Cross-Site Scripting (XSS)/Reflected XSS

Herkese selamlar bu yazımda Hackviser üzerinde bulunan Web security lablarından biri olan **Cross-Site Scripting (XSS)/Reflected XSS labının çözümünü anlatacağım.**

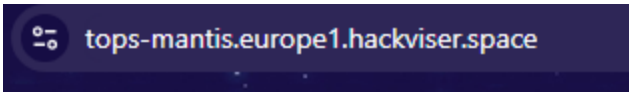
Öncelikle XSS açığının ne olduğunu kısaca bi hatırlayalım:

XSS açığı, web sitelerinin kullanıcı girdilerini doğru bir şekilde filtreleyememesinden kaynaklanır. Saldırgan bu açıktan faydalanarak uygulamada script yürütebilir. Açığın türüne göre bu script'i diğer kullanıcıların bilgisayarında çalıştırabilir. Bu çalıştırmanın sonucunda kullanıcının kişisel bilgilerinin çalınması, kullanıcının botnete dahil edilmesi gibi çeşitli olaylar yaşanabilir.

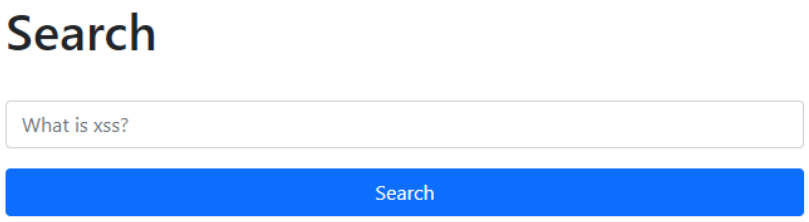
XSS açığını nerelerde bulabileceğimizi düşünüyorsak uygulamada bulunan herhangi bir giriş işlemi yapacağımız yerler login ekranları kısacası uygulamaya veri gireceğimiz kısımlarda XSS arayabiliriz.

Sırada ise makinenin çözümü var.

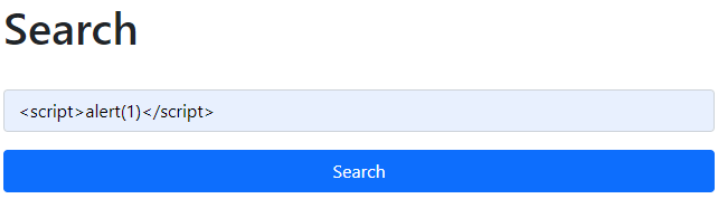
Hackviser üzerinden aşağıdaki linkten siteye bağlantı sağlıyoruz.



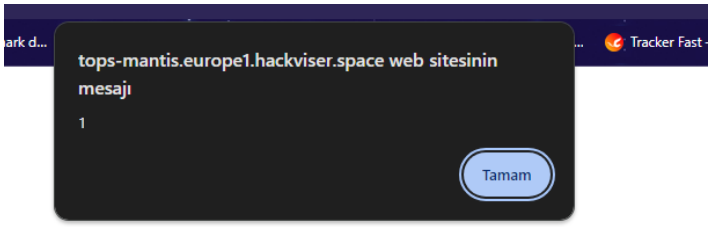
Siteye girdiğimizde ise bizi aşağıdaki gibi bir ekran karşılıyor. Bu ekranda uygulama içinde arama yapabileceğimiz bir kısım var. Bu kısımı görünce beynimizde ufak tefek kıvılcımlar çakıyor ve bu kısımda XSS, SQL Injection gibi açıkların olabileceği aklımıza geliyor. Laboratuvarın da isminden anlaşılacağı üzere bu kısımda bir XSS açığının olduğunu anlamak çok uzun sürmüyor ve akla ilk gelen XSS payloadını deniyorum



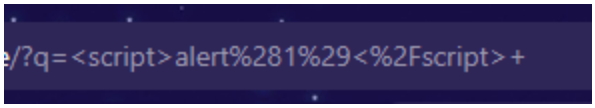
Laboratuvarın da isminden anlaşılacağı üzere bu kısımda bir XSS açığının olduğunu anlamak çok uzun sürmüyor ve akla ilk gelen XSS payloadını deniyorum.
<script>alert(1)</script>



Bu payload'ı denedikten sonra ise aşağıdaki görselde bulunan mesajı alıyorum. Yani benim siteye girdiğim script herhangi bir filtreleme işleminden geçmediği için istediğim kodu çalıştırabiliyorum.



URL de alığımız dönüte göre bu XSS açığının türünün Reflected XSS olduğunu görüyoruz.



Peki bu açığı kullanrak neler yapabileceğimize bakalım. Reflected XSS açığını kullanarak siteye yerleştireceğim scriptler ile kullanıcıalrın cookie'lerini çalabilirim, kullanıcıyı phishing sayfasına yönlendirebilirim... liste uzar gider.

Şimdi de bu açığı nasıl kapatabileceğimize bakalım

1. Kullanıcıdan alınan veriler kısıtlanabilir. Örnek verilmek gerekirse bi arama çüğüna sadece harf ve rakam girilmesi sağlanarak önlem alınabilir.
2. Html encode kullanılarak zararlı scriptlerin tarayıcı tarafından çalıştırılmasını önlenir.
3. Content Security Policy (CSP) kullanılabilir. Bu sayede verilerin hangi kaynaklardan verilerin yüklenilebileceğine sınır getirilebilir.

Bunlar çözümlerden birkaçı. Bu tip zafiyetlerle karşılaşmamak için planlı ve düzenli bir geliştirme aşaması geçirirsek zafiyeetlerin belli oranda önüne geçmiş oluruz

Umarım bu yazıyı sıkılmadan okumuşsunuzdur. Keyifli çalışmalar.