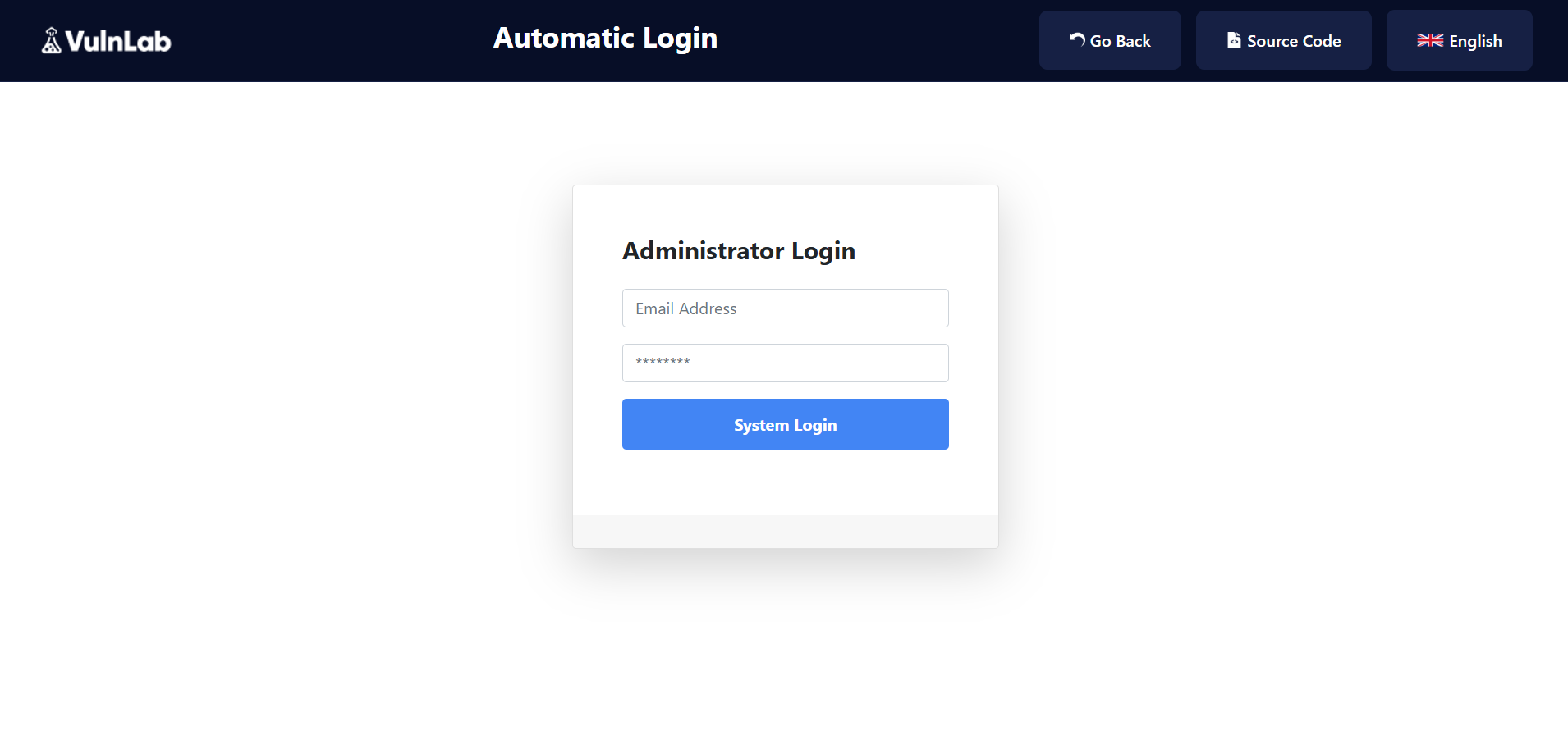
SQL Injection Lab #1 Sisteme Giriş Yapmayı Denemek

**Yapacağımız bu çalışmada Docker üzerinden Yavuzlar Vulnlab SQL injection konusunun birinci aşaması olan sisteme giriş yapmayı denemek konusunu ele alacağız. Web sitesine gittiğimizde aşağıdaki ekran bizi karşılıyor**:



**Öncelikle SQL injection nedir, onu ele alalım. SQL injection, web sayfasının veritabanlarına uygulama sayesinde bir başkası tarafından gönderilen SQL sorgularını kendi istediği şekilde manipüle ederek sisteme giriş yapmasıdır. Peki bu sayfada SQL injection olup olmadığını nasıl anlarız? Bunu anlamak için kaynak kodunu inceleyebilir, manuel yollarla deneyebilir veya çeşitli araçlar kullanabiliriz.**

**Manuel yollarla sistemi manipüle etmek için, sistemi şaşırtıcı özel karakterleri login kısmına girmeliyiz. Yönetici girişi olduğu için de email kısmına “admin” yazmamız yeterli olacaktır. İşte örnek payloadlar:** <https://github.com/payloadbox/sql-injection-payload-list>**. Eğer sisteme direkt giriş yaparsa ya da “SQL syntax error”, “mysql\_fetch”, “unclosed quotation” gibi hatalar görürsek, SQL injection zafiyeti olma ihtimali çok yüksektir.**

**Kaynak kodunu incelemek istersek bir SQL sorgusuyla karşılaşıyoruz:**

**$sql = "SELECT username,password FROM users WHERE username='" . $usr . "' AND password='" . $pwd . "'";**

**Bu kod klasik bir SQL sorgusudur ve sistemde SQL injection zafiyeti olduğunu gösterir. Bu koddaki değişkenler “$pwd” ve “$usr” doğrudan sorguya ekleniyor, yani kullanıcı formuna ne yazarsak doğrudan SQL'e gidiyor. Bu, verilerin doğrulanmadan SQL'e aktarıldığını belirtir. Demek ki biz kullanıcı formuna aşağıdaki gibi bir payload yazarsak:' OR '1'='1 -- o zaman kod şuna dönüşür:**

**$sql = "SELECT username,password FROM users WHERE username='' OR '1'='1' – AND password=''";**

**SQL’de mantıksal operatörlerin sırası şöyledir: 1. AND, 2. OR. Bu yüzden sorgu şu şekilde çalışır:**

**$sql = "SELECT username,password FROM users WHERE username='' OR '1'='1' -- ' AND password=''";**

**Ve bu sayede -- ile SQL sorgusunun geri kalanı (özellikle şifre kontrolü) yorum satırına dönüşür. Artık sistem şifresiz olarak giriş yapabilir. Görevi tamamladığınızda aşağıdaki gibi bir ekran çıkarsa tebrikler, görevi tamamladınız.**

