CyberSapiens

THE CYBER SECURITY EXPERTS

BURPSUITE

By: Trapson Aaron

What exactly is Burp Suite?

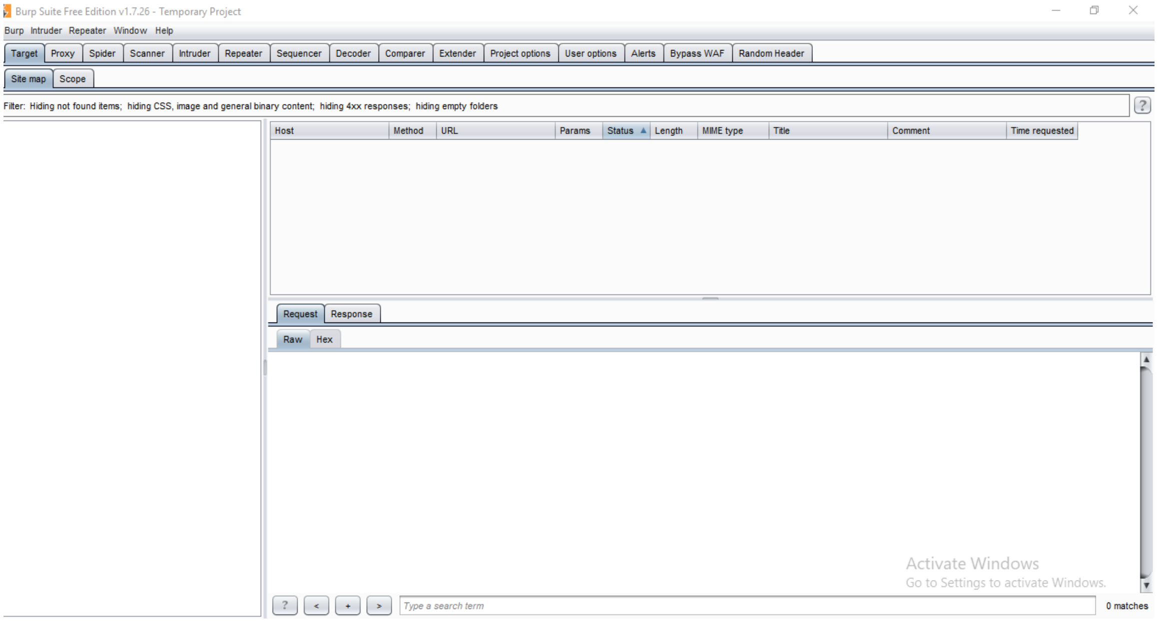
Burp Suite, also known simply as Burp, constitutes a comprehensive toolkit utilized for conducting penetration tests on web applications. It originates from the software development efforts of Portswigger, a company synonymous with its founder, Dafydd Stuttard. The objective behind BurpSuite is to amalgamate various tools into a singular platform, with the option to extend its functionalities through supplementary components termed BApps.

Notably, it stands as the tool of choice for numerous professional web application security analysts and individuals engaged in bug bounty programs. Its user-friendly interface renders it preferable when contrasted with free alternatives such as OWASP ZAP. Burp Suite offers multiple editions: a no-cost community edition, a professional variant priced at $399 per annum, and an enterprise-level edition costing $3999 annually. This exposition provides a succinct overview of the toolkit's offerings. For those new to web application penetration testing, web application hacking, or bug bounty endeavors, we suggest absorbing the content without delving too deeply into technical jargon.

Burp Suite Options

Below are the tools offered by Burp Suite and how they work:

