ACUNETİX

Sızma Testleri
Sonuç Raporu

27.10.2022

İçindekiler

1.1 Gerçekleştirilen Güvenlik Testi İşlemleri

-HTML enjeksiyonu testleri

-XSS testleri

-SQL enjeksiyonu testleri

1.2 Tespit Edilen Açıklıklar

1.2.1 Yansıtılan Siteler Üzerinde HTML Kodu Çalıştırma

Önem Derecesi	Orta
Açıklığın Etkisi	Yetkisiz Erişim
Erişim Noktası	İnternet
Kullanıcı Profili	Anonim Kullanıcı
Bulgu Sebebi	Uygulama geliştirmedeki eksikler/hatalar

http://testphp.vulnweb.com Sızma Testleri ve Güvenlik Denetim Raporu | Gizli

Bulgu 1.1 Açıklaması

Yapılan web sızma testleri esnasında sitenin sol üst tarafında bulunan search art kısmına html komutları girebildiğimiz ve bu komutların bize olumlu dönüş yaptığı görülmüştür

Açığı Bulunduran Sistemler

http://testphp.vulnweb.com/search.php?test=query

Çözüm Önerileri

Arama kısmına karakter sınırlaması getirilmeli ve bazı anahtar kelimelerin kullanılması engellenmelidir.

Bulgu 1.2 Açıklaması

Yapılan web sızma testleri esnasında sitenin sol tarafında bulunan Our Guestbook kısmına html komutları girebildiğimiz ve bu komutların bize olumlu dönüş yaptığı görülmüştür

Açığı Bulunduran Sistemler

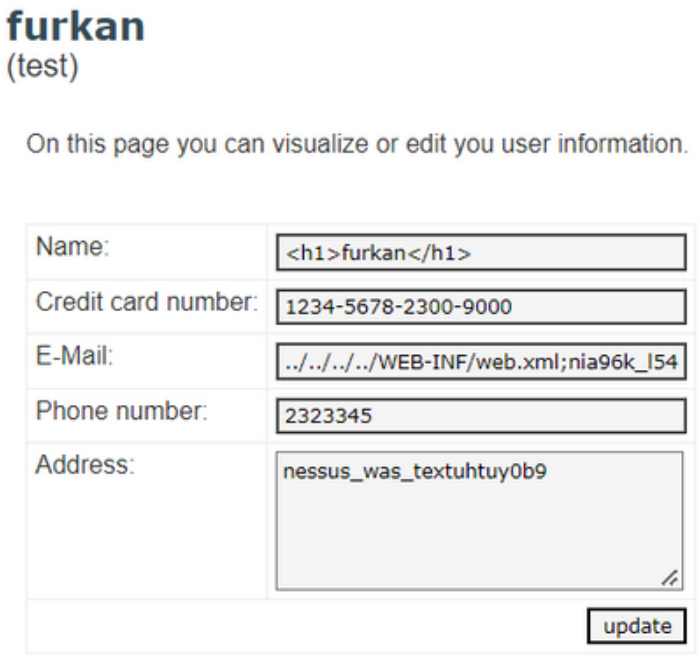
http://testphp.vulnweb.com/guestbook.php

Çözüm Önerileri

Arama kısmına karakter sınırlaması getirilmeli ve bazı anahtar kelimelerin kullanılması engellenmelidir.

Bulgu 1.3 Açıklaması

Yapılan web sızma testleri esnasında User İnfo uptade kısmına html komutları girebildiğimiz ve bu komutların bize olumlu dönüş yaptığı görülmüştür



Açığı Bulunduran Sistemler

http://testphp.vulnweb.com/userinfo.php

Çözüm Önerileri

Arama kısmına karakter sınırlaması getirilmeli ve bazı anahtar kelimelerin kullanılması engellenmelidir.

1.2 Tespit Edilen Açıklıklar

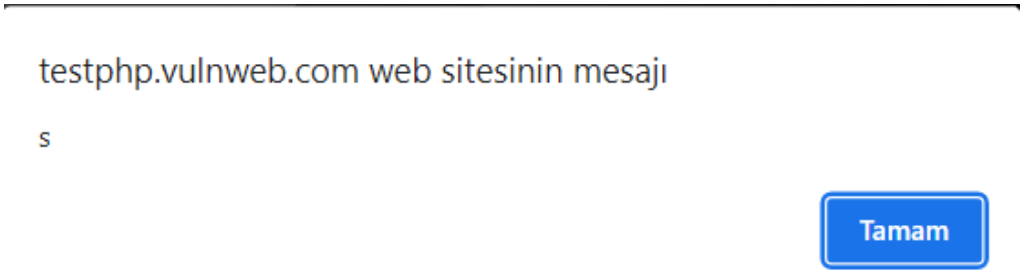
1.2.2 Yansıtılan Siteler Üzerinde Script Çalıştırma/XSS

