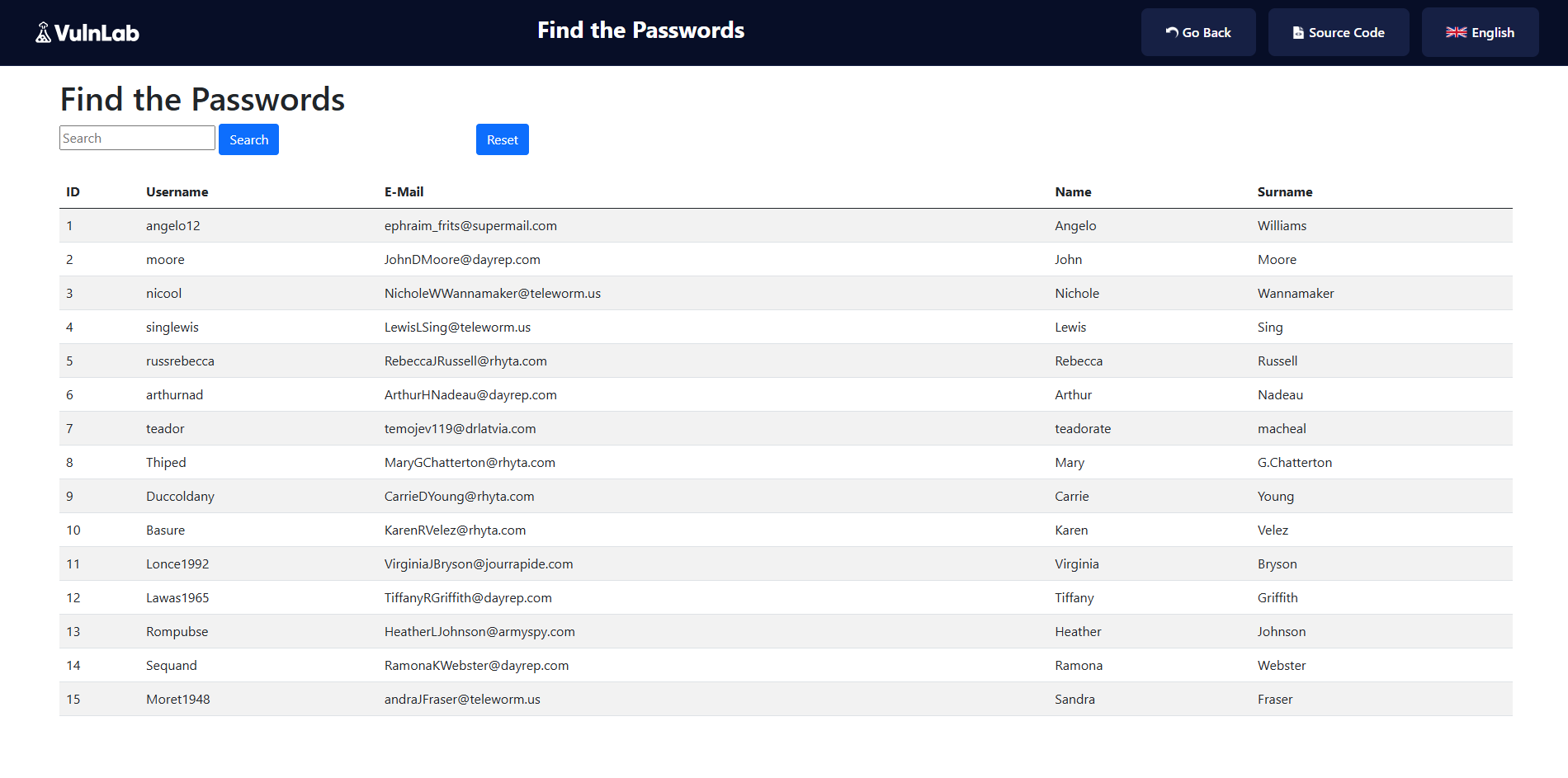
SQL Injection Lab #2 Şifreleri Bulmak

**Yapacağımız bu çalışmada Docker üzerinden Yavuzlar Vulnlab SQL injection konusunun ikinci aşaması olan şifreleri bulmak konusunu ele alacağız. Web sitesine gittiğimizde aşağıdaki ekran bizi karşılıyor**:



