Project 4 — CTF Report

Capture The Flag (CTF) — Web Application Assessment

Name: Oppong Isaac

Target IP: 192.168.248.96

Executive Summary

This report documents a web-application Capture-the-Flag (CTF) exercise conducted against a lab VM (IP 192.168.248.96). Reconnaissance and manual analysis discovered multiple web-accessible files and admin paths that contained six planted flags. Techniques used include network/port scanning, content enumeration, and manual inspection of web resources.

Objective- Deploy the provided VM in VirtualBox (bridged networking).- Enumerate services and web content.- Find and capture six (6) flags planted in the web application.

Environment & Tools- Target VM: Deployed locally in VirtualBox, IP: 192.168.248.96.- Attacker OS: Kali Linux (recommended).- Tools: nmap, gobuster/dirb, curl/wget, browser, Burp Suite (optional).

Deployment Notes

1. Import the provided .ova into Oracle VirtualBox (File → Import Appliance).

2. Set MAC Address Policy to "Include all network adapter MAC addresses".

3. In VM settings → Network → set "Attached to: Bridged Adapter".

4. Start VM and note the IP displayed (192.168.248.96 in this exercise).

Reconnaissance & Enumeration

Host discovery and port scan example:

```
sudo nmap -sV -Pn- 192.168.248.96 -oN nmap_initial.txt
```

Web content enumeration example:

```
gobuster dir -u http://192.168.248.96 -w /usr/share/wordlists/dirb/common.txt -x

php,html,txt,asp,aspx
```

Findings (Flags & How Found)

Flag 1: flag1.txt — Retrieved directly from web root or VM.

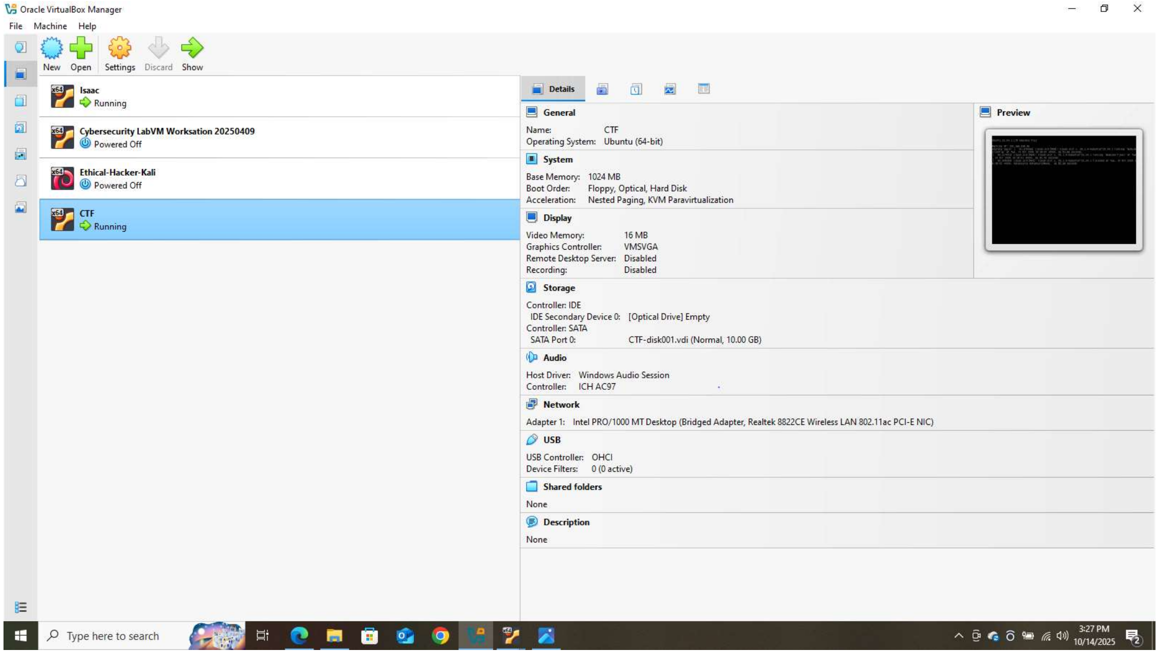
Flag 2: /robotx.txt — Found via directory enumeration (gobuster/dirb).

Flag 3: /pages/BlogPostCcomponent.html — Inspected page source to reveal flag.

Flag 4: /4dm1n — Admin path containing flag.

Flag 5: /c0nf1g — Configuration file containing flag.

Flag 6: /4dm1n — Additional flag in same admin area.



Isaac
Running

Cybersecurity LabVM Worksation 20250409
Powered Off

Ethical-Hacker-Kali
Powered Off

CTF
Running

General

Name: CTF
Operating System: Ubuntu (64-bit)

System

Base Memory: 1024 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, KVM Paravirtualization

Display

Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Controller: SATA
SATA Port 0: CTF-disk001.vdi (Normal, 10.00 GB)

Audio

Host Driver: Windows Audio Session
Controller: ICH AC97

Network

Adapter 1: Intel PRO/1000 MT Desktop (Bridged Adapter, Realtek 8822CE Wireless LAN 802.11ac PCI-E NIC)

USB

USB Controller: OHCI
Device Filters: 0 (0 active)

