Penetration Testing and Vulnerability Scanning of Web Application Using Burp Suite

Dona Rose Mathew
Department of Computer Application
Amal Jyothi College Of Engineering
Kanjirapally, Kottayam
donarosemathew@mca.ajce.in

Jetty Benjamin
Department of Computer Application
Amal Jyothi College Of Engineering
Kanjirapally, Kottayam
jettybenjamin@amaljyothi.ac.in

***Abstract*—The aim of this paper is to identify a web application that can be used to test the effectiveness of Burp Suite web application vulnerability scanners. Burp suite is a prominent penetration testing and vulnerability detection tool created by the Portswigger firm. Burp Suite is designed to be an all-in-one toolkit, and its capabilities can be expanded by installing add-ons called BApps. Its simplicity makes it a better choice than free options like OWASP ZAP.**

Keywords—Vulnerability, Burp Suite, Vulnerability Scanner

I. INTRODUCTION

Burp Suite was founded in 2004 by Dafydd Stuttard, who saw a need for a reliable web application security testing tool. The tool has advanced by leaps and bounds over the last 16 years, adding a slew of new features. Capabilities that support the community of security testers Burp Suite is a programme that Web application protection testing has undeniably become a method of choice. It has also progressed to the point that it can now detect bugs in APIs and mobile apps. As per Sugar Rahalkar's opinion to test the security of web applications effectively, one must first understand the numerous web application vulnerabilities, as well as have a thorough understanding of the testing methods [1].

Editions

Burp Suite, like most other software, comes in a variety of formats. Different users can have different requirements, and one size does not necessarily suit everything. Burp Suite is available in three different editions to meet the needs of different users.

A. Community Edition

B. The Burp Suite Community Edition is the most basic version of the software, and it is available for free download and use. To get started with web application security testing, it comes with a limited collection of tools and features. If you're new to application security and want to learn the basics, the Burp Suite Community Edition is an excellent place to start [1][2].

C. Professional Edition

D. If you have a strong understanding of web application security and are regularly expected to test applications as part of your employment, the Burp Suite Professional Edition is strongly recommended. Individual practitioners who want to undertake both manual and automated security testing should use this version. [1][2].

E. Enterprise Edition

F. While both other editions were targeted at individual practitioners, the Burp Suite Enterprise Edition is useful for organisations looking to integrate security scanning in software pipelines [1][2].

Tools in burpsuite

Burp Suite includes a number of tools for performing various research activities. The tools work well together, and you can transfer interesting requests between them while you work to complete various tasks [3].

A. Target: This tool provides detailed information about your target applications and allows you to control the vulnerability testing process [3].

B. Proxy: This is a man-in-the-middle web proxy that intercepts traffic between the end browser and the target web application [3].

C. Scanner: This is a sophisticated web vulnerability scanner that can crawl content and audit it for a variety of vulnerabilities. And is available only in professional version [3].

D. Intruder: It is a versatile tool for automating and customising web application attacks. It can be used to automate a variety of tasks that occur during the testing of software [3].

E. Repeater: Simple yet powerful tool that manually modify and re-issue web request [3].

F. Sequencer: It is the perfect tool for verifying the cookies and more [3].

G. Decoder: This is a useful tool for decoding and encoding application data manually or intelligently [3].

H. Comparer: This is a useful tool for visually comparing any two pieces of data, such as pairs of identical HTTP messages [3].

I. Extender: This enables you to load Burp plugins, which you can use to expand Burp's features with your own or third-party code [3].

DOI: 10.5281/zenodo.5094090

Burp suite alternatives

Vulnerability Scanner Software is not limited to Burp Suite. Look at other solutions and competing choices. Features and functionality are important to remember when evaluating Burp Suite alternatives. The following are some of the burp suite alternatives [4]:

A. Nessus: It is a vulnerability management software [4].

B. Acunetix: A technology for scanning and auditing all web applications, including HTML5, JS, and single-page applications [4].

C. Netsparker: Netsparker is a web application security scanner that detects security vulnerabilities in websites, web apps, and web services in an automated and user-friendly manner [4].

D. OpenVAS: OpenVAS is a collection of resources and software that together provide a comprehensive and efficient vulnerability scanning and management solution [4].

E. Zenmap: The official Nmap Security Scanner GUI is Zenmap. It is a free, open source and multi-platform. It aims to make Nmap simple to use for beginners while still offering advanced features for seasoned Nmap users [4].

II. LITERATURE SURVEY

Prajakta Subhash Jagtap's “Vulnerability Scanning” examines the current state of open source vulnerability scanning software. A review of the literature on vulnerability, vulnerability scanning, vulnerability scanning software, security vulnerabilities, device security, and application security is carried out. This article examines vulnerability scanning techniques in depth. The author of this paper compared the efficiency of two widely used vulnerability scanning tools, Nessus and Burp Suite [5].

