REFLECTED XSS WRİTE-UP

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

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

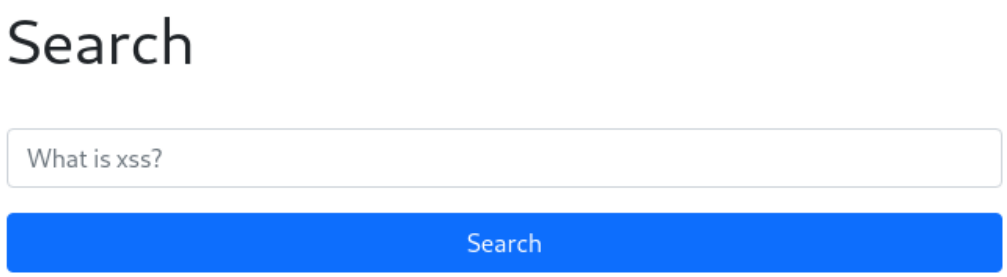
Arama kutusu aracılığıyla XSS'yi tetiklemenin bir yolunu bulun.

ÇÖZÜM: Öncelikle labımız konusu olan Reflected XSS'in ne olduğunu biraz anlatayım.

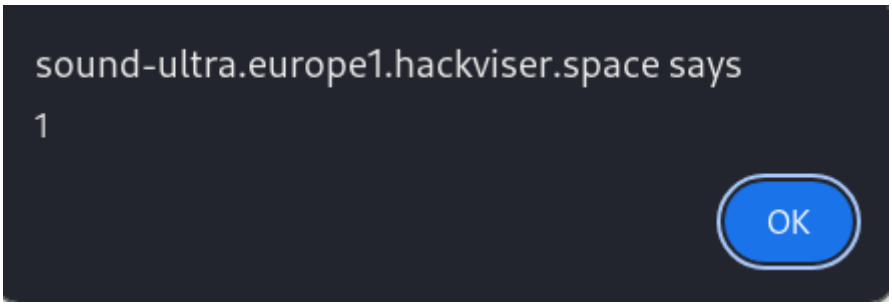
Reflected XSS(Yansıtılan Siteler Arası Komut Dosyası Çalıştırma), web uygulamalarında kullanıcıdan alınan verilerin doğru bir şekilde kontrol edilmediği ve doğrudan çıktıya dahil edildiği bir güvenlik açığıdır.

Şimdi labı çözmeye başlayalım…

Siteye giriş yapınca bizi şöyle bir şey karşılıyor:



<script>alert(1)</script> : Bu XSS denilince akla gelen en yaygın payloaddır. Bu payload'ı siteye deniyorum.



Bu çıktıyı aldıysak burada XSS açığının olduğunu bulmuş olduk.