Search and destroy with Burp Suite

(File Upload Exploit Vulnerability)

Let's upload a PHP shell to gain a reverse shell.

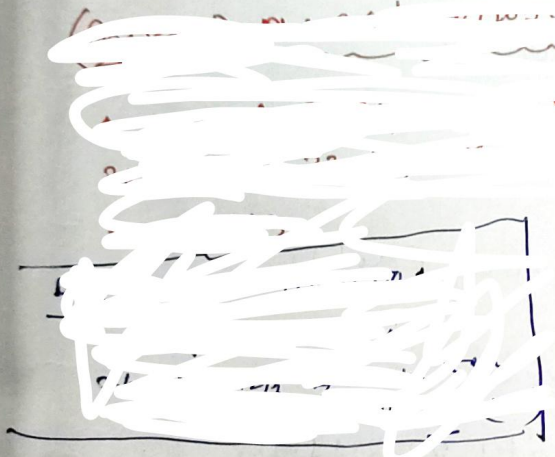
3.1 Create a PHP Reverse shell

Download

127.0.0.1 (IP address of localhost)

online-clipboard.online/send-file-online/

What is Brute Force attack ? with example (username)



This is lack of upbringing

manjog@1983

manjog1983

Burp Suite (BS) - is a popular penetration testing tool used for security testing of web applications.

→ It provides various tools to intercept, analyze, modify, and automate HTTP/s requests.

→ It is widely used by security researchers, ethical hackers and Cybersecurity professionals for finding & exploiting vulnerabilities in web applications.

* Finding vulnerabilities (search) and exploiting them (destroy)

XSS : inject <script> alert(1) </script>
in input fields and observe the responses.

IDOR (Insecure Direct object References):
Modify user ID parameters and check for unauthorized access.

Burpsuite Download and install / Activation

⇒ open Any web Browser
↳ Type
Burp suite download

PortSwisser

Download Burpsuite Community Edition
↳ Go straight to downloads
↳ Professional / Community 2023.11.1.3

Burp Suite Community Edition | Linux (x64)

Download
294 mb

Open The Terminal

Use cd Command
ls
↳ burpsuite_community_linux_v2023_11_1_3.sh

To check the Permission of the file
chmod +x (same file)
Now install it sudo ./ (File Name Again)

Ask for the password (Type the password)

Starting installer

You will set

Welcome to the Burp Suite Community Edition setup wizard

Click Next

Select Destination Directory

Get the default location

click next

↳ next

↳ Next

↳ Finish

127.0.0.1:3000/#/

Close the terminal

↳ Go to start (search (Burp suite) (orange color)

↳ Accept

↳ Temporary Project ↳ Next

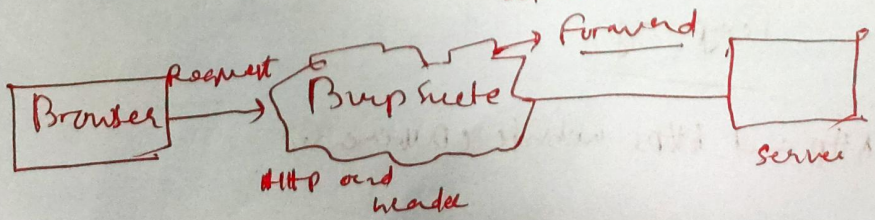
↳ ① use Burp defaults

↳ start Burp

without wasting so much of time.

I am excited, so let's get started.

Burp Suite: proxy tool (sit in the middle between Browser & Server)



Limit

Password [25 characters]

↳ 250000

Interception [On] To catch Packets

If it's OFF

you can't catch or see any data

Posts wisscriner

Proxy setting

127.0.0.1:8080

↳ Localhost

Domain Name ⇒ DNS → connects to IP Address

http: 8080 ↳ port (Listener)

Browser ↳ setting ↳ proxy

↳ • Manual proxy configuration

Http Proxy [127.0.0.1] [8080 port]

↓ Localhost (DNS) (OK)

testphp.vulnweb.com/

Foxyproxy

http and https website (Difference)