And Chanchala Joshi and Umesh Kumar Singh analyse the efficiency of burp suite and other tools web application vulnerability scanners in “Security testing and assessment of vulnerability scanners in quest of current information security landscape”. The defence measures to protect the application are also explained in this document. We may infer from this paper that both Acunetix and Netsparker scanners are capable of detecting cross-site scripting, but the Burp suite result is very weak. However, Acunetix does not properly detect security misconfiguration vulnerabilities; in this case, the results of Netsparker and Burp Suite scanners are superior [6].

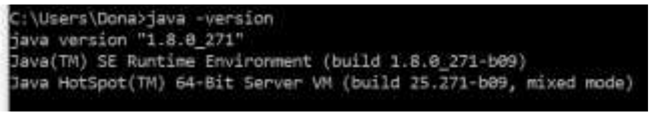
We saw how we could use Burp Suite's capabilities for performing security testing on APIs and mobile apps in sugar Rahalkar's “A complete guide to burp suite”. We also outlined the steps to take in order to get the most out of Burp Suite for web application security testing [1].

All these above authors speakes about Burp Suite. The first author ^{5} speakes about vulnarability scanning tools and also compare Burp Suite with Nessus. While the second auther ^{6} compare 3 tools and analyse the advantages and disadvantages. From that paper ^{6} we can conclude that eventhough detecting cross-site scripting capability is low for Burp Suite security misconfiguraton vulnarability detection is high. The third author ^{1} provides a thorough explanation of burp suite.

III. METHODOLOGY

a. Burp suite installation

We must first ensure that Java is installed on the device before installing or running the Burp Suite. It's a must-have for Burp Suite to work. To check whether Java is installed on a Windows machine, simply open a command prompt and type “java –version,” as shown below in Fig: 3.1.1:

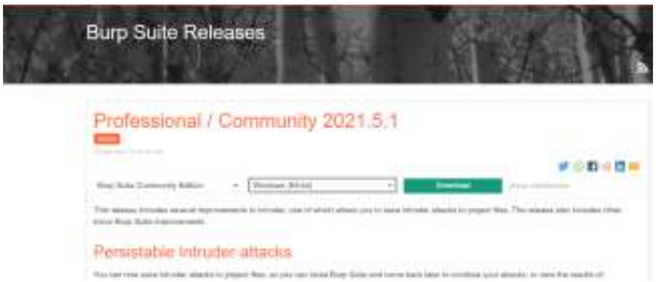


```
C:\Users\Dona>java -version
java version "1.8.0_271"
Java(TM) SE Runtime Environment (build 1.8.0_271-b09)
Java HotSpot(TM) 64-Bit Server VM (build 25.271-b09, mixed mode)
```

Fig: 3.1.1. Java Install

Once java is installed the next step is to install Bur Suite. We can download the edition from:

https://portswigger.net/burp/releases/professional-community-2021-5-1?requestededition=community and is as shown below in fig:3.1.2:



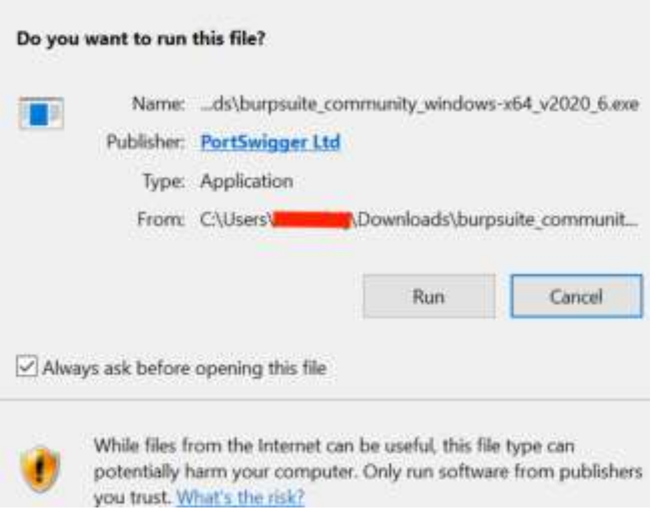
Burp Suite Releases

Professional / Community 2021.5.1

Persistable Intruder attacks

Fig:3.1.2. Burp suite installation

After downloading just open the downloaded file and the pop-up window will be as follows in fig:3.1.3 [7],



Do you want to run this file?

