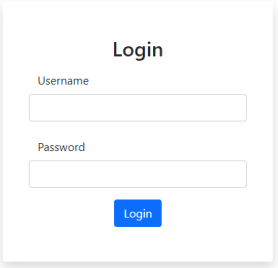
Hackviser SQL Injection Lab

Basic SQL Injection

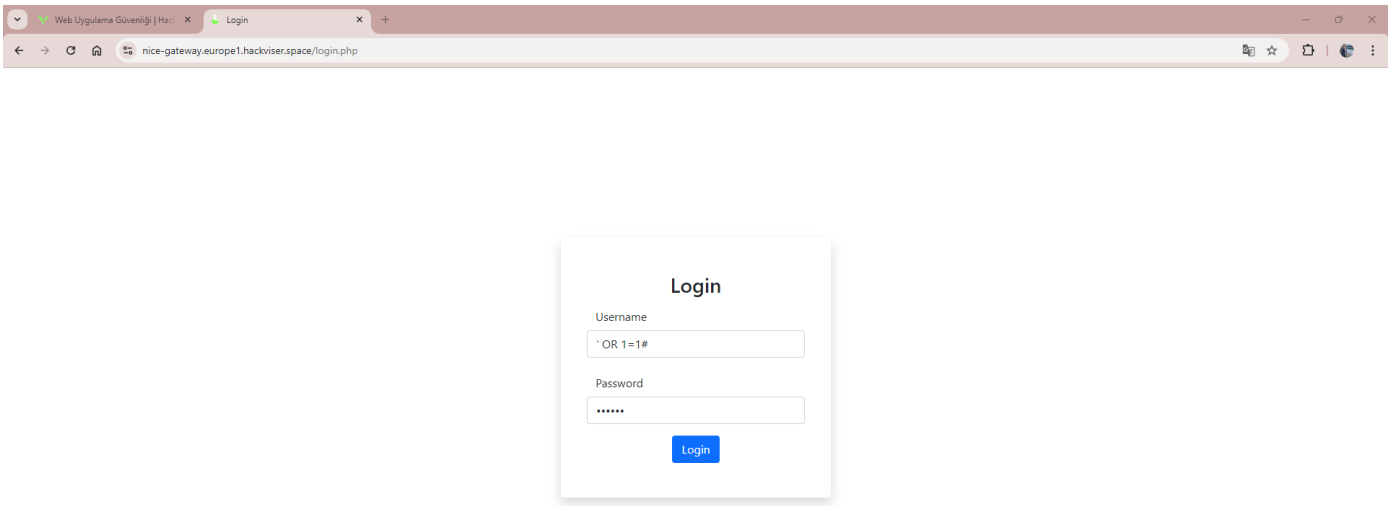
Başlangıçta bize labaratuvar hakkında bilgi vermiş

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

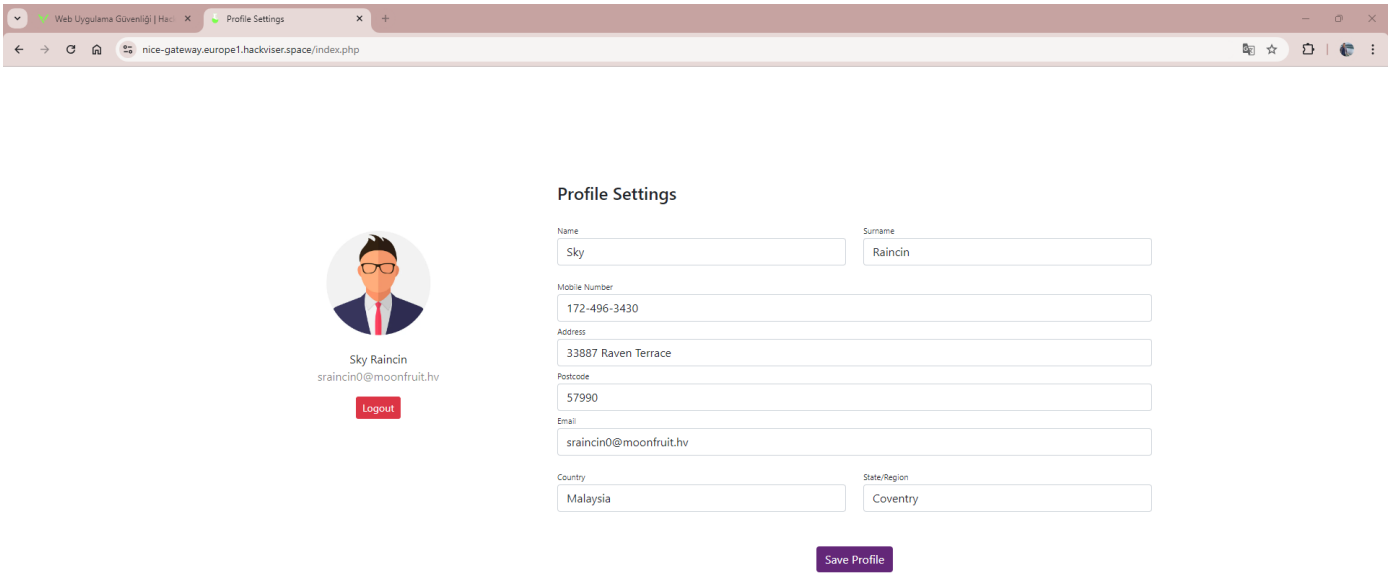
Sky Raincin adlı kullanıcının e-posta adresi nedir?