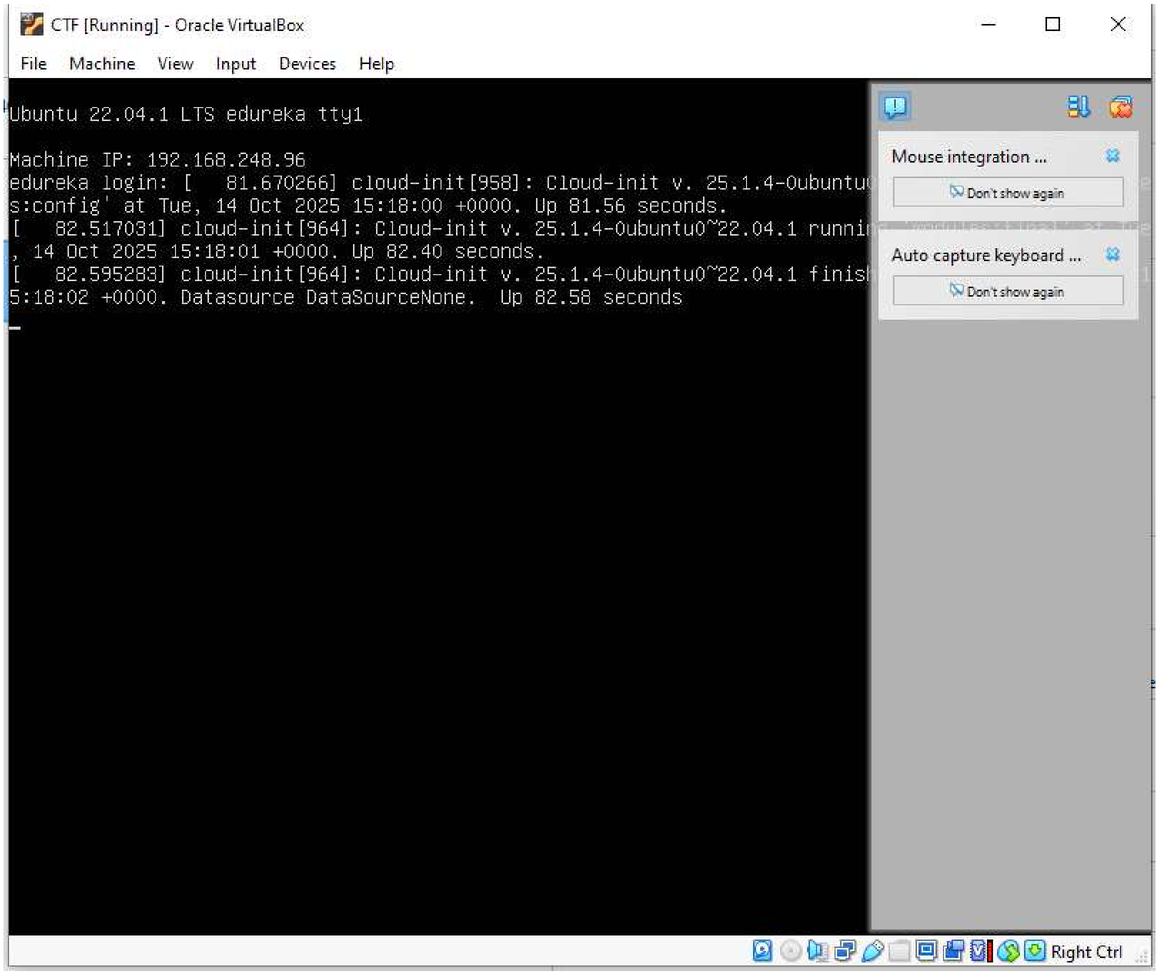
Shared folders

None

Description

None

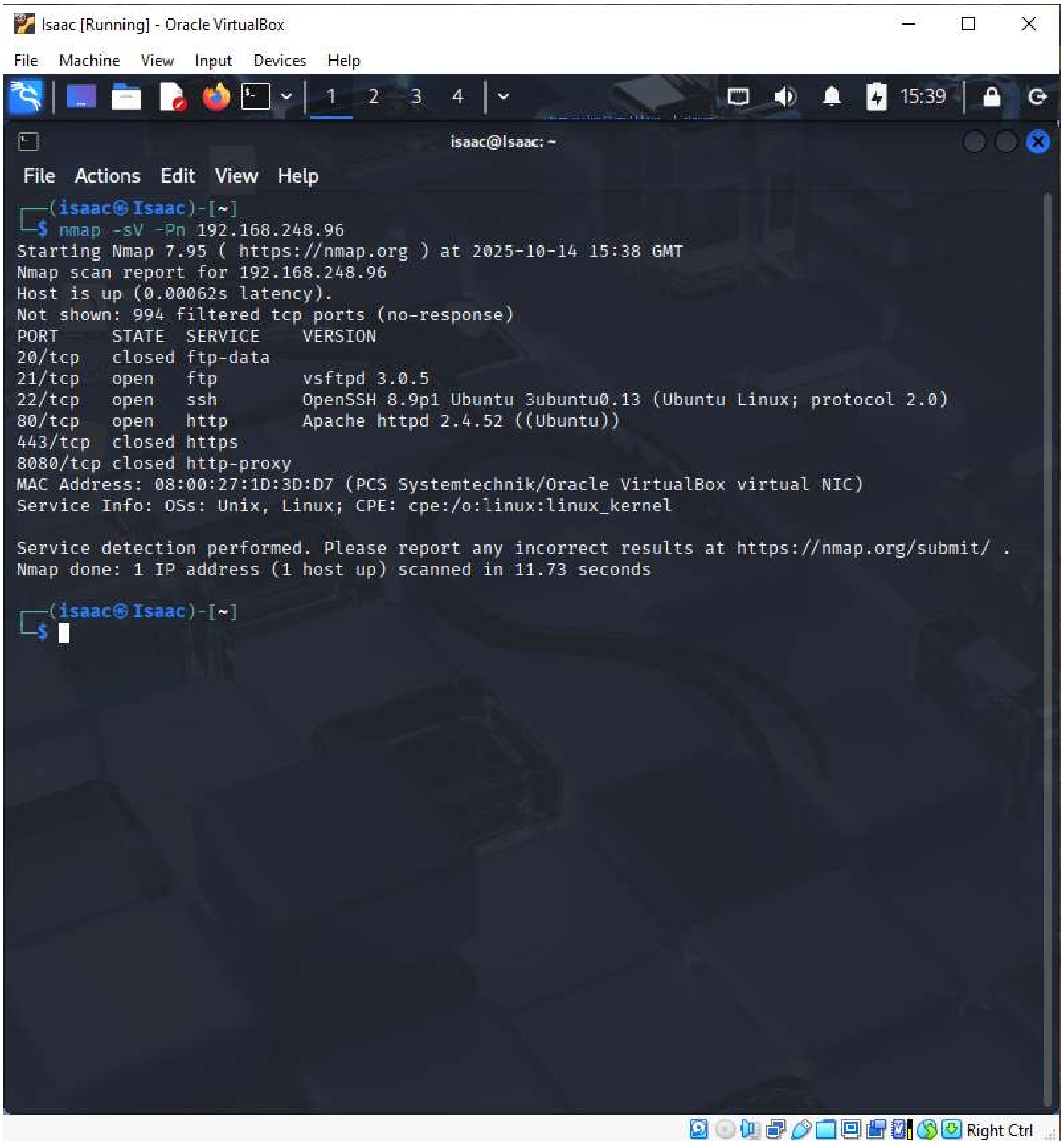
Starting up the CTF file



```
Ubuntu 22.04.1 LTS edureka tty1

Machine IP: 192.168.248.96
edureka login: [   81.670266] cloud-init[958]: Cloud-init v. 25.1.4-0ubuntu
s:config' at Tue, 14 Oct 2025 15:18:00 +0000. Up 81.56 seconds.
[   82.517031] cloud-init[964]: Cloud-init v. 25.1.4-0ubuntu0~22.04.1 runni
, 14 Oct 2025 15:18:01 +0000. Up 82.40 seconds.
[   82.595283] cloud-init[964]: Cloud-init v. 25.1.4-0ubuntu0~22.04.1 finis
5:18:02 +0000. Datasource DataSourceNone.  Up 82.58 seconds
_
```

