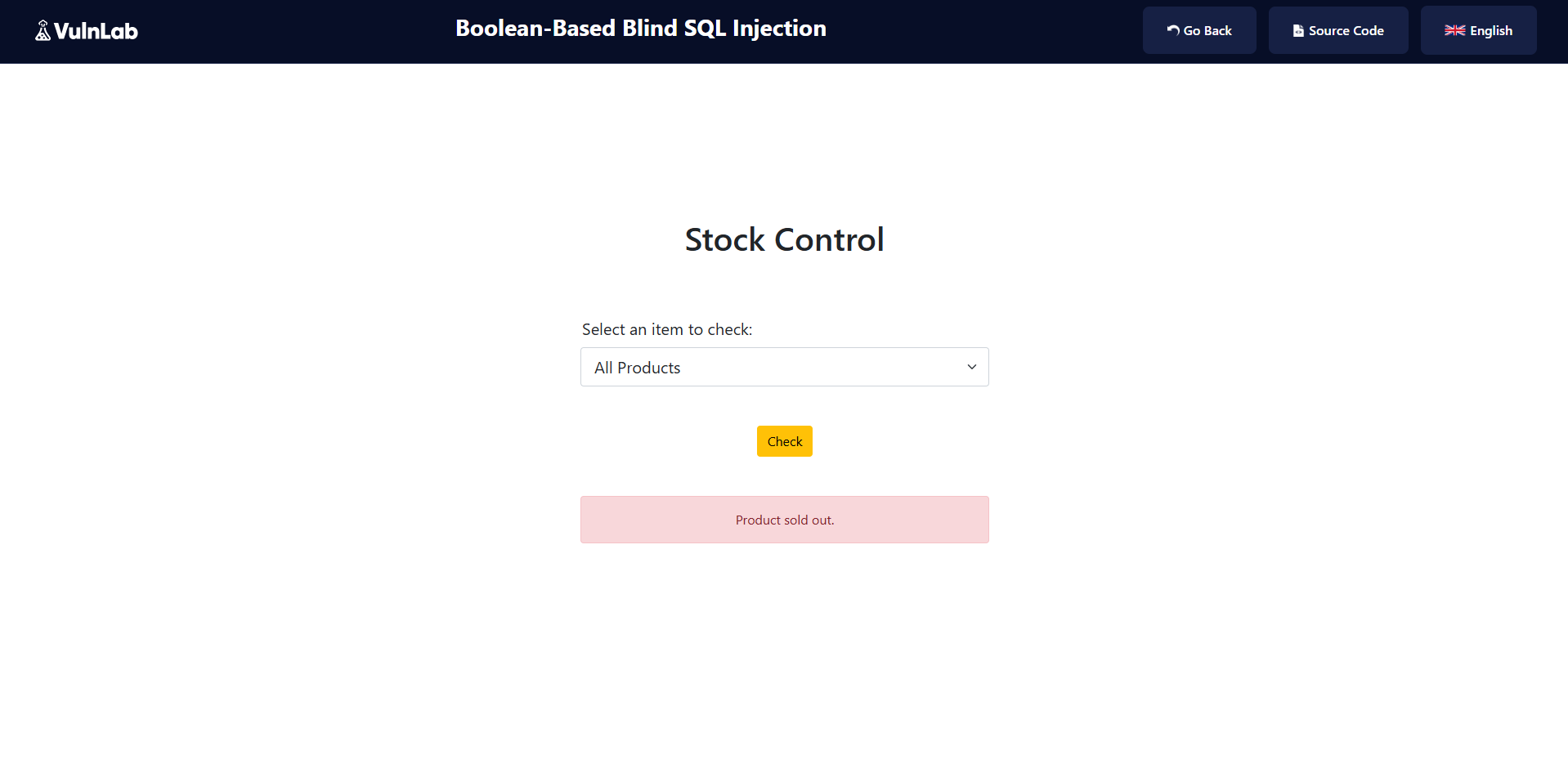
SQL Injection Lab #3 Boolean Tabanlı SQL Enjeksiyonu

**Yapacağımız bu çalışmada Docker üzerinden Yavuzlar Vulnlab SQL injection konusunun üçüncü aşaması olan boolean tabanlı sql injection konusunu ele alacağız. Web sitesine gittiğimizde aşağıdaki ekran bizi karşılıyor**:



**Öncelikle boolean tabanlı sql injection nedir onu ele alalım. Boolean tabanlı SQL Enjeksiyonu, veritabanına bir SQL sorgusu göndererek uygulamanın, sorgu TRUE veya FALSE sonucu döndürmesine bağlı olarak farklı bir sonuç döndürmesini zorlayan çıkarımsal bir SQL Enjeksiyon tekniğidir. Siteyi incelediğimizde bazı stokların olduğunu yani true, bazı stokların olmadığını yani false görüyoruz, buda bizim SQL zafiyeti aramamız için bir neden oluşturuyor. Zafiyetin kesin olduğunu anlamak için yine kaynak koduna bakıyoruz:**

**$query = $db->prepare("SELECT \* FROM stocks WHERE name = '" . $search . "'");**

**Bu satırda kullanıcıdan gelen veri doğrudan SQL sorgusuna eklenmekte. Bu durum, kullanıcı girişinin doğrulanmadan SQL sorgusuna katıldığını ve SQL Injection yapılabileceğini gösterir. Bu durumda artık manuel yöntemler yerine sqlmap i kullanabiliriz bunun nedenini ve sqlmap in kullanımını daha önce anlatmıştık. Hadi o zaman sqlmap e geçelim.**

**Sqlmap imizdeki girceğimiz komut şu şekilde olmalıdır:**

**sqlmap -u "http://localhost:1337/lab/sql-injection/post-blind-boolean/" \**

**--data="search=iphone13" -D sql\_injection -T users --dump –batch**

**Bu komut sayesinde fazla işlem yapmadan direk veri tabanının içindeki kullanıcı verilerine ulaşacağız bu parametreler bunu sağlamaktadır. Bu komutta aslında zafiyeti sömürdüğümüz yer “search=iphone13” kısmı bu kodun açıklaması ise şöyledir, bu urlyi bul, data içerisinde iphone13 ü arat, sql\_injection database klasörünü bul users yani kullanıcıların veritabanlarındaki dataları getir. Bu kodu girdikten sonra aşağıdaki gibi kullanıcı bilgileri size geliyorsa bu labıda bitirmişsiniz demektir, tebrikler.**