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 labaratuvar hakkında bilgi vermiş

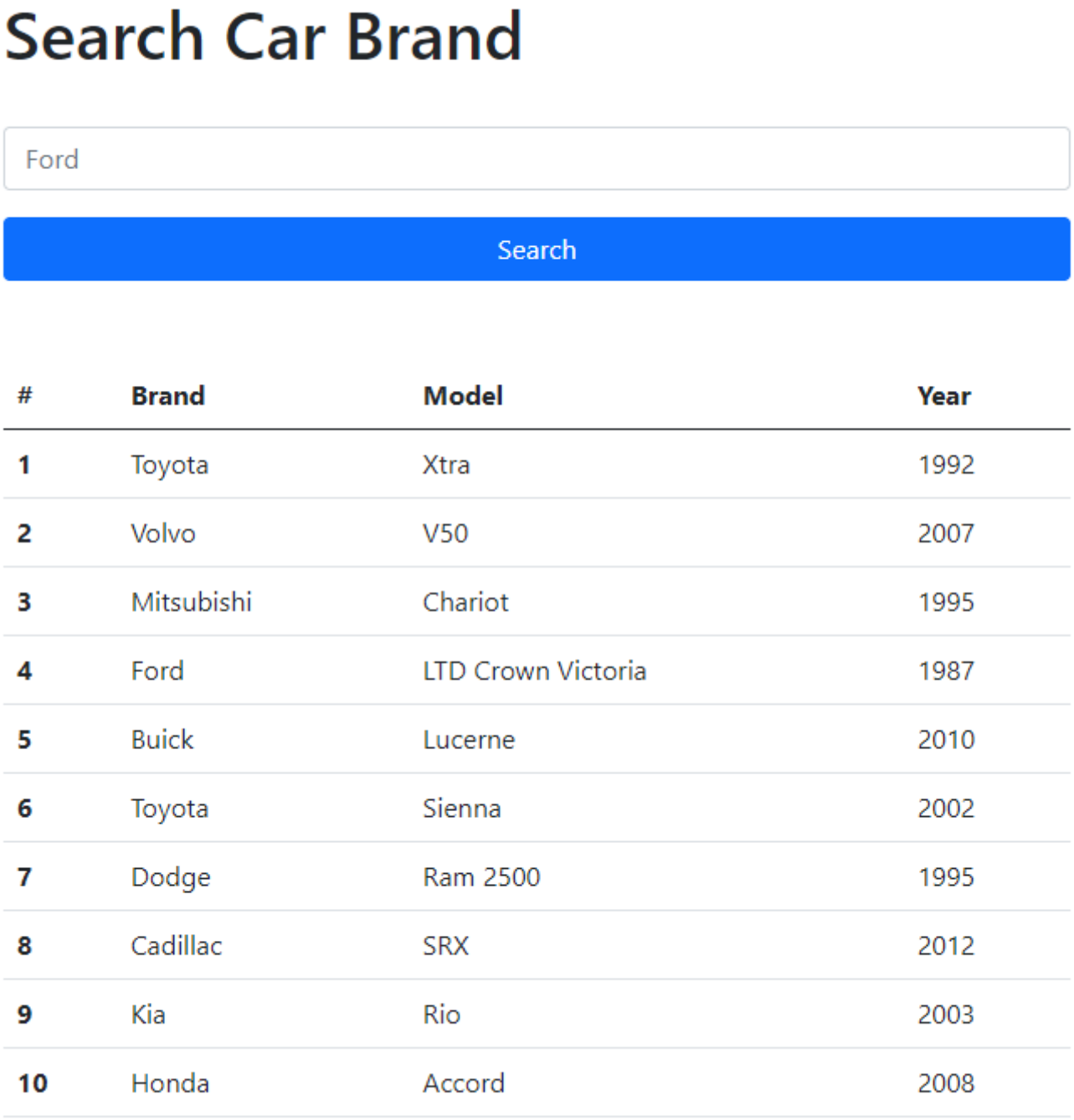
Bu laboratuvar, arama işlevinde SQL Injection zafiyeti içermektedir. Sorgudan elde edilen sonuçlar uygulamanın yanıtında döndürülür, böylece diğer tablolardan veri almak için bir UNION

saldırısı kullanılabilir.

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

Veritabanı adı nedir?

Öncelikle Web sitesine gidelim



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 sunucu bu bilgiyi döndürür.