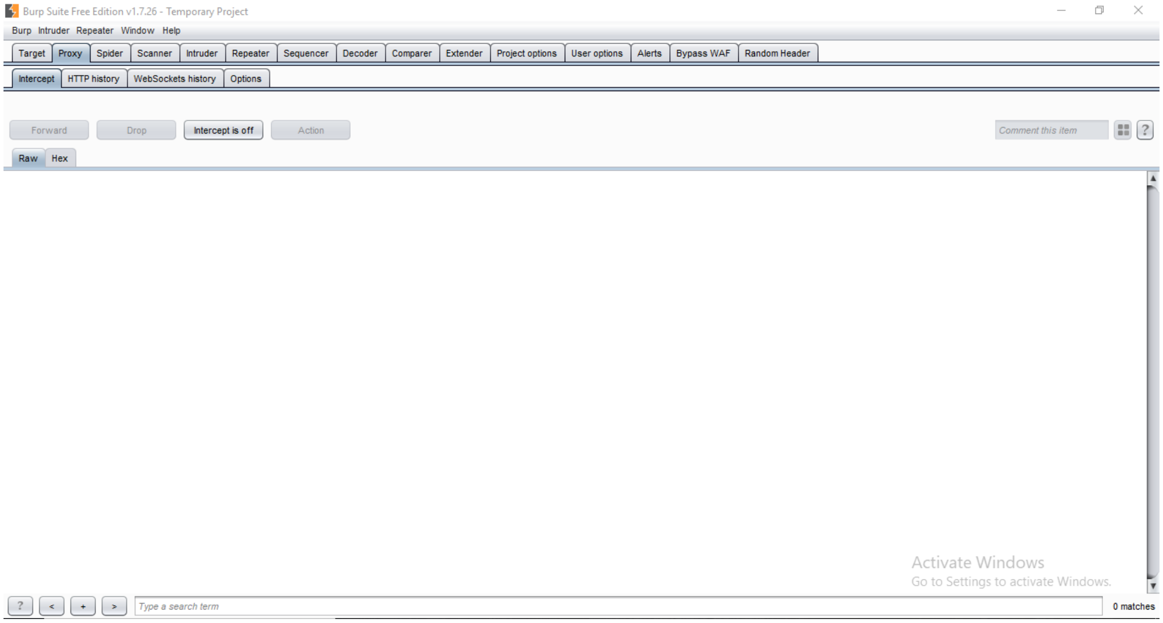
1. **Spider**



Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

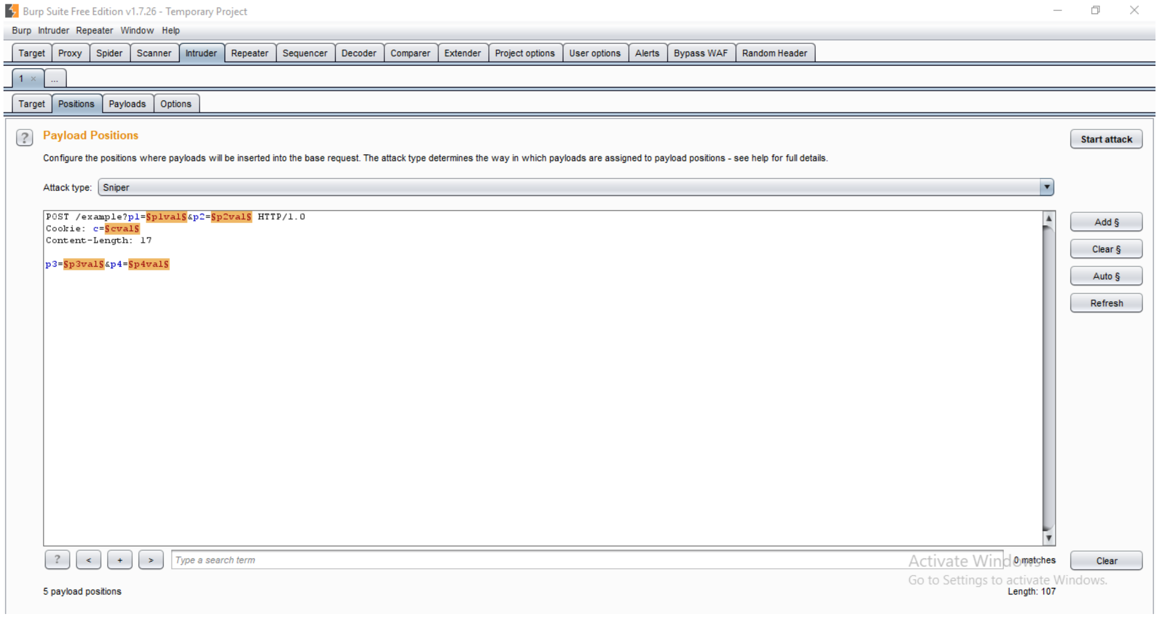
A spider, in the context of Burp Suite, serves as a web crawler utilized to traverse and map the structure of the targeted web application. The primary aim of this mapping endeavor is to compile a comprehensive list of endpoints, enabling analysts to scrutinize their functionalities and identify potential vulnerabilities. The process of spidering is essential because the accumulation of endpoints during reconnaissance expands the array of attack surfaces available for subsequent testing phases.