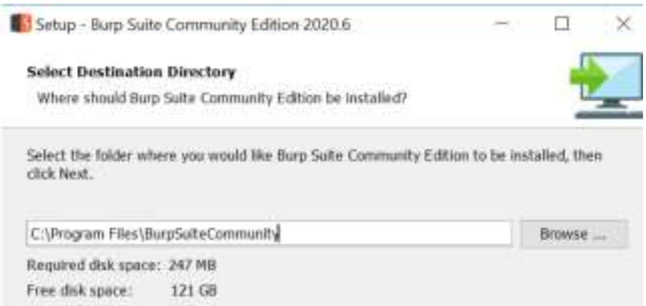
Name: ...ds\burpsuite_community_windows-x64_v2020_6.exe
Publisher: PortSwigger Ltd
Type: Application
From: C:\Users\[redacted]\Downloads\burpsuite_communit...

☑ Always ask before opening this file

While files from the Internet can be useful, this file type can potentially harm your computer. Only run software from publishers you trust. What's the risk?

Fig:3.1.3. pop up window

Choose where you want the Burp suite to be installed on your computer as shown in fig:3.1.4.



Setup - Burp Suite Community Edition 2020.6

Select Destination Directory

Where should Burp Suite Community Edition be installed?

Select the folder where you would like Burp Suite Community Edition to be installed, then click Next.

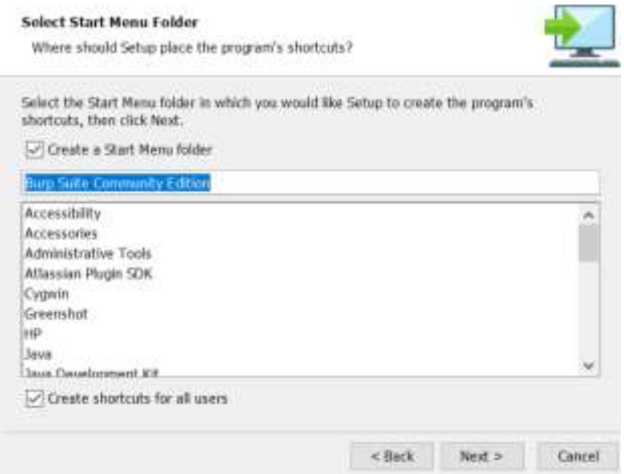
C:\Program Files\BurpSuiteCommunity

Required disk space: 247 MB

Free disk space: 121 GB

Fig: 3.1.4. Select Destination

Select the start menu option for the Burp Suite as in fig.3.1.5



Select Start Menu Folder

Where should Setup place the program's shortcuts?

Select the Start Menu folder in which you would like Setup to create the program's shortcuts, then click Next.

☑ Create a Start Menu folder

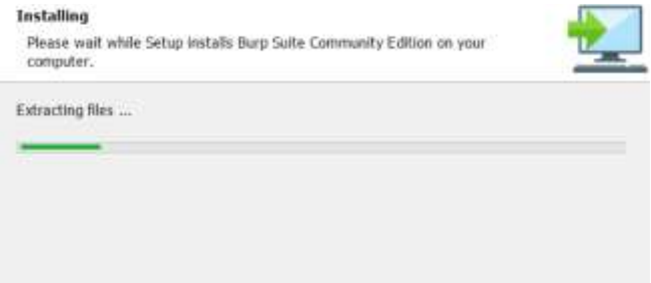
Burp Suite Community Edition

Accessibility
Accessories
Administrative Tools
Atlassian Plugin SDK
Cygwin
Greenshot
HP
Java
Java Development Kit

☑ Create shortcuts for all users

Fig:3.1.5. Burp suite

Now installation will begin as in fig:3.1.6



Installing

Please wait while Setup installs Burp Suite Community Edition on your computer.

Extracting files ...

Fig:3.1.6. Installation

You can start the Burp suite after it has been successfully mounted, and you will see the following screen as in fig:3.1.7:

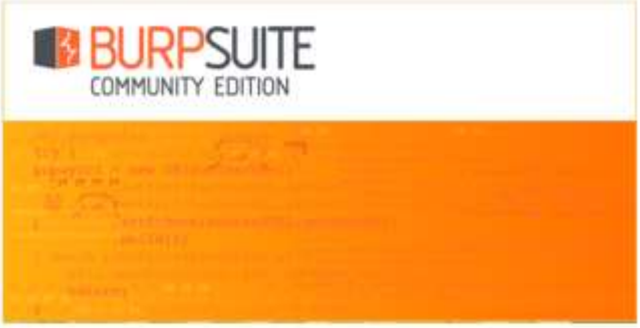
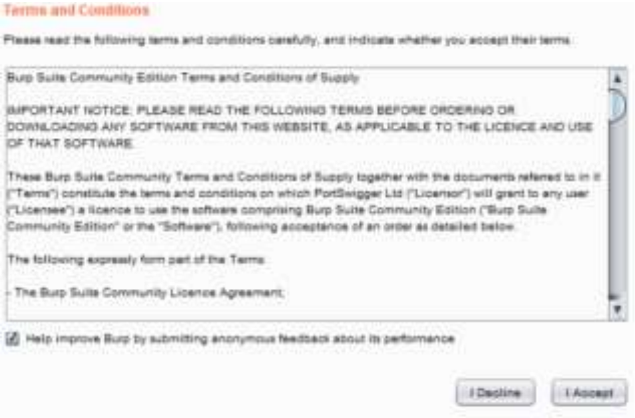


