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 oluşturmadan 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

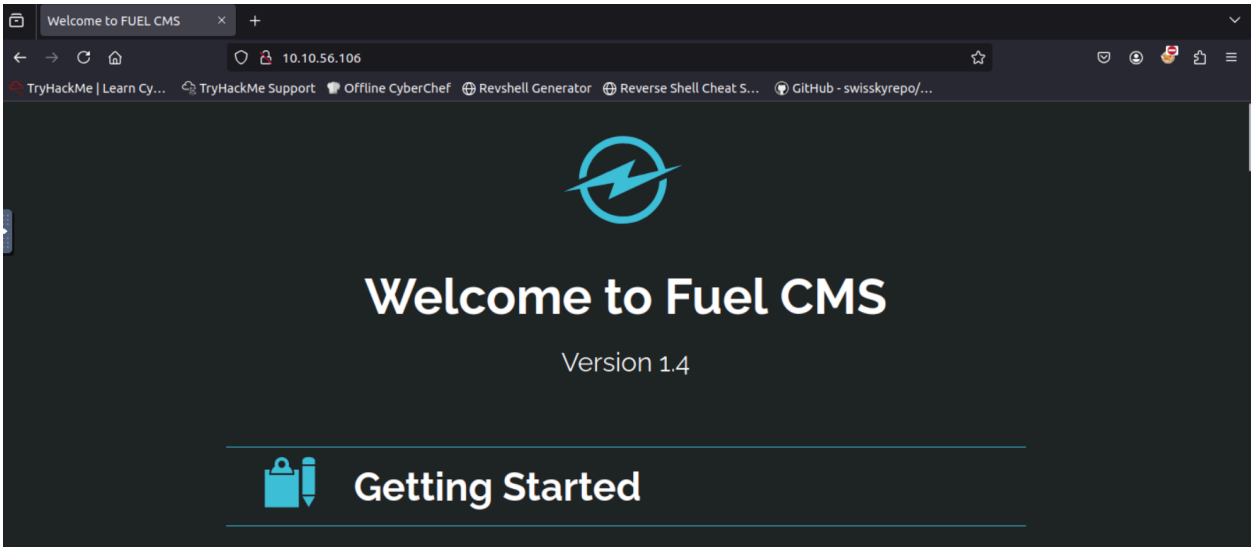
Sorular

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

Cevap ⇒ Cevap Gerekmemektedir.

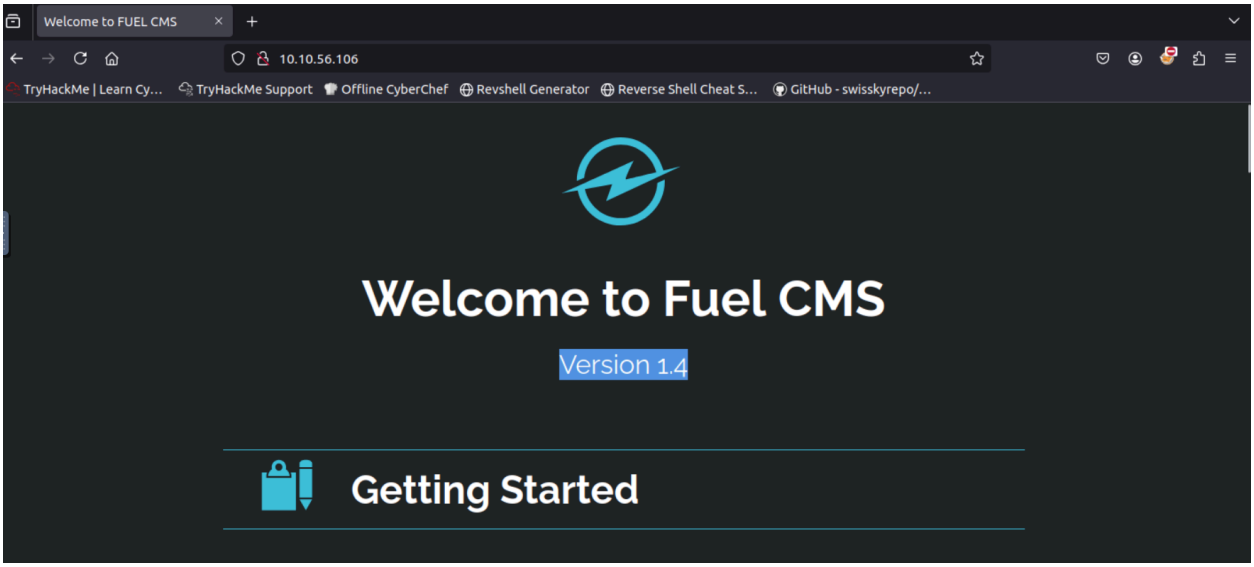
Soru ⇒ Savunmasız makinede çalışan uygulamanın adı nedir?

Cevap ⇒ Fuel CMS



Soru ⇒ Bu uygulamanın sürüm numarası nedir?

