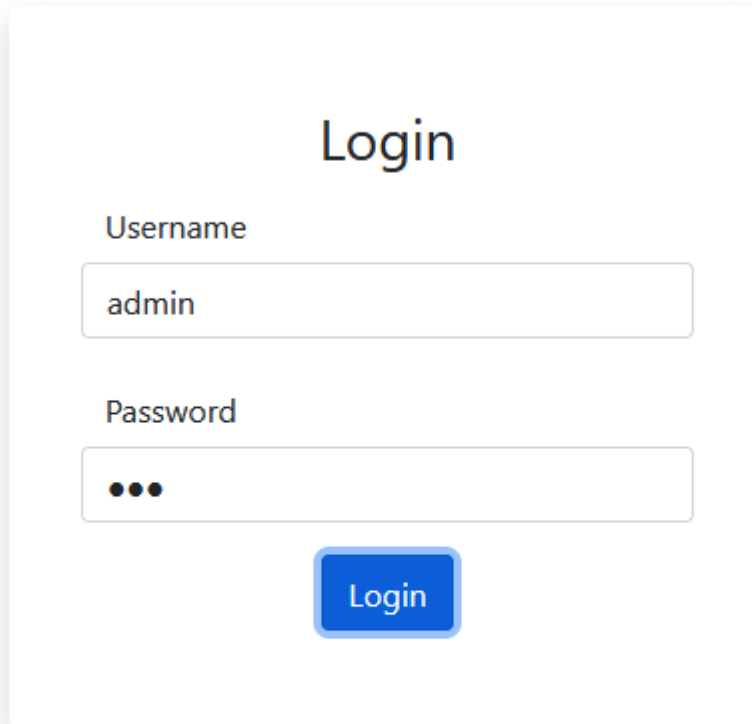


Broken Authentication

Genellikle basit yapılan parolaların brute force yöntemiyle veya tahmin edilebilir şifre denemeleriyle çözülmesi ve asıl kullanıcı yerine giriş yapmasına sebep olan bir zafiyettir. Daha önceki write up'larımızda da yazdığımız gibi Çerezlerin kullanımı nedeniyle de erişim yapılabilir. Bu kısımda da oturum süresinin kısa olmamasından dolayı veya çerezlerin doğru bir şekilde korunmaması (Token kullanılmaması) gibi nedenlerden de kaynaklanabilir.

Örnek senaryomuzda, zayıf parolayı geçip adminin şifresini öğrenmeye çalışıyoruz.



The image shows a login form with a white background and a light gray border. At the top, the word "Login" is centered in a large, dark gray font. Below it, there are two input fields. The first field is labeled "Username" and contains the text "admin". The second field is labeled "Password" and contains three black dots, indicating a password. Below the password field is a blue button with the word "Login" in white text.

```
Target: https://sensible-manta.europel.hackviser.s

1 POST /login.php HTTP/1.1
2 Host: sensible-manta.europel.hackviser.s
3 Cookie: PHPSESSID=ru3r2t2iolmk46r0bes4t8c
4 User-Agent: Mozilla/5.0 (Windows NT 10.0;
5 Accept: text/html,application/xhtml+xml,e
6 Accept-Language: tr-TR,tr;q=0.8,en-US;q=C
7 Accept-Encoding: gzip, deflate, br
8 Content-Type: application/x-www-form-urle
9 Content-Length: 27
10 Origin: https://sensible-manta.europel.ha
11 Referer: https://sensible-manta.europel.h
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17 Priority: u=0, i|
18 Te: trailers
19 Connection: keep-alive
20
21 username=admin&password=$aaa$
```

User name admin yapıyoruz ve password kısmını elimizde daha önce aldığımız 10K wordList adlı txt dosyamızı intruder'a atarak denemeye başlıyoruz. Bu tür şifre veya username isimlerini internetten bulabilirsiniz. Admin ismini, administrator, menager, root gibi kelimelerle değiştirebilirsiniz de. Bende pro özelliği olmayacağından uzun sürmesini ön görerek devam etmedim.