A green chameleon logo

Description automatically generated

BURPSUITE -SETUP GUIDE FOR JUNIORS

TEAM PROJECT-A 374

​​

**TABLE OF CONTENTS**

1-SUMMARY……………………………………………………………………………………..

2-INTRODUCTION……………………………………………………………………………..

3- OVERVIEW………………………………………………………………………………..

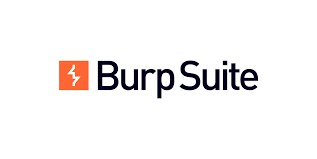
4-STEP HOW TO USE IT…………………………………………………………………….

5-RESULTS…………………………………………………………………………………………

6-CONCLUSIONS……………………………………………………………………………….

7-REFERENCES……………………………………………………………………………………

**EXECUTIVE SUMMARY**



Vulnerabilities related to reflected cross-site scripting occur when data is unsafely copied from a request and echoed into the application's instant response. By using the vulnerability, an attacker can create a request that, if made by another user of the application, will result in the execution of the attacker's JavaScript code in the user's browser during that user's session with the application. The code provided by the attacker is capable of carrying out a multitude of tasks, including taking advantage of the victim's login credentials or session token, acting arbitrarily on their behalf, and recording all of their keystrokes.

**INTRODUCTION**

A collection of tools called Burp, or Burp Suite, is used to test web applications for vulnerabilities. It is created by Portswigger, a business that Dafydd Stuttard, the company's founder, also goes by. BurpSuite is intended to be an all-in-one toolkit, and installing BApps, or add-ons, will expand its functionality.

Professional web app security researchers and bug bounty hunters use it the most. It is a better option than free alternatives like OWASP ZAP because of how simple it is to use. Burp Suite comes in three editions: community, which is free of charge; professional, which costs $399 annually; and enterprise, which costs $3999 annually. An overview of BurpSuite's toolkit is provided in this article.

**STEPS HOW TO USE IT**



* First, ensure that Burp is correctly configured with your browser.
* With intercept turned off in the Proxy "Intercept" tab, visit the web application you are testing in your browser.
* Visit the page of the website you wish to test for XSS vulnerabilities
* Return to Burp.
* In the Proxy "Intercept" tab, ensure "Intercept is on
* Enter some appropriate input in to the web application and submit the request
* The request will be captured by Burp. You can view the HTTP request in the Proxy "Intercept" tab.
* You can also locate the relevant request in various Burp tabs without having to use the intercept function, e.g. requests are logged and detailed in the "HTTP history" tab within the "Proxy" tab.
* Right click anywhere on the request to bring up the context menu.
* Click "Send to Repeater"
* We can assess whether the attack payload appears unmodified in the response. If so, the application is almost certainly vulnerable to XSS.
* You can find the response quickly using the search bar at the bottom of the response panel.
* The highlighted text is the result of our search
* Go to the "[Repeater](https://portswigger.net/burp/help/repeater.html)" tab.
* Here we can input various XSS payloads into the input field.
* We can test various inputs by editing the "Value" of the appropriate parameter in the "Raw" or "Params" tabs.
* A simple payload such as **<s>** can often be used to check for issues.
* In this example we have used a payload that attempts to perform a proof of concept pop up in our browser.
* Click "Go
* Right click on the response to bring up the context menu.
* Click "Show response in browser" to copy the URL.
* You can also use "Copy URL" or "Request in browser
* Copy the URL in to your browser's address bar.
* In this example we were able to produce a proof of concept for the vulnerability.

**RESULTS**

**A screenshot of a computer

Description automatically generated**

A screenshot of a computer

Description automatically generated

A screenshot of a computer program

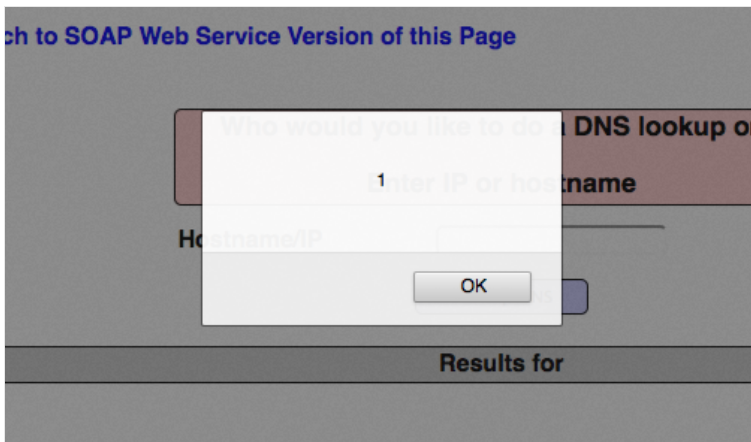
Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer screen

Description automatically generated



**CONCLUSION**

One popular tool for testing for vulnerabilities is Burp Suite Professionals. It is a thorough platform for assessing an online application's security.Brute-forcing credentials using Burp Suite is an additional tool for penetration testing.

From the first mapping and analysis of an application's attack surface to the identification and exploitation of security flaws, its many tools work well together to enable the entire testing process.To carry out our security duties, we use a range of Burp Suite tools, such as spider, intruder, repeater, etc.

With Burp, you have total control over combining state-of-the-art manual techniques with state-of-the-art automation to expedite, enhance, and enjoy your work..

**REFERENCES**

1-portswigger.net. (n.d.). *Using Burp to Manually Test for Reflected XSS*. [online] Available at: https://portswigger.net/support/using-burp-to-manually-test-for-reflected-xss.

‌2-Sahu, V. (2023). *What is Burp Suite?* [online] Scaler Topics. Available at: https://www.scaler.com/topics/cyber-security/burp-suite/.

‌