EE vulnerabilities.' Below this is a note: 'Please refer to the official GitHub page for the updated test case list.' Under 'Estimated system impact', it says 'Overall: High' with icons for memory, CPU, time, and scanner. The scanner icon is highlighted as 'High'. At the bottom, it shows author information (Enrico Milanese), version (2.0), source (https://github.com/portswigger/j2ee-scan), and update date (25 Aug 2021). It also shows the current rating (5 stars) and popularity (represented by a progress bar), and buttons for 'Reinstall' and 'Submit rating'.

InQL Scanner

The InQL Scanner is a powerful Burp Suite extension that helps security professionals identify and exploit vulnerabilities within GraphQL APIs. It provides a wide range of features that allow users to easily and efficiently discover and test GraphQL endpoints, as well as identify and exploit any vulnerabilities that may exist. With its intuitive interface and extensive capabilities, the InQL Scanner is an essential tool for anyone looking to secure their GraphQL APIs. Whether you're a beginner or an experienced security professional, the InQL Scanner is an invaluable addition to your toolkit.



A screenshot of the InQL Scanner interface within the Burp Suite application. The top navigation bar includes links for Dashboard, Target, Proxy, Intruder, Repeater, Collaborator, Sequencer, Decoder, Comparer, Logger, Extensions, Learn, Flow, and InQL Scanner (which is underlined, indicating it is the active tab). Below the navigation bar, there is a sub-navigation menu with items: InQL Timer, JSON Web Tokens, BurpJSLinkFinder, Autorize, Nuclei, Sentinel, and SAML Raider Certificates. The main content area is titled "Queries, Mutations and Subscriptions" and contains a large, empty white space, suggesting a workspace for querying or testing GraphQL endpoints.

CORS*, Additional CORS Checks

CORS*, Additional CORS Checks is a Burp Suite extension that helps to identify potential cross-origin resource sharing vulnerabilities. CORS is a security feature that controls how web applications can access resources from other domains. This extension enhances the capabilities of Burp Suite by providing additional checks for CORS misconfigurations, which can lead to security vulnerabilities if not properly configured. By using this extension, penetration testers can more effectively identify and mitigate potential CORS issues, ensuring that the web application being tested is properly protected against cross-origin attacks.

The screenshot shows the Burp Suite interface with the 'CORS*' tab selected. At the top, there is a toolbar with various icons and a search bar labeled 'URL for CORS requests: www.example.com'. Below the toolbar, there are several configuration options: 'Activate CORS*?' (unchecked), 'Only in scope?' (checked), and 'Ignore extensions: ico, svg, js, css, png' (checked). A 'Clear CORS requests' button is also present. The main area is a table with columns: ID, Host, URL, Origin, Method, Status, Length, and MIME. There is one entry in the table with ID 1, Host 'www.example.com', URL '/index.html', Origin 'www.example.com', Method 'GET', Status '200', Length '1234', and MIME 'text/html'. At the bottom of the table, there is a button labeled 'Send CORS requests for selected entry'.