**Bu aşamada sistem veritabanındaki kullanıcı bilgilerini dışarı çıkarmaya çalışacağız. Bunun için SQL injection zafiyetinden yararlanarak kullanıcı adlarını ve şifrelerini ele geçirmeyi hedefliyoruz. Öncelikle SQL injection ile veritabanından nasıl veri çekileceğini anlamamız gerekiyor. SQL injection, geliştiricinin kullanıcıdan gelen veriyi doğrudan SQL sorgusuna yerleştirmesi sonucu oluşur. Bu zafiyet sayesinde saldırgan, veritabanına kendi sorgularını ekleyebilir ve sistemin vermemesi gereken bilgileri alabilir.** **Sayfayı analiz ettiğimizde giriş ekranında yalnızca kullanıcı adı girmemiz isteniyor. Şifre kısmı bulunmuyor. Bu da bize, girilen kullanıcı adının veritabanından çekilerek arka planda listelendiğini gösteriyor. Bu verilere ulaşmak için manuel yöntemler kullanabiliriz, fakat bu yöntem uzun sürebileceğinden bir SQL injection aracı olan sqlmap ‘ i kullanacağız. Bu aracın ne işe yaradığını, işlevini ve hangi makinede bulunduğunu konuşmadan önce kaynak kodumuzu inceleyelim ve bir açık olup olmadığını kontrol edelim.**

**$query = $mysqli->query("SELECT \* FROM users WHERE name LIKE '%" . $\_GET['search'] . "%'");**

**Kaynak kodu incelediğimizde karşımıza böyle bir kod çıkıyor. Bu kod search yani arama kısmının doğrudan sql sorgusunun içine eklendiğini gösteriyor. Yani sistemde SQL injection açığı vardır. Açığı tespit ettiğimize göre artık sqlmap aracını anlatmaya başlayabiliriz.**

**Sqlmap, açık kaynak kodlu sql injection açıkları tespit ve istismar etme aracıdır. Kendisine sağlanan hedef web uygulamasının kullandığı veri tabanı sistemine gönderdiği çeşitli sorgular/komutlar ile sistem üzerindeki sql injection tipini tespit eder. Yine kendisine sağlanan parametrelere göre çeşitli bilgileri hedef veri tabanından alır. Yani aslında Sqlmap bizim manuel olarak yaptığımız girdi ve komutları kendisi binlercesini otomatik olarak dener ve açığı bulur. Daha sonra biz istediğimiz bilgilere erişmek için (örn: passwords, databases) belirli parametreler gireriz ve istediğimiz bilgilere ulaşırız. İşte bazı Sqlmap parametreleri:**

**SQLMAP İle Hedef Hakkında Elde Edilebilen Veriler:​**

**Veritabanı türü ve versiyonu (–banner,–all)​**

**Mevcut kullanılan veritabanı ve erişilebilen tüm veritabanı isimleri (–current-db, –dbs)​**

**Veritabanı tabloları(tables) ve bu tablolara ait kolonları(columns) (–tables, –columns)​**

**Veritabanı datası(–dump, –dump-all)​**

**Veritabanı mevcut kullanıcısı ve tüm kullanıcılar(–current-user,–users)​**

**Veritabanı kullanıcı parolası (–passwords)​**

**Veritabanı kullanıcısının DB admin olup olmadığı bilgisi(–is-dba)**

**Hedef sunucu hakkında bilgi(İşletim sistemi, Uygulamanın kullanıldığı teknoloji vs. , -f)​**

**SQLMAP İle Farklı Tiplerde Hedef Belirtilebilmektedir:**

**​**

**URL (–url, -r )​**

**Burp suite ve WebScarp proxy logu (–log , -l)​**

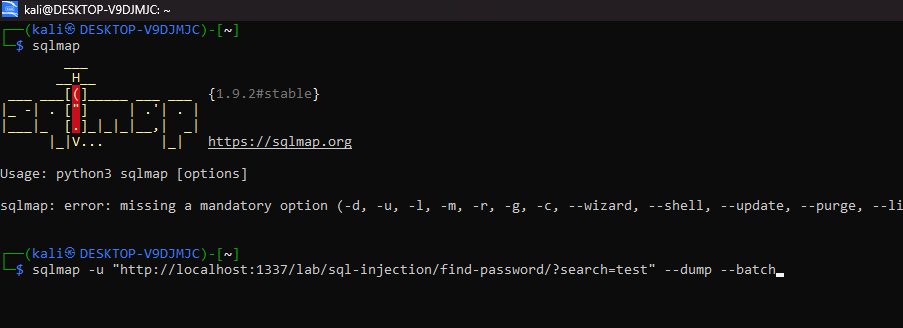
**HTTP talepleri bir dosyadan okutulabilmektedir. (–r)​**

