

## STORED XSS WRITE-UP

Bu yazımda Hackviser platformu üzerindeki Web Lab kısmında bulunan XSS labı içerisindeki Reflected XSS labının çözümünü anlatacağım.

**SENARYO:** Bu laboratuvar Stored XSS (Cross-Site Scripting) zafiyeti örneğidir. Websitesinde bulunan sohbet ekranından gönderdiğiniz mesajlar sunucu tarafında filtrelenmeden veritabanına kaydedilmektedir.

Bir mesaj göndererek tüm kullanıcılarda XSS zafiyetini tetiklemenin bir yolunu bulun.

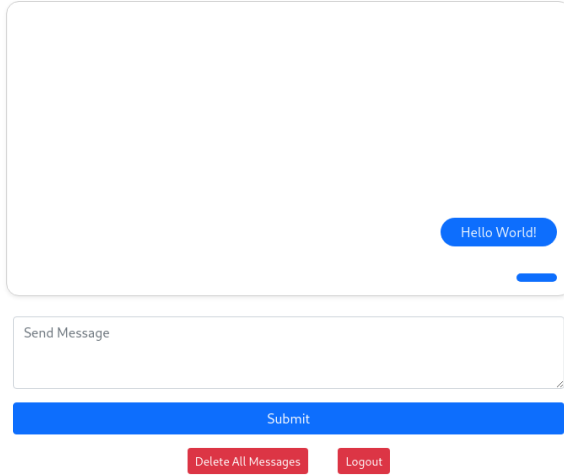
*STORED XSS: En tehlikeli XSS saldırısı olan bu türde saldırıya izin veren kod sunucuda tutulur ve otomatik olarak yürütülür.*

*Bir web uygulamasının veri giriş noktalarında eğer denetleme/filtreleme/bloklama mekanizması yine yoksa ve saldırganın bu veri giriş noktasına girdiği script kodları (örn; javascript, visual basic script) veritabanına kaydolurken sayfaya çıktı olarak yansıtılıyorsa saldırganların bu yolla kendi değerlerini veritabanına kaydedip sayfaya yansıtması işlemine denir.*

**ÇÖZÜM:** Elimizde bir websitesi var. Giriş yaptıktan sonra:

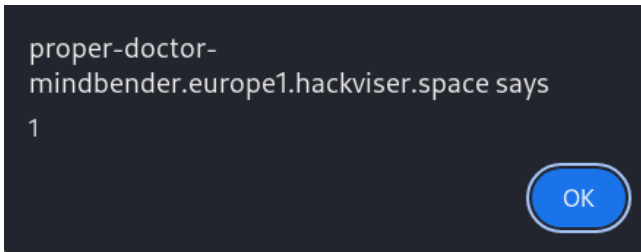
### Messages

— All users can see your message therefore be careful.



Böyle bir sayfa karşılıyor.

XSS zafiyetinin en çok kullanılan payloadını[<script>alert(1)</script>] deniyorum.



Bu aldığımız sonuç ile XSS zafiyeti olduğunu bulmuş olduk.