Fig 3.1.7. Burp Suite start Screen

Accept the certificate (fig:3.1.8) in order to continue with the start-up.



Terms and Conditions

Please read the following terms and conditions carefully, and indicate whether you accept their terms.

Burp Suite Community Edition Terms and Conditions of Supply

IMPORTANT NOTICE: PLEASE READ THE FOLLOWING TERMS BEFORE ORDERING OR DOWNLOADING ANY SOFTWARE FROM THIS WEBSITE, AS APPLICABLE TO THE LICENCE AND USE OF THAT SOFTWARE.

These Burp Suite Community Terms and Conditions of Supply together with the documents referred to in it ("Terms") constitute the terms and conditions on which PortSwigger Ltd ("Licensor") will grant to any user ("Licensee") a licence to use the software comprising Burp Suite Community Edition ("Burp Suite Community Edition" or the "Software"), following acceptance of an order as detailed below.

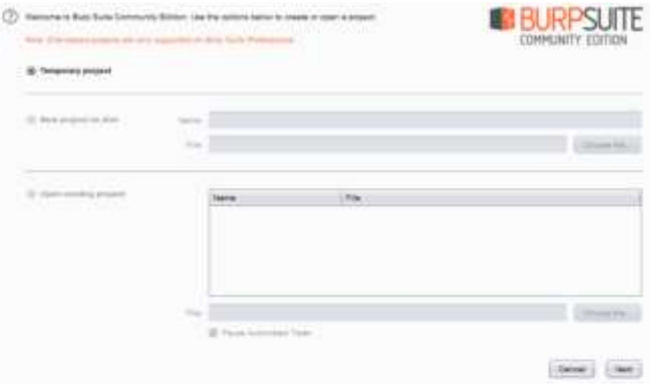
The following expressly form part of the Terms:

- The Burp Suite Community Licence Agreement;

☑ Help improve Burp by submitting anonymous feedback about its performance

Fig:3.1.8. Terms & Conditions

If you're using the community version of Burp Suite, you'll need to create a Temporary project.



Welcome to Burp Suite Community Edition. Use the options below to create or open a project.

Note: Disk-based projects are only supported on Burp Suite Professional.

● Temporary project

○ New project on disk

Name

File

○ Open existing project

Name	File

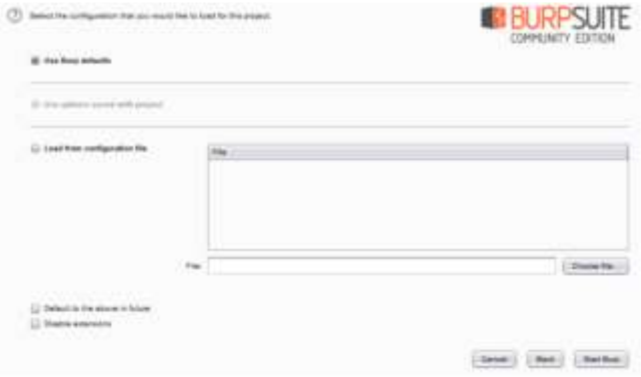
File

☐ Pause Automated Tasks

Fig:3.1.9. create temporary project

To start Burp suite, click the Start Burp button in the bottom-right corner.

DOI: 10.5281/zenodo.5094090
***ISBN:978-93-5426-386-6@2021** MCA, Amal Jyothi College of Engineering Kanjirappally, Kottayam*



Select the configuration that you would like to load for this project.

● Use Burp defaults

○ Use options saved with project

○ Load from configuration file

File

File:

□ Default to the above in future

□ Disable extensions

Fig:3.1.10. Burp Suite start

With that, the Burp suite has been successfully built and started. You can use the Chromium browser that comes pre-configured with the new version of the Burp Suite.

