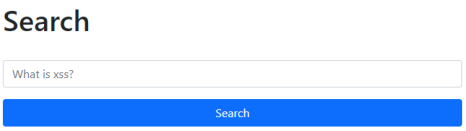
Hackviser Cross-Site Scripting (XSS)

Reflected XSS

Başlangıçta bize lab hakkında bilgi vermiş

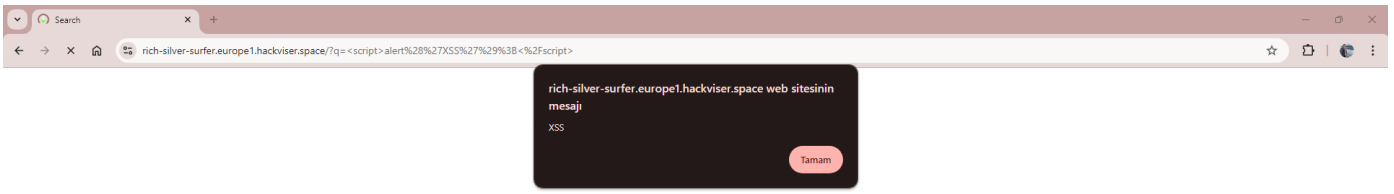
Bu laboratuvar Reflected XSS (Cross-Site Scripting) zafiyeti örneğidir. Tamamlayabilmek için, web sitesindeki arama kutusunu kullanarak web sitesinde zararlı betik çalıştırmalısınız.

Arama kutusu aracılığıyla XSS'yi tetiklemenin bir yolunu bulun.