Machine IP (CTF): 192.168.248.96

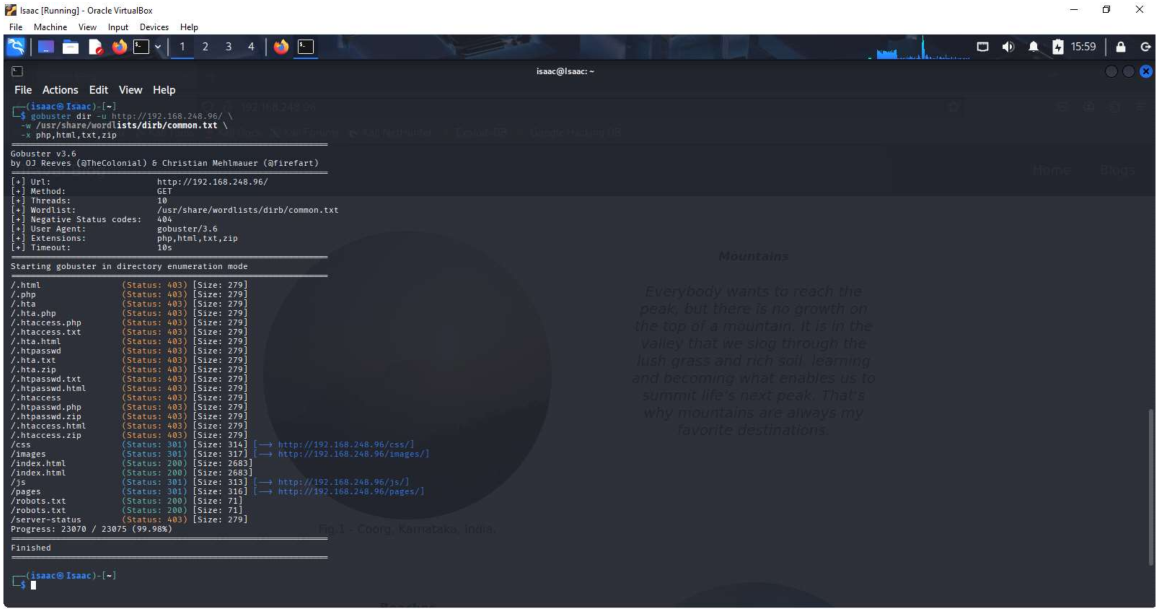
PERFORMING RECONNAISSANCEUSING: NMAP,GOBUSTER,



Isaac [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
15:39
isaac@Isaac: ~
File Actions Edit View Help
Right Ctrl

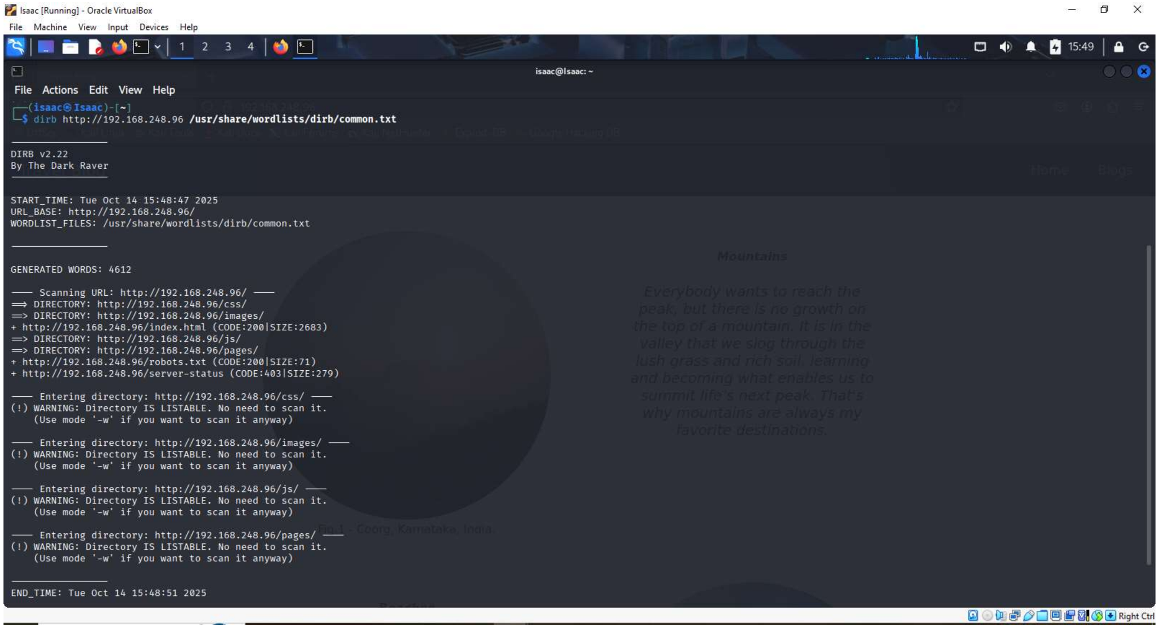
```
┌──(isaac㉿Isaac)-[~]
└─$ nmap -sV -Pn 192.168.248.96
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-14 15:38 GMT
Nmap scan report for 192.168.248.96
Host is up (0.00062s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE  SERVICE    VERSION
20/tcp   closed ftp-data
21/tcp   open   ftp        vsftpd 3.0.5
22/tcp   open   ssh        OpenSSH 8.9p1 Ubuntu 3ubuntu0.13 (Ubuntu Linux; protocol 2.0)
80/tcp   open   http       Apache httpd 2.4.52 ((Ubuntu))
443/tcp  closed https
8080/tcp closed http-proxy
MAC Address: 08:00:27:1D:3D:D7 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.73 seconds

┌──(isaac㉿Isaac)-[~]
└─$ 
```

sudo nmap -sV -Pn 192.168.248.96


Isaac [Running] - Oracle VirtualBox
File Machine View Input Devices Help
15:59
isaac@Isaac: ~
File Actions Edit View Help