2. Proxy


Burp Suite Free Edition v1.7.26 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts Bypass WAF Random Header
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is off
Action
Comment this item
Raw Hex
Activate Windows
Go to Settings to activate Windows.
?
<
+
>
Type a search term
0 matches

Within BurpSuite, there exists an intercepting proxy, facilitating users in viewing and manipulating the contents of requests and responses as they traverse the network. Moreover, this proxy empowers users to seamlessly redirect monitored requests or responses to other pertinent tools within the BurpSuite environment, eliminating the need for manual copying and pasting. Users can fine-tune the proxy server to operate on a designated loop-back IP address and port, offering flexibility in configuration. Additionally, the proxy configuration allows for the filtering of specific types of request-response pairs as per the user's requirements.

3. Intruder


Burp Suite Free Edition v1.7.26 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts Bypass WAF Random Header
1 ...
Target Positions Payloads Options
Start attack
Add §
Clear §
Auto §
Refresh
Type a search term
0 matches
Clear
Activate Windows
Go to Settings to activate Windows.

Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Sniper

```
POST /example?p1=§p1val§&p2=§p2val§ HTTP/1.0
Cookie: c=§cval§
Content-Length: 17

p3=§p3val§&p4=§p4val§
```

5 payload positions

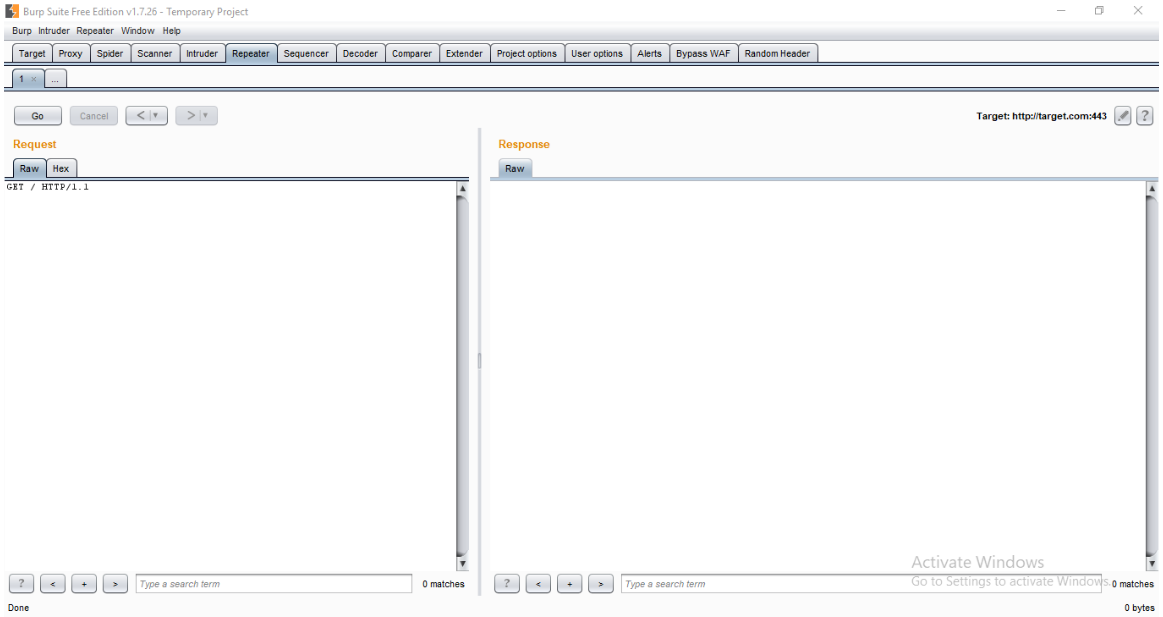
Length: 107

This is an essential tool within BurpSuite, functions as a versatile fuzzer designed to systematically test input points within web applications. It operates by injecting a variety of values into designated input fields, observing the resulting output for signs of success or failure, such as changes in response codes or content length. BurpSuite offers multiple payload options through Intruder, including brute-force, dictionary file, and single values, catering to different testing scenarios.

