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 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 ?

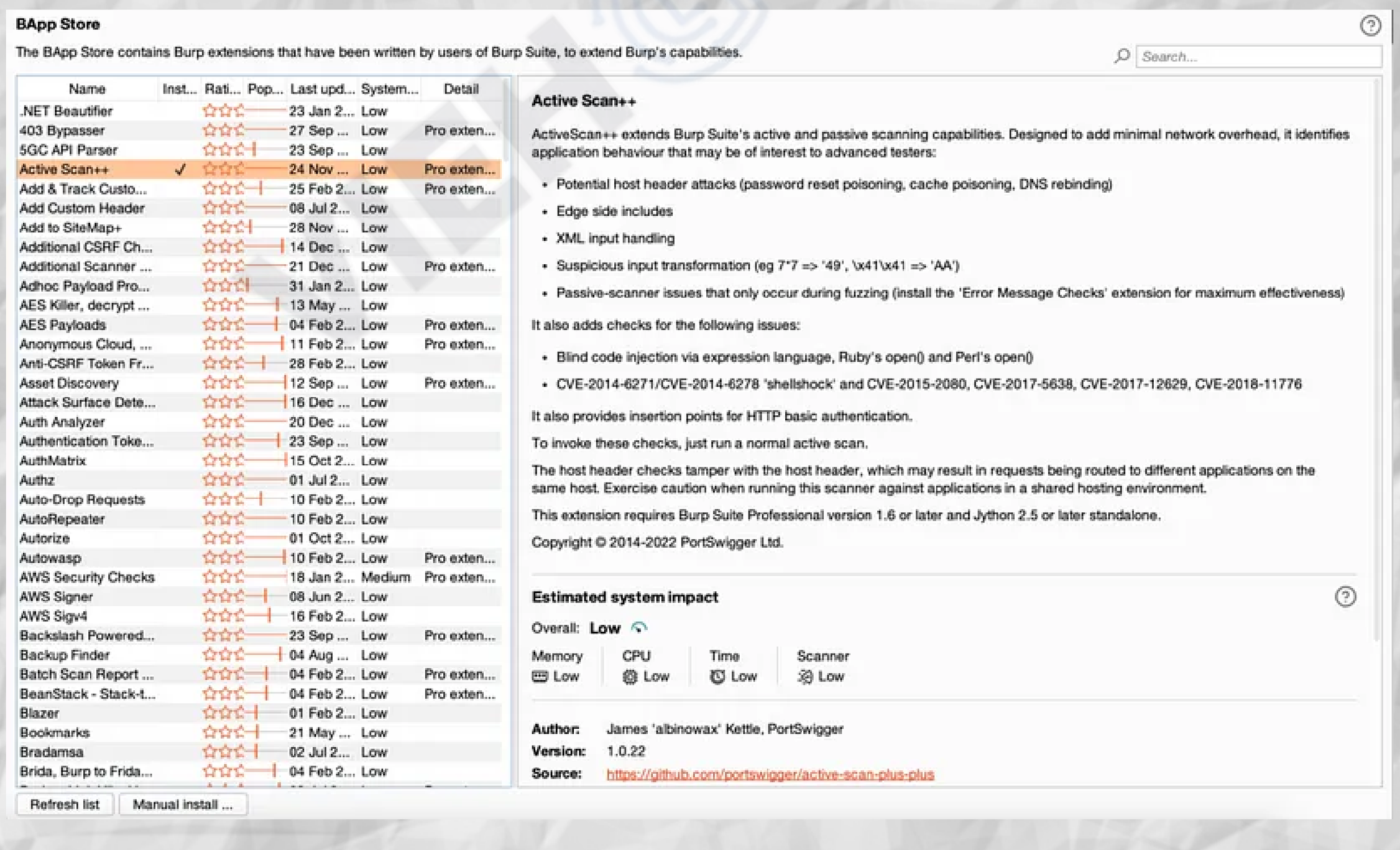
Burp Suite is a powerful tool used for web application security testing. It is a comprehensive platform that includes a range of tools to help identify vulnerabilities and security flaws in web applications. The suite includes a web proxy, spider, scanner, and intruder, which can be used to intercept 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 ++

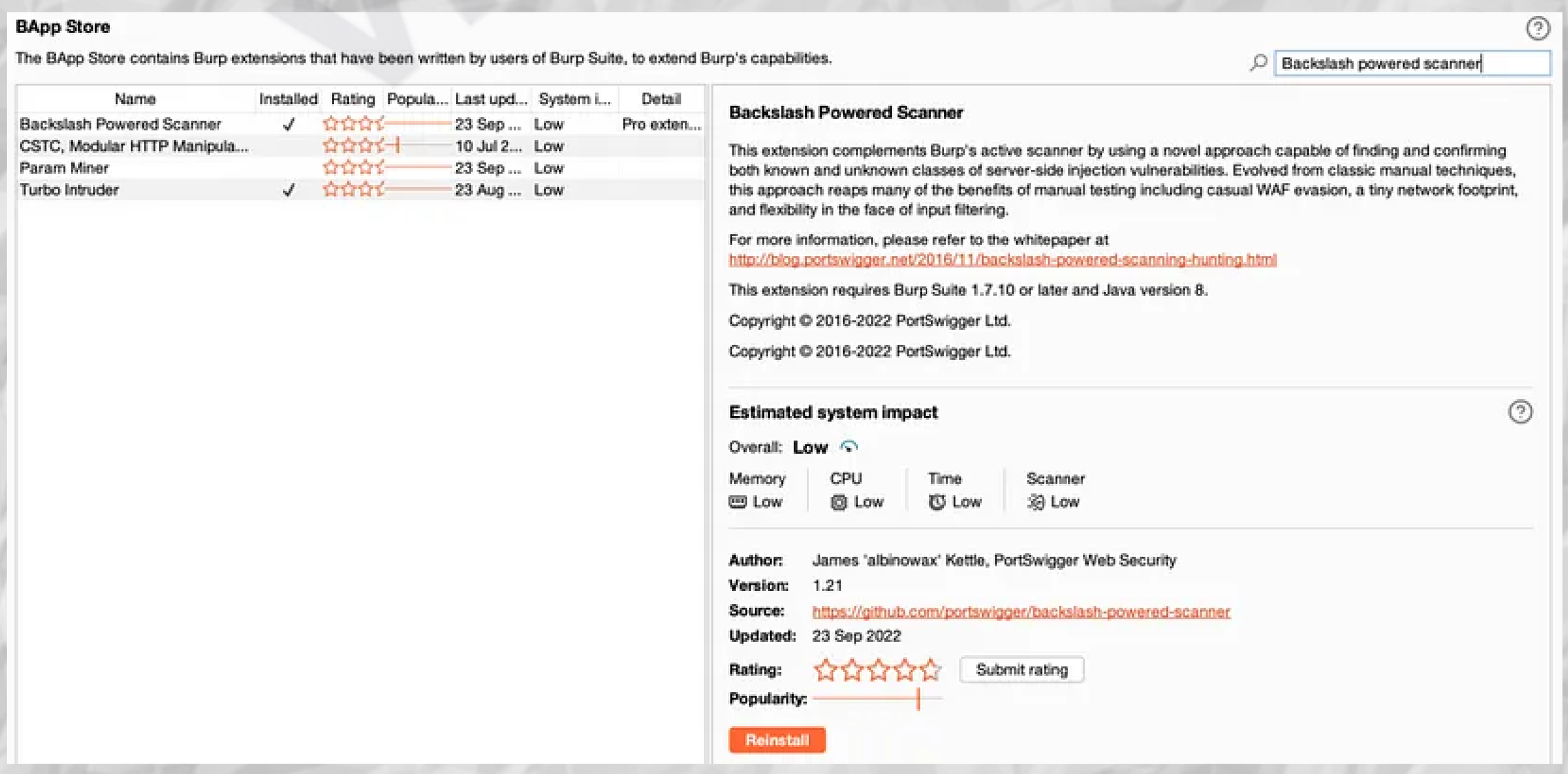
Active Scan++ is a powerful Burp Suite extension that enhances the active scanning capabilities of the popular web application testing tool. This extension utilizes advanced techniques and algorithms to identify a wide range of vulnerabilities in web applications, including cross-site scripting, SQL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