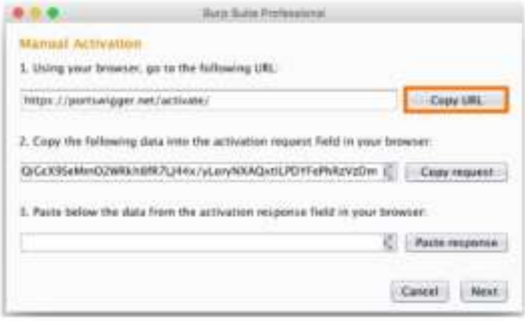
If it's a professional edition you need to activate your licence key:

When launching burp suite for first time, you need to provide your burp suite license key. Your license key can be downloaded from your account page.
Standard activation process is as follows [8]:

- When prompted to enter your licence key, either paste it or choose it from a file using the select licence key file button. After that, press the next button.
- Enter your proxy details in the corresponding field if you are only able to access the internet using a web proxy server.
- To activate your licence, click the next button. The wizard for getting started will appear.

In some case you need to manually activate your license (computer with no internet connection) [8]:

- In such circumstances, rather than clicking next, select manual activation.
- Click on copy URL



Manual Activation

1. Using your browser, go to the following URL:

https://portswigger.net/activate/

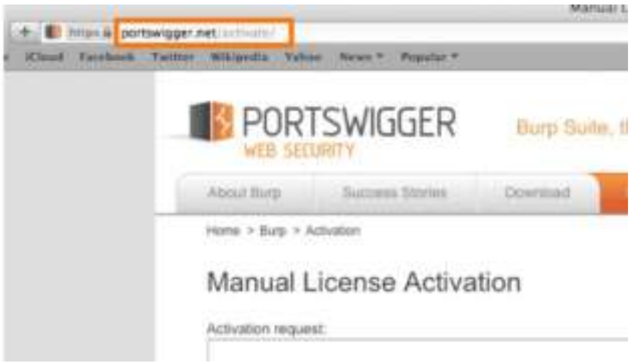
2. Copy the following data into the activation request field in your browser:

QiGcX95eMmO2WRkh8fR7LJ44x/yLoryNXAQxtILPDYFePhRzVzDm

3. Paste below the data from the activation response field in your browser:

Fig:3.1.11. Manual Activation

- Paste the URL into your browser to access manual licence activation page as in fig:3.1.12

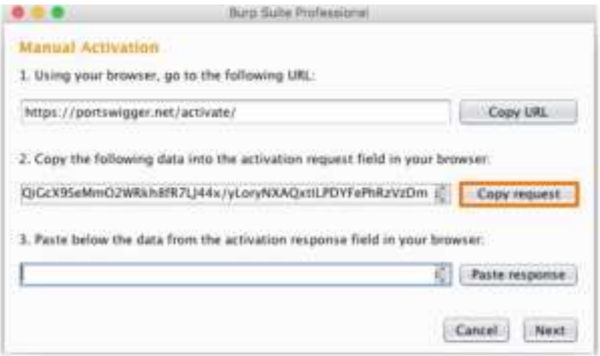


Manual License Activation

Activation request:

Fig:3.1.12. Browser

- Go back to activation wizard and click on copy request button



Manual Activation

1. Using your browser, go to the following URL:

https://portswigger.net/activate/

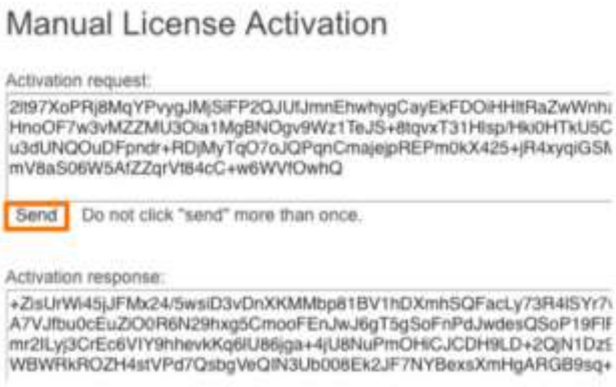
2. Copy the following data into the activation request field in your browser:

QiGcX95eMmO2WRkh8fR7LJ44x/yLoryNXAQxtILPDYFePhRzVzDm

3. Paste below the data from the activation response field in your browser:

Fig:3.1.13. Activation Wizard

- Return to licence activation page in your browser and paste request into activation request field and click on send. Select and copy the text appeared in activation respond field.



Manual License Activation

Activation request:

2I197XoPRj8MqYPvygJMjSiFP2QJUfJmnEhwhygCayEkFDOiHHItRaZwWnh
HnoOF7w3vMZZMU3Oia1MgBNOgv9Wz1TeJS+8tqvxT31Hisp/Hk0HTkU5C
u3dUNQOuDFpndr+RDjMyTqO7oJQPqnCmajejpREPm0kX425+jR4xyqiGS
mV8aS06W5AfZZqrVt84cC+w6WVfOwhQ

Do not click "send" more than once.