Intruder is specifically employed for:

- Conducting brute-force attacks on password forms, PIN forms, and other input fields requiring authentication, systematically attempting numerous combinations to gain unauthorized access.
- Executing dictionary attacks on password fields, as well as fields suspected of vulnerability to cross-site scripting (XSS) or SQL injection, by systematically testing against a predefined list of words or phrases.
- Assessing and potentially bypassing rate-limiting mechanisms implemented within the web application, allowing testers to evaluate the effectiveness of such controls and identify potential vulnerabilities.

4. Repeater


Burp Suite Free Edition v1.7.26 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts Bypass WAF Random Header
1 ×
...
Go
Cancel
Request
Raw
Hex
Response
Raw
?
<
+
>
Type a search term
0 matches
Done
0 bytes
Activate Windows
Go to Settings to activate Windows.

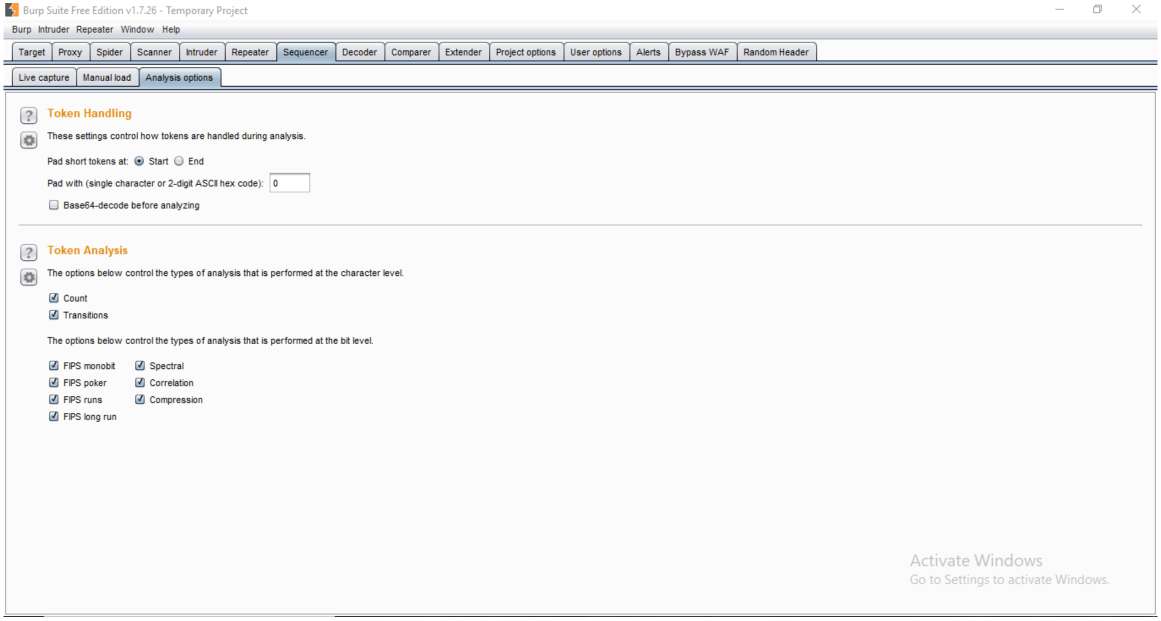
Target: http://target.com:443

```
GET / HTTP/1.1
```

This is a component of BurpSuite, empowers users to send requests iteratively while allowing for manual modifications. It serves several crucial purposes:

- Verification of whether user-supplied values undergo validation.
- Assessment of the adequacy and effectiveness of validation mechanisms applied to user-supplied values.
- Determination of the expected values in input parameters or request headers by analyzing server responses.
- Evaluation of how the server handles unexpected values, shedding light on potential vulnerabilities.
- Examination of whether the server implements input sanitation measures and the effectiveness of such measures.
- Analysis of the server's input sanitization methods to discern the style employed.
- Identification of the primary session cookie among the various cookies present.
- Inspection of how Cross-Site Request Forgery (CSRF) protection is implemented and exploration of potential bypass techniques if applicable.