Proxy

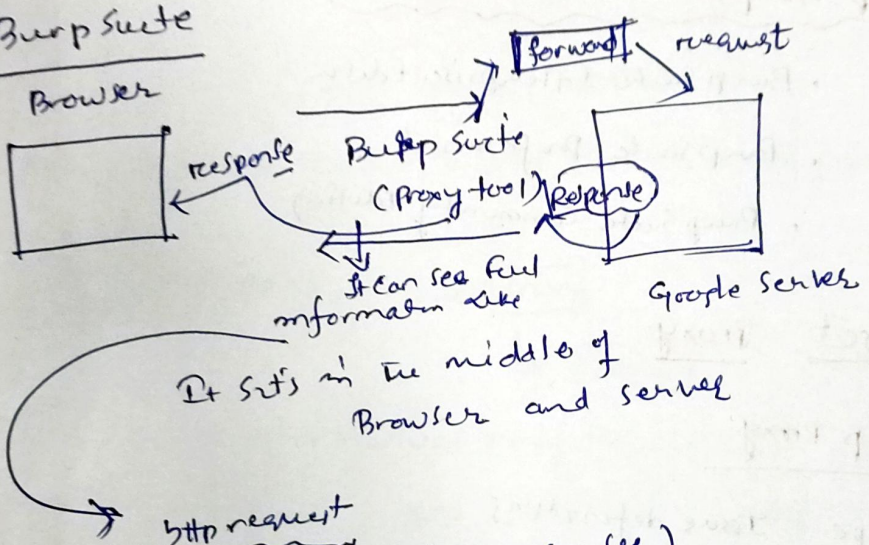
Prerequisites

Full course in a single go

1. System
2. How website works
3. HTTP (about) How it works
4. Request, Response, Headers.

Burp Suite

Browser



It sits in the middle of Browser and server

http request

what headers (All u can see)

Password Limit (25 characters) from browser

↳ from 250000 (change (or) alter request)

↳ I can send to the web server.

↳ Also Burp Suite can check how server responses to my request (that's what my Job)

If not backend validation.

not High Class CPU

Reset

(Long Password Vulnerability)

Interception

↳ ON (to capture the request)

If u will make it OFF ↳ whether u will forward it or not

⇒ request/response will go through (Burp Suite)

But u can't see

⇒ All will come in Burp Suite history

Set up Burp Suite in ur Browser

- Burp Suite Enterprise Edition
- Burp Suite Professional
- Burp Suite Community Edition

Target Proxy

Setup Proxy

↳ Scope Issue definitions

Proxy

Forward | Drop | Intercept is off | Action | open browser

HTTP history → (what has been already viewed)

Proxy Setup

Proxy setting

↳ ⓘ Proxy listners

Running ☑

↳ Interface

↓ 127.0.0.1:8080

(ip add^n of localhost)

google.com
facebook.com } Domain Name (DN)
↳ every (DN) has a ip address
↳ 41.11.181.1

* DNS (converts domain name into ip address)

ping google.com | IPV4 and IPV6

127.0.0.1 : 8080
↳ Port Number (Listen)

(To differentiate various services, port no's are given)

Browser ↳ settings ↳ seach proxy
↳ Settings
• Manual proxy configuration
127.0.0.1 Port 8080
OK

Next (Go to Burp Suite)
To capture my request / packet
↳ Intercept is on

Go Browser
testphp.vulnweb.com
FoxyProxy

GET / HTTP/1.1
↳ version
Host
User-Agent
then Forward

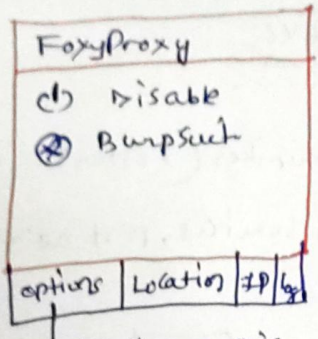
Alternate way to setup proxy / disable

(only single click)

Browser name

~~Proxy~~ Foxyproxy Firefox

Foxyproxy standard - Get this Extension for



click on this

proxies

Add

Title: Burpsuite

Hostname: 127.0.0.1

Type: HTTP Port: 8080

Save

Pin to toolbox

To work with HTTPS websites (Burp suite)

Proxy Settings

Import / export CA Certificate

Export :

○ Certificate in DER format

Next

Select file → Cert → file
→ Save → Next → Close

Next

Go to Browser → Setting → search Certificate → view certificate → import → Cert → ok