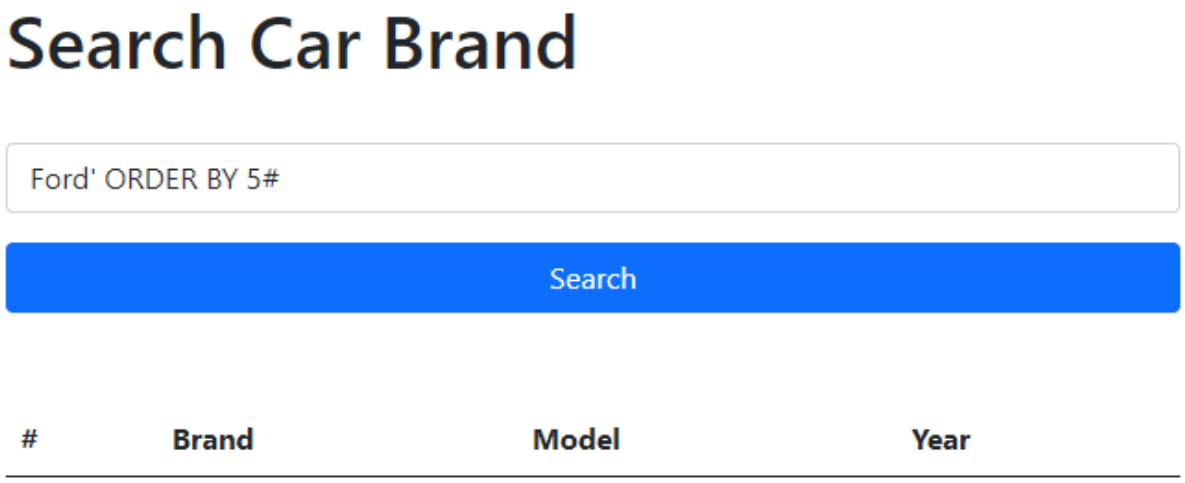
Search Car Brand

Ford' ORDER BY 1#

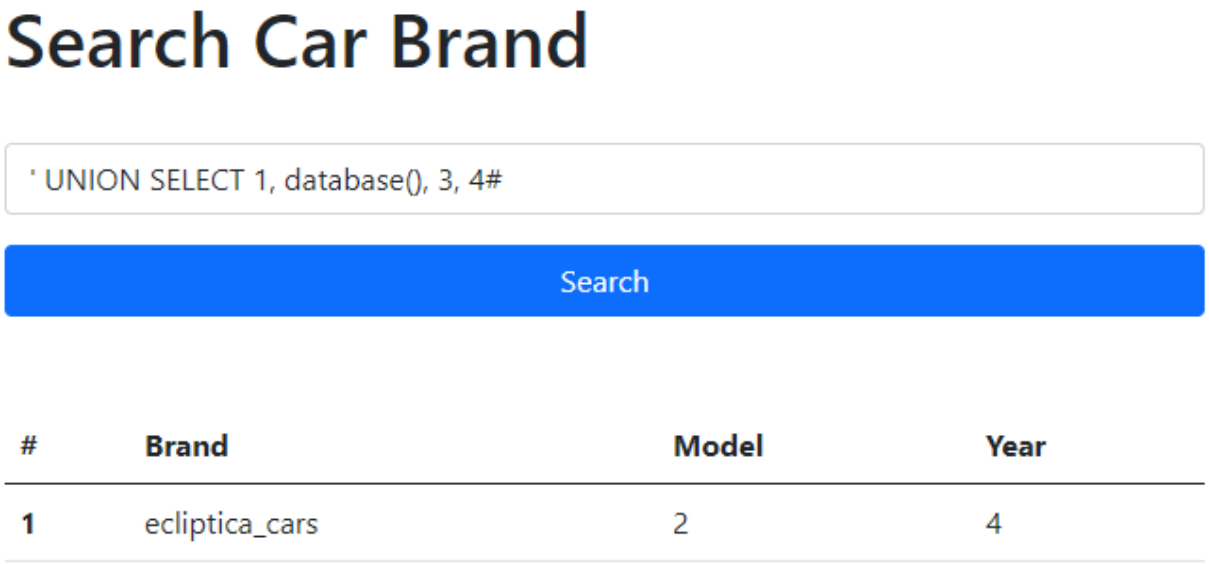
Search

#	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.



5 Yazdığımızda bi çıktı alamıyoruz demekki 4 sütun var



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

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

Boolean-Based Blind SQL Injection

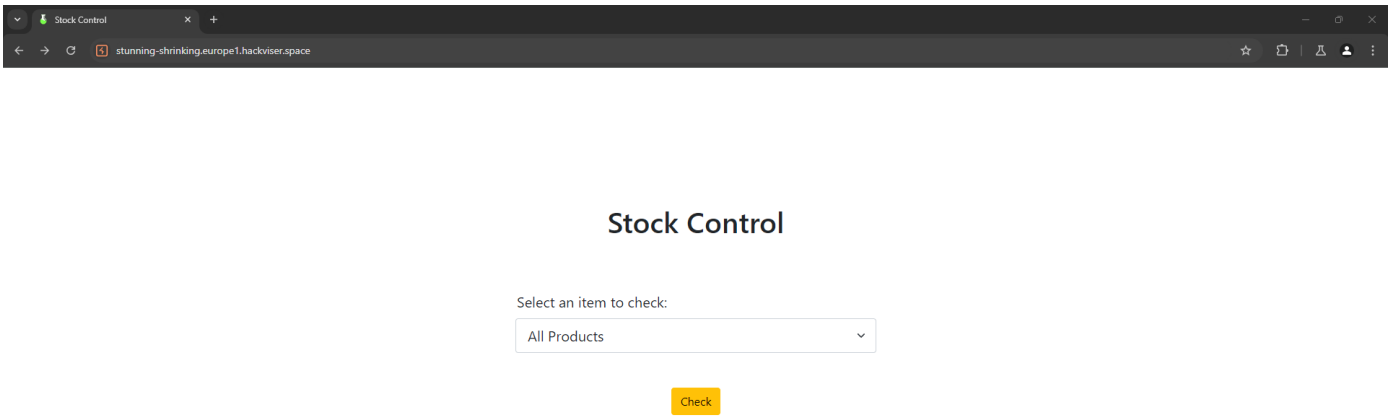
Başlangıçta bize labaratuvar hakkında bilgi vermiş

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.