5. Sequencer



Token Handling

These settings control how tokens are handled during analysis.

Pad short tokens at: ● Start ○ End

Pad with (single character or 2-digit ASCII hex code): 0

□ Base64-decode before analyzing

Token Analysis

The options below control the types of analysis that is performed at the character level.

☑ Count
☑ Transitions

The options below control the types of analysis that is performed at the bit level.

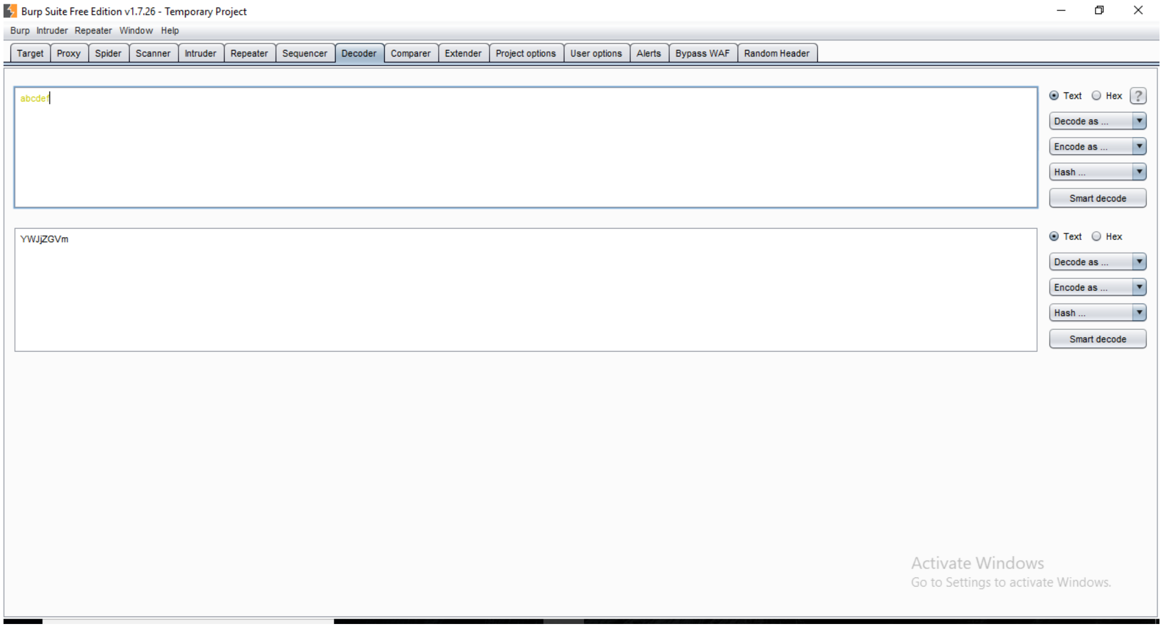
☑ FIPS monobit ☑ Spectral
☑ FIPS poker ☑ Correlation
☑ FIPS runs ☑ Compression
☑ FIPS long run

The Sequencer, a tool within BurpSuite, functions as an entropy checker, specifically assessing the randomness of tokens generated by web servers. These tokens are commonly utilized for authentication purposes in critical operations, such as cookies and anti-CSRF tokens. The ideal scenario entails these tokens being generated in a fully random manner, ensuring uniform distribution of the probability of each possible character appearing at any given position, both at the bit-wise and character-wise levels.

The process of entropy analysis involves testing tokens against predefined parameters to determine their characteristics. Initially, it assumes that the tokens are random. Subsequently, these tokens are scrutinized for specific traits. A term known as significance level is established, representing the minimum probability value that a token must exhibit for a given characteristic. If a token's probability falls below this significance level for a particular trait, the hypothesis of randomness is rejected.