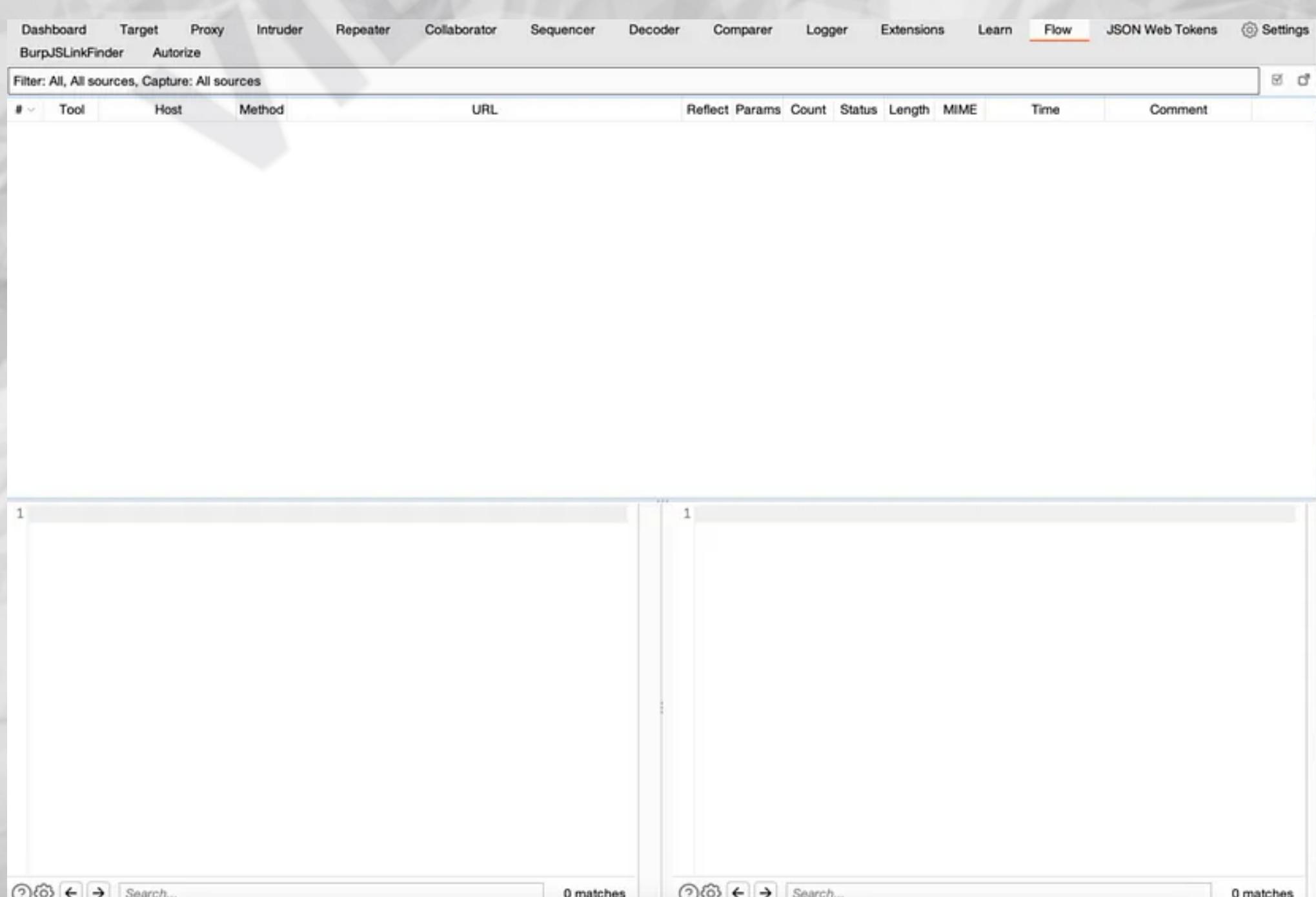
403 Bypasser

403 Bypasser is a Burp Suite extension that helps security professionals bypass HTTP 403 (Forbidden) error messages while testing web applications. This extension allows users to easily modify request headers and bypass restrictions put in place by the server. It is particularly useful for identifying hidden directories and files that may be inadvertently left open to access. 403Bypasser is an essential tool for any security tester, as it allows them to uncover potential vulnerabilities that may be overlooked with traditional testing methods. Its seamless integration with Burp Suite makes it a valuable addition to any security toolkit.

InQL Timer	JSON Web Tokens	BurpJSLinkFinder	Autorize	Nuclei	Sentinel	SAML Raider Certificates	403 Bypasser																																								
<p>Query Payloads</p> <table border="1"><tr><td>Clear</td><td>%09</td></tr><tr><td>Remove</td><td>%20</td></tr><tr><td></td><td>%23</td></tr><tr><td></td><td>%2e</td></tr><tr><td></td><td>%2f</td></tr><tr><td></td><td>.</td></tr><tr><td></td><td>;</td></tr><tr><td></td><td>..</td></tr><tr><td></td><td>;%09</td></tr><tr><td></td><td>;%no</td></tr></table> <p>Header Payloads</p> <table border="1"><tr><td>Clear</td><td>Client-IP: 1...</td></tr><tr><td>Remove</td><td>X-Real-Ip: 1...</td></tr><tr><td></td><td>Redirect: 1...</td></tr><tr><td></td><td>Referer: 12...</td></tr><tr><td></td><td>X-Client-IP: ...</td></tr><tr><td></td><td>X-Custom-I...</td></tr><tr><td></td><td>X-Forwarded-For: ...</td></tr><tr><td></td><td>X-Forwarded-Port: ...</td></tr><tr><td></td><td>X-Forwarded-Proto: ...</td></tr><tr><td></td><td>X-Forwarded-Ssl: ...</td></tr></table>								Clear	%09	Remove	%20		%23		%2e		%2f		.		;		..		;%09		;%no	Clear	Client-IP: 1...	Remove	X-Real-Ip: 1...		Redirect: 1...		Referer: 12...		X-Client-IP: ...		X-Custom-I...		X-Forwarded-For: ...		X-Forwarded-Port: ...		X-Forwarded-Proto: ...		X-Forwarded-Ssl: ...
Clear	%09																																														
Remove	%20																																														
	%23																																														
	%2e																																														
	%2f																																														
	.																																														
	;																																														
	..																																														
	;%09																																														
	;%no																																														
Clear	Client-IP: 1...																																														
Remove	X-Real-Ip: 1...																																														
	Redirect: 1...																																														
	Referer: 12...																																														
	X-Client-IP: ...																																														
	X-Custom-I...																																														
	X-Forwarded-For: ...																																														
	X-Forwarded-Port: ...																																														
	X-Forwarded-Proto: ...																																														
	X-Forwarded-Ssl: ...																																														

Flow

Burp Suite's Flow extension is a powerful tool for analyzing HTTP requests and responses in a web application. It allows users to view and manipulate the flow of communication between the client and server, providing insight into how the application functions and potentially exposing vulnerabilities. With Flow, users can analyze the content and structure of requests and responses, modify them in real-time, and track the effects of these modifications on the application's behavior. This extension is especially useful for penetration testers and security professionals looking to uncover weaknesses in web applications and improve their overall security posture.



WSDL Wizard

The WSDL Wizard Burp Suite extension is a valuable tool for testing web service applications. It allows users to import and analyze WSDL (Web Service Description Language) files, providing a thorough analysis of the application's security vulnerabilities. This extension integrates seamlessly with other Burp Suite tools, such as the Scanner and Intruder modules, to provide a comprehensive security assessment of the web service. Its user-friendly interface makes it easy for even novice users to analyze WSDL files and identify potential security risks. Overall, the WSDL Wizard extension is a must-have for any security professional testing web service applications.

The screenshot shows the BApp Store interface for the WSDL Wizard extension. At the top, there is a search bar with the text "WSDL Wizard". Below the search bar, a table lists the extension's details:

Name	Installed	Rating	Popula...	Last updated	System im...	Detail
WSDL Wizard	✓	★★★1	—	01 Jul 2014	Low	Detail

The "Detail" link is highlighted. The main content area displays the extension's description and settings. The description states: "This extension scans a target server for WSDL files. After performing normal mapping of an application's content, right click on the relevant target in the site map, and choose 'Scan for WSDL files' from the context menu. The extension will search the already discovered contents for URLs with the .wsdl file extension, and also try to guess the locations of any additional WSDL files based on the file names known to be in use. The results of the scanning appear within the extension's output tab in the Burp Extender tool." The "Estimated system impact" section shows "Overall: Low" with "Memory: Low", "CPU: Low", "Time: Low", and "Scanner: Low". The "Author" is listed as "Smege Sec", "Version" as "1.02", "Source" as "<https://github.com/portswigger/wsdl-wizard>", and "Updated" as "01 Jul 2014". The "Rating" is shown as "★★★1" with a "Submit rating" button, and the "Popularity" is indicated by a low rating bar. A "Reinstall" button is located at the bottom of the extension's card.