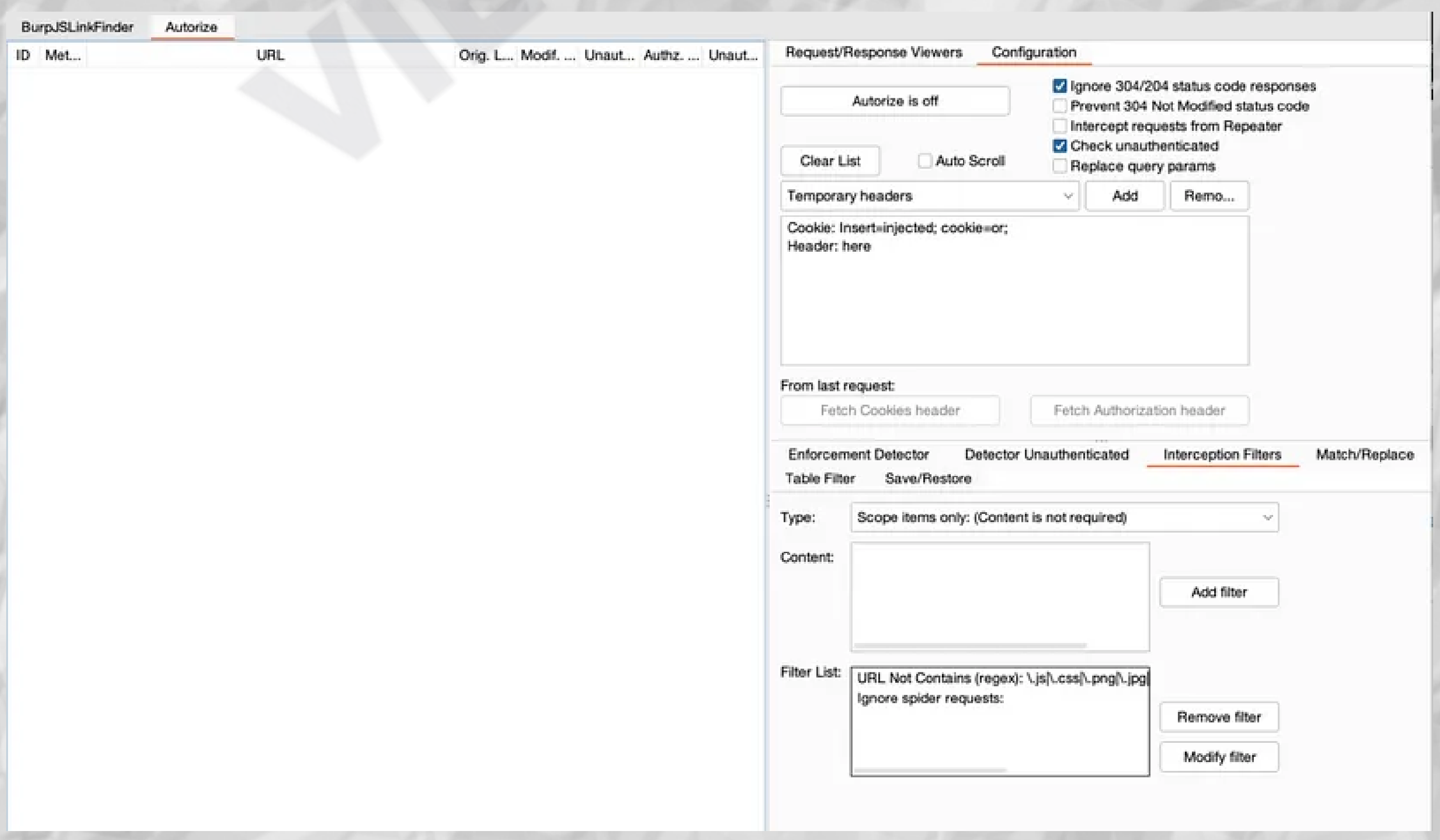
Backslash Powered Scanner

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.



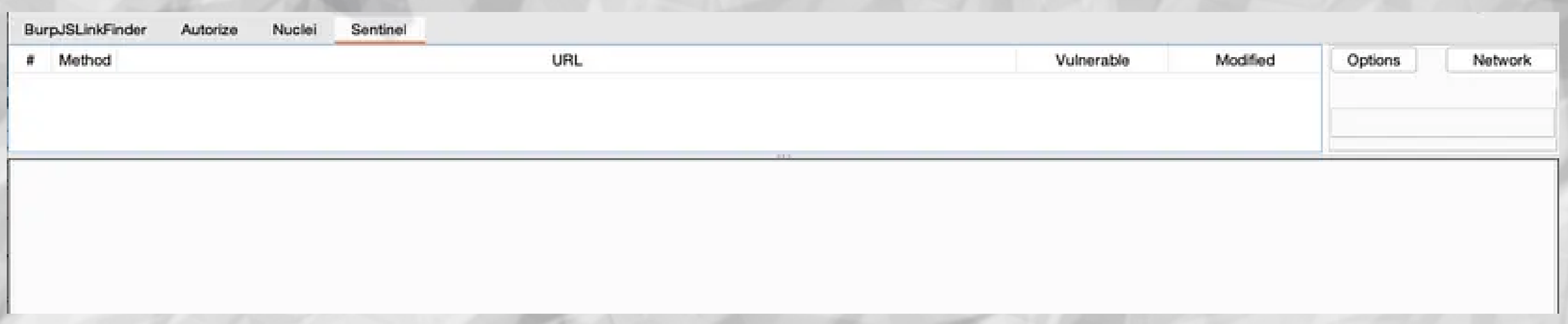
Autorize

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.



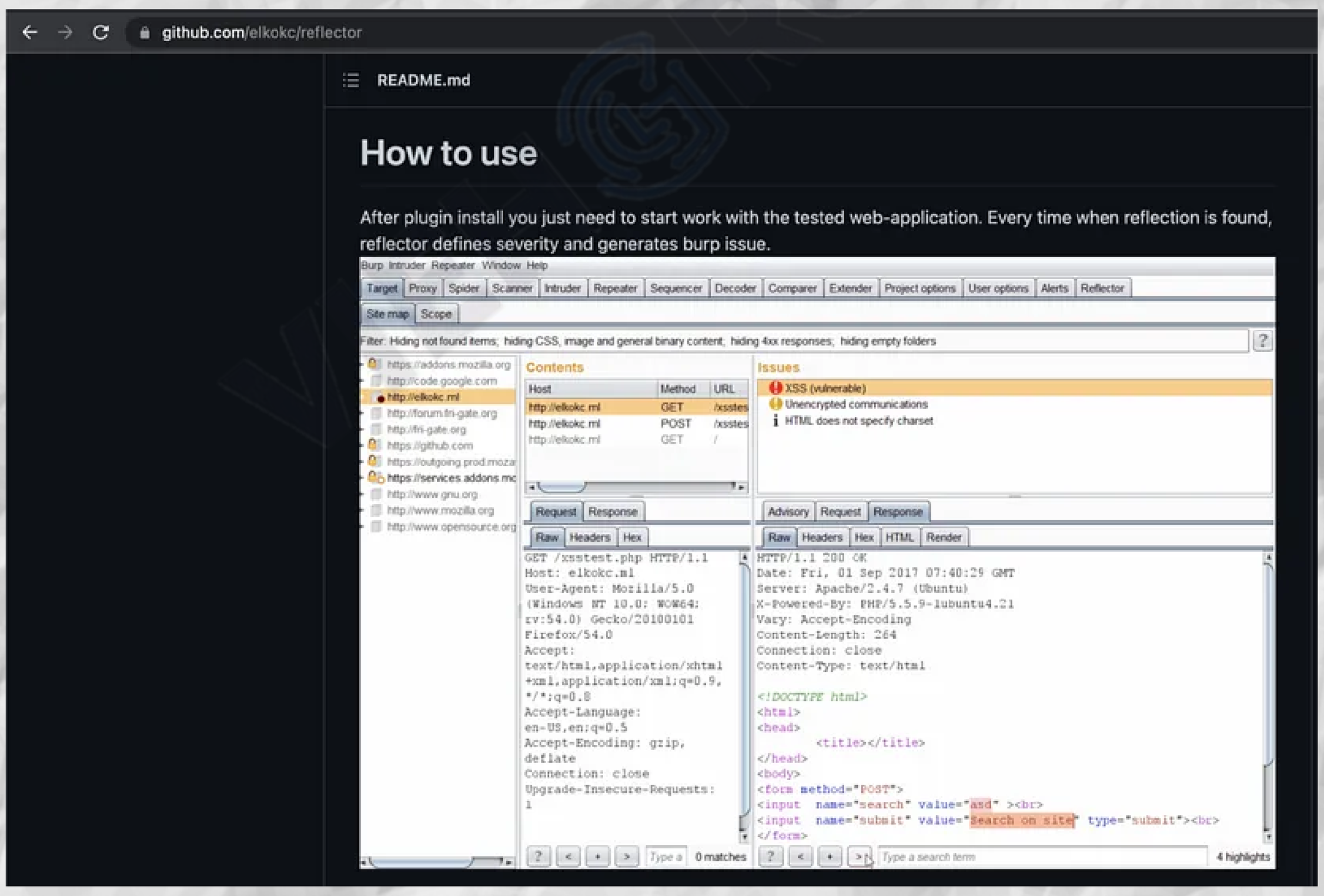
Sentinel

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.