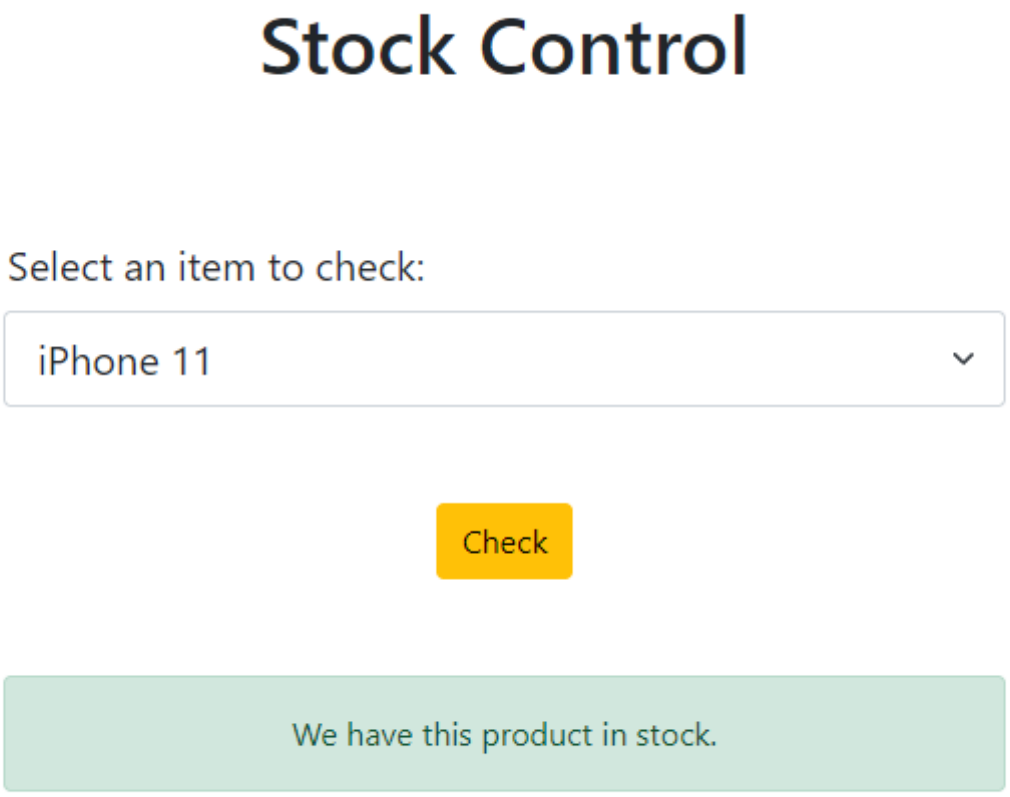
Veritabanı adı nedir?