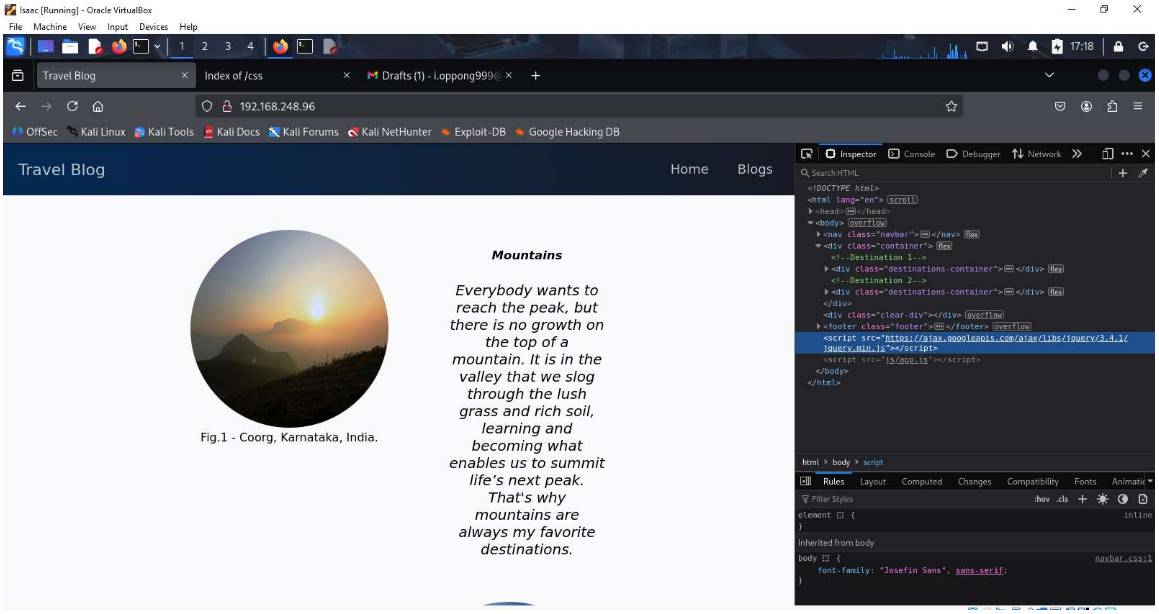
```
┌──(isaac㉿Isaac)-[~]
└─$ gobuster dir -u http://192.168.248.96/ \
  -w /usr/share/wordlists/dirb/common.txt \
  -x php,html,txt,zip
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.248.96/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html,txt,zip
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 279]
/.php                 (Status: 403) [Size: 279]
/.hta                 (Status: 403) [Size: 279]
/.hta.php             (Status: 403) [Size: 279]
/.htaccess.php        (Status: 403) [Size: 279]
/.htaccess.txt        (Status: 403) [Size: 279]
/.hta.html            (Status: 403) [Size: 279]
/.htpasswd            (Status: 403) [Size: 279]
/.hta.txt             (Status: 403) [Size: 279]
/.hta.zip             (Status: 403) [Size: 279]
/.htpasswd.txt        (Status: 403) [Size: 279]
/.htpasswd.html       (Status: 403) [Size: 279]
/.htaccess            (Status: 403) [Size: 279]
/.htpasswd.php        (Status: 403) [Size: 279]
/.htpasswd.zip        (Status: 403) [Size: 279]
/.htaccess.html       (Status: 403) [Size: 279]
/.htaccess.zip        (Status: 403) [Size: 279]
/css                  (Status: 301) [Size: 314] [--> http://192.168.248.96/css/]
/images               (Status: 301) [Size: 317] [--> http://192.168.248.96/images/]
/index.html           (Status: 200) [Size: 2683]
/index.html           (Status: 200) [Size: 2683]
/js                   (Status: 301) [Size: 313] [--> http://192.168.248.96/js/]
/pages                (Status: 301) [Size: 316] [--> http://192.168.248.96/pages/]
/robots.txt           (Status: 200) [Size: 71]
/robots.txt           (Status: 200) [Size: 71]
/server-status        (Status: 403) [Size: 279]
Progress: 23070 / 23075 (99.98%)
===============================================================
Finished
===============================================================

┌──(isaac㉿Isaac)-[~]
└─$ 
```

Using gobuster to assist in finding hidden directories/files


Isaac [Running] - Oracle VirtualBox
File Machine View Input Devices Help
15:49
isaac@Isaac: ~
File Actions Edit View Help
Right Ctrl

```
┌──(isaac㉿Isaac)-[~]
└─$ dirb http://192.168.248.96 /usr/share/wordlists/dirb/common.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Tue Oct 14 15:48:47 2025
URL_BASE: http://192.168.248.96/
WORDLIST_FILES: /usr/share/wordlists/dirb/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.248.96/ ----
==> DIRECTORY: http://192.168.248.96/css/
==> DIRECTORY: http://192.168.248.96/images/
+ http://192.168.248.96/index.html (CODE:200|SIZE:2683)
==> DIRECTORY: http://192.168.248.96/js/
==> DIRECTORY: http://192.168.248.96/pages/
+ http://192.168.248.96/robots.txt (CODE:200|SIZE:71)
+ http://192.168.248.96/server-status (CODE:403|SIZE:279)

---- Entering directory: http://192.168.248.96/css/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.248.96/images/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.248.96/js/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.248.96/pages/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Tue Oct 14 15:48:51 2025
```

dirb to confirm the hidden directories


Isaac [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Travel Blog
Index of /css
Drafts (1) - i.oppong999
192.168.248.96
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Home
Blogs
Inspector Console Debugger Network
Search HTML
Rules Layout Computed Changes Compatibility Fonts Animatic
Filter Styles
17:18

Travel Blog

Mountains

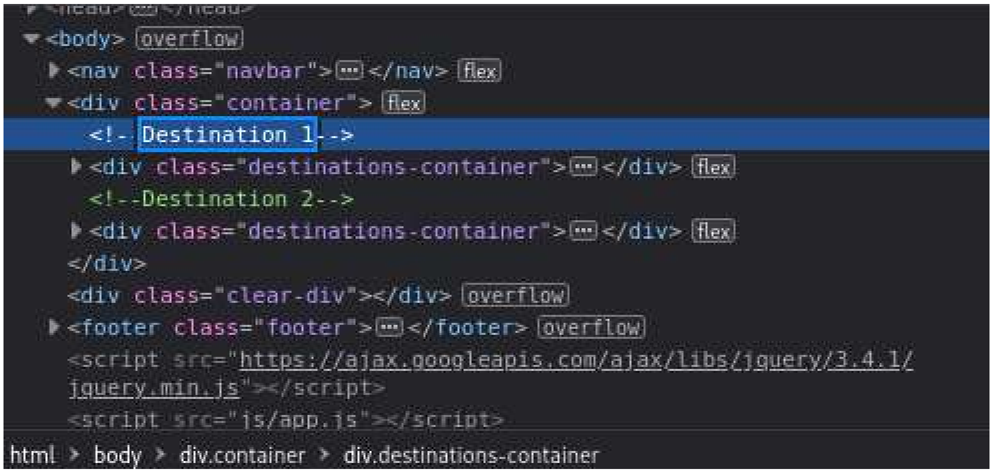
Everybody wants to reach the peak, but there is no growth on the top of a mountain. It is in the valley that we slog through the lush grass and rich soil, learning and becoming what enables us to summit life's next peak. That's why mountains are always my favorite destinations.