**Google üzerinden URL toplayıp input olarak alabilmektidir.(-g)​**

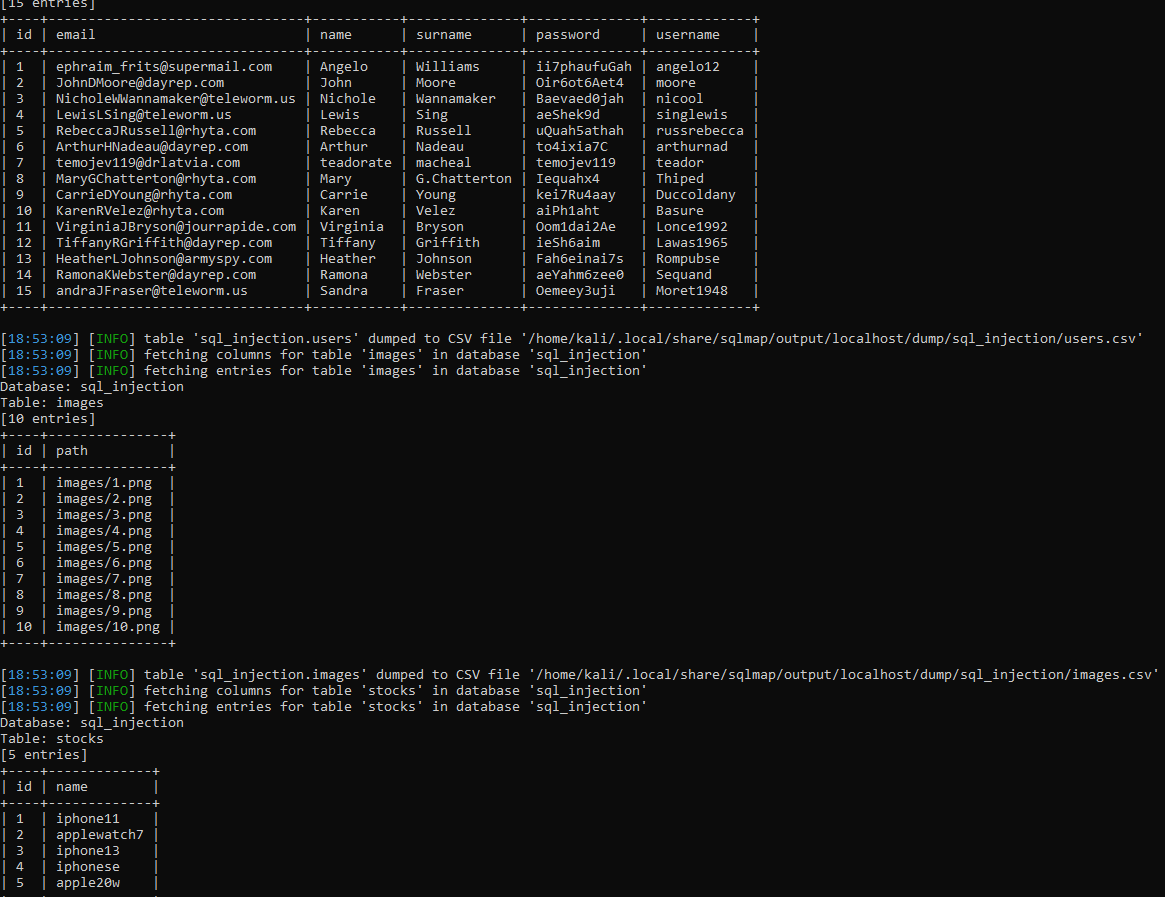
**/sqlmap/sqlmap.conf dosyası -c parametresi ile verilerek tüm konfigrasyon input olarak verilebilir. (-c)**

**Sqlmap ‘ in ne olduğundan ve parametrelerinden bahsettik şimdi diğer adımlara geçebiliriz.**

**Sqlmap gibi araçlar genellikle kali Linux gibi işletim sistemlerinde hazır olarak mevcuttur, fakat sizde mevcut değil ise araştırarak kurulum yapabilirsiniz. Öncelikle arama kısmına herhangi bir şey yazıp bir sonuç döndürmeyen bir kelime yazarak örneğin “test” bir url elde etmeliyiz. Daha sonra bu url yi sqlmap aracında kullanmak için –u parametresinden yararlanacağız ayrıca –-dump ve –batch gibi parametreler kullanarak işlemlerin yapılmasını ve veritabanı datasını almış olacağız artık sqlmap i çalıştırabiliriz.**



**Bu işlemi gerçekleştirdikten sonra veriler aşağıdaki gibi gelecektir:**



**Eğer verileriniz bu şekilde geldiyse tebrikler parola ve şifrelere eriştiniz demektir.**

**☺☺☺**