**BOOLEAN-BASED BLIND SQL INJECTION WRİTE-UP**

Bu yazımda Hackviser platformu üzerinde bulunan Web Lab’ları içerisindeki SQL Injection kategorisindeki Boolean-Based Blind SQL Injection labınının çözümünü anlatacağım.

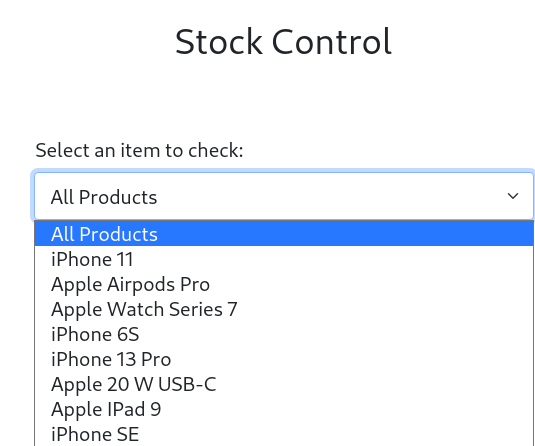
**SENARYO:** Bu laboratuvar, stok kontrol fonksiyonunda bir SQL Injection güvenlik açığı içermektedir. İş mantığı nedeniyle, sunucudan yalnızca "stokta mevcut" veya "stokta mevcut değil" yanıtı dönmektedir.

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

Veritabanı adı nedir?

*BOOLEAN-BASED BLIND SQL INJECTION: Ekrana hata mesajının yazdırılmadığı, kör olarak uygulanması gereken SQL Injection tekniğidir. “,’#< gibi karakterlerin kullanılması ile ortaya çıkar.*

**ÇÖZÜM:** Bu soruyu çözmek için Burp Suite programına ihtiyacımız olacak. Burp Suite aracını hiç bilmeyenler için [Burp Suite Nedir?](https://www.beyaz.net/tr/guvenlik/makaleler/burp_suite_nedir.html) Ziyaret edebilir.

 Böyle bir sayfamız var ve “stokta var” , “stokta yok” gibi sonuçlar dönderiyor. Örneğin iphone 6s telefonunu seçip check butonuna basıyorum.

 Stokta yok dedi.

Burp Suite programını kullanma sebebimiz labın Boolean-Based Blind SQL olmasıdır. Kaç sütun olduğunu bulmak için yine payload denemeleri yapıyorum. Union komutu yardımıyla

 Girdikten sonra sayfa Stokta olmayan ürün stokta var olarak göründü ve 2,3 yazdığımda direkt sayfa ile bağlantısı kesildiği için 2 sütundan oluştuğunu bulduk.

Bize normal şartlarda “Product sold out.” Çıktısı veriyor. Şimdi basit bir sql payload deneyeceğim.

 Şimdi çıktıya bakacağım.

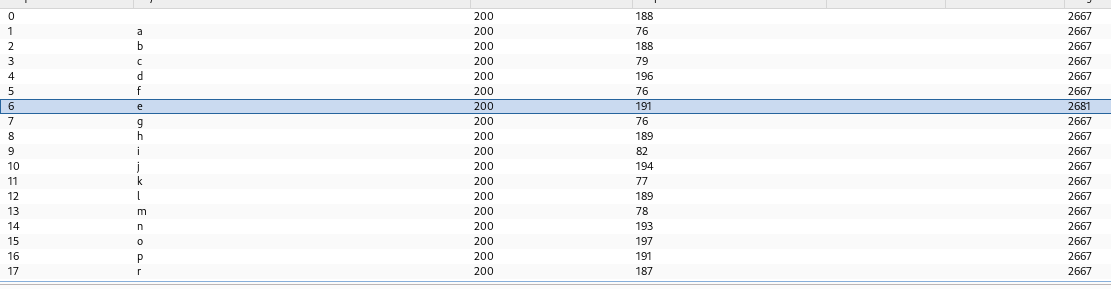


Evet, şimdi burada bir boolean based sql açığı olduğunu doğruladık. Şimdi bu açığı sömürmemiz gerekiyor ve bunun için de payload lazım.

Uzunca bir araştırma sonucu *‘ and substring(database(),1,1)=’x’#* payloadını kullanmamız gerektiğini buldum. Biz 2 tablo olduğunu bulmuştuk daha önce. Burada Intruder üzerinden brute force saldırısı yapacağız. Şimdi Intruder’i ayarlıyoruz.



Artık brute force saldırısı yapmaya hazırız.



Kendi eklediğim list ile(harfleri tek tek ekledim.) brute force saldırısı yaptık. Burada en sağ kısımdaki length uzunluğuna baktığımızda 2681 ile diğerlerinden farklı bir harf var “e”. İlk harfimizi bulduk. Şimdi ‘ and substring(database(),2,1)=’x’# yaparak 2.harfimizi bulmayı deneyelim.

Ve sonuç aldıkça bu sayıyı arttıralım.














Daha sonra çıktıda herhangi bir değişiklik olmadı ve böylelikle cevaba ulaşmış olduk.

Cevap: **echo\_store**