To Trust → 2 buttons Enable
- ✓ Actalis Authentication Root CA
- ✓ AffirmTrust Premium ECC

Now https → Intercepting off (as it is)

(Simple demonstration)

Go To testphp.vulnweb.com

Search Art
tarish → go → searched for: tarish

Make intercept ON

and again go to

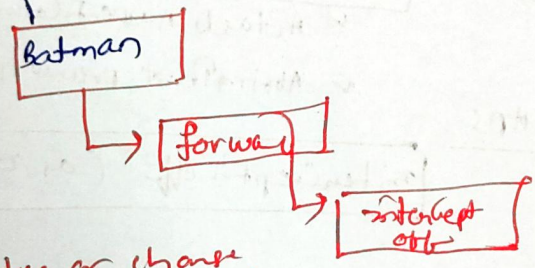
Search art
tarish → go

How u can see what requests are coming ?

1 POST /search.php?test=query HTTP/1.1
2 Host: testphp.vulnweb.com
3 User-Agent: Mozilla/5.0
4 Accept:
5. Accept-Language:
6. Accept-Encoding
7. Content-Type
8. Content-Length
9. Origin
10. Connection
11. Referer
12 Upgrade-Insecure-Requests: 1
13.
14 searchfor=tautology&goButton=go

then · Forward

Now u can change to Batman



Now you can alter or change the request from the browser

Note: In Burp Suite, the Intercept feature is used to capture and modify HTTP request before they are sent to the server. However, in each transition, Intercept may be turned ON for the following reasons.

Repeater

* Burp Suite Repeater is a tool that allows you to manually modify and resend HTTP requests to test how the server responds.

⇒ It is useful for testing vulnerabilities, debugging requests, and analyzing server behavior.

http request

Cross-Site Scripting (XSS) Vulnerabilities

(XSS) is a type of web security vulnerability that allows an attacker to inject malicious scripts into web pages viewed by other users.

⇒ This can lead to data theft, session hijacking, defacement, and more.

Types of XSS

1. Stored XSS (Persistent XSS)

- The malicious script is permanently stored on the target server (e.g.: in a database, msg board, or comment section)
- Impact: Everytime a user visits the affected page, the script executes in the browser.
- Example

```
<script> alert ('Hacked'); </script>
```

2. Reflected XSS (Non-Persistent XSS):

- The malicious script is not stored on the server but is reflected from a web request (e.g., a search bar or URL parameter)
- The attacker tricks the user into clicking a malicious link containing the script.

Example:

https://example.com/search?q=<script>alert('Hacked!');</script>

* The application does not properly validate input, the script will execute in the victim's browser.

Password Attack Using xHydra in Kali Linux

- xHydra is the GUI version of Hydra, a powerful password cracking tool.
- It is used for brute-force password attacks on various protocols like SSH, FTP, HTTP and more.
- Helps in penetration testing to identify weak passwords.

Slide 2:

- This guide is for educational purposes only.
- Unauthorized access to systems is illegal.
- Always perform penetration testing with permission.

Slide 3:

Steps:

1. open Kali Linux
2. open a terminal and type:
   xhydra
3. press enter to launch the GUI.

Slide 4: Selecting the Target

Steps:

1. Go to the "Target" tab
2. Enter the IP address of the target machine
3. choose the protocol to attack (e.g.; SSH, FTP, HTTP, etc)

Slide 5: Configuring Username and Password Options

Steps:

1. Go to the "password" tab
2. Choose how to test Credentials
   - Single username → Enter manually.
   - Username list → Load a list of usernames (userlist.txt)
   - Single password → Enter manually
   - Password list → Load a dictionary file (crack you.txt)

Slide 6: Setting Attack Parameters

Steps:

1. Go to the 'Tunning' tab
2. Set the number of threads (higher = faster attack, but can overload the target).
3. Configure timing options to adjust the delay between attempts

Slide 7: Launching the Attack

steps:

1. Click the "start" button.
2. xHydra begins brute-forcing the credentials
3. If successful, valid login details will be displayed

Slide 8: Analyzing results

Slide 9: Protecting Against xHydra Attacks

- ☑ Use strong passwords (complex, long and random)
- ☑ Enable Account Lockout (After multiple failed attempts)
- ☑ Use Multi-factor Authentication (MFA)
- ☑ Restrict Login Attempts with Security policies and Firewalls.