Öncelikle web sitesine gidelim

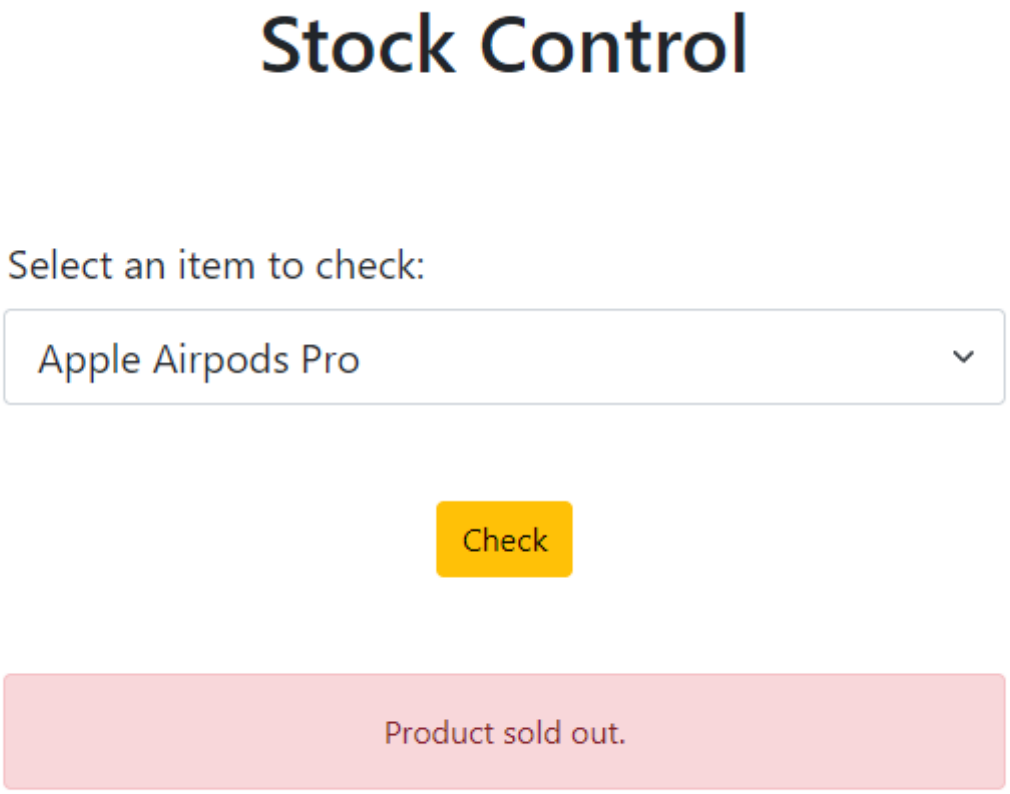


Bize ürünlerin stoklarını kontrol edebileceğimiz bir web sitesi karşılıyor

Bazı ürünler mevcut



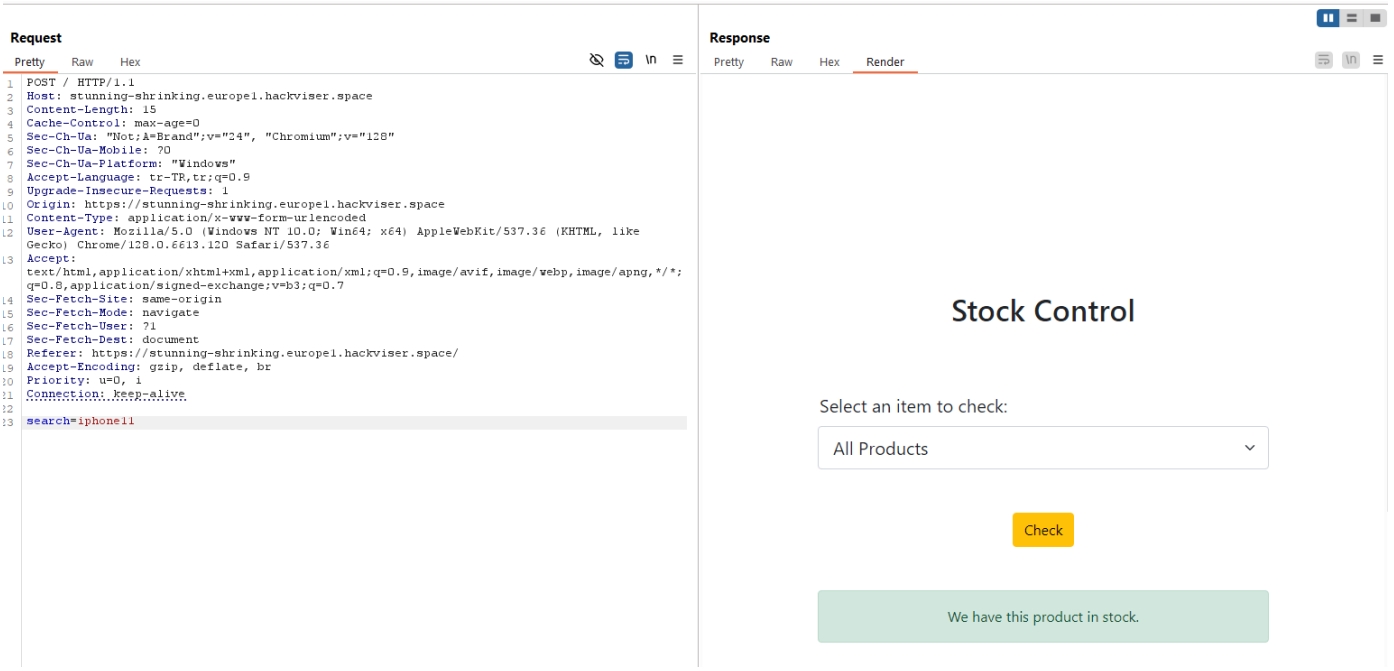
Bazı ürünler stokta yok



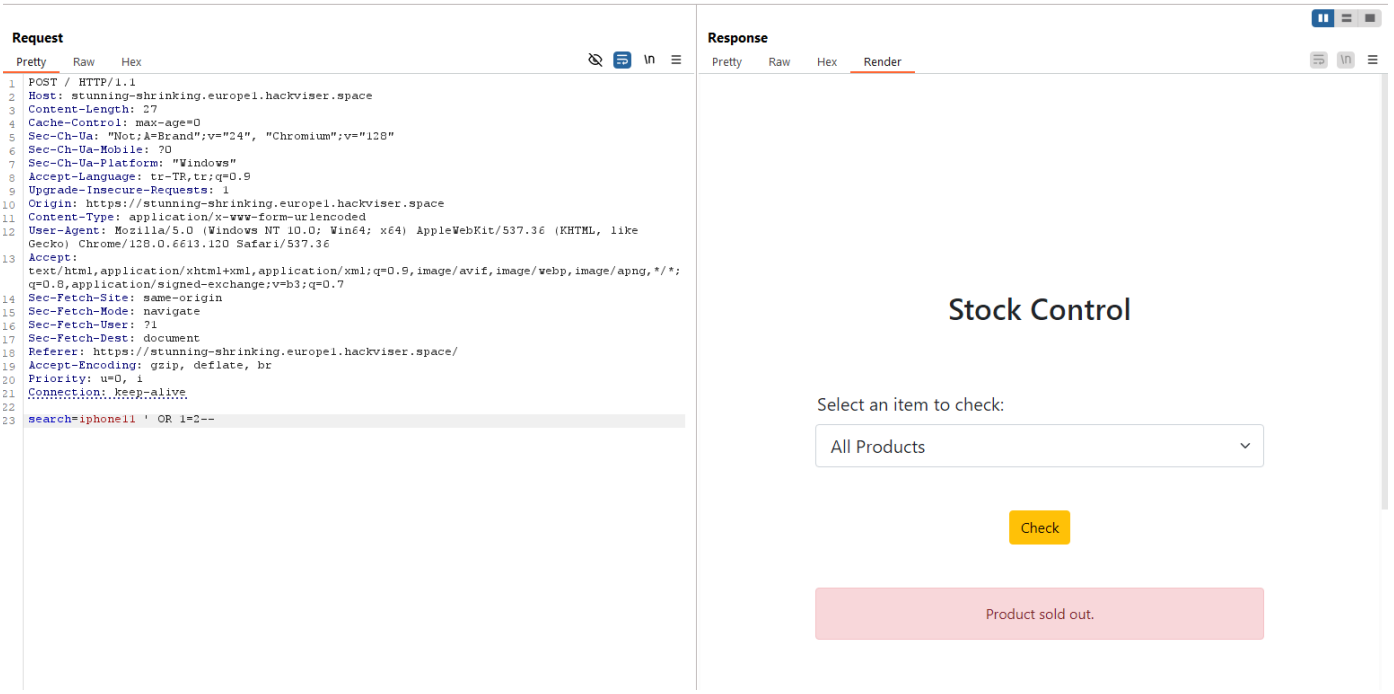
Bu tür bir laboratuvar, **Blind SQL Injection (Kör SQL Enjeksiyonu)** saldırısı için mükemmel bir örnektir. Çünkü doğrudan bir hata mesajı veya veritabanı çıktısı almazsınız, ancak aldığınız yanıtlar (örneğin, "stokta mevcut" veya "stokta mevcut değil") size enjeksiyon saldırısı yaparak belirli bilgileri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

