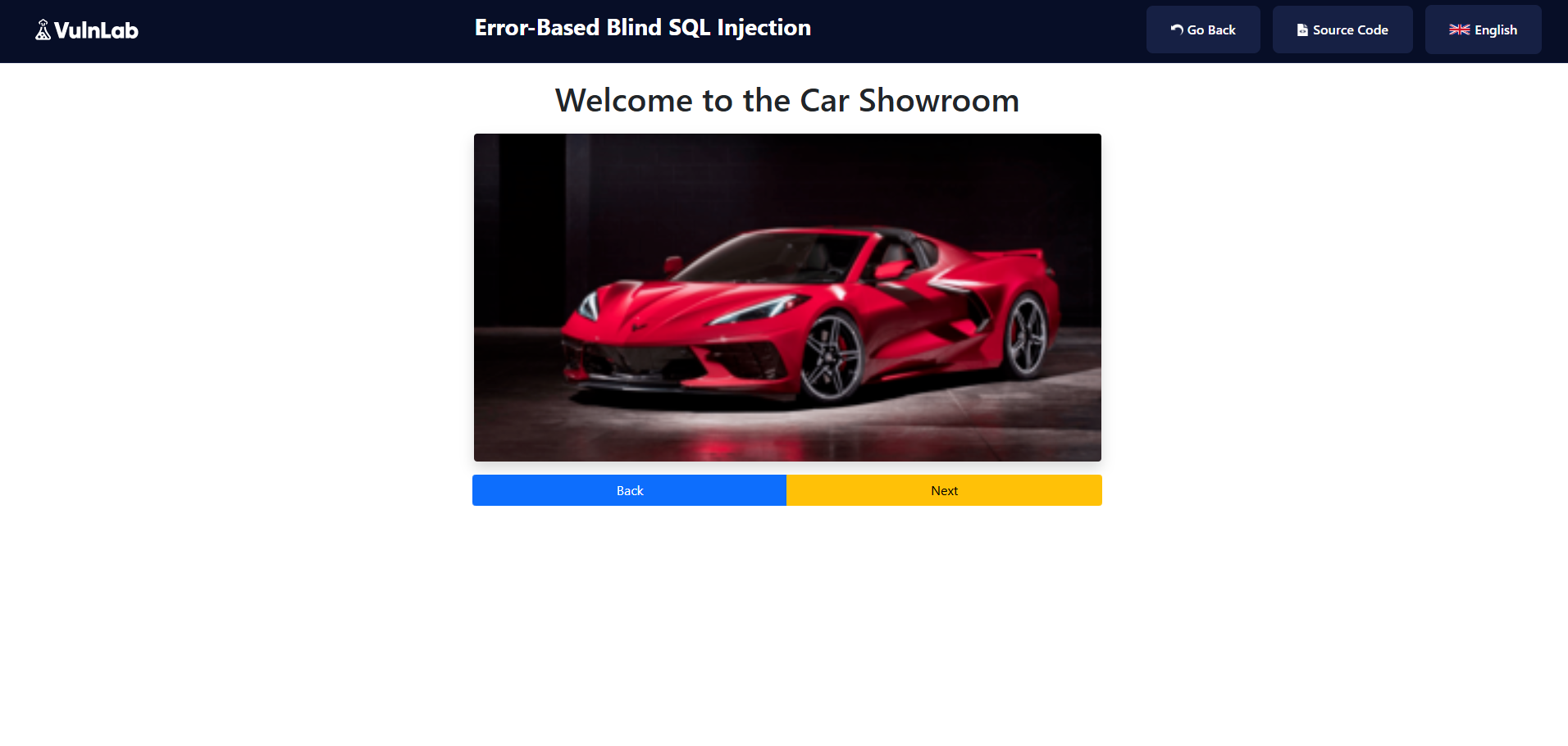
SQL Injection Lab #4 Error Tabanlı SQL Enjeksiyonu

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



**Öncelikle error tabanlı SQL enjeksiyonu nedir onu ele alalım**. **Error tabanlı SQL Injection**, **SQL Injection saldırılarının bir türüdür ve genellikle web uygulamaları veritabanı hata mesajlarını kullanıcıya döktüğünde ortaya çıkar. Bu tür bir saldırıda, saldırgan veritabanının hata mesajlarından yararlanarak veritabanının yapısı, tabloları, sütunları ve hatta bazı durumlarda verilerin kendisini öğrenebilir. Ne olduğunu öğrendiğimize göre kesin bir zafiyet olup olmadığını anlamak için kaynak kodunu inceleyelim.**

**if (isset($\_GET['img'])) {**

**$img = $\_GET['img'];**

**$user = $db->query("SELECT \* FROM images WHERE id = $img");**

**}**

**Bu kod kullanıcının url ye istediği parametreyi girebileceğini gösteriyor. Buda kullanıcın SQL injection zafiyetini sömürebileceği anlamına geliyor. O zaman yine her zamanki gibi manuel yöntemler yerine sqlmap kullanmaya geçelim.**

**Bu durumda kullanacağımız kod bu olmalıdır: sqlmap -u "http://localhost:1337/lab/sql-injection/get-blind-error/index.php?img=1" -p img --dbms=mysql --batch –dump**

**Her zamanki gibi bu koduda açıklayacağım, -u parametresi sayesinde hedef web sayfasını belirleriz, diğer parametrelerle gerekli veritabanlarını çekiyoruz veritabanımızı mysql olarak varsayıyoruz ve içinden bilgileri çekiyoruz –dump ile bu kodda asıl zafiyeti sömürdüğümüz yer ise –p img parametresidir. Eğer bu kodu girdikten sonra karşınıza aşağıdaki gibi bir ekran çıkıyorsa bu labı da başarıyla tamamladınız demektir tebrikler.**

