DOM-BASED XSS WRİTE-UP

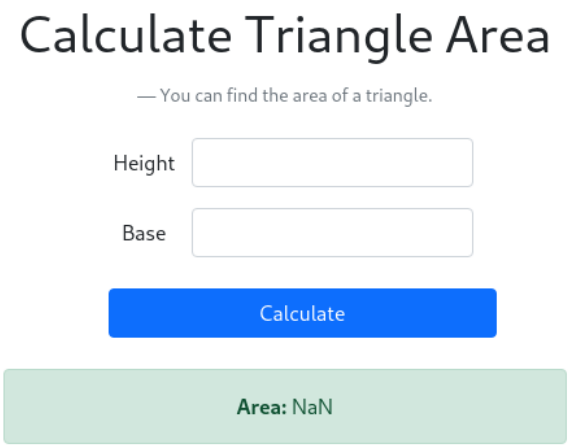
Bu yazımda Hackviser platformu üzerindeki Web Lab kısmında bulunan XSS labı içerisideki Reflected XSS labının çözümünü anlatacağım.

DOM-BASED XSS: Bu saldırı saldırganın (içerisine script kodları ekleyerek) özenle hazırladığı bir url'i internette bir yolla paylaşması sonrası linke gidildiğinde kodların sunucuya hiç gitmeden (istemci) tarayıcıda dönüp ekrana yansıtılmasına denir.

SENARYO: 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.

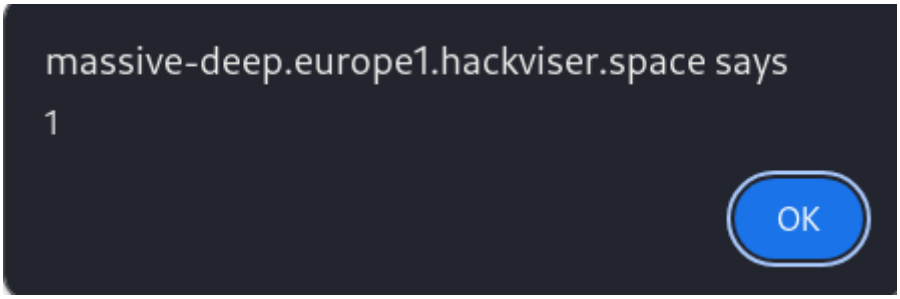
Web sitesinin çalışmasını bozmadan XSS zafiyetini tetiklemenin bir yolunu bulun.

ÇÖZÜM: Siteye giriş yapıyoruz.



Bize senaryo içerisinde bu değerlerin script etiketi içerisinde yazıldığını söylemiş. Bizim payloadımız şuydu:

<script>alert(1)</script> Zaten script etiketi içerisinde yazıldığını söylediği için sadece alert(1) komutunu deneyeceğim.



Sadece alert(1) yazdığımızda da XSS zafiyetinin olduğunu bulmuş olduk.