Fig.1 - Coorg, Karnataka, India.

```
<!DOCTYPE html>
<html lang="en"> scroll
  <head>⋯</head>
  <body> overflow
    <nav class="navbar">⋯</nav> flex
    <div class="container"> flex
      <!--Destination 1-->
      <div class="destinations-container">⋯</div> flex
      <!--Destination 2-->
      <div class="destinations-container">⋯</div> flex
    </div>
    <div class="clear-div"></div> overflow
    <footer class="footer">⋯</footer> overflow
    <script src="https://ajax.googleapis.com/ajax/libs/jquery/3.4.1/
    jquery.min.js"></script>
    <script src="js/app.js"></script>
  </body>
</html>
html > body > script
```

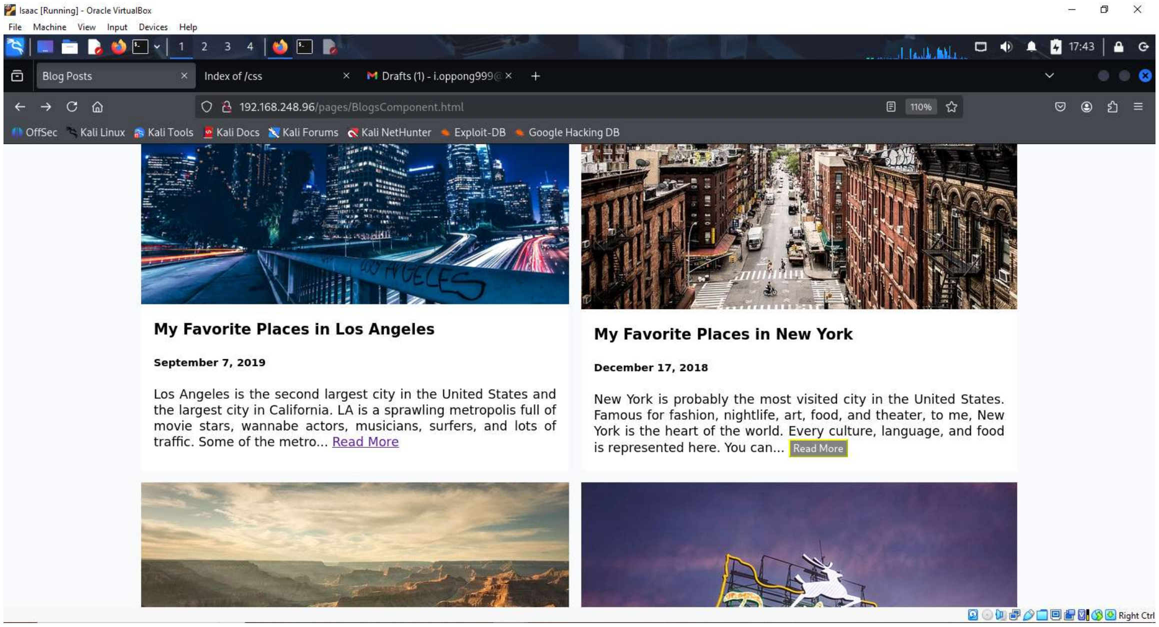
```
element { 	inline
}
Inherited from body
body { 	navbar.css:1
  font-family: "Josefin Sans", sans-serif;
}
```

Opening http://192.168.248.96 in a web browser (firefox)



```
<head>⋯</head>
<body> overflow
  <nav class="navbar">⋯</nav> flex
  <div class="container"> flex
    <!-Destination 1-->
    <div class="destinations-container">⋯</div> flex
    <!--Destination 2-->
    <div class="destinations-container">⋯</div> flex
  </div>
  <div class="clear-div"></div> overflow
  <footer class="footer">⋯</footer> overflow
  <script src="https://ajax.googleapis.com/ajax/libs/jquery/3.4.1/
  jquery.min.js"></script>
  <script src="js/app.js"></script>
html > body > div.container > div.destinations-container
```

The beginning of the test


Isaac [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Blog Posts
Index of /css
Drafts (1) - i.oppong999@
192.168.248.96/pages/BlogsComponent.html
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

My Favorite Places in Los Angeles

September 7, 2019

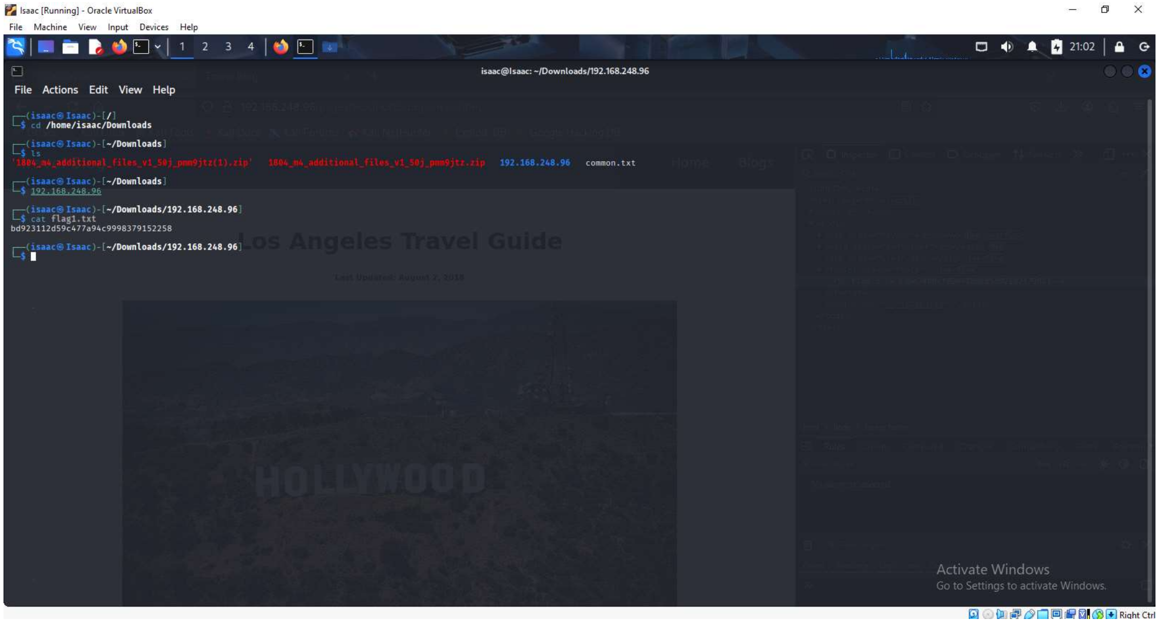
Los Angeles is the second largest city in the United States and the largest city in California. LA is a sprawling metropolis full of movie stars, wannabe actors, musicians, surfers, and lots of traffic. Some of the metro... Read More