Turbo Intruder

Turbo Intruder is a powerful Burp Suite extension that allows for efficient and effective web application testing. Its unique design allows for high-speed, multi-threaded attacks on web targets, making it a valuable tool for any penetration tester.

With Turbo Intruder, users can easily perform brute force attacks, analyze responses, and customize payloads. This extension is a must-have for any security professional looking to thoroughly test the security of their web applications. Its advanced features and user-friendly interface make it a top choice for web application penetration testing.

BApp Store

The BApp Store contains Burp extensions that have been written by users of Burp Suite, to extend Burp's capabilities.

Name	Installed	Rating	Popula...	Last updated	System im...	Detail
Turbo Intruder	✓	★★★☆☆	23 Aug 2022	Low		

Turbo Intruder

Turbo Intruder is a Burp Suite extension for sending large numbers of HTTP requests and analyzing the results. It's intended to complement Burp Intruder by handling attacks that require extreme speed or complexity. The following features set it apart:

- Fast - Turbo Intruder uses a HTTP stack hand-coded from scratch with speed in mind. As a result, on many targets it can seriously outpace even fashionable asynchronous Go scripts.
- Flexible - Attacks are configured using Python. This enables handling of complex requirements such as signed requests and multi-step attack sequences. Also, the custom HTTP stack means it can handle malformed requests that break other libraries.
- Scalable - Turbo Intruder can achieve flat memory usage, enabling reliable multi-day attacks. It can also be run in headless environments via the command line.
- Convenient - Boring results can be automatically filtered out by an advanced diffing algorithm adapted from Backslash Powered Scanner

On the other hand it's undeniably harder to use, and the network stack isn't as reliable and battle-tested as core Burp's.

Basic use

To use it, simply highlight the area you want to inject over, then right click and "Send to Turbo Intruder". This will open a window containing a Python snippet which you can customise before launching the attack.

For full usage instructions, please refer to [the documentation](#).

Copyright © 2018-2022 PortSwigger Ltd.

Estimated system impact

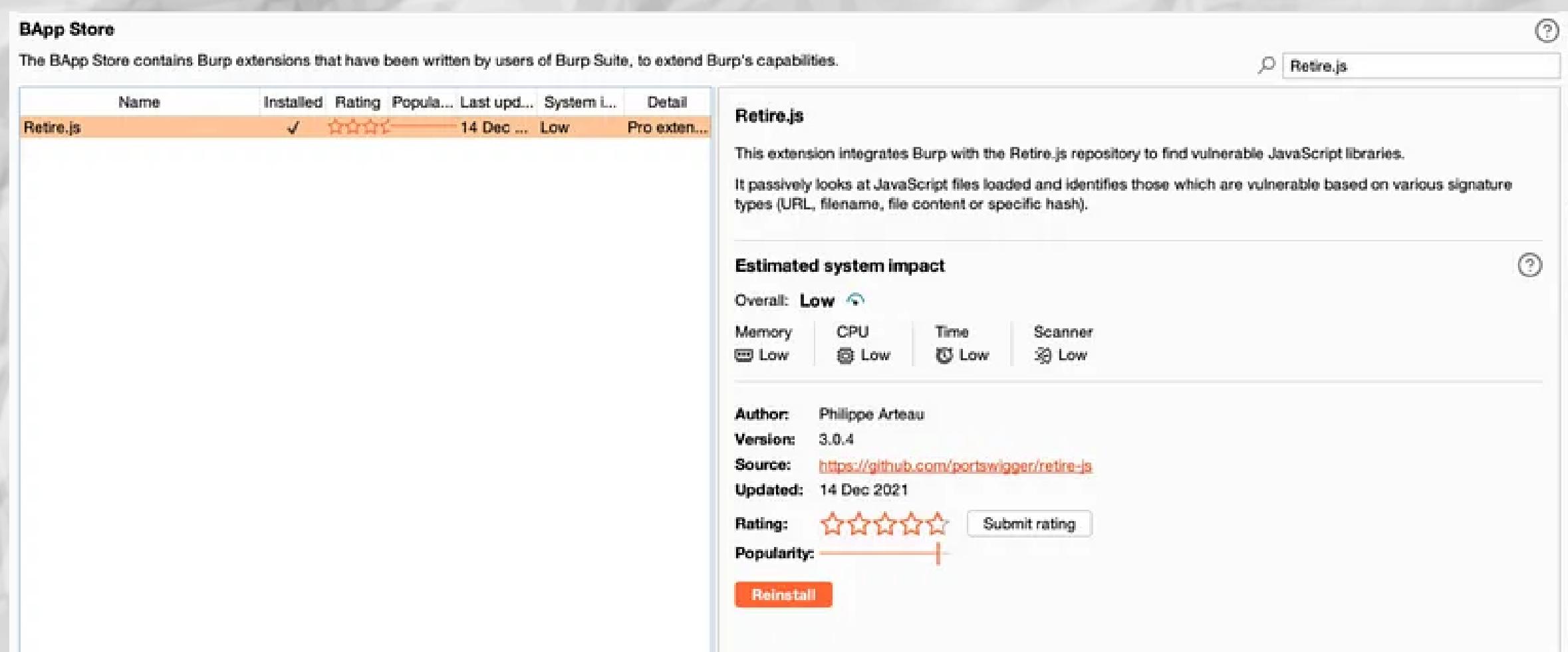
Overall: Low

Memory	CPU	Time	Scanner
Low	Low	Low	Low

Author: James 'albinowax' Kettle, PortSwigger Web Security
Version: 1.30
Source: <https://github.com/portswigger/turbo-intruder>

Retire.js

Retire.js is a powerful Burp Suite extension that helps identify and mitigate the use of vulnerable JavaScript libraries within web applications. It scans for outdated and potentially insecure versions of JavaScript libraries and provides recommendations for updating to more secure versions. This tool is essential for ensuring the security of web applications, as JavaScript libraries are often targeted by attackers due to their widespread use and the potential for vulnerabilities to be exploited. By using Retire.js, developers can proactively identify and address any potential security risks before they are exploited. With its seamless integration into the Burp Suite ecosystem, Retire.js makes it easy to maintain the security of web applications and protect against potential vulnerabilities.