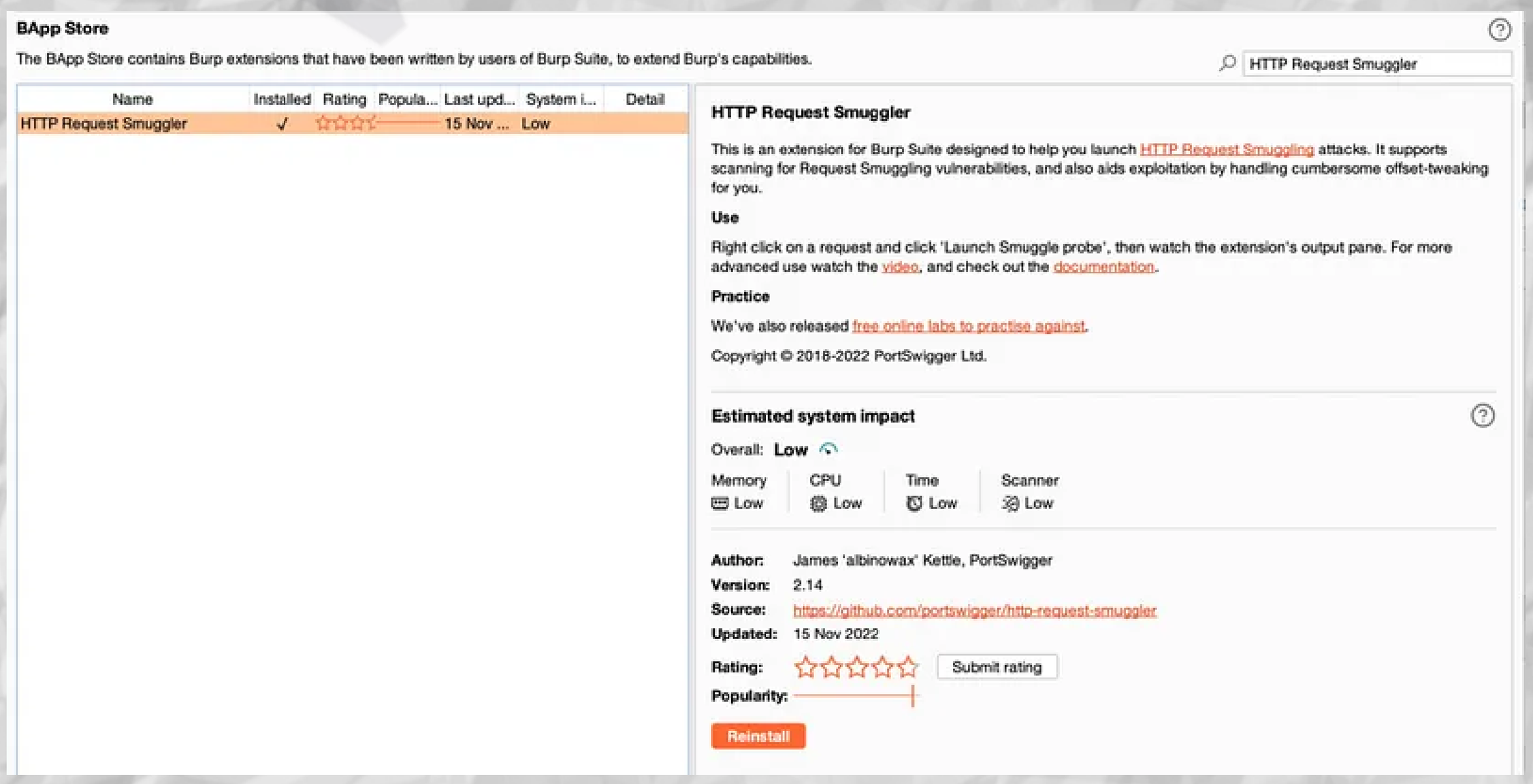
Reflector

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.



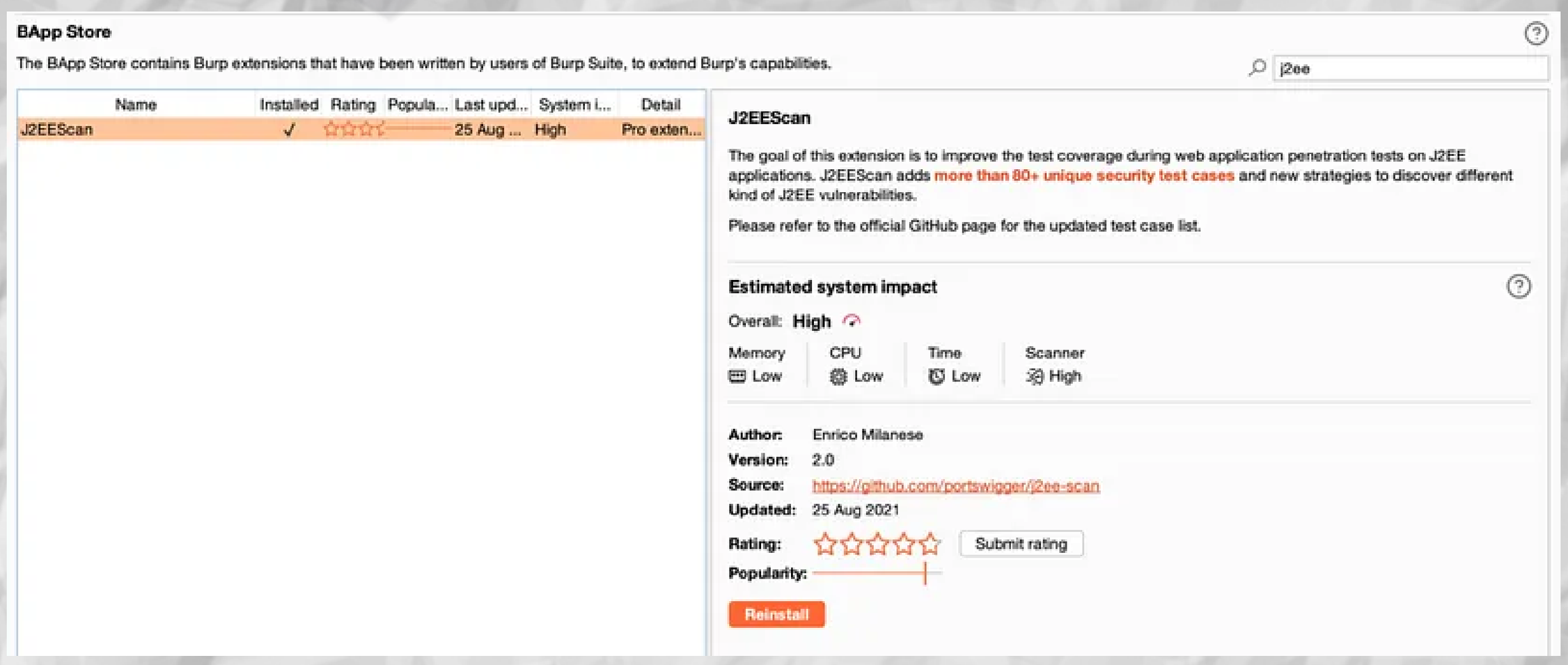
HTTP Request Smuggler

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.



J2EEScan

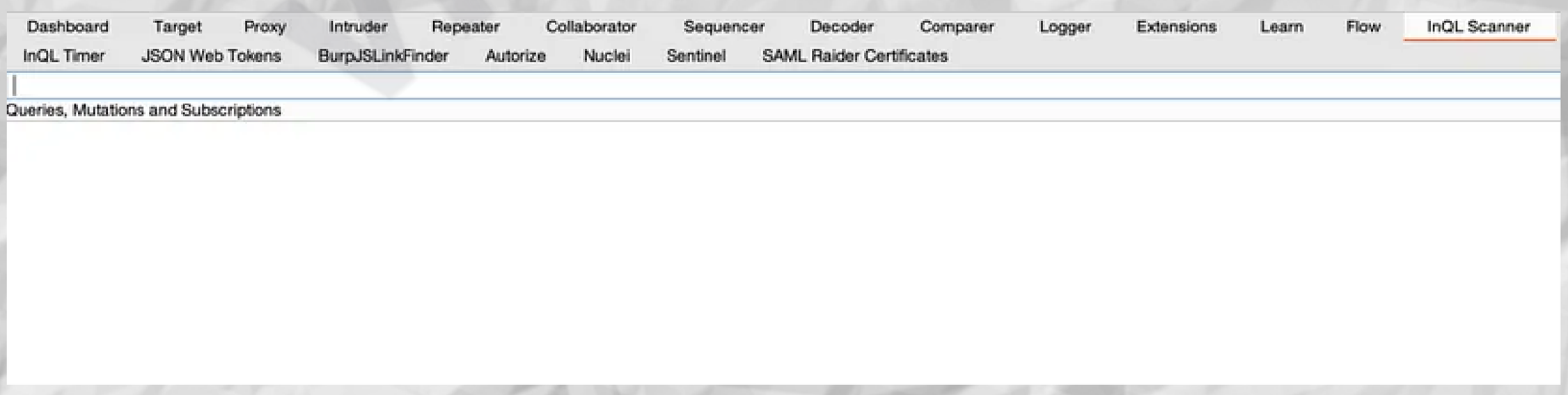
J2EEScan is a powerful Burp Suite extension that is designed specifically for scanning Java EE web applications.It can detect a variety of vulnerabilities related to authentication, authorization, and session management, and provide recommendations for remediation.The extension also has the ability to 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.



