




LinkedIn: [Kelvin Kimotho](#)

Secrets 

Medium

Web Exploitation

picoCTF 2022

AUTHOR: GEOFFREY NJOGU

Description

We have several pages hidden. Can you find the one with the flag?

The website is running [here](#).

This challenge launches an instance on demand.

Its current status is:

RUNNING

Instance Time Remaining:

5:55

Restart Instance

Hints ?

1

folders folders folders

Solution

From the challenge description it was clear that some pages and directories were hidden and it was hard to guess the page names and the hidden directory.

So, I this task i had to use *Gobuster* a brute-force scanner tool to enumerate directories and files of websites. The tool also assists in finding DNS subdomains and virtual host names.

The command format for using this tool is “*gobuster dir -u <target_url> -w <path_to_wordlist>*”. So, I went ahead enumerating my target site using this tool.

```
(kali@kali)-[~/Desktop]
└─$ sudo gobuster dir -u http://saturn.picoctf.net:64700 -w /home/kali/Downloads/directory-list-2.3-medium.txt

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

[+] Url:             http://saturn.picoctf.net:64700
[+] Method:          GET
[+] Threads:         10
[+] Wordlist:         /home/kali/Downloads/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:      gobuster/3.6
[+] Timeout:         10s

Starting gobuster in directory enumeration mode

/secret (Status: 301) (Size: 169) (→ http://saturn.picoctf.net/secret/)
Progress: 6319 / 220560 (2.86%)
[!] Keyboard interrupt detected, terminating.
Progress: 6330 / 220560 (2.87%)

Finished
```

I realize that a directory named "secret" existed and considering that i was looking for hidden files and directories, this was a directory of interest. I went ahead and accessed the /secret page on my browser but i didn't get the flag.

Finally. You almost found me. you are doing well



I continued enumerating the secret directory looking for other possible hidden directories within the secret directory. I discovered two directories, assets and hidden directories.

```
(kali@kali)-[~/Desktop]
$ sudo gobuster dir -u http://saturn.picoctf.net:50355/secret -w custom_wordlist.txt

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

[+] Url: http://saturn.picoctf.net:50355/secret
[+] Method: GET
[+] Threads: 10
[+] Wordlist: custom_wordlist.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

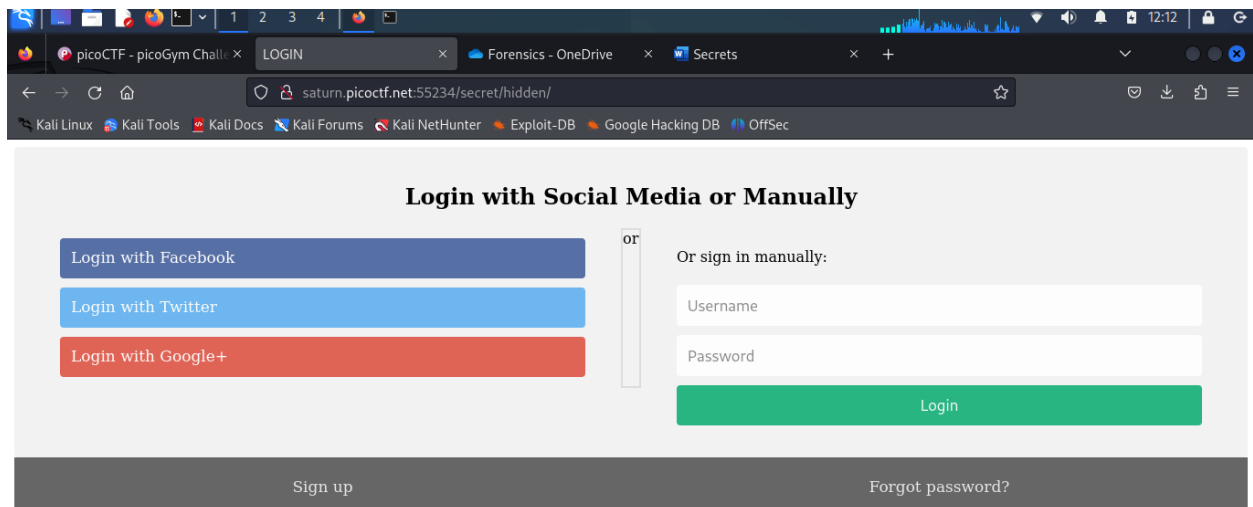
Starting gobuster in directory enumeration mode

/assets (Status: 301) [Size: 169] [→ http://saturn.picoctf.net/secret/assets/]
/hidden (Status: 301) [Size: 169] [→ http://saturn.picoctf.net/secret/hidden/]
Progress: 2203 / 2204 (99.95%)

Finished

(kali@kali)-[~/Desktop]
$
```