The screenshot shows the BApp Store interface. At the top, there's a search bar with the text "Retire.js". Below the search bar, a table lists extensions. The "Retire.js" row is highlighted with an orange background. The table columns include Name, Installed, Rating, Popularity, Last updated, System impact, and Detail. The "Retire.js" row shows a green checkmark in the Installed column, a 5-star rating, and a popularity bar. The Last updated column shows "14 Dec ...". The System impact column shows "Low". The Detail column contains a detailed description of the extension.

BApp Store

The BApp Store contains Burp extensions that have been written by users of Burp Suite, to extend Burp's capabilities.

Name	Installed	Rating	Popularity	Last upd...	System i...	Detail
Retire.js	✓	★★★★★	14 Dec ...	Low	Pro exten...	View Details

Retire.js

This extension integrates Burp with the Retire.js repository to find vulnerable JavaScript libraries. It passively looks at JavaScript files loaded and identifies those which are vulnerable based on various signature types (URL, filename, file content or specific hash).

Estimated system impact

Overall: Low

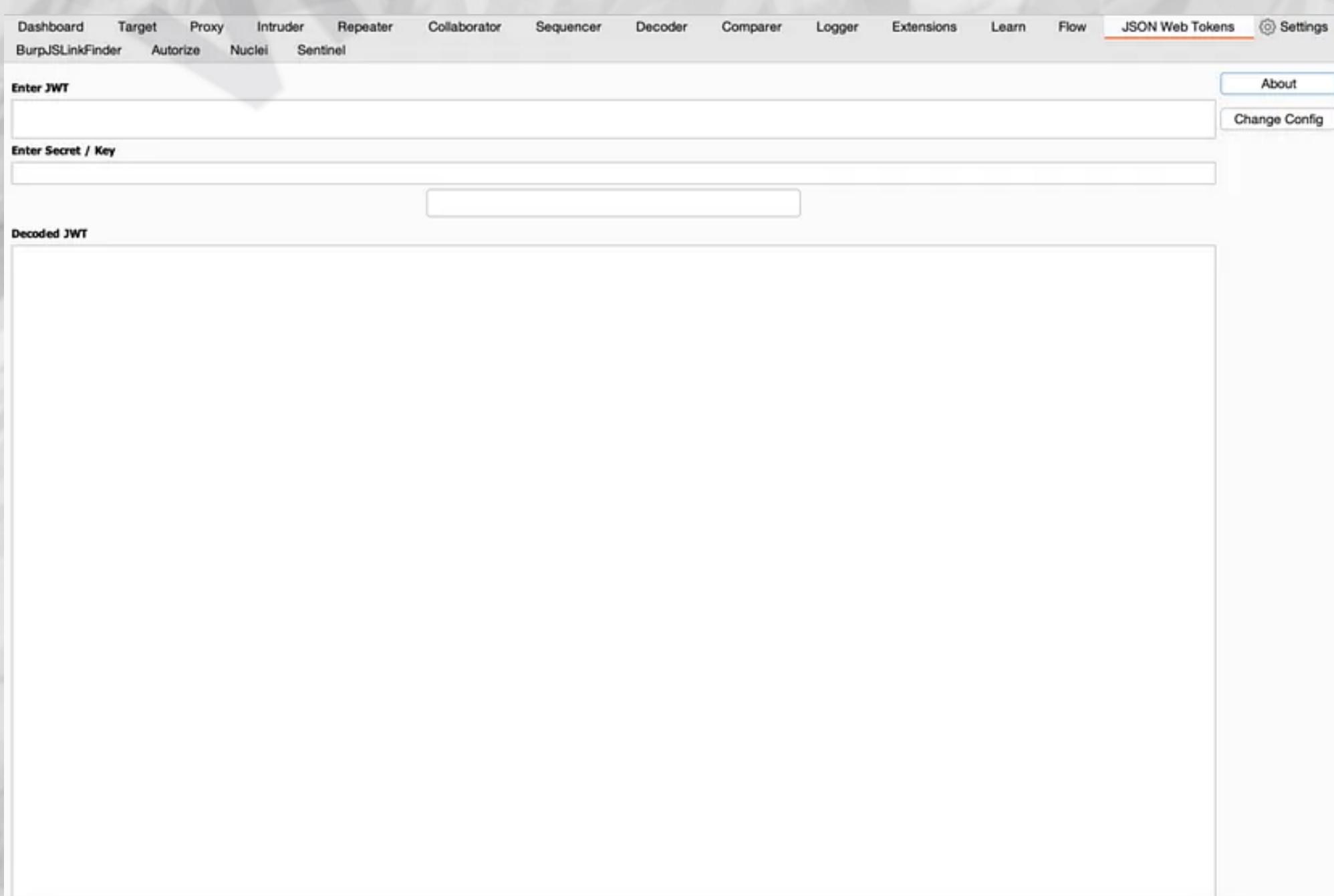
Memory	CPU	Time	Scanner
Low	Low	Low	Low

Author: Philippe Arteau
Version: 3.0.4
Source: <https://github.com/portswigger/retire-js>
Updated: 14 Dec 2021
Rating: ★★★★★
Popularity: 

[Reinstall](#)