My Favorite Places in New York

December 17, 2018

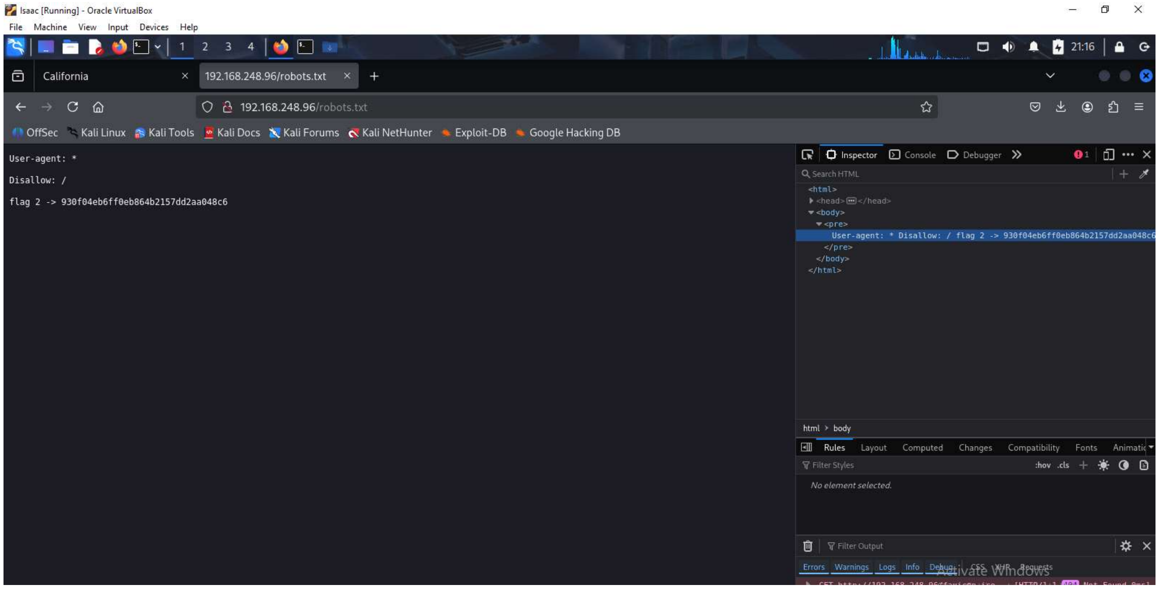
New York is probably the most visited city in the United States. Famous for fashion, nightlife, art, food, and theater, to me, New York is the heart of the world. Every culture, language, and food is represented here. You can... Read More

Checking for the active Read More


Isaac [Running] - Oracle VirtualBox
File Machine View Input Devices Help
isaac@Isaac: ~/Downloads/192.168.248.96
File Actions Edit View Help

```
┌──(isaac㉿Isaac)-[/]
└─$ cd /home/isaac/Downloads

┌──(isaac㉿Isaac)-[~/Downloads]
└─$ ls
'1804_m4_additional_files_v1_50j_pmm9jtz(1).zip'   1804_m4_additional_files_v1_50j_pmm9jtz.zip   192.168.248.96   common.txt

┌──(isaac㉿Isaac)-[~/Downloads]
└─$ 192.168.248.96

┌──(isaac㉿Isaac)-[~/Downloads/192.168.248.96]
└─$ cat flag1.txt
bd923112d59c477a94c9998379152258

┌──(isaac㉿Isaac)-[~/Downloads/192.168.248.96]
└─$ 
```

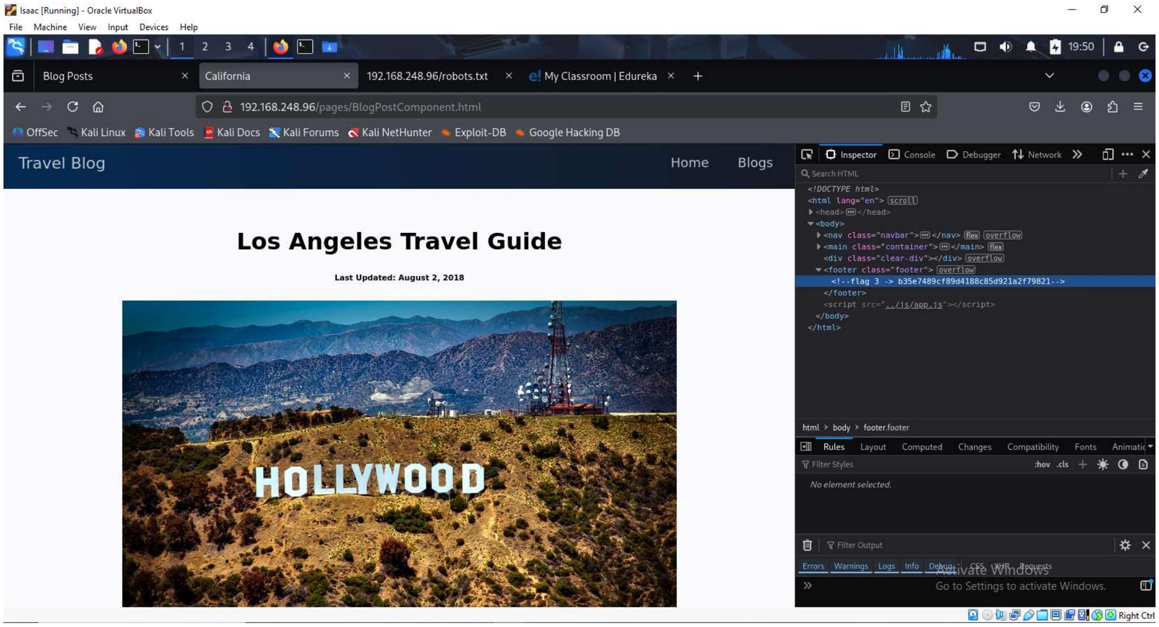
Flag 1: cat flag1.txt


Isaac [Running] - Oracle VirtualBox
File Machine View Input Devices Help
California
192.168.248.96/robots.txt
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Inspector Console Debugger
Search HTML
Rules Layout Computed Changes Compatibility Fonts
No element selected.

```
User-agent: *

Disallow: /

flag 2 -> 930f04eb6ff0eb864b2157dd2aa048c6
```

```
<html>
  <head></head>
  <body>
    <pre>
      User-agent: * Disallow: / flag 2 -> 930f04eb6ff0eb864b2157dd2aa048c6
    </pre>
  </body>
</html>
```

