**DICTIONARY ATTACK WRİTE-UP**

Bu yazımda sizlere Hackviser platformu üzerinde bulunan Web Lab kısmı altında Broken Authentication zafiyetinin Dictionary Attack labının çözümünü anlatacağım.

**SENARYO:** Bu laboratuvar, zayıf parolaya sahip bir oturum açma sayfası içerir.

Laboratuvarı tamamlamak için, sözlük saldırısı ile "admin" kullanıcısının şifresini bulun.

**"admin" kullanıcısının parolası nedir?**

**ÇÖZÜM:** Siteye giriş yapalım. Bizi bir login sayfası karşılıyor. Burada bir şeyler girmeyi deneyip Burp Suite aracında yakalayalım.

 Bizi ilgilendiren kısım burası.

Şimdi kullanıcı adını biliyoruz ve şifreyi bulacağız. Bunun için de brute-force yapacağız. Ben bunun için hydra aracını kullanacağım.



Burada önemli bazı kısımlara değineceğim.

-l: kullanıcı adı belirtiyoruz.

-P: şifre kısmıdır. Daha sonrasında yazdığımız kullanmak istediğimiz wordlist dosyasıdır.

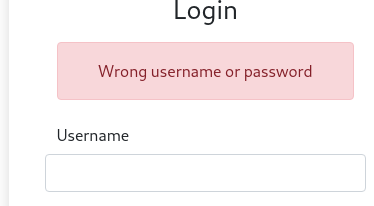
Burada wordlist dosyasında 500-worst-password-txt kullanmamın sebebi bize soruda verdiği ipucudur. Soruda bize (zayıf parolaya sahip bir oturum açma sayfası içerir.) dediğinden dolayı.

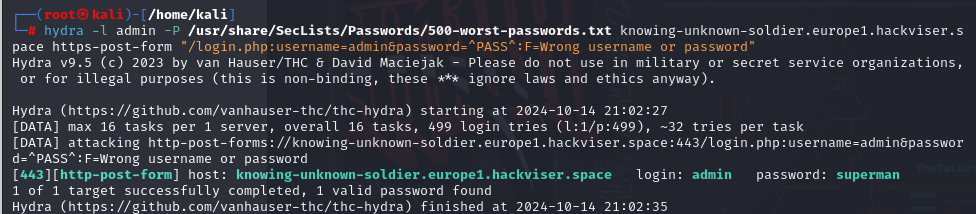
Daha sonra saldırı yapacağımız siteyi belirtiyoruz.

https-post-form: Login’de deneme yaparken POST kullandığımızı belirtiyoruz. Üstteki fotoda gördük.

*"/login.php:username=admin&password=^PASS^:F=Wrong username or password"*

*Burası önemli. Burada login.php sayfa URL’sinden aldım. Username:password formatını düzgün yazılması gerekiyor ve ayrıca :F’den sonra yanlış deneme sonucu bize ne olarak dönüş yaptığını girdik.*

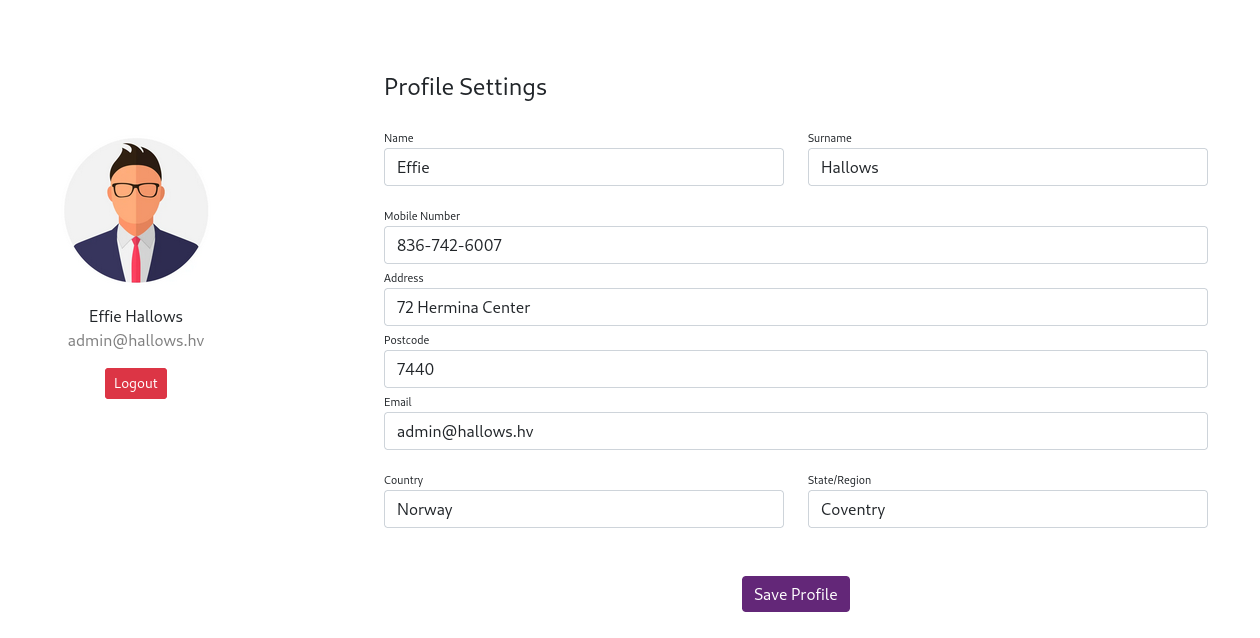
* Burada da göründüğü gibi. Şimdi aracımızı başlatalım.*



Evet, cevaba ulaşmış olduk böylelikle.

CEVAP: **superman**

Giriş yaparak şifrenin doğru olup olmadığını kontrol edelim.



Böylelikle labımızı çözmüş olduk.