- Doğru veya yanlış bir yanıt alarak (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

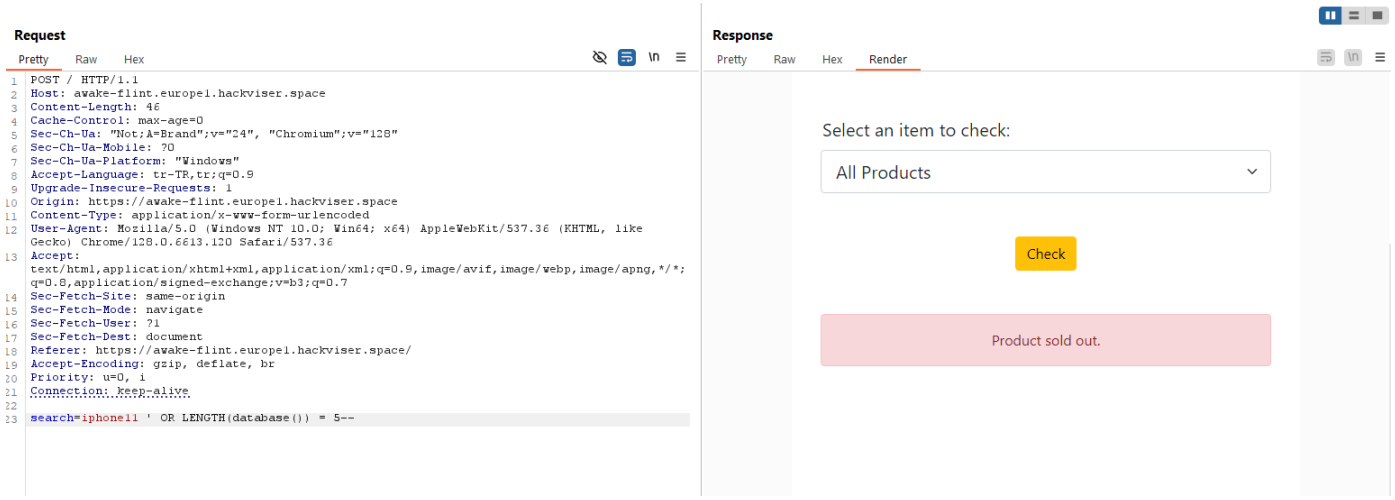


İsteğimizi repeater'a yolladık şimdi basit bi sorguyla SQLi kontrol edelim.