Girişte bizi böyle bi ekran karşılıyor. Basic bir XSS payloadı deneyelim

<script>alert('XSS');</script>



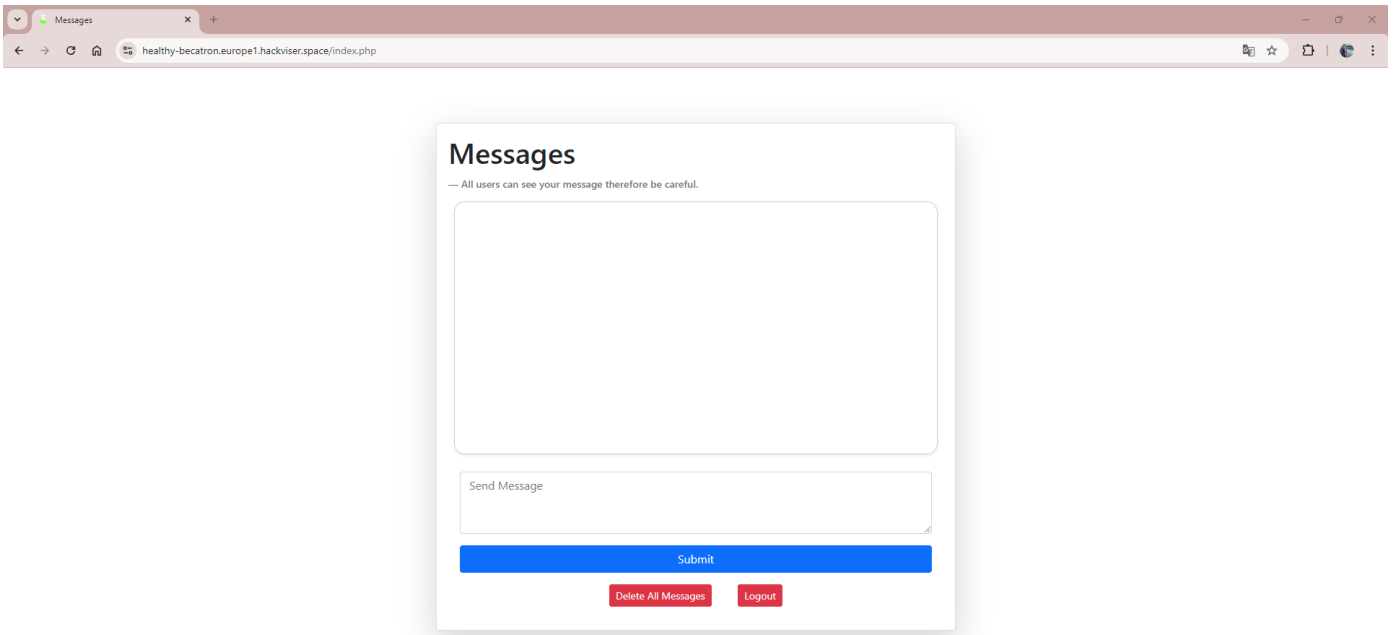
Ve evet XSS'i bulduk

Stored XSS

Başlangıçta bize lab hakkında bilgi vermiş

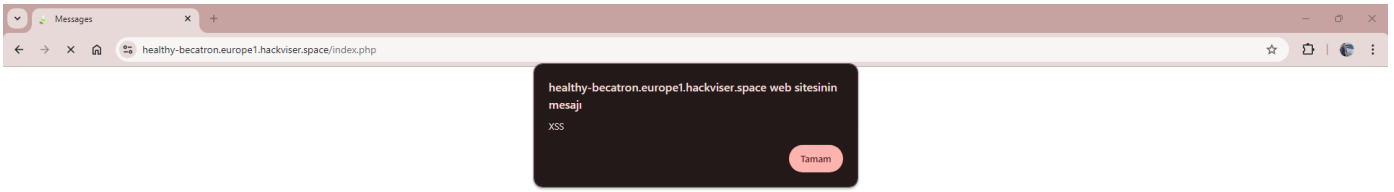
Bu laboratuvar Stored XSS (Cross-Site Scripting) zafiyeti örneğidir. Websitesinde bulunan sohbet ekranından gönderdiğiniz mesajlar sunucu tarafında filtrelenmeden veritabanına kaydedilmektedir.

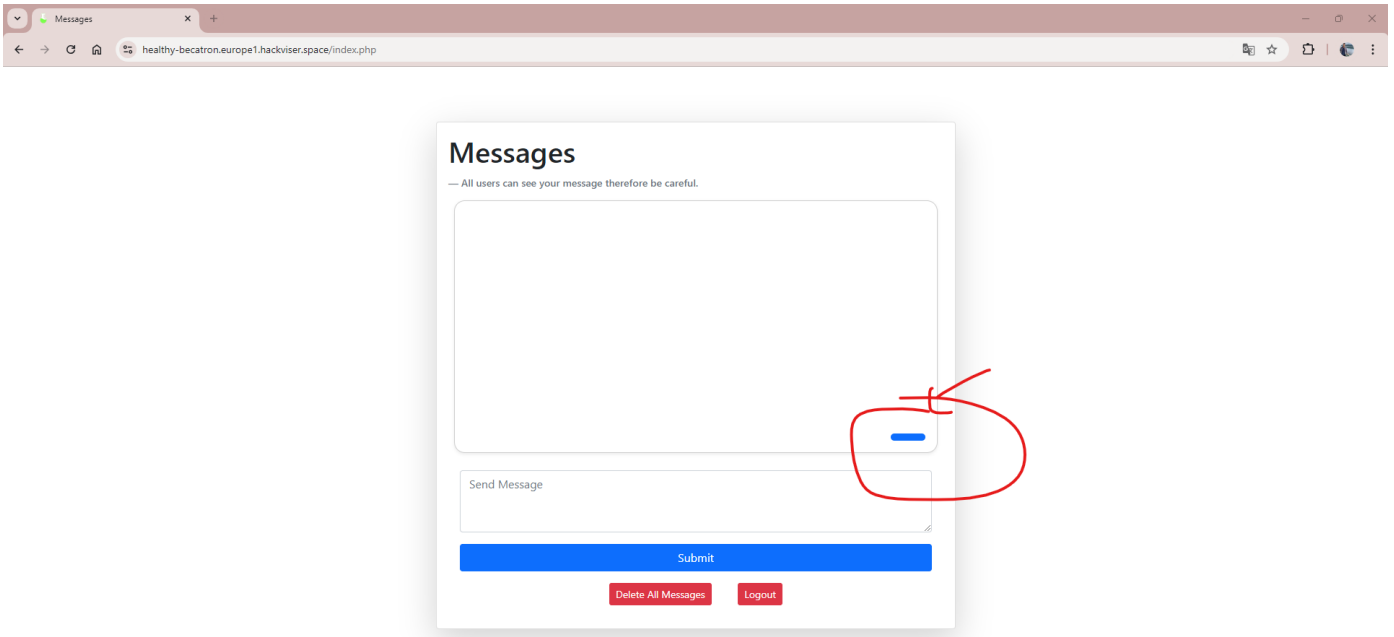
Bir mesaj göndererek tüm kullanıcılarda XSS zafiyetini tetiklemenin bir yolunu bulun.