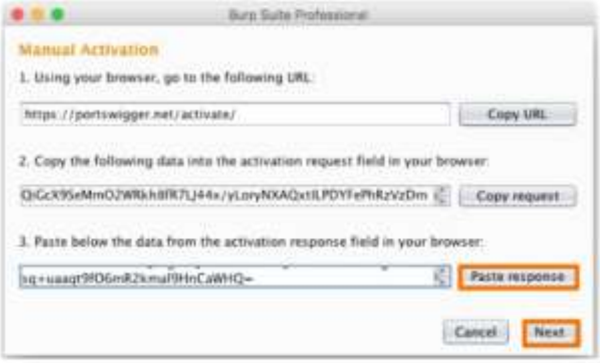
Activation response:

+ZisUrWi45jJFMx24/5wsiD3vDnXKMMbp81BV1hDXmhSQFacLy73R4ISYr7
A7VJfbu0cEuZiO0R6N29hxg5CmooFEnJwJ6gT5gSoFnPdJwdesQSoP19FI
mr2ILyj3CrEc6VIY9hhevkKq6lU86jga+4jU8NuPmOHiCJCDH9LD+2QjN1Dz
WBWRkROZH4stVPd7QsbgVeQIN3Ub008Ek2JF7NYBexsXmHgARGB9sq+

Fig:3.1.14. Manual License Activation

- Go back to licence activation wizard. Click on paste response button to paste response.

DOI: 10.5281/zenodo.5094090
ISBN:978-93-5426-386-6@2021 MCA, Amal Jyothi College of Engineering Kanjirappally, Kottayam



Burp Suite Professional

Manual Activation

1. Using your browser, go to the following URL:

https://portswigger.net/activate/

2. Copy the following data into the activation request field in your browser:

QiGcX9SeMmO2WRkh8fR7LJ44x/yLoryNXAQxtILPDYFePhRzVzDm

3. Paste below the data from the activation response field in your browser:

sq+uaaqt9fO6mR2kmuI9HnCaWHQ=

- click on next. If the activation was successful, the next screen will appear, prompting you to click Finish to complete the process and load the Burp start-up wizard.

Burp Suite Professional

Success

Your license is successfully installed and activated.

Fig:3.1.15. success Window

If you don't want to use Burp's built-in browser, you can use any other browser. However, in this situation, you'll need to take some extra measures to configure your browser (you need to change your proxy setting), as well as install Burp's CA certificate.

b. Burp Suite tabs and uses

i. Proxy

acts as a web proxy server between your browser and the applications you want to use [9].

1. Intercept

This is where your browser's http requests are shown. Each message can be viewed and edited from this page. After you've made your changes, simply press the forward button. To finish loading the tab, press this forward button if any intercepted messages are pending.

We can toggle intercept on/off to search normally without being tracked.

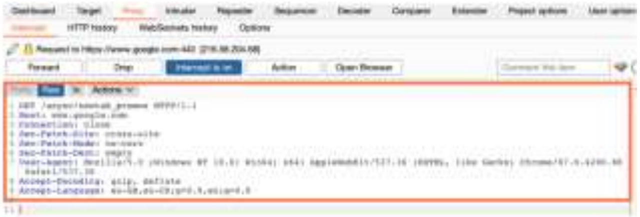


Fig:3.2.1.1.1. Intercept tab

2. HTTP history

All requests and responses are saved in this tab. You can view the request you've made in this tab even if intercept is turned off.

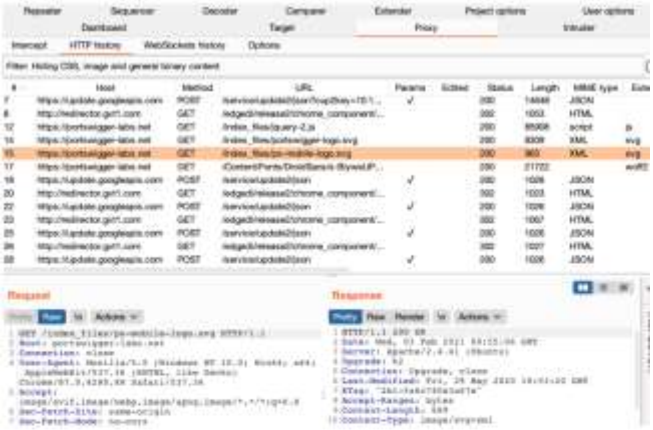


Fig:3.2.1.2.1. HTTP history tab

ii. Target

It contains detailed information about your targeted application [9].

1. Site Map

The site map of the target application generated by burp suite can be viewed here. All of the URLs you've visited in your browser are shown in the site map. Requested items are shown in black, while others are shown in grey.