I tried accessing hidden from the browser which rendered a page but the flag was not there still even after examining the page source code.



```
1 <!DOCTYPE html>
2 <html>
3 <head>
4 <title>LOGIN</title>
5 <!-- CSS -->
6 <link href="/superhidden/login.css" rel="stylesheet" />
7 </head>
8 <body>
9 <div class="container">
10 <div class="row">
11 <div class="col">
12 <div class="row">
13 <div class="col">
14 <div class="col">
15 <div class="col">
16 <div class="col">
17 <div class="col">
18 <div class="col">
19 <div class="col">
20 <div class="col">
21 <div class="col">
22 <div class="col">
23 <div class="col">
24 <div class="col">
25 <div class="col">
26 <div class="col">
27 <div class="col">
28 <div class="col">
29 <div class="col">
30 <div class="col">
31 <div class="col">
32 <div class="col">
33 <div class="col">
34 <div class="col">
35 <div class="col">
36 <div class="col">
37 <div class="col">
38 <div class="col">
39 <div class="col">
40 <div class="col">
41 <div class="col">
```

```
/* {
  box-sizing: border-box;
}

/* style the container */
.container {
  position: relative;
  border-radius: 5px;
  background-color: #f2f2f2;
  padding: 20px 0 30px 0;
}

/* style inputs and link buttons */
input,
.btn {
  width: 100%;
  padding: 12px;
  border: none;
  border-radius: 4px;
  margin: 5px 0;
  opacity: 0.85;
  display: inline-block;
  font-size: 17px;
  line-height: 20px;
  text-decoration: none; /* remove underline from anchors */
}

input:hover,
.btn:hover {
  opacity: 1;
}

/* add appropriate colors to fb, twitter and google buttons */
.fb {
  background-color: #3b5998;
  color: white;
}

.twitter {
  background-color: #55acee;
  color: white;
```

The js file had some message left for me ” Thank you for the attempt but oops! try harder”.

```
<script>alert(' Thank you for the attempt but oops! try harder')</script>;
```

I went ahead and tried enumerating the hidden directory hoping to find something meaningful. I ran the following command ” `sudo gobuster dir -u http://saturn.picoctf.net:55234/secret/hidden -w dir_wordlist.txt` ”.

```
picoCTF - picoGym Chall: x LOGIN x http://saturn.picoctf.net:552 x Forensics - OneDrive x Secrets x + v
kali@kali: ~/Desktop
File Actions Edit View Help
(kali@kali)~/Desktop
$ sudo gobuster dir -u http://saturn.picoctf.net:55234/secret/hidden -w dir_wordlist.txt

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

[+] Url: http://saturn.picoctf.net:55234/secret/hidden
[+] Method: GET
[+] Threads: 10
[+] Wordlist: dir_wordlist.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

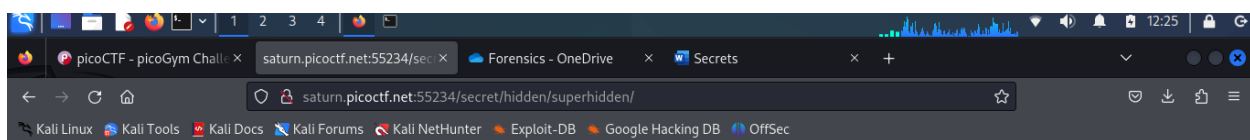
Starting gobuster in directory enumeration mode

/superhidden (Status: 301) [Size: 169] [→ http://saturn.picoctf.net:55234/secret/hidden/superhidden/]
/superhidden (Status: 301) [Size: 169] [→ http://saturn.picoctf.net:55234/secret/hidden/superhidden/]
Progress: 3254 / 4404 (73.89%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 3263 / 4404 (74.09%)

Finished

(kali@kali)~/Desktop
$
```

The gobuster tool discovered a directory named **superhidden**. I went ahead and tried accessing the directory from browser and this is the message I got.



Finally. You found me. But can you see me

I went ahead and examined the source code of this page and the flag was stored in a h3 html tag.

```
picoCTF - picoGym Chall: x saturn.picoctf.net:55234/sec x http://saturn.picoctf.net:552 x Forensics - OneDrive x Secrets x + v
view-source:http://saturn.picoctf.net:55234/secret/hidden/superhidden/
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
1 <!DOCTYPE html>
2 <html>
3 <head>
4 <title></title>
5 <link rel="stylesheet" href="mycss.css" />
6 </head>
7
8 <body>
9 <h1>Finally. You found me. But can you see me</h1>
10 <h3 class="flag">picoCTF{succ3ss_@h3n1c@10n_39849bcbf}</h3>
11 </body>
12 </html>
13
```

Flag: **picoCTF{succ3ss_@h3n1c@10n_39849bcbf}**