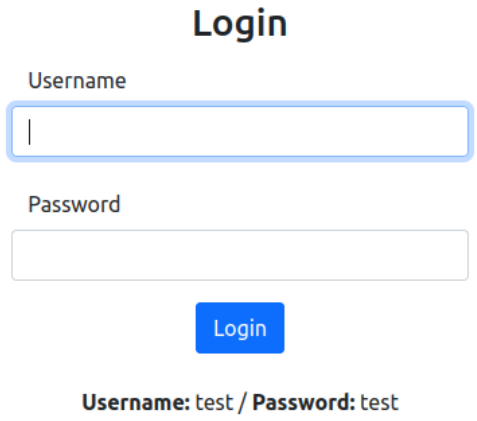
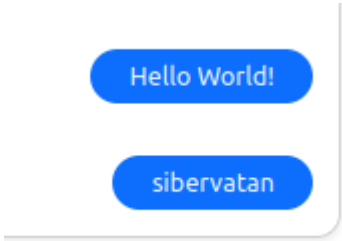
XSS

1.2 Stored XSS Nedir ;Stored XSS, zararlı kodun sunucuya kaydedilip daha sonra kullanıcılar tarafından görüntülendiğinde çalıştırıldığı bir güvenlik açığıdır. Bu saldırı, veritabanına kaydedilen içerikle kalıcı hale gelir ve birçok kullanıcıyı etkileyebilir.
Önlem İçin Tavsiye ; Kullanıcı girdilerini doğrulayıp temizlemek, veritabanına kaydetmeden önce tehlikeli karakterleri güvenli hale getirmek ve HTML kodlaması uygulamak bu saldırıyı önler.
Bizlere bir url web sitesi paylaşılıyor ve login kısmı ile karşılaşıyoruz , bizlerede test:test adında bir kullanıcı var olduğunu yazmışlar giriş yapalım.



Ve giriş yapınca şu şekilde bizleri bir alan karşılıyor.

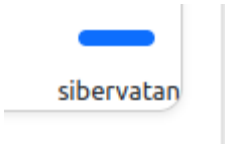
SiberVatan yazıp kaynak kodu inceliyelim.

Evet yorumuzun mesaj 

uygulamasının ekranında gözüküyor ve kaynak koda bakalım.

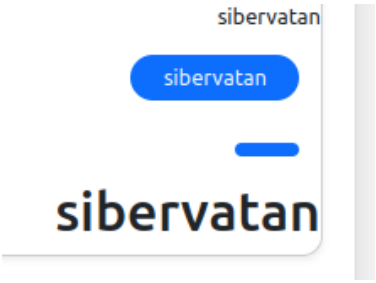
```
<div class="msg col-md-6 m-3 px-4 bg-primary text-wrap " style="border-radius: 20px; padding: 5px;width: fit-content;color: aliceblue;">Hello World!</div><div
-6 m-3 px-4 bg-primary text-wrap " style="border-radius: 20px; padding: 5px;width: fit-content;color: aliceblue;">sibervatan</div>            </div>
```

Burada bir mesaj olarak alması için konumunu , html kodları var.
Her mesaj sonunda 2 defa kapanıyor olarak gözüküyor bu resimden fazlalık gibi görünebilir ama üst kodların devamı. Az önceki gibi ** ** yapıp çıkmaya çalışalım.

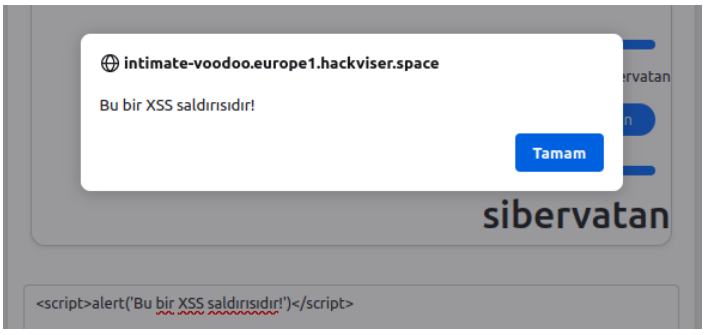
Bu şekilde görünüyor. Daha farklı 

şeylerde deniyelim.

** <h1>sibervatan </h1>**



Şu şekilde oynamalar yaptım ama halen cevabımız bu değil, “ **Stored XSS** ” de her kullanıcı sayfaya geldiğinde veya yenilediğinde çıktı çıkartmayı sağlamamız lazım. Az önce Reflected’de payloadı biz yazarak alert alıyorduk.

Ve yaptık her 

sayfayı yenilediğimizde bu kod veritabanına kaydolduğundan ötürü her kullanıcıya bu alert çıkabilir.

Çözüm: <script>alert('Bu bir XSS saldırısıdır!')</script>