

## Broken Authentication

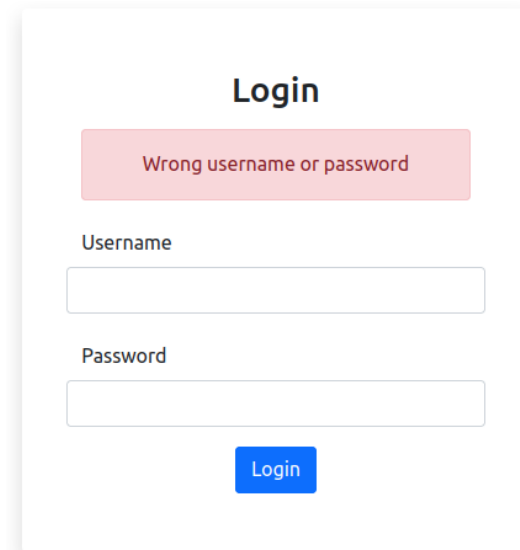
**Nedir;** bir uygulamanın kullanıcı kimlik doğrulama mekanizmalarında zayıf noktaların bulunması sonucu ortaya çıkan zafiyet türüdür.

**Önlem;** güçlü parola politikaları uygulanmalı, çok faktörlü kimlik doğrulama kullanılmalı ve oturum süreleri sıkı bir şekilde kontrol edilmelidir.

### 9.1 Dictionary Attack

**Bizden istenilen:** "admin" kullanıcısının parolası nedir?

Bunun için elimizde tek bir info var o da kullanıcı adını bilmemiz, internetten , bir tane password listesi buldum onu deniyeceğim, burada Burp Suite üzerinden gösterecem.



İntruder'a gönderdim ve seçtim.

password değerini



Denenmesi gereken parolaları yazdım, ve saldırıyı başlatıyorum.

Bana response olarak dönen durum kodlarını inceliyorum ve 1 adet yönlendirme olan 302 kodu var gerisi başarısız istek, superman'ı deniyelim.

Ve giriş yapıyoruz

Payload	Status code
superman	302
11111	400
asdasd	400
password	400
admin	400
123	400
12345	400
123	400
123	400
123	400

Username

admin

Password

superman

Login



Effie Hallows  
admin@hallows.hv

Oturumu kapat

#### Profil Ayarları

İsim	Effie	Soyadı	Hallows
Cep numarası	836-742-6007		
Adres	72 Hermina Center		
Posta kodu	7440		
E-posta	admin@hallows.hv		
Ülke	Norway	Eyalet/Bölge	Coventry

Ve  
cevabını bulduk.  
**Cevap : superman**

sorumuzun