UNION-BASED SQL INJECTION WRİTE-UP

Bu yazımda Hackviser platformu üzerinde bulunan Web Lab'ları içerisindeki SQL Injection kategorisindeki Union-Based SQL Injection labının çözümünü anlatacağım.

SENARYO: 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.

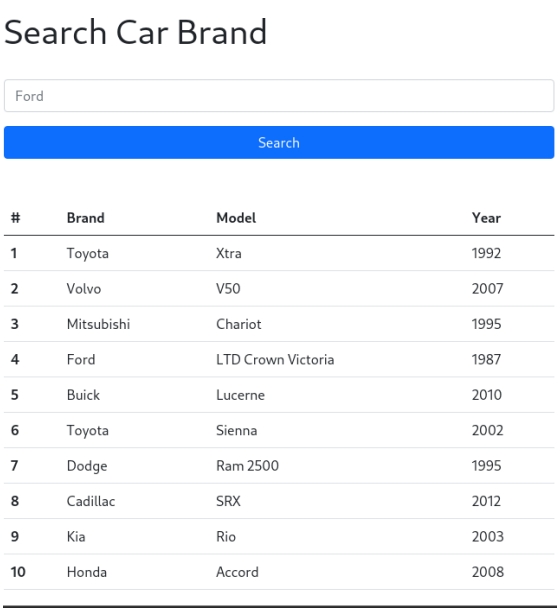
Veritabanı adı nedir?

ÇÖZÜM: Bu labı çözmek için bazı SQL komutlarını bilmemiz gerekiyor. Union ismi de oradan gelmektedir.

UNION SQL INJECTION: Ek tabloları almak için UNION tabanlı SQL enjeksiyonu anlamına gelir.

Bu saldırı, bir hacker'ın veri tabanındaki hassas olabilecek diğer tablolardan veri almak için UNION select gibi bir anahtar kelime kullanarak orijinal meşru bir sorgunun sonuçlarını ek bir sorguyla eklediği sorgulardır.

Şimdi siteye giriş yapalım.

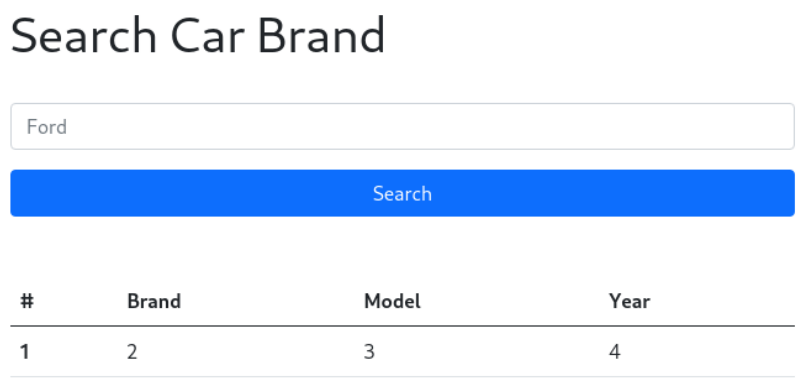


Sitede bizi böyle bir şey karşılıyor.

Şimdi de Union SQL payloadları araştırıp denemeler yapacağım.

Burada bizim kaç sütun olduğunu bulabilmemiz için "'UNION SELECT 1#" payloadını denememiz gerekiyor. Eğer hata alırsa "'UNION SELECT 1,2#" diyerek sayıyı artırmamız gerekiyor. Sayılar eşleşince sonuç alacağız.

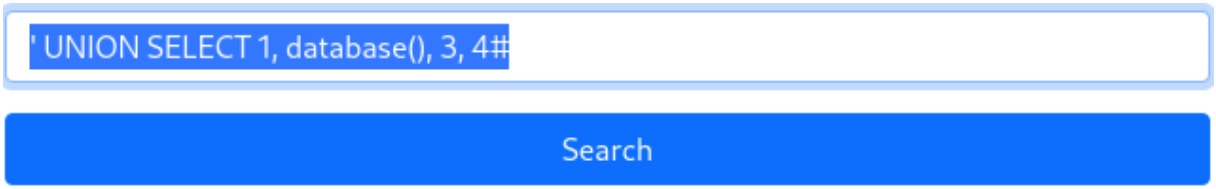
Uzunca denemeler sonucunda “'UNION SELECT 1, 2,3,4#” kodunun çalıştığını buldum sonuç şu şekilde oldu:



Toplam 4 sütunumuz varmış.

Şimdi cevaba gidebiliriz. Sayıların yerine bulmak istediğimiz cevabı yazıyoruz. Örneğin:

' UNION SELECT 1, database(), 3, 4# bize database ismini verecektir. Deneyelim:



#	Brand	Model	Year
1	ecliptica_cars	3	4

Burada cevaba ulaştık. Cevap: **ecliptica_cars**