Flag 2: http://192.168.248.96/robotx.txt

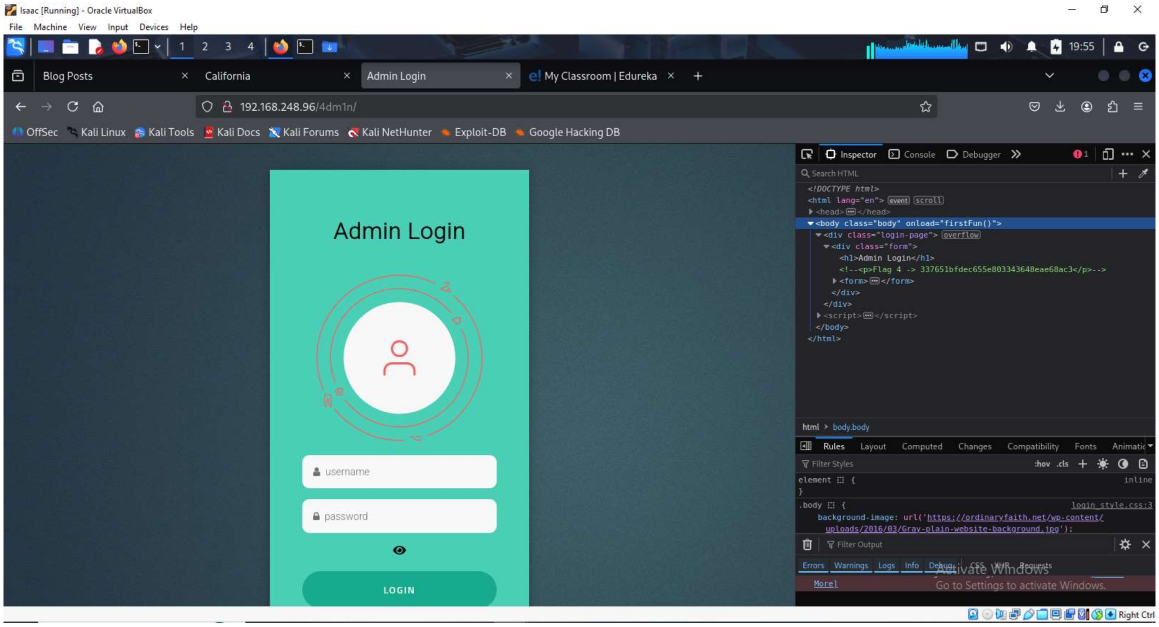

Isaac [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Blog Posts
California
192.168.248.96/robots.txt
My Classroom | Edureka
192.168.248.96/pages/BlogPostComponent.html
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Travel Blog
Home
Blogs
HOLLYWOOD
Inspector Console Debugger Network
Search HTML
html > body > footer.footer
Rules Layout Computed Changes Compatibility Fonts
No element selected.

Los Angeles Travel Guide

Last Updated: August 2, 2018

```
<!DOCTYPE html>
<html lang="en">
  <head></head>
  <body>
    <nav class="navbar"></nav>
    <main class="container"></main>
    <div class="clear-div"></div>
    <footer class="footer">
      <!--flag 3 -> b35e7489cf89d4188c85d921a2f79821-->
    </footer>
    <script src="../js/app.js"></script>
  </body>
</html>
```

Flag 3: http://192.168.248.96/pages/BlogPostCcomponent.html



Isaac [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Blog Posts
California
Admin Login
My Classroom | Edureka
192.168.248.96/4dm1n/
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Admin Login
username
password
LOGIN
Inspector Console Debugger
Search HTML
Rules Layout Computed Changes Compatibility Fonts Animatic
Filter Styles
Filter Output
Errors Warnings Logs Info Debug CSS XHR Requests
Activate Windows
Go to Settings to activate Windows.
Right Ctrl

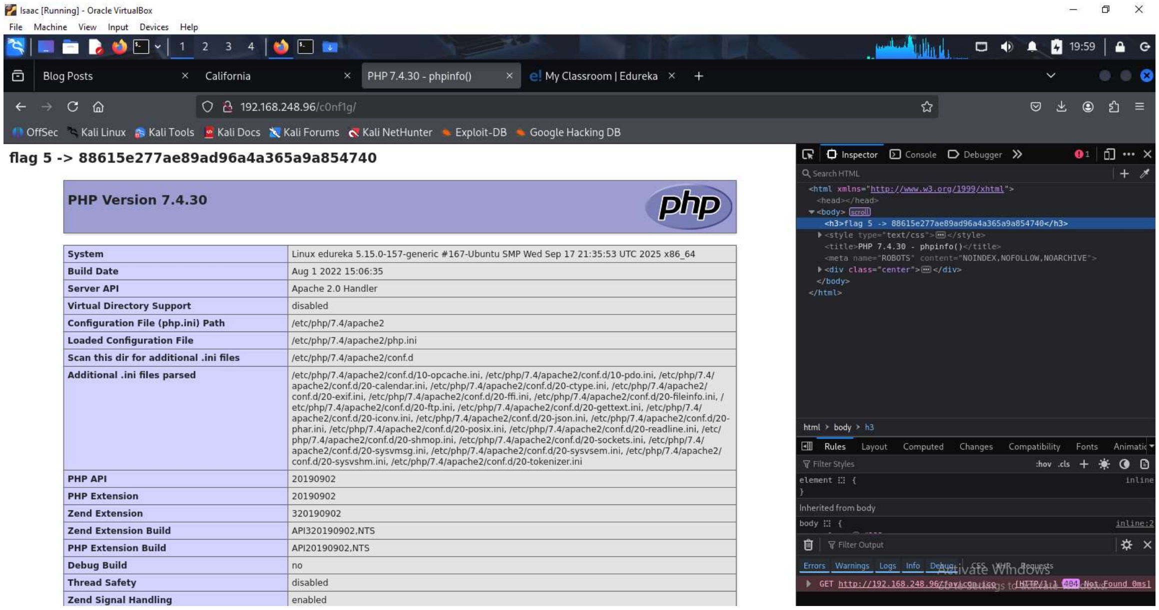
```
<!DOCTYPE html>
<html lang="en"> event scroll
  <head>⋯</head>
  <body class="body" onload="firstFun()">
    <div class="login-page"> overflow
      <div class="form">
        <h1>Admin Login</h1>
        <!--<p>Flag 4 -> 337651bfdec655e803343648eae68ac3</p>-->
        <form>⋯</form>
      </div>
    </div>
    <script>⋯</script>
  </body>
</html>
```

html > body.body

```
element {
}
.body {                                   login_style.css:3
  background-image: url('https://ordinaryfaith.net/wp-content/
    uploads/2016/03/Gray-plain-website-background.jpg');
```

More!

Flag 4: http://192.168.248.96/4dm1n



Isaac [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Blog Posts
California
PHP 7.4.30 - phpinfo()
My Classroom | Edureka
192.168.248.96/c0nf1g/
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
php
Inspector Console Debugger
Search HTML
Rules Layout Computed Changes Compatibility Fonts Animatic
Filter Styles
Filter Output
Errors Warnings Logs Info Debug CSS XHR Requests
Activate Windows

flag 5 -> 88615e277ae89ad96a4a365a9a854740

PHP Version 7.4.30

System	Linux edureka 5.15.0-157-generic #167-Ubuntu SMP Wed Sep 17 21:35:53 UTC 2025 x86_64
Build Date	Aug 1 2022 15:06:35
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.4/apache2
Loaded Configuration File	/etc/php/7.4/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.4/apache2/conf.d
Additional .ini files parsed	/etc/php/7.4/apache2/conf.d/10-opcache.ini, /etc/php/7.4/apache2/conf.d/10-pdo.ini, /etc/php/7.4/apache2/conf.d/20-calendar.ini, /etc/php/7.4/apache2/conf.d/20-ctype.ini, /etc/php/7.4/apache2/conf.d/20-exif.ini, /etc/php/7.4/apache2/conf.d/20-ffi.ini, /etc/php/7.4/apache2/conf.d/20-fileinfo.ini, /etc/php/7.4/apache2/conf.d/20-ftp.ini, /etc/php/7.4/apache2/conf.d/20-gettext.ini, /etc/php/7.4/apache2/conf.d/20-iconv.ini, /etc/php/7.4/apache2/conf.d/20-json.ini, /etc/php/7.4/apache2/conf.d/20-phar.ini, /etc/php/7.4/apache2/conf.d/20-posix.ini, /etc/php/7.4/apache2/conf.d/20-readline.ini, /etc/php/7.4/apache2/conf.d/20-shmop.ini, /etc/php/7.4/apache2/conf.d/20-sockets.ini, /etc/php/7.4/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.4/apache2/conf.d/20-sysvsem.ini, /etc/php/7.4/apache2/conf.d/20-sysvshm.ini, /etc/php/7.4/apache2/conf.d/20-tokenizer.ini
PHP API	20190902
PHP Extension	20190902
Zend Extension	320190902
Zend Extension Build	API320190902,NTS
PHP Extension Build	API20190902,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled