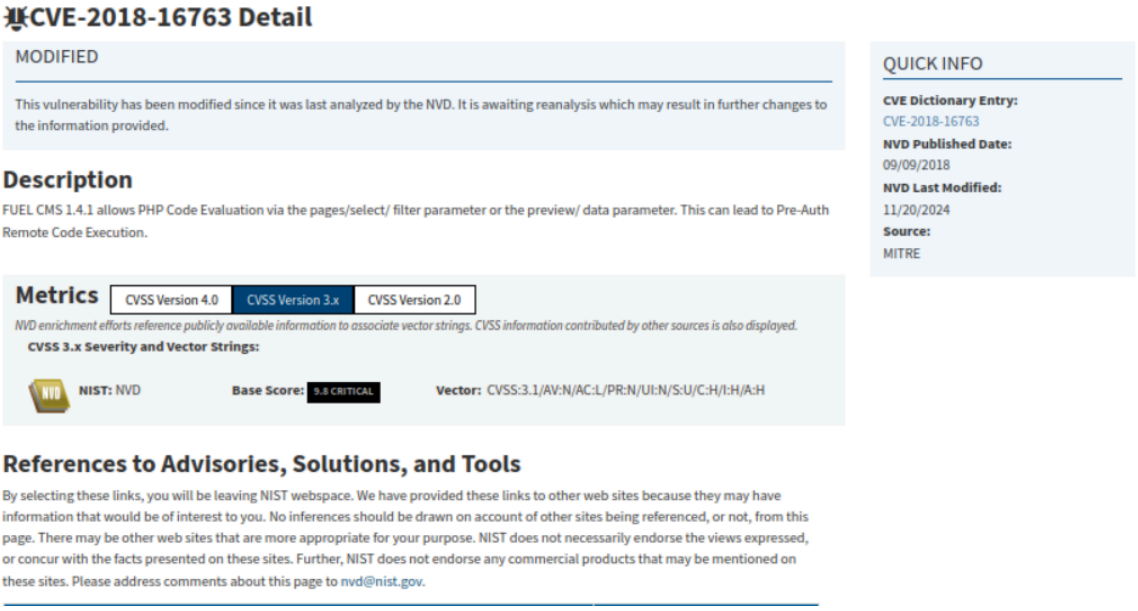
Cevap ⇒ 1.4



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

Format: CVE-XXXX-XXXXX

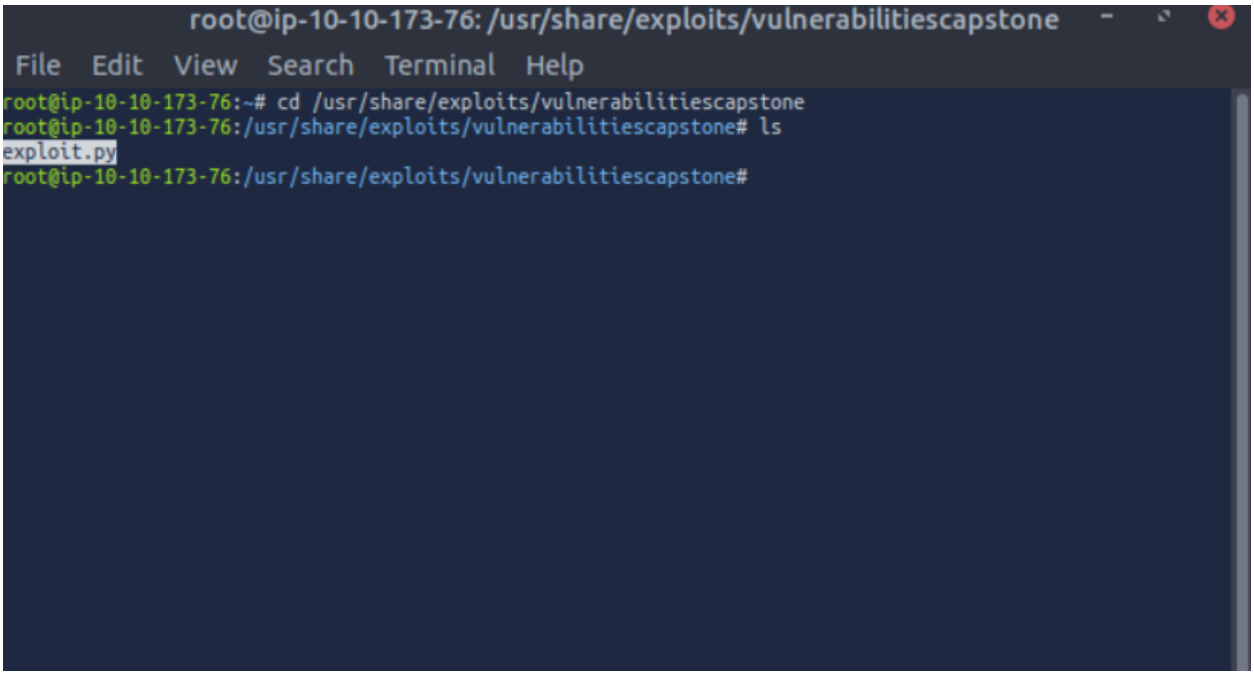
Cevap ⇒ CVE-2018-16763



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.



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}