Önem Derecesi	Orta
Açıklığın Etkisi	Yetkisiz Erişim/Bilgi İfşası
Erişim Noktası	İnternet
Kullanıcı Profili	Anonim Kullanıcı
Bulgu Sebebi	Uygulama geliştirmedeki eksikler/hatalar

http://testphp.vulnweb.com Sızma Testleri ve Güvenlik Denetim Raporu | Gizli

Bulgu 1.1 Açıklaması

Yapılan web sızma testleri esnasında sitenin sol üst tarafında bulunan search art kısmına script komutları girebildiğimiz ve bu komutların bize olumlu dönüş yaptığı görülmüştür



Payload: <script>alert('s')</script>

Açığı Bulunduran Sistemler

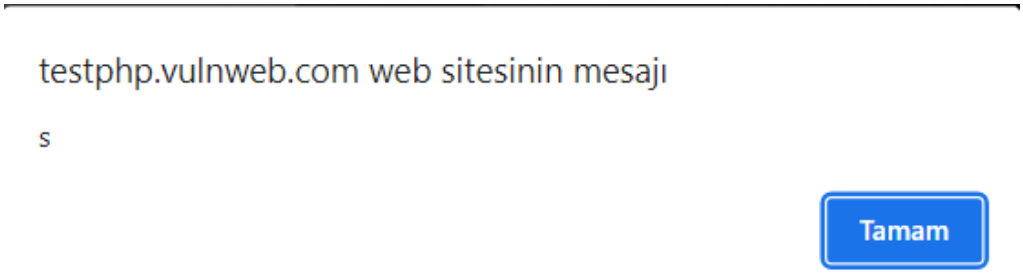
http://testphp.vulnweb.com/search.php?test=query

Çözüm Önerileri

Gelen hertürlü bilginin kullanılmadan önce zararlı karakterlerden filtrelenmesi önerilmektedir

Bulgu 1.2 Açıklaması

Yapılan web sızma testleri esnasında sitenin sol tarafında bulunan guest book kısmına script komutları girebildiğimiz ve bu komutların bize olumlu dönüş yaptığı görülmüştür



Payload: <script>alert('s')</script>

Açığı Bulunduran Sistemler

http://testphp.vulnweb.com/guestbook.php

Çözüm Önerileri

Gelen hertürlü bilginin kullanılmadan önce zararlı karakterlerden filtrelenmesi önerilmektedir

1.2 Tespit Edilen Açıklıklar

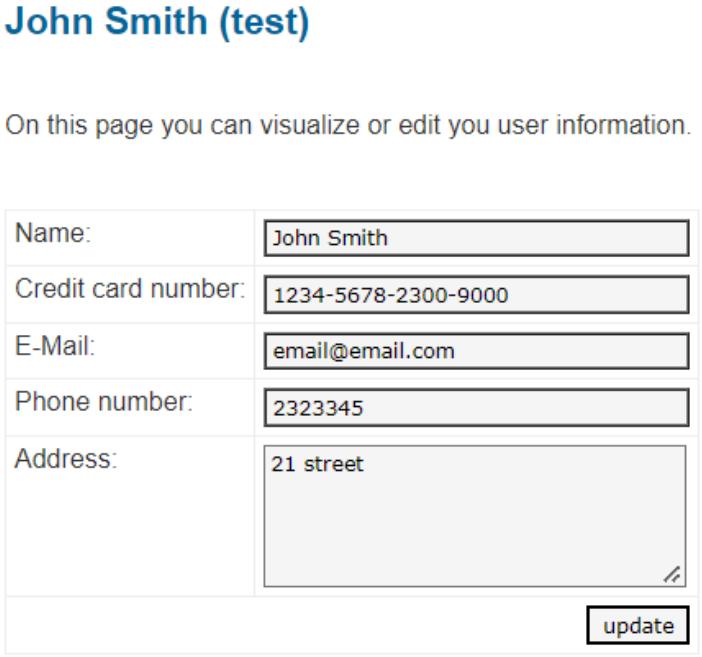
1.2.3 Yansıtılan Siteler Üzerinde Script Çalıştırma/XSS

Önem Derecesi	Acil
Açıklığın Etkisi	Yetkisiz Erişim/Bilgi İfşası
Erişim Noktası	İnternet
Kullanıcı Profili	Anonim Kullanıcı
Bulgu Sebebi	Uygulama geliştirmedeki eksikler/hatalar

http://testphp.vulnweb.com Sızma Testleri ve Güvenlik Denetim Raporu | Gizli

Bulgu 1.1 Açıklaması

Yapılan web sızma testleri esnasında sitenin login ekranında bulunan giriş kısmına bazı SQL komutları girebildiğimiz ve bu komutların bize olumlu dönüş yaptığı görülmüştür



Payload:
username:admin
password ' OR 1 -- -

Açığı Bulunduran Sistemler

http://testphp.vulnweb.com/login.php

Çözüm Önerileri

Uygulamanın bütün girdi noktalarından gelen değişkenler girdi kontrolüne sokulmalı ve bu girdilerdeki bütün meta karakterlerin filtrelenmesi önerilmektedir