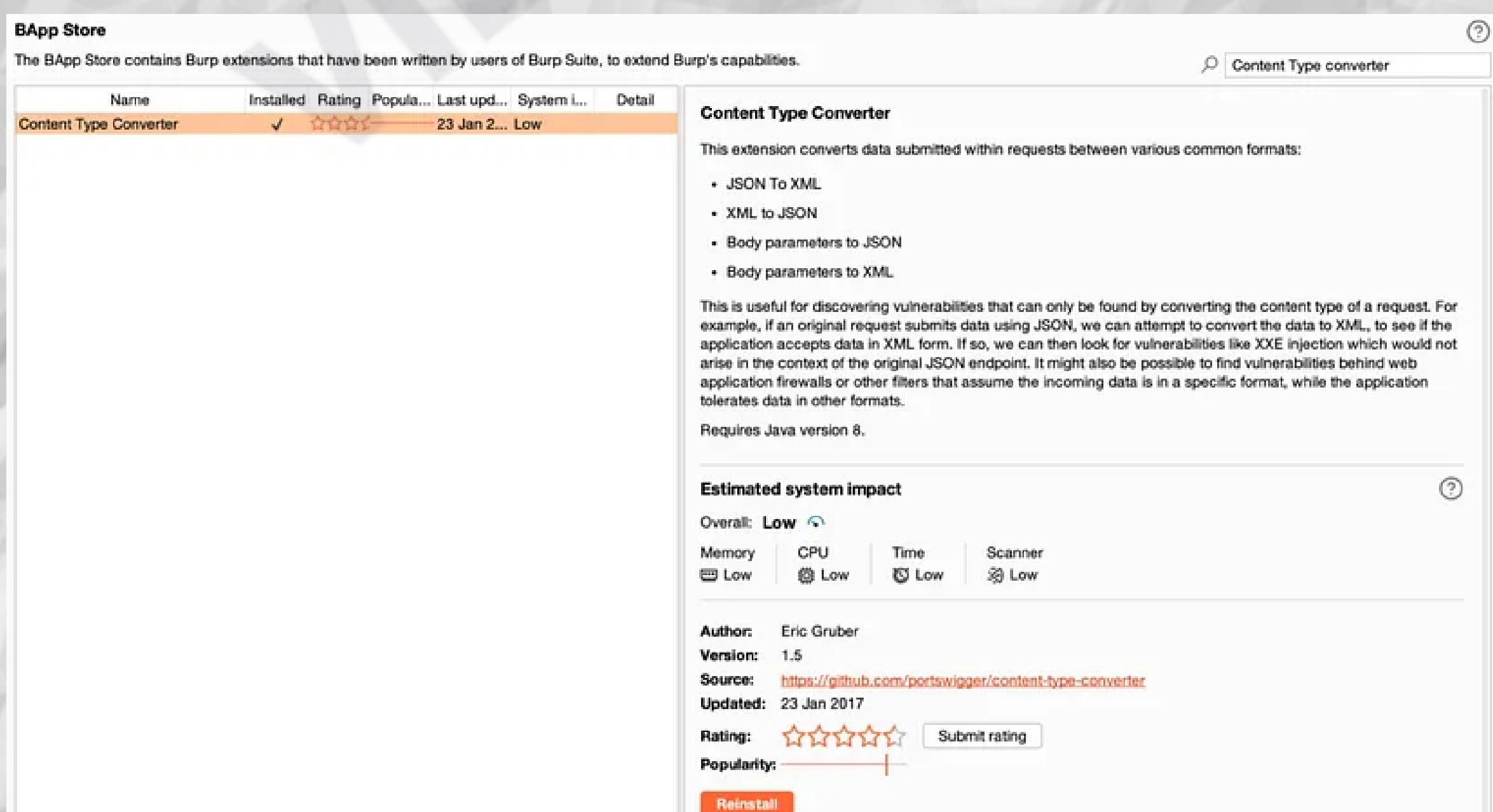
JSON Web Tokens

The JSON Web Tokens (JWT) Burp Suite extension is a powerful tool for testing and securing applications that use JSON Web Tokens for authentication and authorization. With this extension, you can decode and validate JWTs, as well as manipulate them for testing purposes. The JWT extension also allows you to test for vulnerabilities such as weak signing algorithms and insecure handling of refresh tokens. Overall, the JWT extension is a must-have for any security professional working with applications that utilize JSON Web Tokens. Its integration with the rest of the Burp Suite makes it a valuable addition to your toolkit for testing and securing your applications.



Content Type Converter

The Content-Type Convertor Burp Suite extension is a valuable tool for web application testers. It allows users to modify the content type of requests and responses within the Burp Suite proxy. This can be useful for testing applications that may handle different content types in different ways. For example, a request with a content type of “application/json” may be processed differently than one with a content type of “application/xml.” By modifying the content type, testers can ensure that the application is properly handling all potential content types. The Content Type Convertor extension is easy to use and integrates seamlessly with other Burp Suite tools, making it a must-have for any web application tester’s toolkit.



The screenshot shows the BApp Store interface. At the top, there's a search bar with the text "Content Type converter". Below the search bar, a table lists extensions. One row is highlighted for the "Content Type Converter" extension, which has a green checkmark in the "Installed" column, a rating of 4 stars, and was last updated on 23 Jan 2017. The system impact is listed as "Low".

Name	Installed	Rating	Popula...	Last upd...	System I...	Detail
Content Type Converter	✓	★★★★★	23 Jan 2017	Low		

Content Type Converter

This extension converts data submitted within requests between various common formats:

- JSON To XML
- XML to JSON
- Body parameters to JSON
- Body parameters to XML

This is useful for discovering vulnerabilities that can only be found by converting the content type of a request. For example, if an original request submits data using JSON, we can attempt to convert the data to XML, to see if the application accepts data in XML form. If so, we can then look for vulnerabilities like XXE injection which would not arise in the context of the original JSON endpoint. It might also be possible to find vulnerabilities behind web application firewalls or other filters that assume the incoming data is in a specific format, while the application tolerates data in other formats.

Requires Java version 8.