InQL Scanner

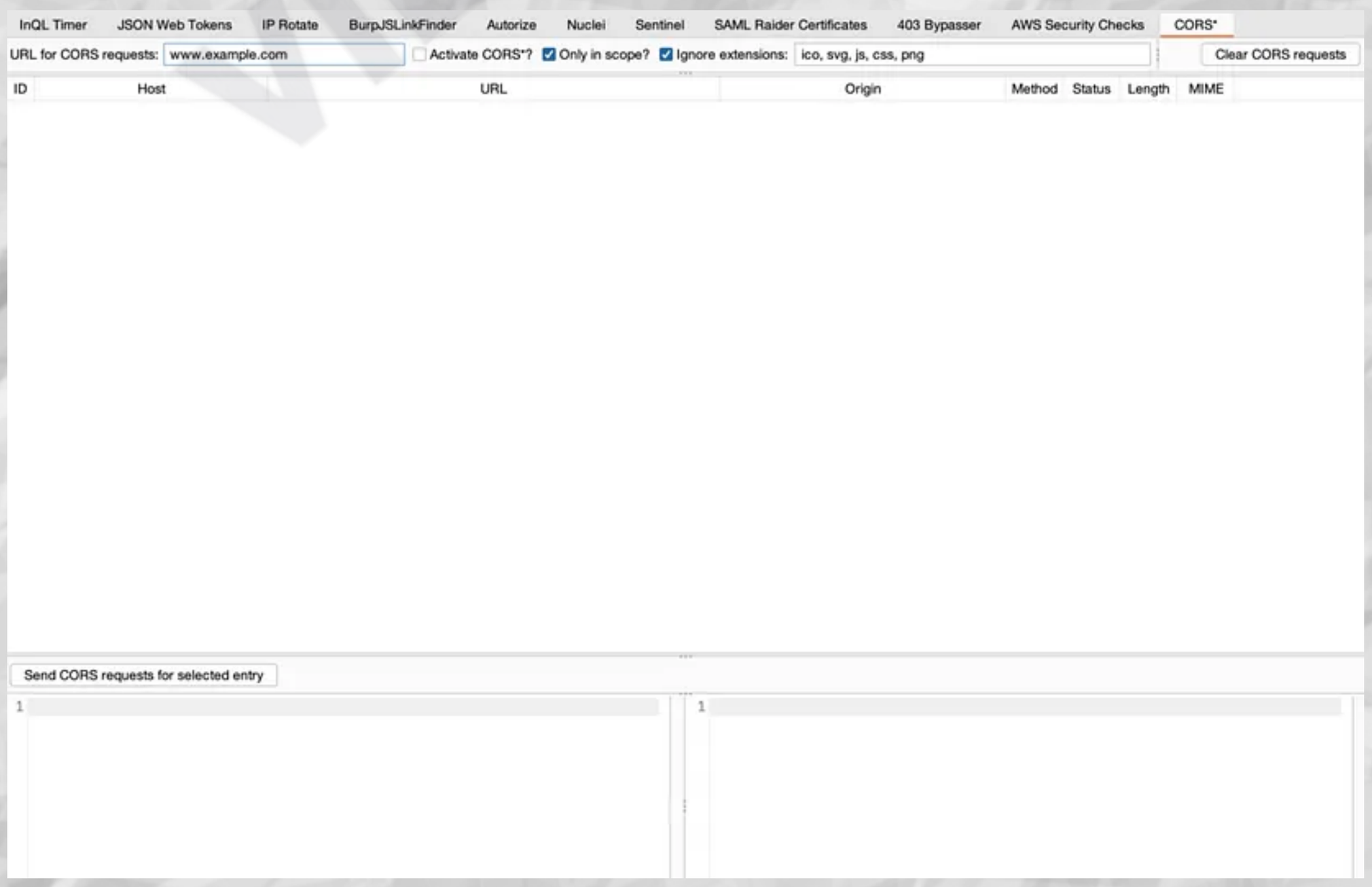
The InQL Scanner is a powerful Burp Suite extension that helps security professionals identify and exploit vulnerabilities within GraphQL APIs.It provides a wide range of features that allow users to easily and efficiently discover and test GraphQL endpoints, as well as identify and exploit any vulnerabilities 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.



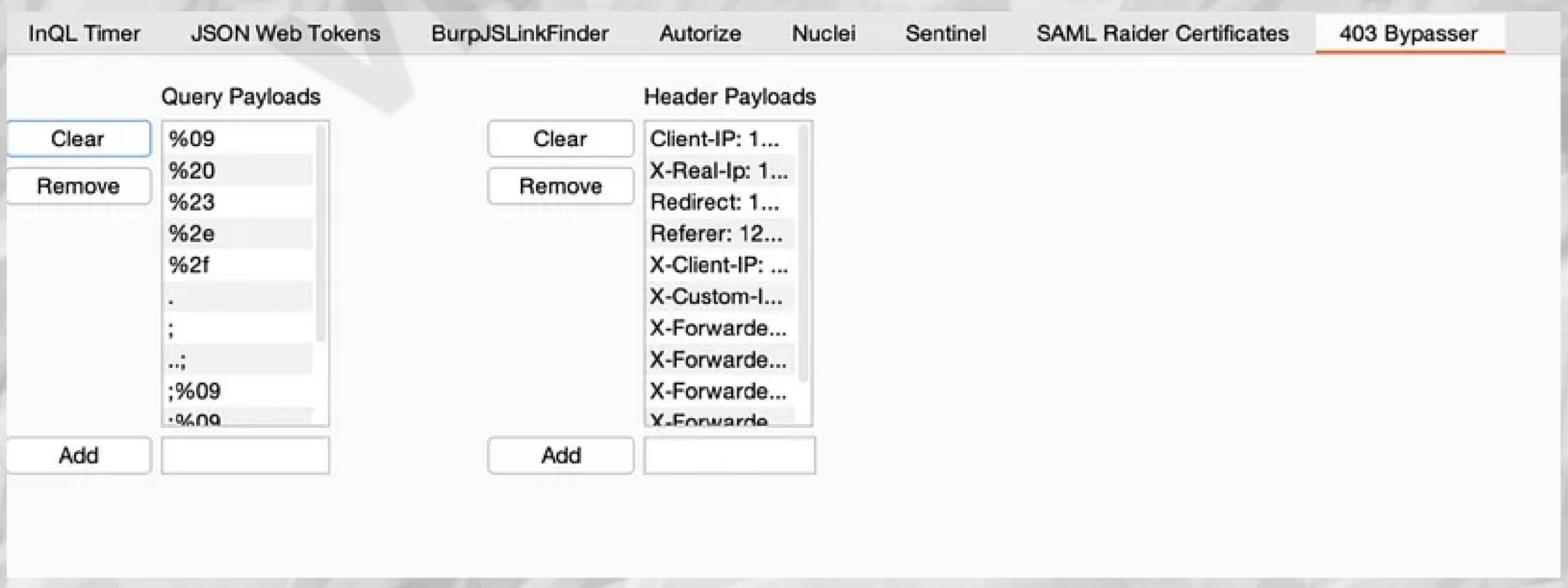
CORS*, Additional CORS Checks

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.



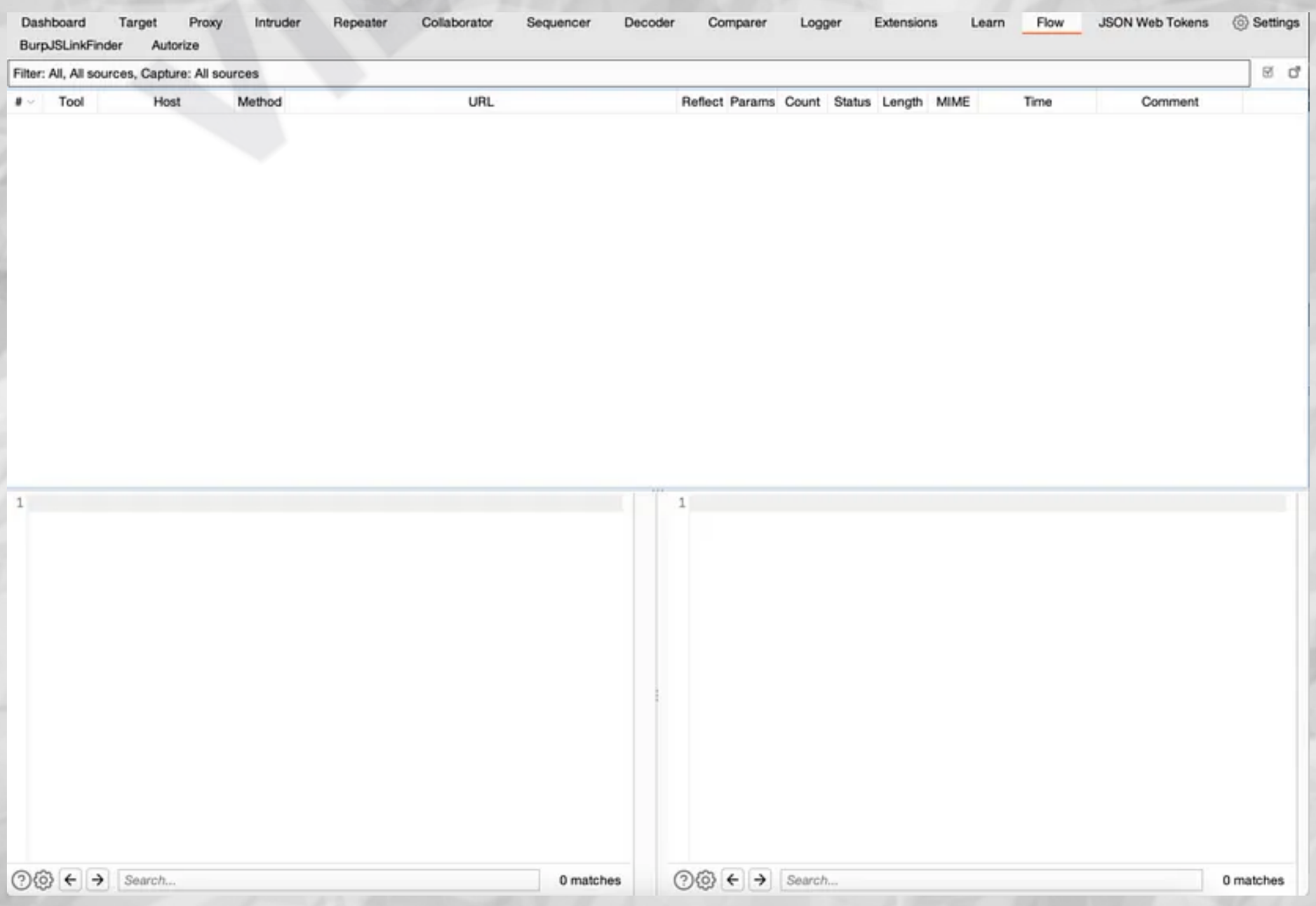
403 Bypasser

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.



