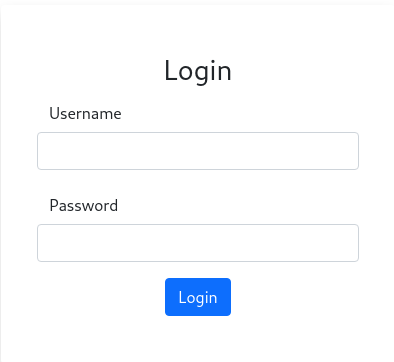
**BASIC SQL INJECTION WRİTE-UP**

Bu yazımda Hackviser platformu üzerinde bulunan Web Lab’ları içerisindeki SQL Injection kategorisindeki Basic SQL Injection labınının çözümünü anlatacağım.

**SENARYO:** Bu laboratuvar, oturum açma işlevinde bir SQL Injection güvenlik açığı barındırmaktadır. Laboratuvarı çözmek için, bir SQL Injection saldırısı gerçekleştirerek oturum açma adımını atlayın.

Sky Raincin adlı kullanıcının e-posta adresi nedir?

**ÇÖZÜM:**

**** Elimizde bir login sayfası var ve SQL Injection olduğunu biliyoruz.

*SQL INJECTION: Bu güvenlik açığı çok ciddi bir güvenlik açığıdır. Direkt veritabanına erişim sağlamamıza yarar. Veritabanlarına erişmek de her zaman en kritik açık olmuştur.*

SQL INJECTION payload olarak en çok kullanılan payload (' or 1=1 # ) kullanılır. Payload’ın içeriğini kısaca açıklayayım.

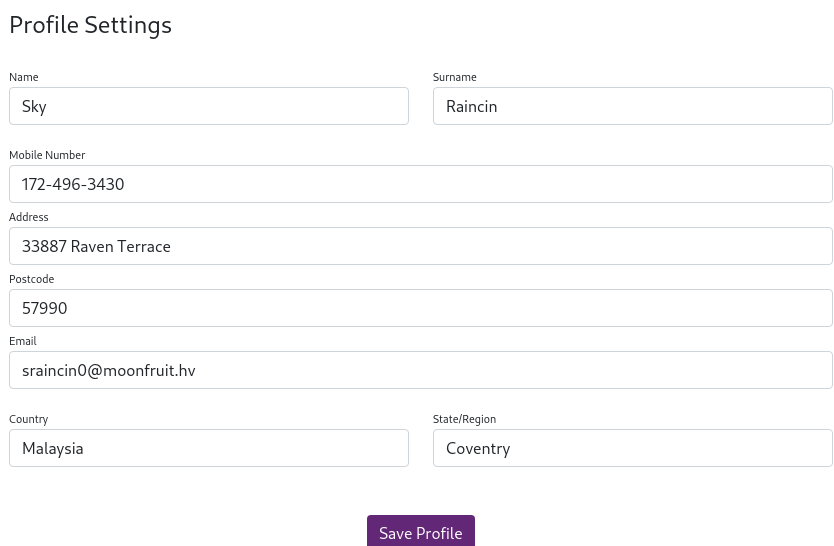
‘ : Önceki yazılan tüm kodları yorum satırı içerisine alır.

Or: Şart ifadesidir , “veya” anlamı taşır.

1=1: or ifadesinden sonra yazdığımız koşuldur. Doğru bir ifadedir. Bir önceki kodlarda sorunlar olsa da 1=1 ifadesi doğru olduğu için SQL açığı varsa komut çalışacaktır.

#: Bu ifade de sonrasında yazılan tüm komutları yorum satırı yapmaya yarar.

Şimdi payloadımızı deneyerek içeri girmeye çalışıyoruz.

 İçeri girmeyi başardık. Cevaba bakalım.

**sraincin0@moonfruit.hv**