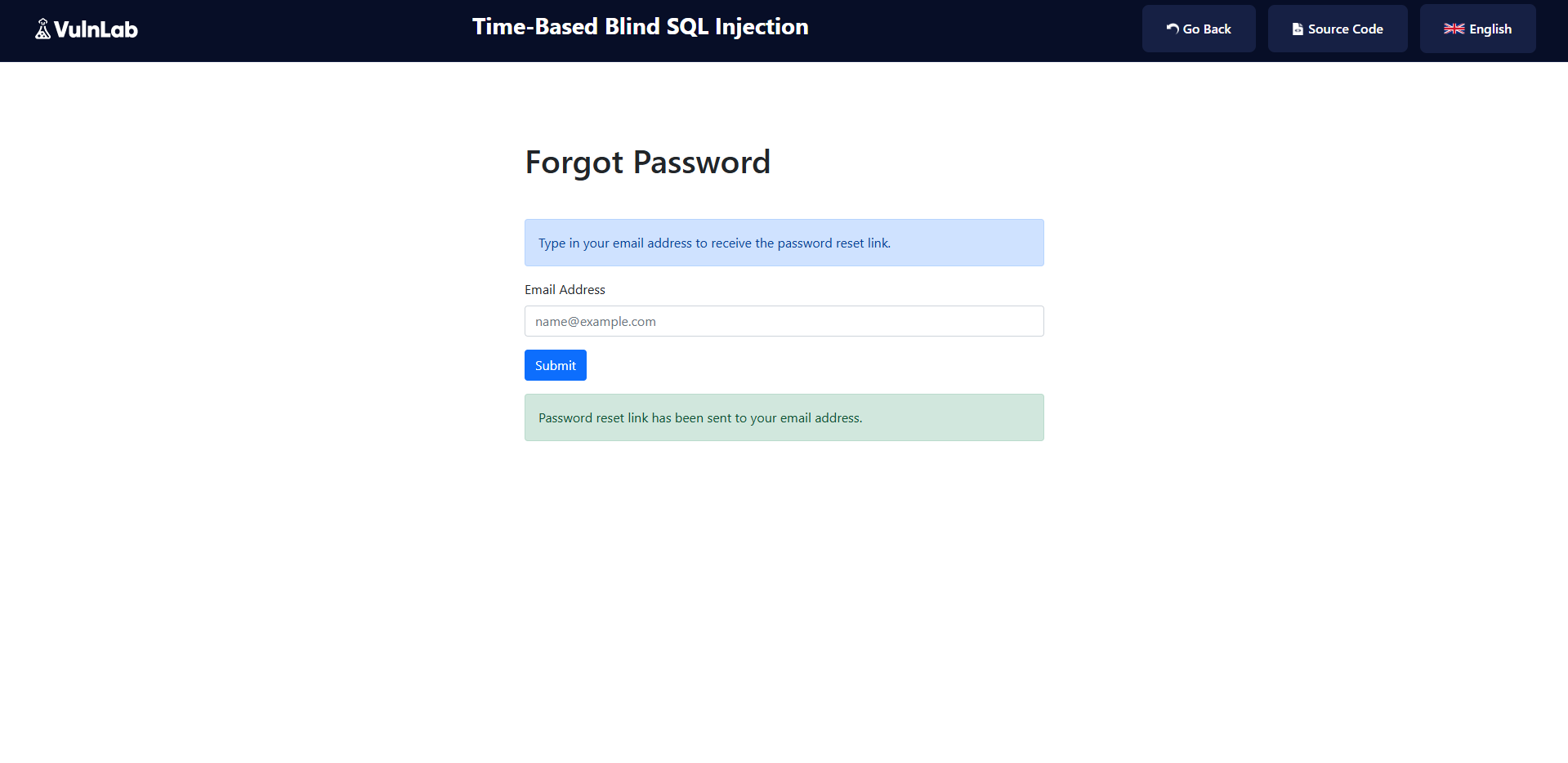
SQL Injection Lab #5 Zaman Tabanlı SQL Enjeksiyonu

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



**Öncelikle zaman tabanlı sql enjeksiyonu nedir onu ele alalım. Zaman tabanlı SQL injection, veritabanına yapılan sorgularda veritabanı yanıtının ne kadar sürede döneceğini zamanlayarak veritabanındaki bilgilerin sızdırılmasına dayanır. Bu tür saldırılar, doğru SQL sorgusunu oluşturmak için hedef sunucunun yanıt süresini kullanır. Zaman tabanlı SQL injection nın ne olduğunu anladığımıza göre her zamanki gibi kesin bir zafiyet testi için kaynak kodunu inceleyelim:**

**$user = $db -> query("SELECT \* FROM users WHERE email = '{$email}'");**

**Bu kod, kullanıcı tarafından sağlanan email parametresini doğrudan SQL sorgusuna ekler. Bu ise bize sql injection açığı olduğunu gösterir artık zafiyeti sömürmek için zaman tabanlı sql enjeksiyonunu kullanarak sqlmap ten devam edebiliriz.**

**Bu durumda kullanmamız gereken sqlmap kodu şu olacaktır:**

**sqlmap -u "http://localhost:1337/lab/sql-injection/post-blind-time/" --data="email=test@example.com" --technique=T --time-sec=5 --dump –batch**

**Bu tekniğin özelliği yavaş olmasıdır çünkü sunucudan zaman gecikmesi yaparak verileri çekmemizi sağlar. Bu kod sayesinde ise verileri direk ekranınızda göreceksiniz. Kodun parametrelerinin açıklaması ise şöyledir:**

**-u: Hedef URL'yi belirtir.**

**--data="email=test@example.com": POST verisini belirtir, bu durumda email parametresini test ederiz.**

**--technique=T: T (Time-based) seçeneği zaman tabanlı SQL Injection testini yapar.**

**--time-sec=5: Sunucudan 5 saniye gecikme bekler.**

**--dump: Elde edilen veritabanı içeriğini doğrudan ekrana döker.**

**--batch: Kullanıcı etkileşimi olmadan otomatik olarak işlem yapılmasını sağlar.**

**Eğer ekranızda teker teker arama yapılıp en sonunda şifreleri bulup karşınıza çıktıysa tebrikler bu bölümü tamamlamışsınız demektir.**