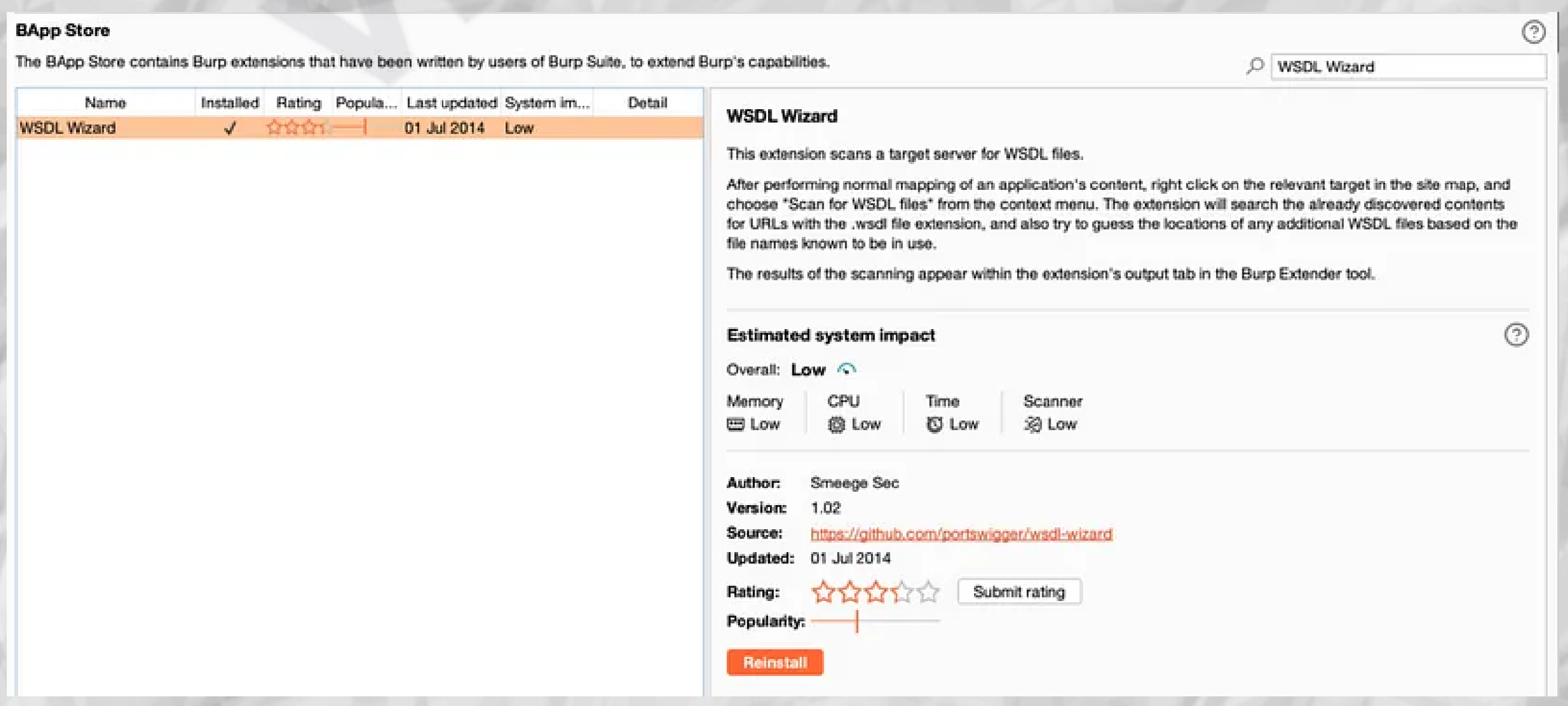
Flow

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.



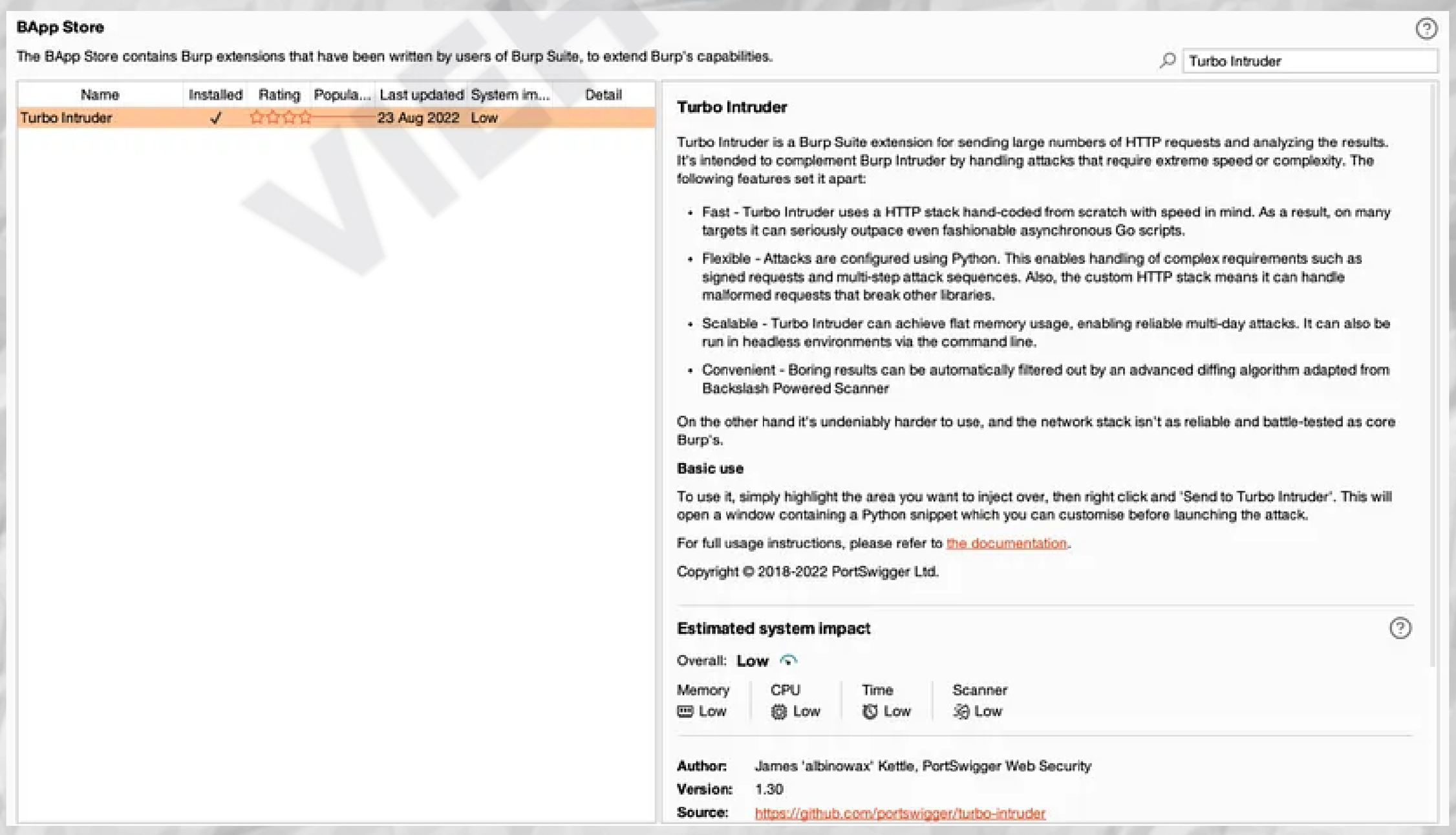
WSDL Wizard

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.



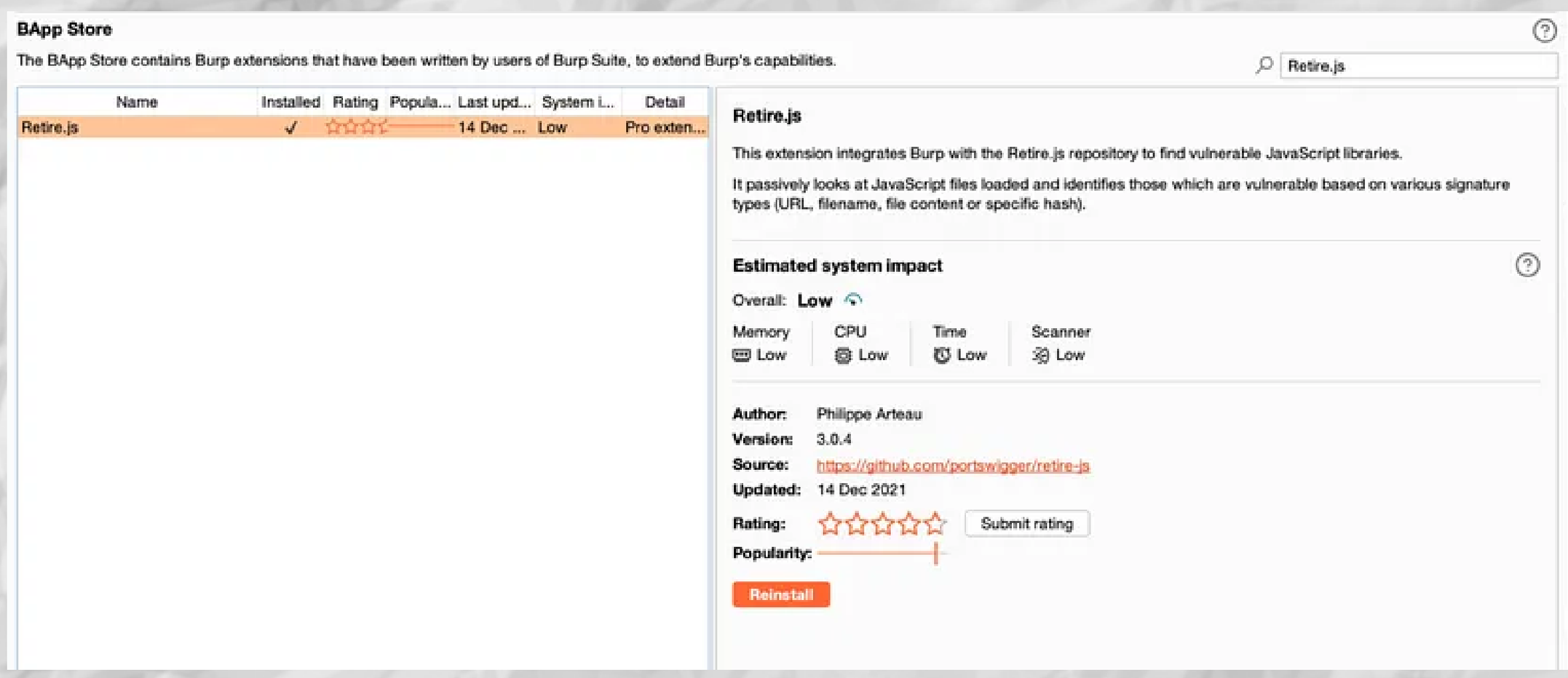
Turbo Intruder

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.