By leveraging the Sequencer, users can identify weak tokens and discern their construction patterns, enabling further enumeration of potential vulnerabilities.

6. Decoder



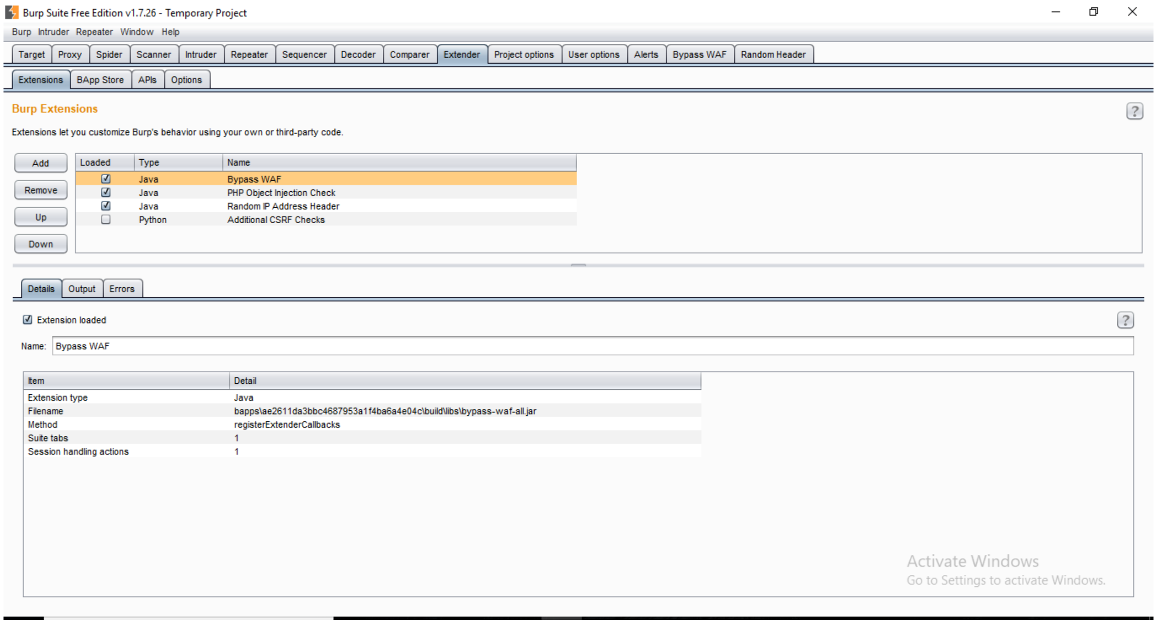
```
abcdef
```

```
YWJjZGVm
```

The Decoder feature within BurpSuite provides a convenient catalog of prevalent encoding methods such as URL, HTML, Base64, Hex, among others. This tool proves invaluable when searching for data segments within parameter or header values, facilitating the identification of encoded information. Moreover, it serves as a versatile resource for constructing payloads across different vulnerability classes.

Decoder is particularly instrumental in uncovering instances of Insecure Direct Object References (IDOR) and session hijacking. By decoding encoded data, security analysts can reveal sensitive information and potential vulnerabilities within web applications, aiding in the prevention and mitigation of security threats.

7. Extender


Burp Suite Free Edition v1.7.26 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts Bypass WAF Random Header
Extensions BApp Store APIs Options
Add
Remove
Up
Down
Details Output Errors
Activate Windows
Go to Settings to activate Windows.

Burp Extensions

Extensions let you customize Burp's behavior using your own or third-party code.