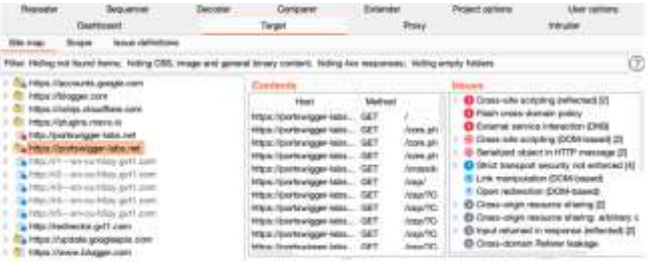
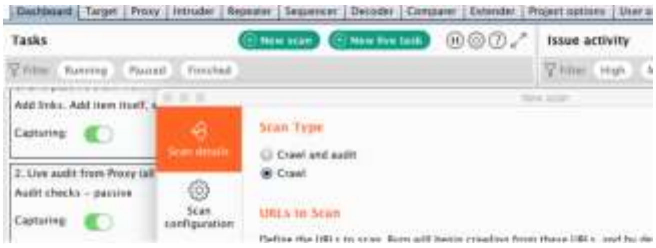


Fig:3.2.2.1.1. site map tab

In order to add your URL to the scope just right click on the URL in the site map and select "add to scope".

iii. Scanner

Detects content and security flaws on websites automatically. The scanner can crawl the application depending on its configuration [9].



Add links. Add item itself,

Capturing:

2. Live audit from Proxy (all

Audit checks - passive

Capturing:

Scan Type

○ Crawl and audit

● Crawl

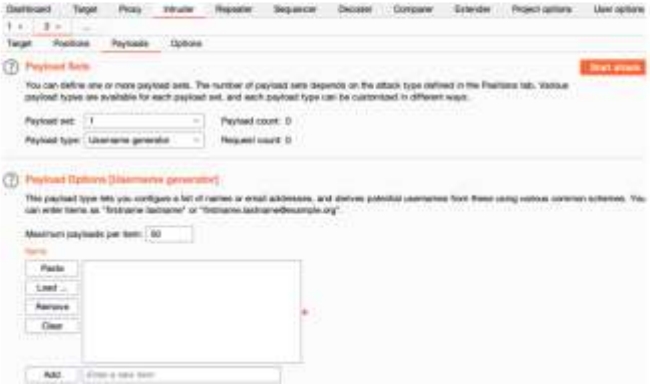
URLs to Scan

DOI: 10.5281/zenodo.5094090

Fig:3.2.3. Scanner

iv. Intruder

It's a platform for automating custom web application attacks. It's flexible and strong. It can be used for a wide variety of tasks.



You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1
Payload count: 0
Payload type: Username generator
Request count: 0

This payload type lets you configure a list of names or email addresses, and derives potential usernames from these using various common schemes. You can enter items as "firstname lastname" or "firstname.lastname@example.org".

Maximum payloads per item: 50

Fig:3.2.4.1. Payloads tab

v. Repeater

Burp repeater is a method for manually altering HTTP requests and checking the page's responses. Right click on a request and select “send to repeater” (fig:3.2.5.1).

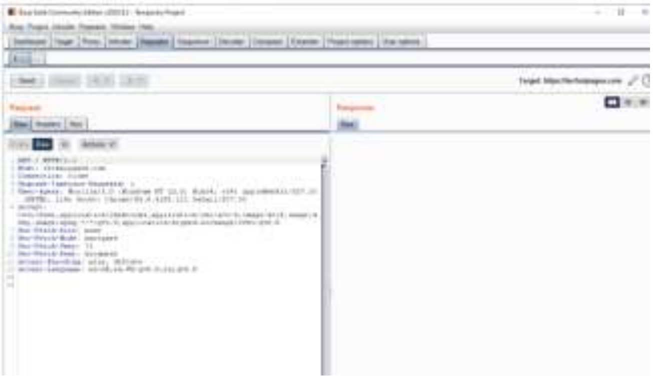
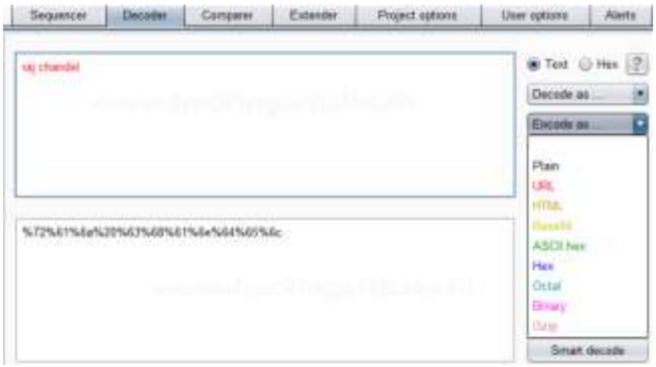