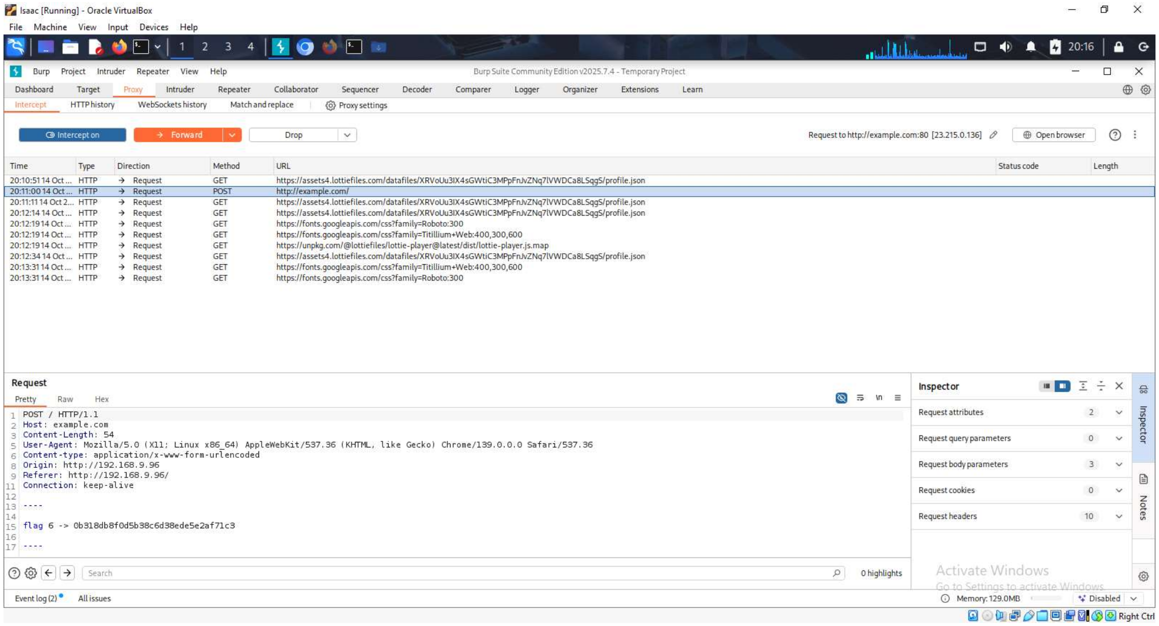
```
<html xmlns="http://www.w3.org/1999/xhtml">
  <head></head>
  <body> scroll
    <h3>flag 5 -> 88615e277ae89ad96a4a365a9a854740</h3>
    <style type="text/css">⋯</style>
    <title>PHP 7.4.30 - phpinfo()</title>
    <meta name="ROBOTS" content="NOINDEX,NOFOLLOW,NOARCHIVE">
    <div class="center">⋯</div>
  </body>
</html>
```

html > body > h3

```
element {                                 inline
}
Inherited from body
body {                                    inline:2
```

```
GET http://192.168.248.96/favicon.ico [HTTP/1.1 404 Not Found 0ms]
```

Flag 5: http://192.168.248.96/c0nf1g


Isaac [Running] - Oracle VirtualBox
File Machine View Input Devices Help
20:16
Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.7.4 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on
Forward
Drop
Open browser
Pretty Raw Hex
Search
0 highlights
Event log (2) All issues
Inspector
Notes
Activate Windows
Go to Settings to activate Windows
Memory: 129.0MB
Disabled
Right Ctrl

Request to http://example.com:80 [23.215.0.136]

Time	Type	Direction	Method	URL	Status code	Length
20:10:51 14 Oct ...	HTTP	→ Request	GET	https://assets4.lottiefiles.com/datafiles/XRVoUu3IX4sGWtiC3MPpFnJvZNq7lVWDCa8LSqgS/profile.json		
20:11:00 14 Oct ...	HTTP	→ Request	POST	http://example.com/		
20:11:11 14 Oct 2...	HTTP	→ Request	GET	https://assets4.lottiefiles.com/datafiles/XRVoUu3IX4sGWtiC3MPpFnJvZNq7lVWDCa8LSqgS/profile.json		
20:12:14 14 Oct ...	HTTP	→ Request	GET	https://assets4.lottiefiles.com/datafiles/XRVoUu3IX4sGWtiC3MPpFnJvZNq7lVWDCa8LSqgS/profile.json		
20:12:19 14 Oct ...	HTTP	→ Request	GET	https://fonts.googleapis.com/css?family=Roboto:300		
20:12:19 14 Oct ...	HTTP	→ Request	GET	https://fonts.googleapis.com/css?family=Titillium+Web:400,300,600		
20:12:19 14 Oct ...	HTTP	→ Request	GET	https://unpkg.com/@lottiefiles/lottie-player@latest/dist/lottie-player.js.map		
20:12:34 14 Oct ...	HTTP	→ Request	GET	https://assets4.lottiefiles.com/datafiles/XRVoUu3IX4sGWtiC3MPpFnJvZNq7lVWDCa8LSqgS/profile.json		
20:13:31 14 Oct ...	HTTP	→ Request	GET	https://fonts.googleapis.com/css?family=Titillium+Web:400,300,600		
20:13:31 14 Oct ...	HTTP	→ Request	GET	https://fonts.googleapis.com/css?family=Roboto:300		

Request

```
POST / HTTP/1.1
Host: example.com
Content-Length: 54
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36
Content-type: application/x-www-form-urlencoded
Origin: http://192.168.9.96
Referer: http://192.168.9.96/
Connection: keep-alive

----

flag 6 -> 0b318db8f0d5b38c6d38ede5e2af71c3

----
```

Request attributes	2
Request query parameters	0
Request body parameters	3
Request cookies	0
Request headers	10

Flag 6: http://192.168.248.96/4dm1n

Vulnerability Analysis & Risk- Exposed configuration/backup files — risk: credentials leak.- Exposed admin interfaces with weak authentication — risk: admin takeover.- Hidden files in webroot — risk: sensitive data exposure.

Remediation Recommendations- Remove sensitive files from webroot.- Harden admin interfaces (strong auth, MFA, IP restrictions).- Disable directory listing.- Use secure secrets management.- Implement logging and monitoring.

Conclusion

All six flags were located by combining network discovery and focused web enumeration. The primary lesson is that simple enumeration often reveals leftover files and admin interfaces; preventing exposure requires proper server configuration and operational discipline