Daha demin denediğimiz XSS payloadını burada'da deneyebiliriz

<script>alert('XSS');</script>





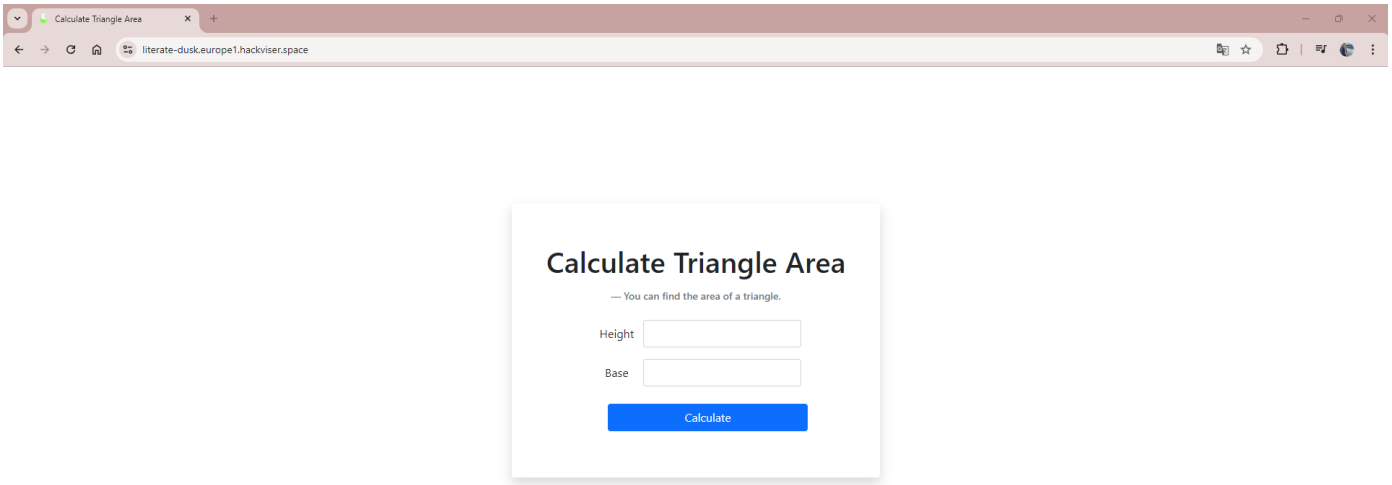
Ve evet yine XSS'i bulmuş oluyoruz stored ve reflected arasındaki tek fark biri site içerisinde kaydoluyor diğeri kaydolmuyor ondan ötürü aynı payloadla bu açığı tetikleyerek çalıştırmayı başardık