Fig:3.2.5.1. Repeater tab

vi. Decoder

It's a straightforward method for converting encoded data into its canonical form, as well as raw data into different encoded and hashed formats (fig 3.2.6.1).



raj chandel

%72%61%6a%20%63%68%61%6e%64%65%6c

Fig:3.2.6.1. Decoder tab

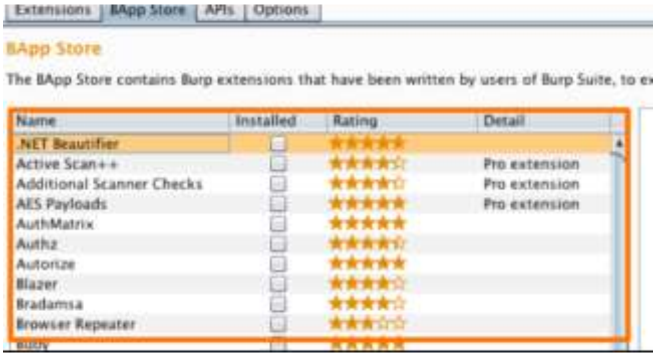
vii. Comparer

This is used to perform a visual comparison of bit of application data to find interesting difference.

Fig:3.2.7.1. Comparer

viii. Extender

Burp Extender allows you to expand Burp’s features with your own or third-party code by using Burp extensions.



The BApp Store contains Burp extensions that have been written by users of Burp Suite, to ex

Name	Installed	Rating	Detail
.NET Beautifier	□	★★★★★	
Active Scan++	□	★★★★☆	Pro extension
Additional Scanner Checks	□	★★★★☆	Pro extension
AES Payloads	□	★★★★★	Pro extension
AuthMatrix	□	★★★★★	
Authz	□	★★★★☆	
Autorize	□	★★★★★	
Blazer	□	★★★★☆	
Bradamsa	□	★★★★☆	
Browser Repeater	□	★★★☆☆	
Buby	□	★★★★★	

Fig:3.2.8.1. Extender

IV. RESULT

Burp Suite aspires to be an all-in-one toolkit, and its features can be expanded by adding BApps, or add-ons . Burp Suite is available as a community edition which is free, professional edition that costs $399/year and an enterprise edition that costs $3999/Year [10].

To use Burp Suite for research, simply go to the proxy tab and on/off intercept. Burp Suite can behave as a man in the centre after that. All requests will be routed via this Burp Suite, and the resulting page will only be loaded if you click forward.

While intercept is enabled, you can see all of your browsing history in HTTP history.

By just right clicking on each link you can send them to repeater tab, intruder tab, comparer tab etc.

V. CONCLUSION

From this paper we can conclude that Burp Suite is one of the most popular penetration testing and vulnerability detection tool that is used to assess the security of web applications. By comparing with some alternative tools Burp Suite have both advantages and disadvantages. In terms of discovered bugs, ease of use, licencing versatility, and breadth of features, Burp Suite provides the most value to independent security consultants.

VI. FUTURE WORKS

This paper is about the Burp Suite. There could be some changes that can be made to make it more user-friendly. The following ideas could be some of them:

- ➢ The capability of detecting cross-site scripting would need to be improved in the future.
- ➢ Providing an extension to anyone who wishes to use the prototype in a scanner is almost impossible[11]. It will be better if this problem is solved.

VII. REFERENCE

[1] Sugar Rahalkar, "A complete Guid to Burp Suite Pune, Maharashtra, India,2021

[2] https://portswigger.net/burp#:~:text=Burp%20Suite%20Enterprise%20Edition%3A%20automated,scanning%20across%20their%20entire%20portfolios

[3] https://portswigger.net/burp/documentation/desktop/tools

[4] https://www.g2.com/products/burpsuite/competitors/alternatives

[5] Prajakta Subhash Jagtap, "Vulnarability Scanning", M.Tech Student, K J Somaiya College of Engineering, 2012.

[6] Chanchala Joshi, Umesh Kumar Sigh, "security testing and assessment of vulnerability scanner in quest of current information security landscape", Institute of Computer Science Vikram University, Ujjain, M.P. India, 2016.

[7] https://www.studytonight.com/post/how-to-install-burp-suite-on-windows-10

[8] https://portswigger.net/burp/documentation/desktop/getting-started

[9] portswigger.net

[10] https://www.geeksforgeeks.org/what-is-burp-suite/

[11] https://raw.finnwea.com/similar-request-excluder/TijmeGommers-GraphWave-Thesis-Public-Digital-1.103.6-bd716cc3.pdf