Estimated system impact

Overall: Low

Memory	CPU	Time	Scanner
Low	Low	Low	Low

Author: Eric Gruber
Version: 1.5
Source: <https://github.com/portswigger/content-type-converter>
Updated: 23 Jan 2017

Rating: ★★★★★ [Submit rating](#)

Popularity: 

[Reinstall](#)

BurpJSFinder

JS Finder is a Burp Suite extension that helps security professionals discover and analyze JavaScript code within web applications. This tool can be particularly useful in identifying potential vulnerabilities and insecure coding practices within the application. It allows users to search for specific keywords or patterns within the JavaScript code, as well as highlight and decode obfuscated code. With JS Finder, users can easily identify and address any potential security issues within their web applications, ensuring that they are as secure as possible. This extension is an essential tool for any security professional looking to thoroughly assess the security of their web applications.

BurpJSLinkFinder

Autorize

Nuclei

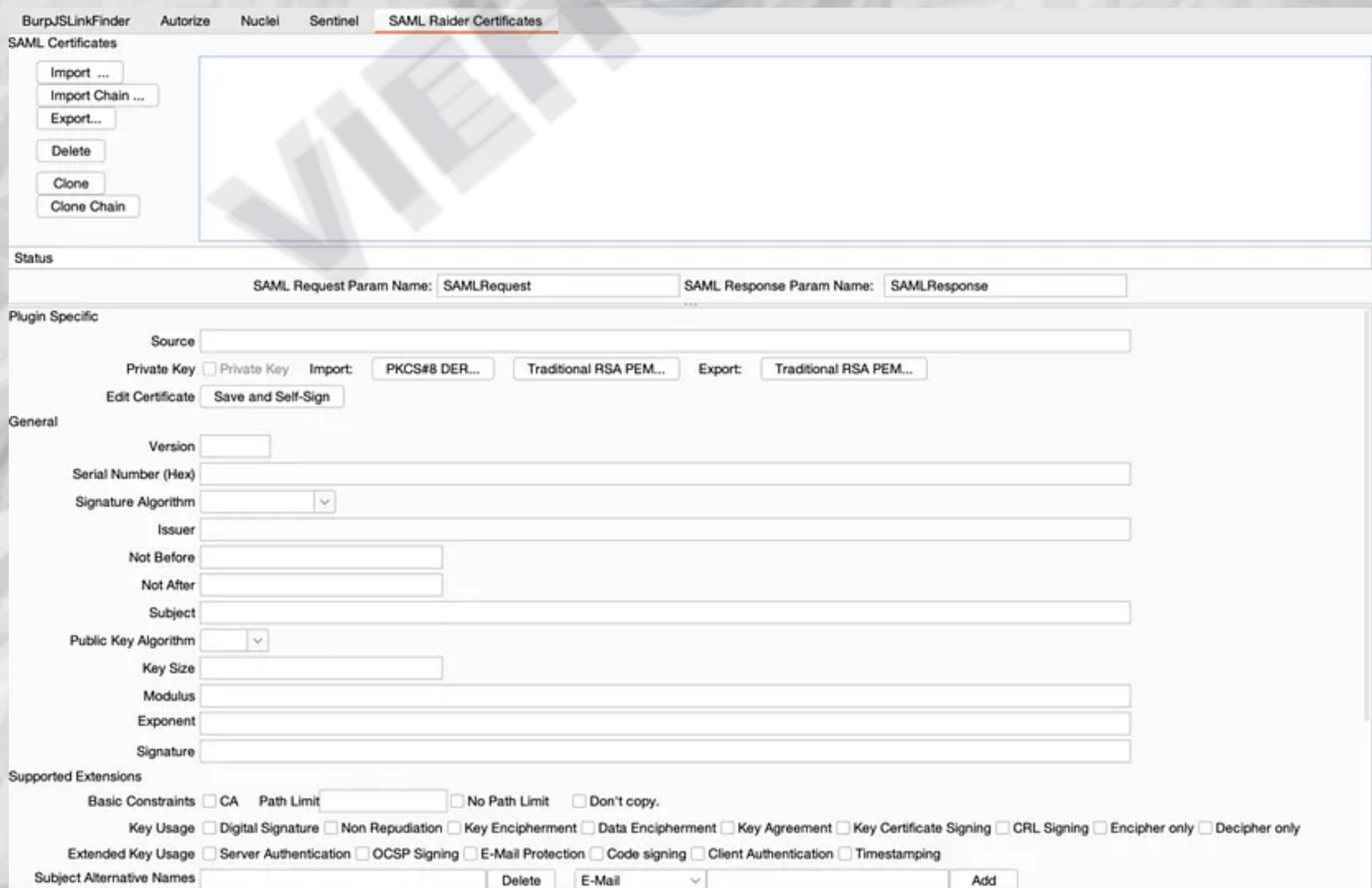
Sentinel

LinkFinder Log:

Burp JS LinkFinder loaded.
Copyright (c) 2019 Frans Hendrik Botes

SAML Raider

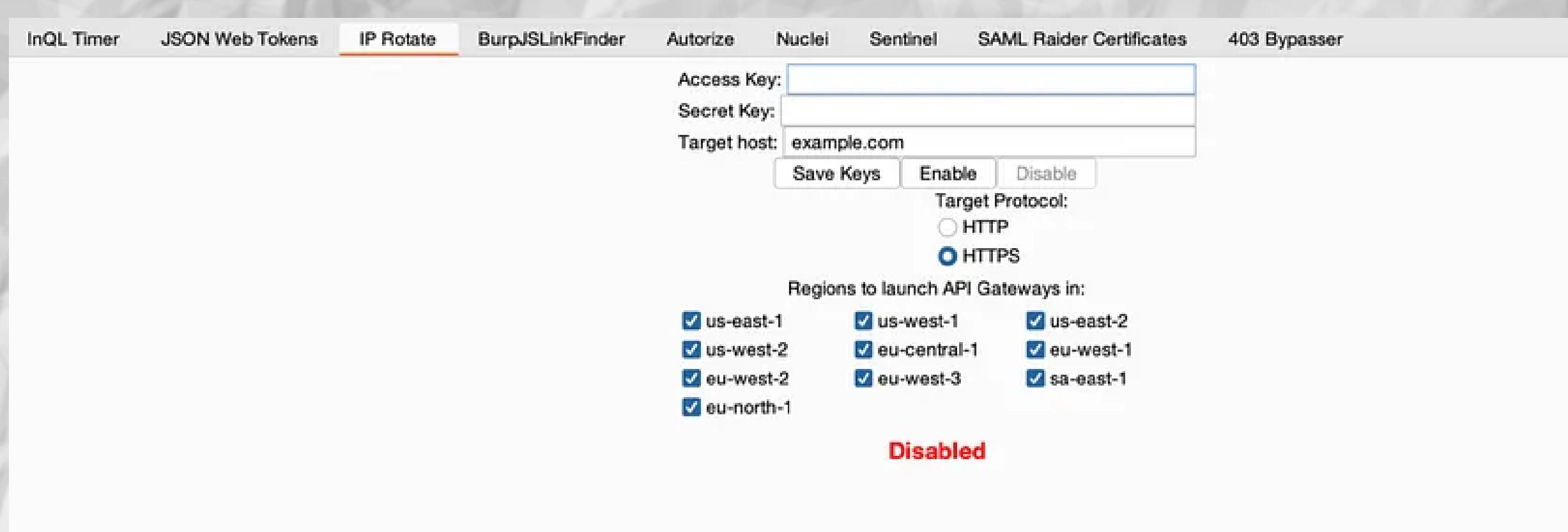
SAML Raider is a Burp Suite extension that helps security professionals to assess the security of SAML-based Single Sign-On (SSO) systems. This extension allows users to intercept and manipulate SAML messages, as well as perform security testing on SAML-based systems. SAML Raider is a valuable tool for identifying vulnerabilities and misconfigurations in SAML implementations and can help organizations to improve the security of their SSO systems. This extension is easy to use and integrates seamlessly with other Burp Suite tools, making it a powerful addition to any security professional's toolkit.



The screenshot shows the 'SAML Raider Certificates' tab in the Burp Suite interface. The tab bar includes links for BurpJSLinkFinder, Autorize, Nuclei, Sentinel, and SAML Raider Certificates (which is the active tab). The main area is titled 'SAML Certificates' and contains several buttons: Import ..., Import Chain ..., Export..., Delete, Clone, and Clone Chain. Below this is a 'Status' section with fields for 'SAML Request Param Name' (set to 'SAMLRequest') and 'SAML Response Param Name' (set to 'SAMLResponse'). The 'Plugin Specific' section contains fields for 'Source' (with options for Private Key, Import, Traditional RSA PEM, and Export), 'Edit Certificate' (with 'Save and Self-Sign' button), and a 'General' section with fields for 'Version', 'Serial Number (Hex)', 'Signature Algorithm', 'Issuer', 'Not Before', 'Not After', 'Subject', 'Public Key Algorithm', 'Key Size', 'Modulus', 'Exponent', and 'Signature'. At the bottom, there are sections for 'Supported Extensions' (with checkboxes for CA, Path Limit, No Path Limit, and Don't copy) and 'Extended Key Usage' (with checkboxes for Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment, Key Agreement, Key Certificate Signing, CRL Signing, Encipher only, Decipher only, Server Authentication, OCSP Signing, E-Mail Protection, Code signing, Client Authentication, and Timestamping). A 'Subject Alternative Names' section at the bottom right includes fields for Delete, E-Mail, and Add.

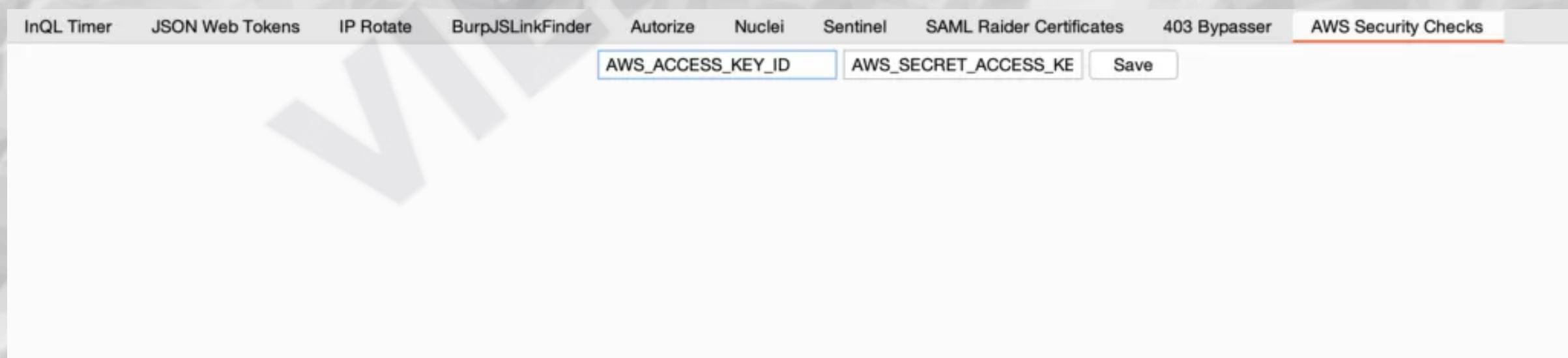
IP Rotate

The IP Rotate Burp Suite extension is a valuable tool for those conducting web security assessments or engaging in web-based activities that may require anonymity. This extension allows users to rotate their IP address with each request, making it more difficult for target websites or systems to track or block their activity. This can be particularly useful for testing the effectiveness of IP-based firewall rules or avoiding detection by intrusion detection systems. Additionally, the IP Rotate extension can be configured to use a specified range of IP addresses, allowing users to select the location and type of IP addresses used in their requests. Overall, the IP Rotate extension is a useful addition to the Burp Suite toolkit for those looking to add an extra layer of security and anonymity to their web-based activities.