DOM-Based XSS

Başlangıçta bize lab hakkında bilgi vermiş

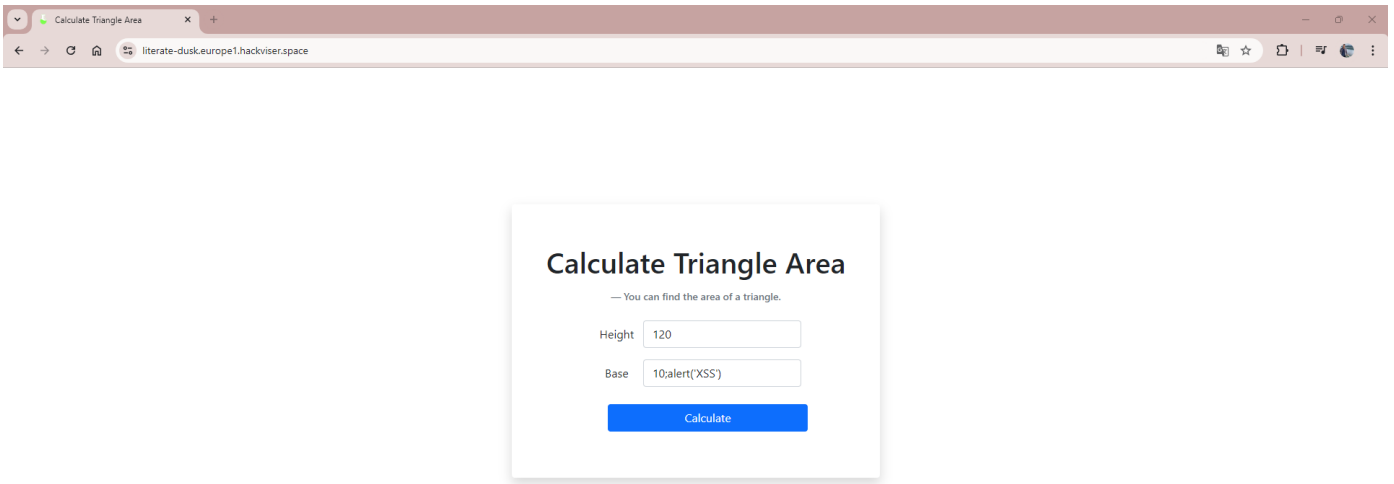
Bu laboratuvar DOM-Based XSS (Cross-Site Scripting) zafiyeti örneğidir. Websitesinde bulunan hesaplama formunun JavaScript kodlarına göz atıldığında, URL ile alınan "height" ve "base" parametrelerinin filtrelenmeden "<script>" etiketleri arasına yazıldığı görülmektedir.

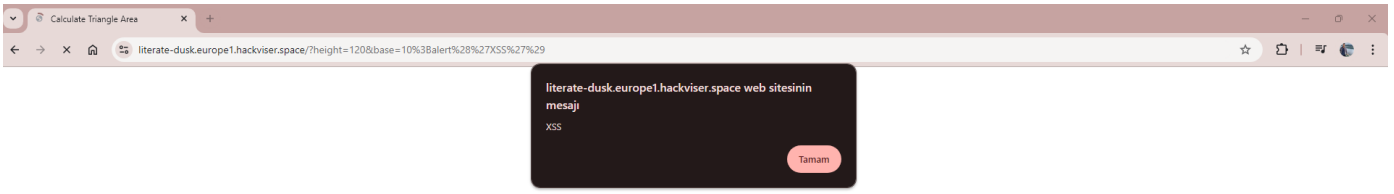
Web sitesinin çalışmasını bozmadan XSS zafiyetini tetiklemenin bir yolunu bulun.



Yine bi alert çalıştırmayı deneyelim

;alert('XSS')





Ve evet yine XSS'i tetiklemeyi başarıyoruz

Başka bir yazıda görüşmek üzere !

Linkedin

Github

İnstagram

Medium

Ayberk İlbaş