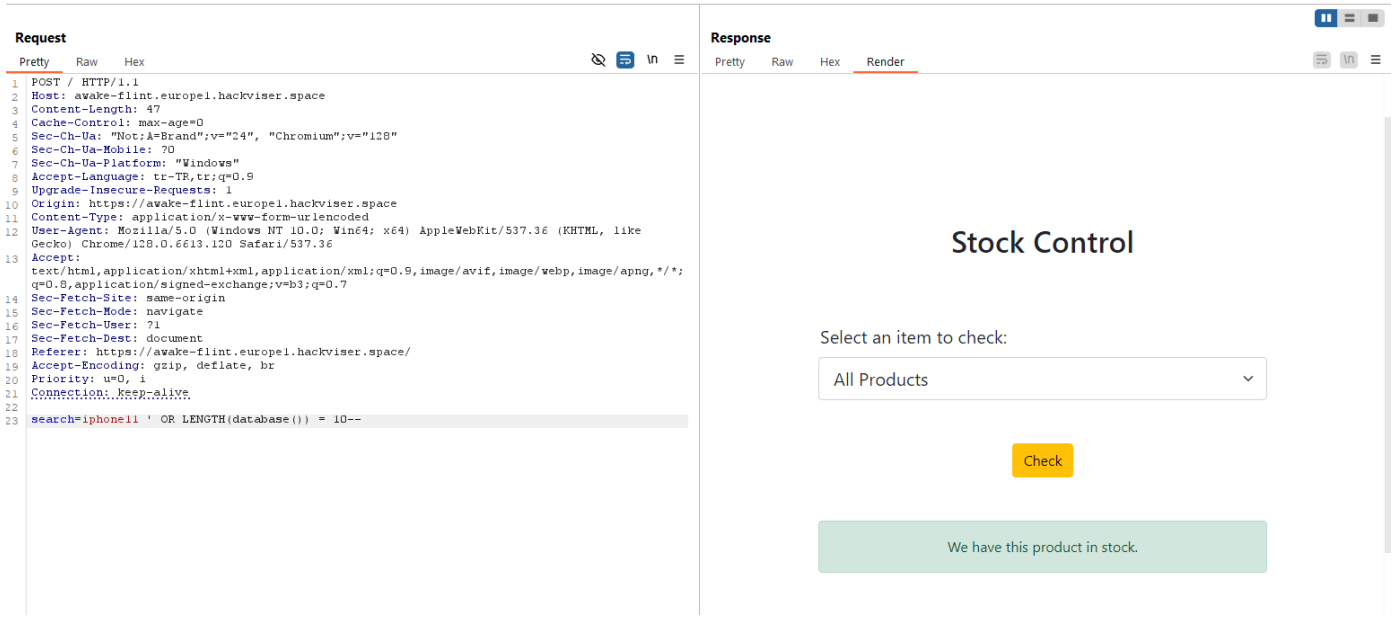


Evet, **search=iphone11 ' OR 1=2--** sorgusunu kullanarak "iphone 11 var veya 1'in 2'ye eşit olup olmadığını" sorguladık. 1 hiçbir zaman 2'ye eşit olmayacağı için bu koşul her zaman yanlış dönecek ve sistem bize "stokta yok" yanıtını verecektir. Bu şekilde, SQL enjeksiyonunun nasıl çalıştığını doğrulamış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