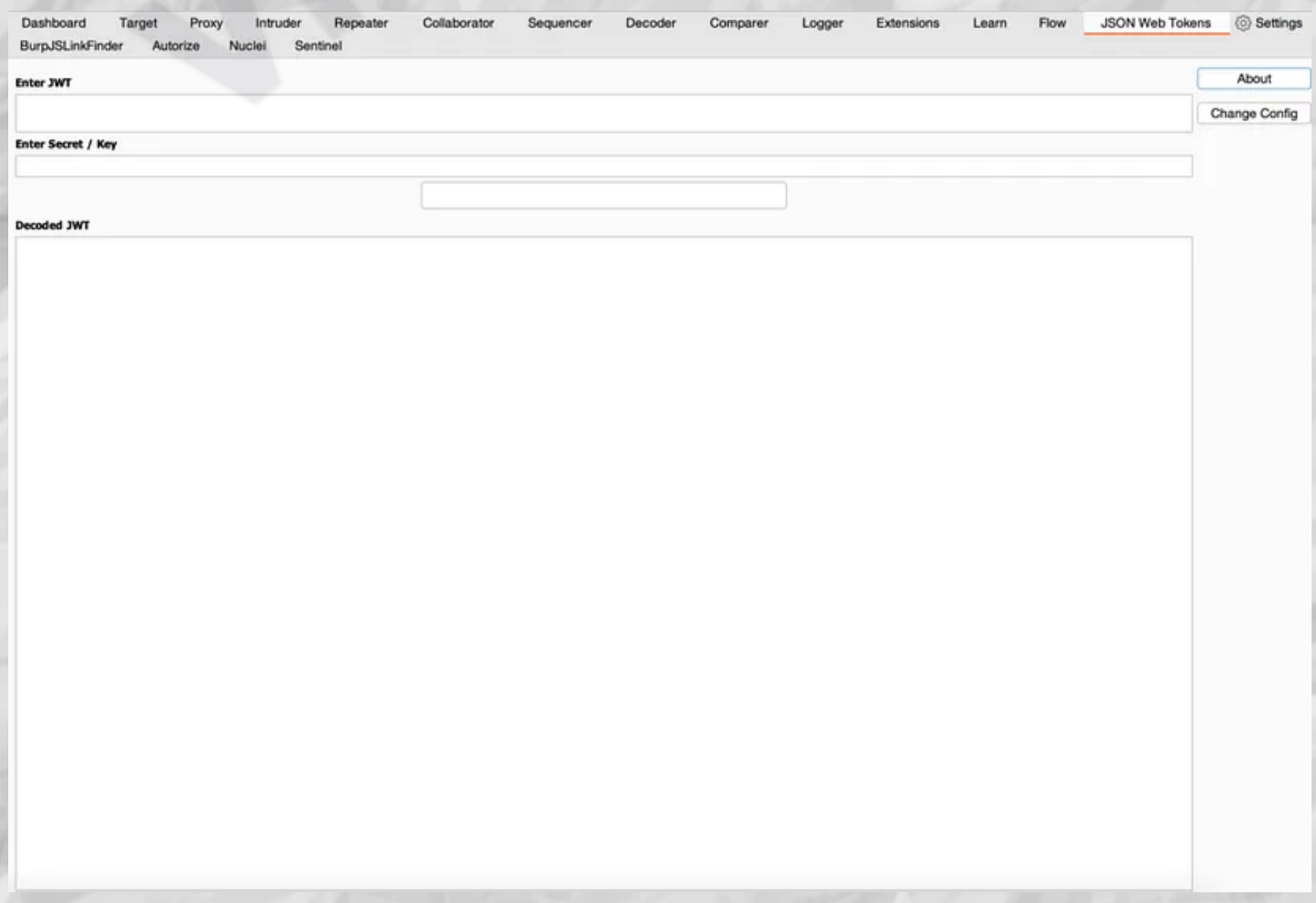
Retire.js

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.



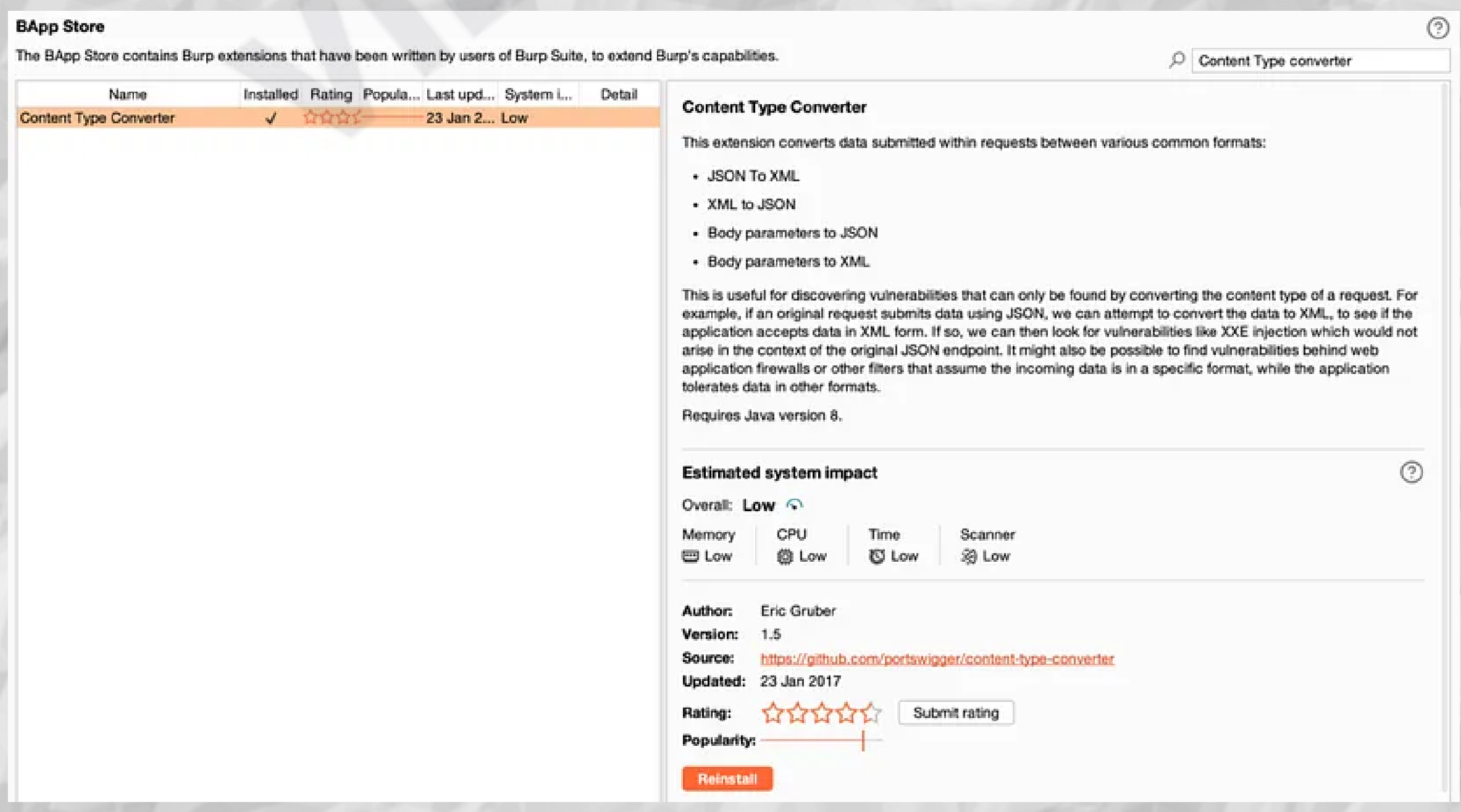
JSON Web Tokens

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.