AWS Security Checks

The AWS Security Checks extension for Burp Suite is an essential tool for any organization utilizing Amazon Web Services. This extension helps to identify and mitigate potential security vulnerabilities within your AWS infrastructure. With its powerful scanning capabilities, the AWS Security Checks extension can detect issues with access control, networking, and data storage, as well as identify misconfigurations that could potentially lead to a security breach. This extension is an invaluable resource for ensuring the security of your AWS environment and should be a key component of any organization's security toolkit.



Headless Burp

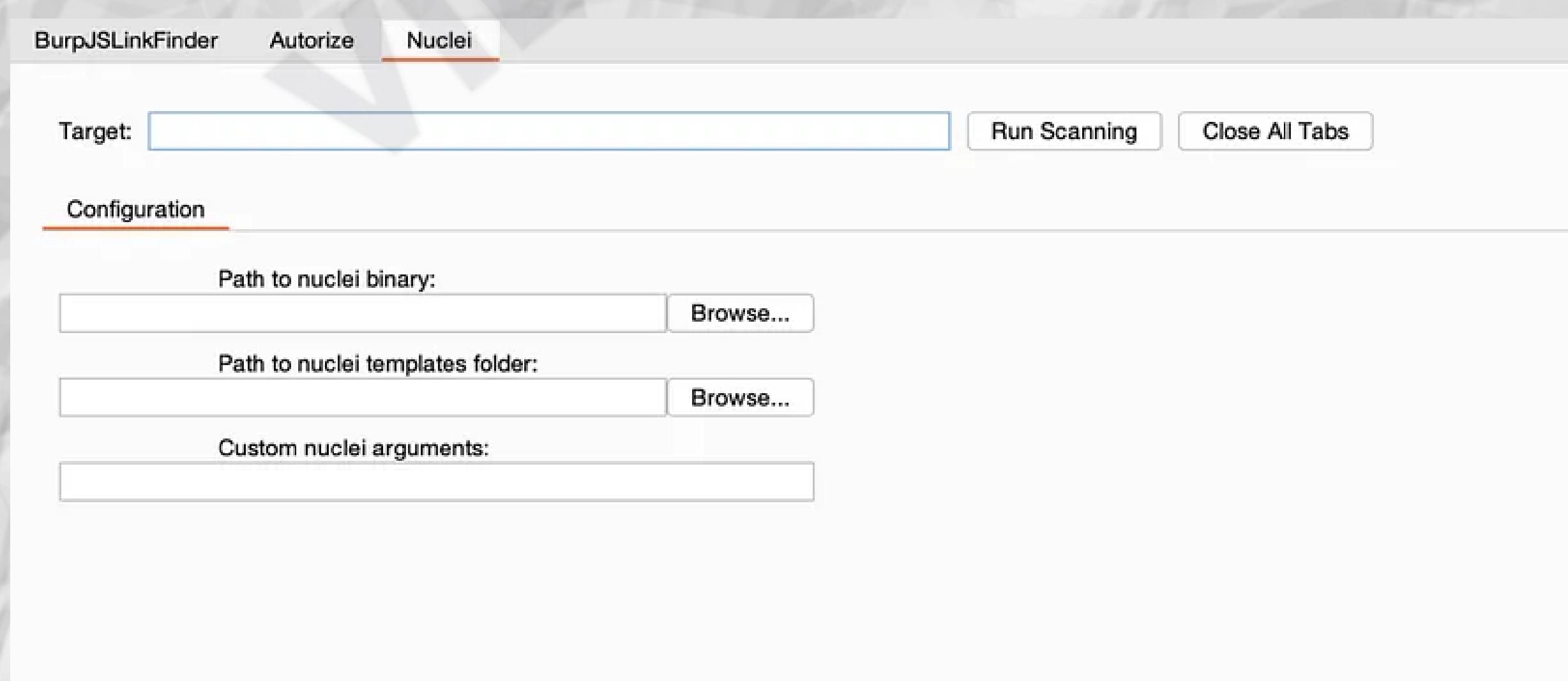
The Headless Burp Suite extension is a powerful tool for performing automated security testing on web applications. It allows users to run scans and perform actions in a headless environment, meaning that it can be run without the need for a graphical user interface. This makes it ideal for use in continuous integration environments, where regular security testing can be seamlessly incorporated into the development process. With the ability to integrate with other Burp Suite tools and customize scan settings, the Headless extension is a valuable asset for any security professional looking to improve their testing efficiency.

The screenshot shows the BApp Store interface for the Headless Burp extension. The search bar at the top right contains the text "Headless Burp". The main area displays a table of extensions, with "Headless Burp" highlighted. The extension details page on the right includes:

- Headless Burp**: A brief description stating it allows running Burp Suite's Spider and Scanner tools in headless mode via command-line.
- System Impact**: Overall: Low. Components: Memory (Low), CPU (Low), Time (Low), Scanner (Low).
- Author**: Anand Sudhir Prayaga, Rita Nordtug
- Version**: 1.0
- Source**: <https://github.com/portswigger/headless-burp>
- Updated**: 09 Jul 2018
- Rating**: ★★★★☆ (4 stars)
- Popularity**: (represented by a progress bar)

Nuclei Burp Integration

The Nuclei Burp Integration extension is a powerful tool for performing targeted and comprehensive vulnerability testing within the Burp Suite environment. It allows for the integration of custom templates to be used for scanning, providing detailed and actionable information on identified vulnerabilities. This extension also allows for seamless integration with the rest of the Burp Suite toolset, making it easy to prioritize and track identified vulnerabilities during the testing process. Overall, the Nuclei Burp Integration extension is a valuable asset for any penetration tester looking to effectively identify and address potential security risks.



Thanks for showing your interest



Jai Hind