Loaded	Type	Name
☑	Java	Bypass WAF
☑	Java	PHP Object Injection Check
☑	Java	Random IP Address Header
□	Python	Additional CSRF Checks

☑ Extension loaded

Name: Bypass WAF

Item	Detail
Extension type	Java
Filename	bapps\ae2611da3bbc4687953a1f4ba6a4e04c\build\libs\bypass-waf-all.jar
Method	registerExtenderCallbacks
Suite tabs	1
Session handling actions	1

BurpSuite boasts support for external components known as BApps, which seamlessly integrate into the tool suite to bolster its functionalities. Comparable to browser extensions, these BApps can be accessed, customized, installed, and uninstalled via the Extender window. While certain BApps are compatible with the community version, others necessitate the paid professional edition for utilization. These extensions contribute to enhancing the capabilities of BurpSuite, catering to diverse user requirements and facilitating an optimized experience for security professionals and researchers alike.

8. Scanner

The scanner functionality, unfortunately, isn't accessible in the community edition of BurpSuite. This automated tool conducts comprehensive website scans, systematically examining for numerous common vulnerabilities. It compiles a detailed report listing identified issues along with corresponding information regarding confidence levels for each finding and the complexity associated with their exploitation. Regular updates ensure that the scanner remains current, encompassing new and lesser-known vulnerabilities to enhance detection capabilities and maintain robust security assessments.

Adding extensions to Burp Suite Enterprise Edition

In Burp Suite Enterprise Edition, integrating extensions involves uploading them to your Extension Library. Once uploaded, users gain access to these extensions from a centralized repository. They can then selectively apply these extensions on a site-by-site basis, allowing for their utilization during scans conducted within the platform. This centralized approach streamlines the management and deployment of extensions, ensuring consistent usage across different projects and enhancing the efficiency of security assessments.

Here is a link of a demonstration YouTube video by PortSwigger:

https://youtu.be/A06QsitVg8U

Prerequisite permissions for adding extensions

To add extensions to the library in Burp Suite Enterprise Edition, users must possess the prerequisite permission of "`Manage extensions.`" By default, this permission is solely allocated to the built-in `Administrator` role.

> A word of caution:
>
> *Exercise caution when assigning this permission to additional users. It's important to note that during a scan, extensions execute on your scanning machine with the permissions of the burpsuite operating system user. Consequently, there exists a potential security risk if an individual inadvertently uploads a fraudulent extension crafted by a malicious third party.*

Adding BApps to Burp Suite Enterprise Edition

To add a BApp:

1. Download the BApp from the BApp Store. Make sure that it is compatible with Burp Suite Enterprise Edition - you can filter the store to make this easier.
2. Log in to Burp Suite Enterprise Edition as a user with permission to manage extensions.
3. From the settings menu ⚙, select **Extensions** to open the Extension library.
4. On the BApp extensions tab, click **Upload BApp**.
5. Select the `.bapp` file that you downloaded from the BApp Store.

The extension is now in your Extension library. Your users can apply the extension to specific sites to use it during scans.

Adding custom extensions to Burp Suite Enterprise Edition

If you're proficient in Java, you can create your own custom extensions for Burp Suite Enterprise Edition. Learn more about Creating Burp extensions.

To add a custom extension:

1. Log in to Burp Suite Enterprise Edition as a user with permission to manage extensions.
2. From the settings menu ⚙, select **Extensions** to open the Extension library.
3. On the Custom extensions tab, click **Upload extension**.
4. Select the JAR file for the extension.
5. Enter a name and description for the extension, then click **Add**.

The extension is now in your Extension library. Your users can apply the extension to specific sites to use it during scans.

Adding BChecks to Burp Suite Enterprise Edition

You can download BChecks created by PortSwigger, and by the Burp Suite community, from the BChecks GitHub repository.

If you have access to Burp Suite Professional, you can also create your own BChecks, enabling you to target your scans and make your testing workflow as efficient as possible. For more information, see Creating BChecks.

To add a BCheck:

1. Log in to Burp Suite Enterprise Edition as a user with permission to manage extensions.
2. From the settings menu ⚙, select **Extensions** to go to the Extension library.
3. On the BChecks tab, click **Upload BCheck**.
4. Select the BCheck you want to upload.
   Files that you want to import should be in plain text format with a `.bcheck` extension.

The extension is now in your Extension library. Your users can apply the extension to specific sites to use it during scans.

References

1. https://portswigger.net/burp/documentation/enterprise/user-guide/extensions/adding-extensions
2. https://www.geeksforgeeks.org/what-is-burp-suite/