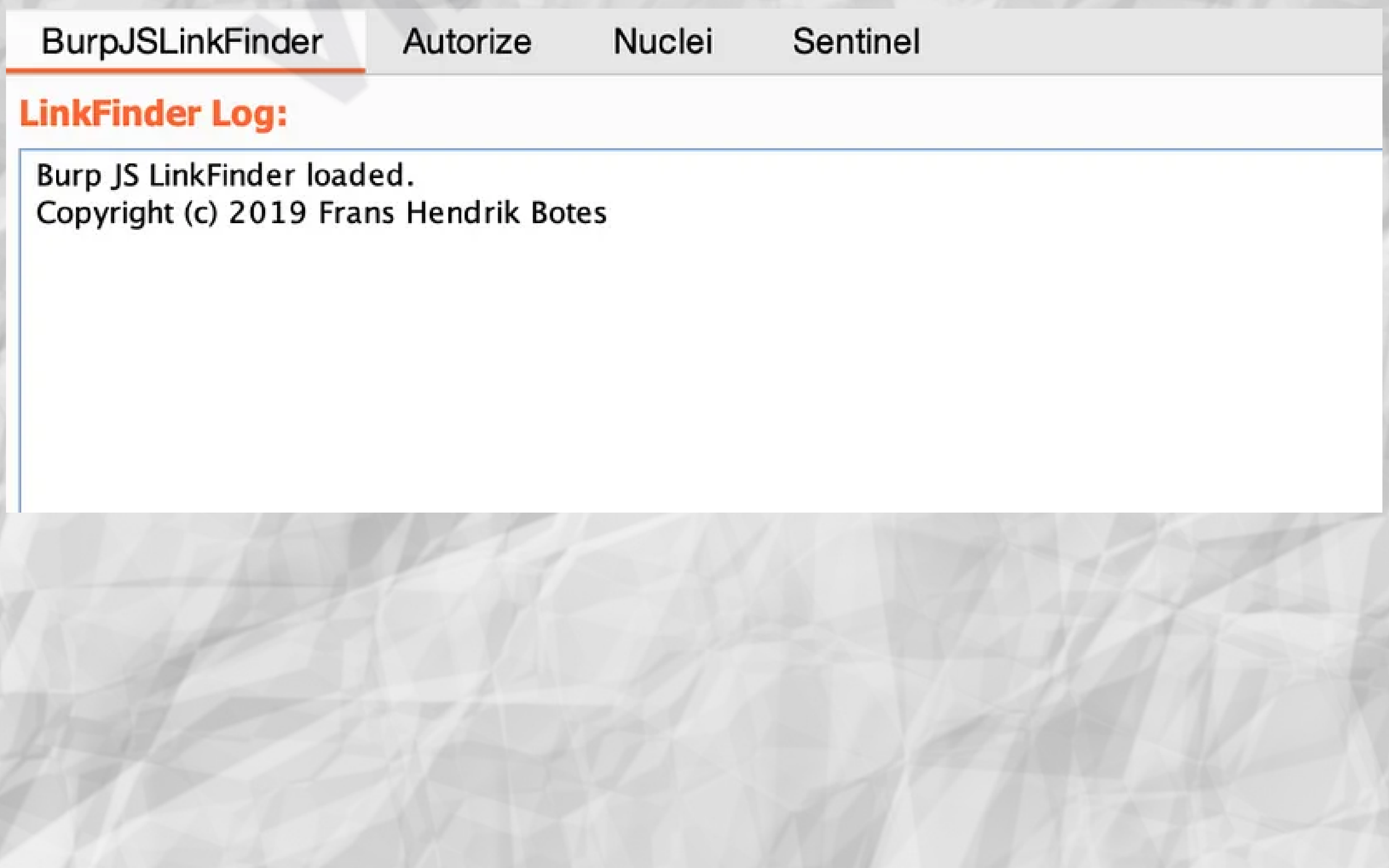
Content Type Converter

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.



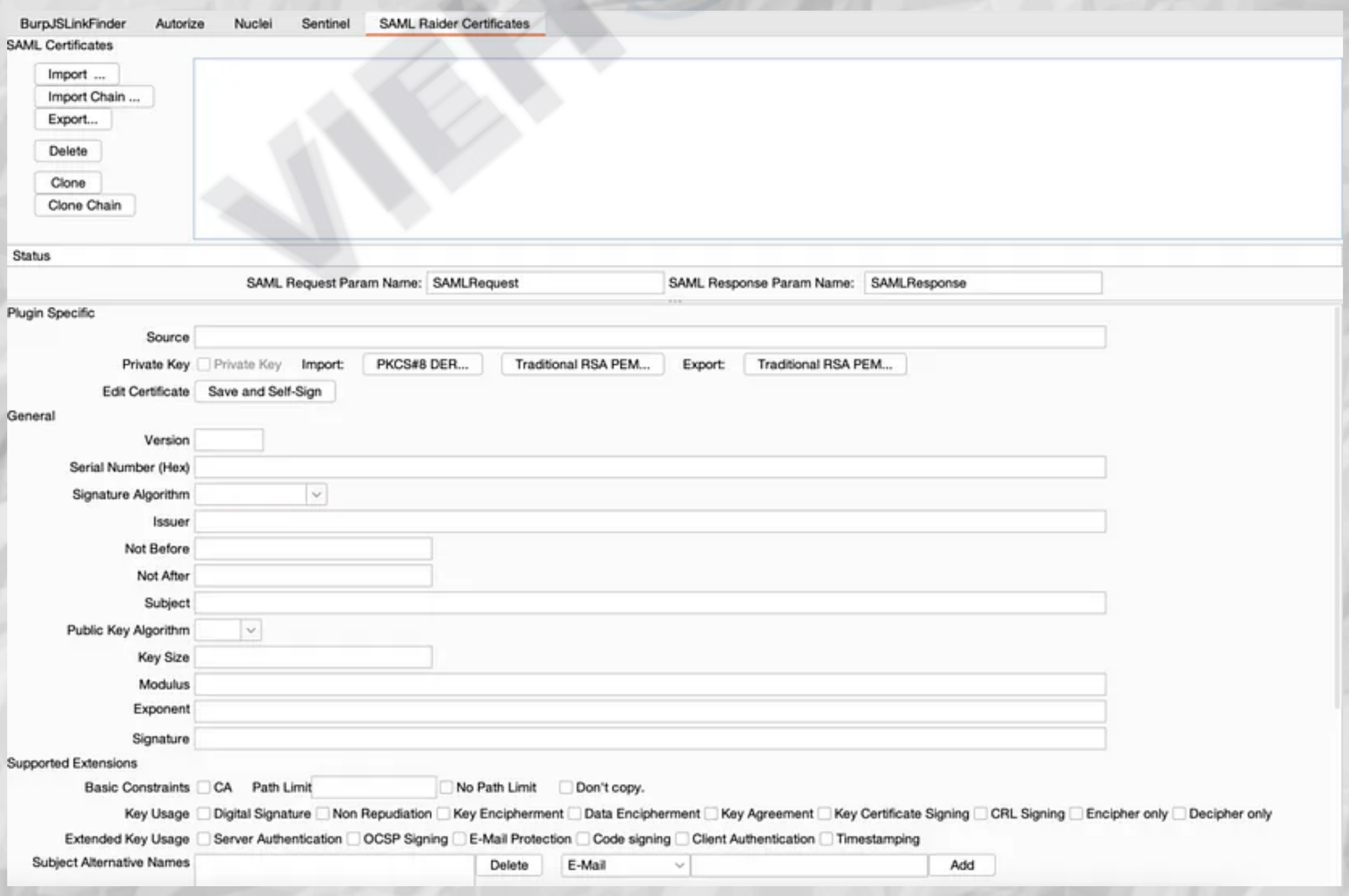
BurpJSFinder

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.



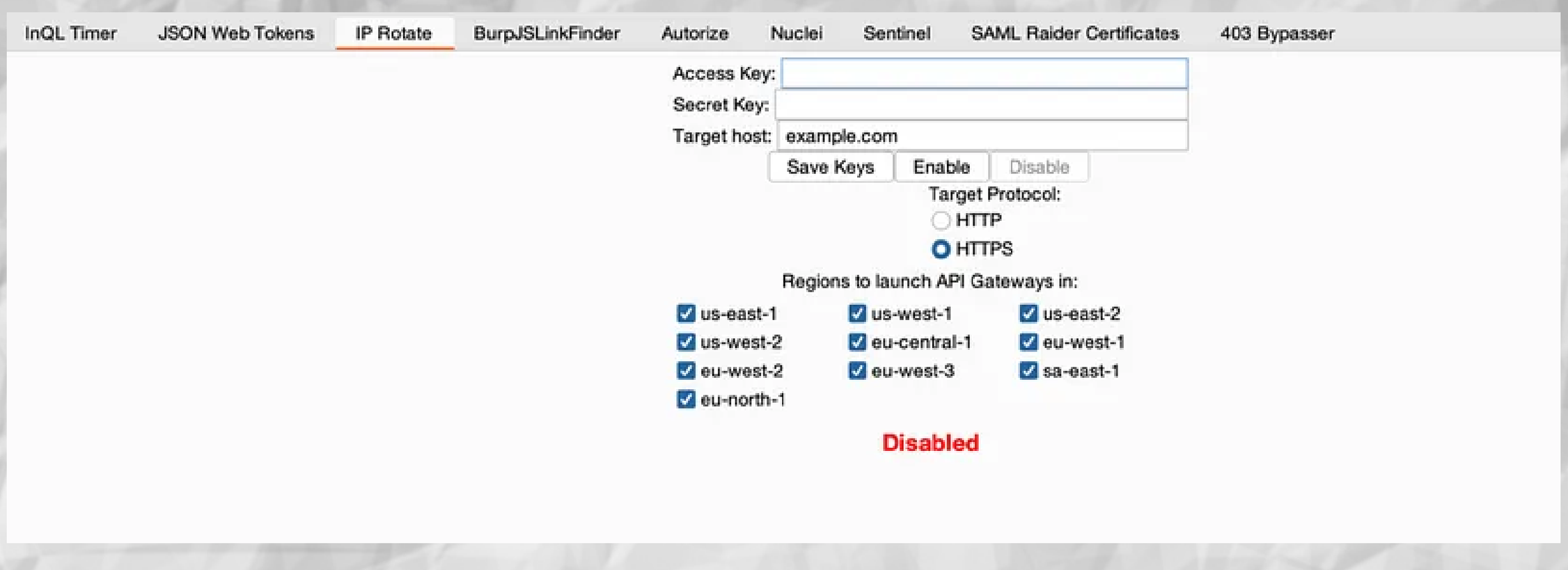
SAML Raider

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.