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

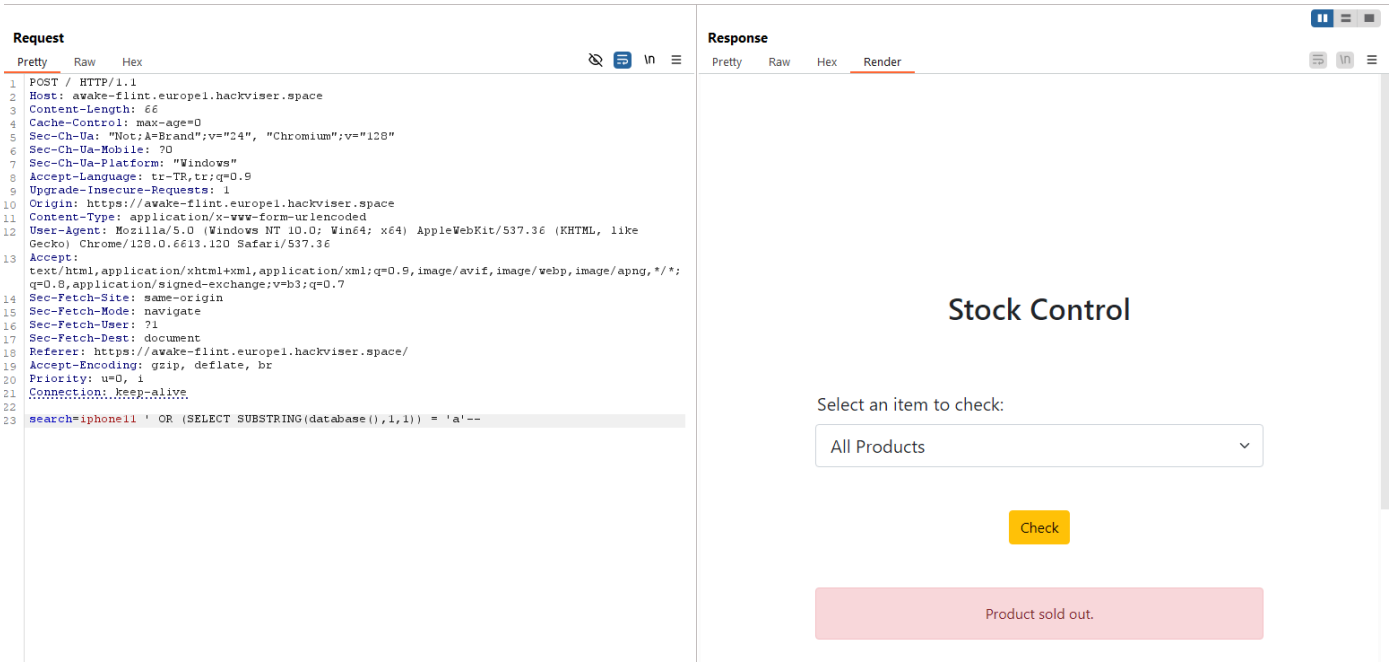


5 karakter olmadığını görüyoruz yükselterek tekrar deneyelim

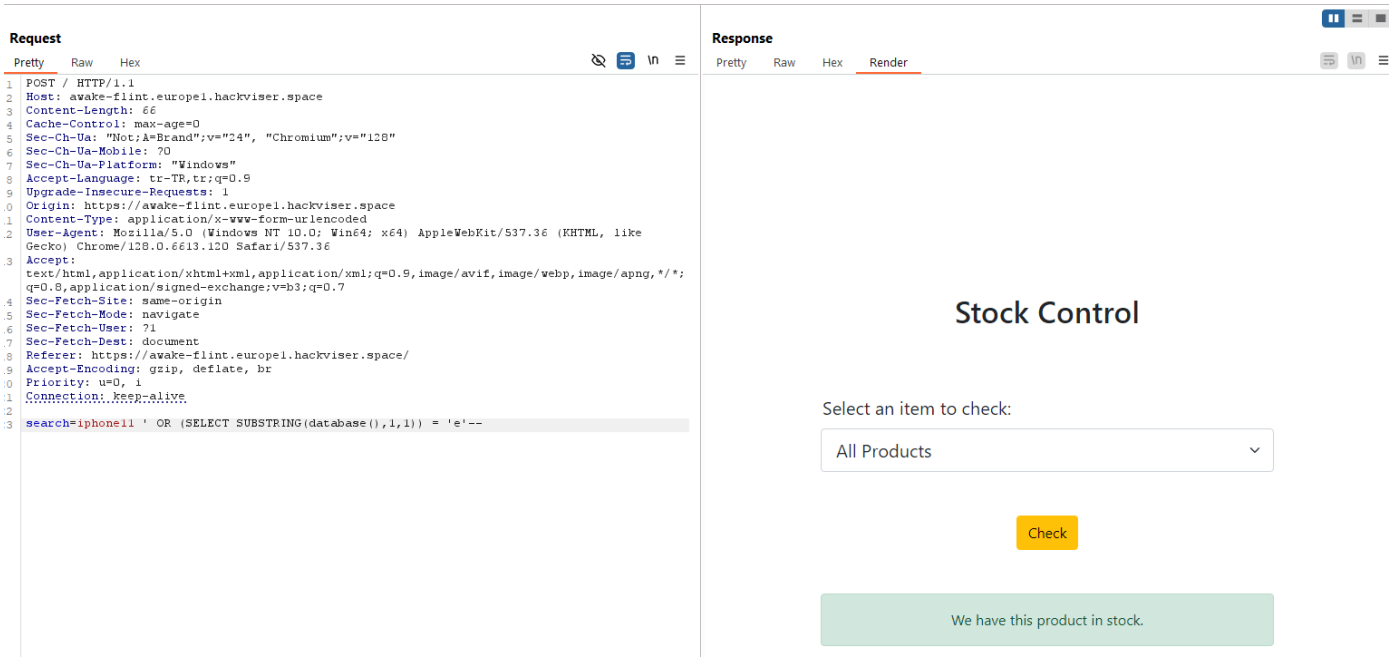


10 karakter olduğunu doğruladık şimdi sırasıyla 1 den başlayarak veri tabanının adını bulmaya çalışalım.

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



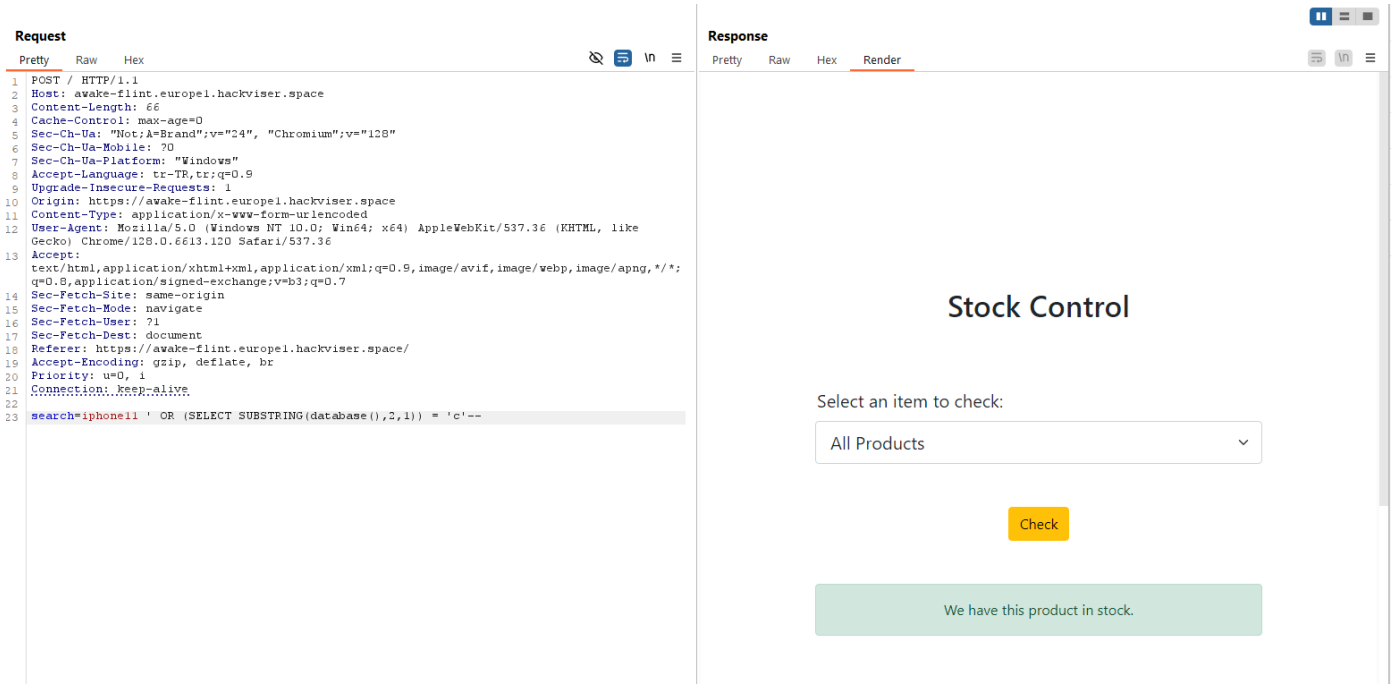
İlk olarak a denedik ve başarısız olduk



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

İnstagram

Medium

Ayberk İlbaş