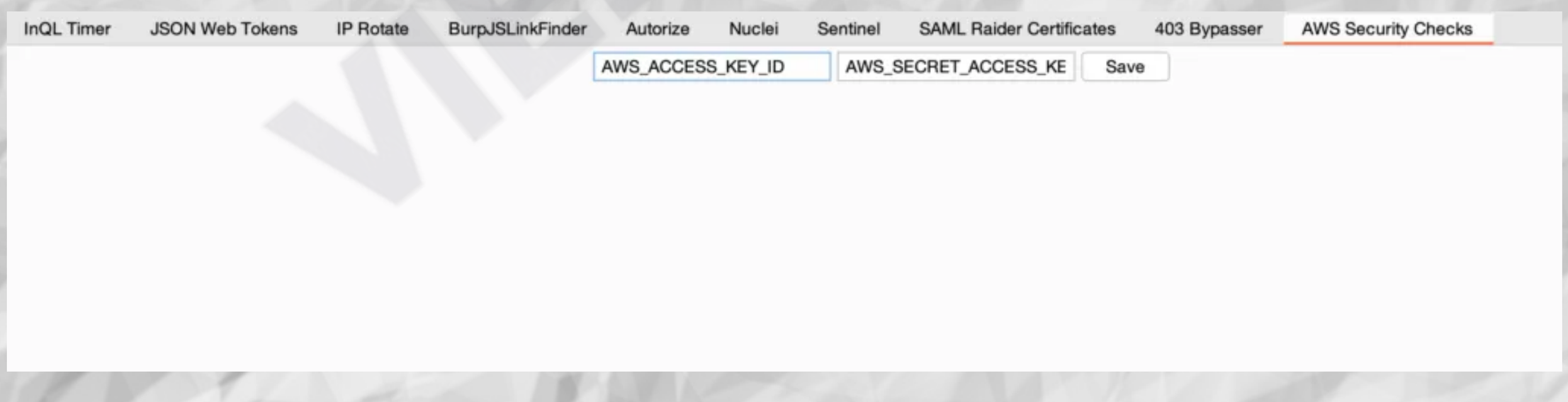
IP Rotate

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.



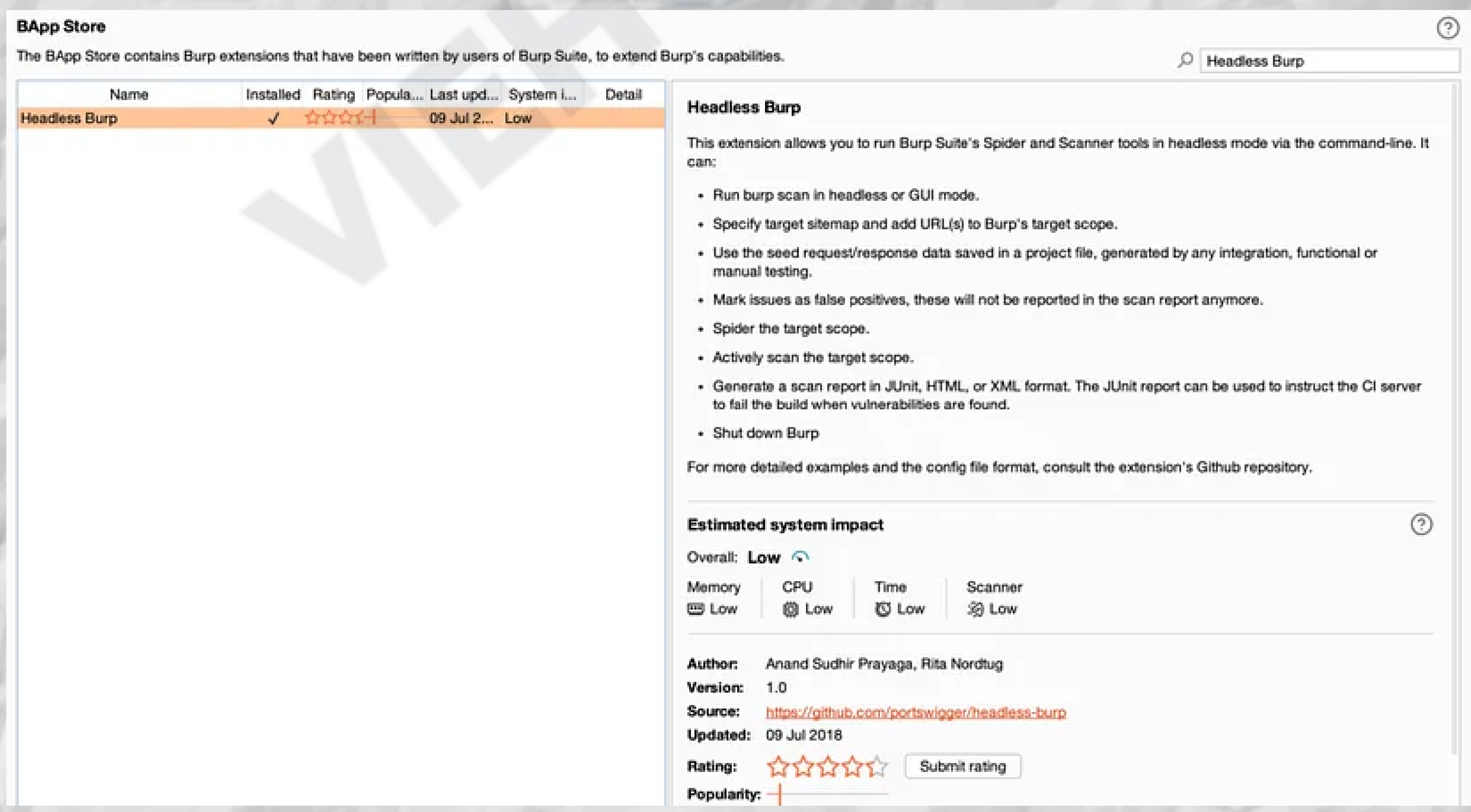
AWS Security Checks

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.



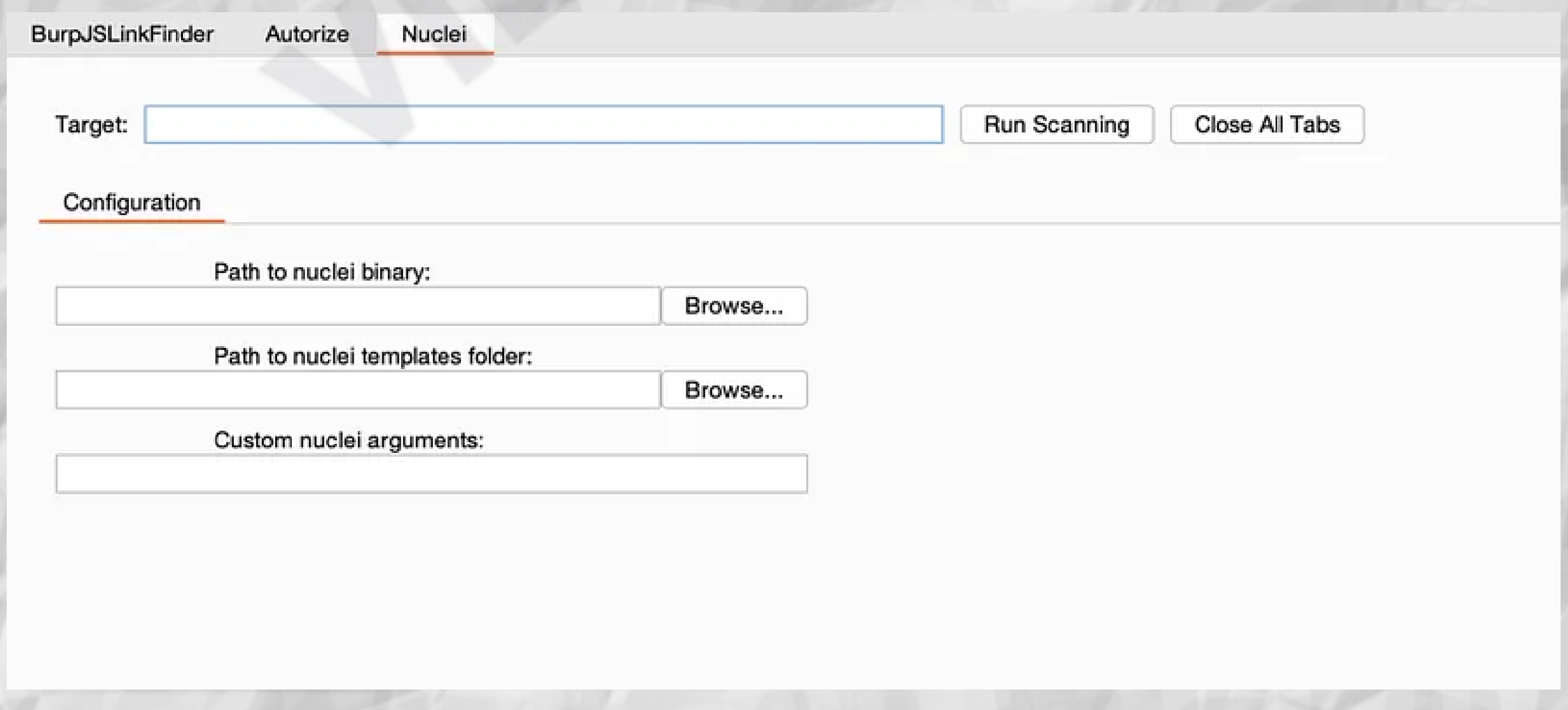
Headless Burp

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.



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