

Acunetix WVS Sızma Testleri Sonuç Raporları

Web Uygulama Güvenlik Testleri

Tespit Edilen Açıklar

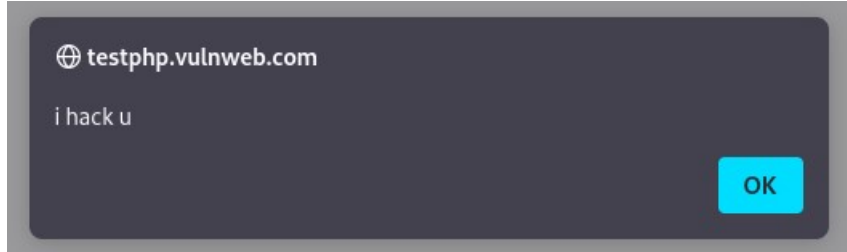
1) XSS

Önem Derecesi	Kritik
Açıklığın Etkisi	Bilgi İfşası
Erişim Noktası	İnternet
Bulgu Kategorisi	Web
Bulgu Sebebi	Uygulama Geliştirmedeki Eksiklikler

XSS (Cross site scripting) bir web sayfasına script kodları üzerinden yapılan bir saldırıdır.

URL	http://testphp.vulnweb.com/
HTTP Talep Türü	GET
Payload	<script>alert(`i hack u`)</script>

Web sitesinin arama kısmına belirlenen payload girilerek XSS çalıştırılır. Ve aşağıdaki gibi bir ekran ile karşılaşılır.



Çözüm Önerileri

Kötü amaçlı kod girişi engellenmelidir.

2) SQL Injection Zafiyeti

Önem Derecesi	Acil
Açıklığın Etkisi	Yetkisiz Erişim, Bilgi İfşası
Erişim Noktası	İnternet
Bulgu Kategorisi	Web
Bulgu Sebebi	Uygulama Geliştirmedeki Eksiklikler

SQL injection bir güvenlik açığıdır. Burada web uygulamasında yapılan SQL sorgusuna müdahale edilir ve veri tabanında bulunan verilere yetki dışı erişim sağlanır.

Bu web sitesi için önce <http://testphp.vulnweb.com/index.php> adresinden kullanıcı girişi adresine yani <http://testphp.vulnweb.com/login.php> adresine gidilir.

URL	http://testphp.vulnweb.com/login.php
HTTP Talep Türü	GET
Payload	' OR '1'='1

Sayfada bulunan “username” ve “password” kısmına yukarda verilen payload girilir. Ve ardından sistemde kayıtlı kullanıcının bilgileri ekrana gelir.

1} (test)

On this page you can visualize or edit you user information.

Name:	<input type="text" value="1"/>
Credit card number:	<input type="text" value="99887766554405jSDagD"/>
E-Mail:	<input type="text" value="dskonni@email.comwDTccIEI"/>
Phone number:	<input type="text" value="123545154689qq"/>
Address:	<input type="text" value="12148415487"/>
<input type="button" value="update"/>	

Çözüm Önerileri


Karakter filtrelemesi yapılmalı ve form girdi değerleri kontrol edilmelidir.

3) XSS

Önem Derecesi	Kritik
Açıklığın Etkisi	Yetersiz Erişim, Bilgi İfşası
Erişim Noktası	İnternet
Bulgu Kategorisi	Web
Bulgu Sebebi	Yapılandırma Eksiği

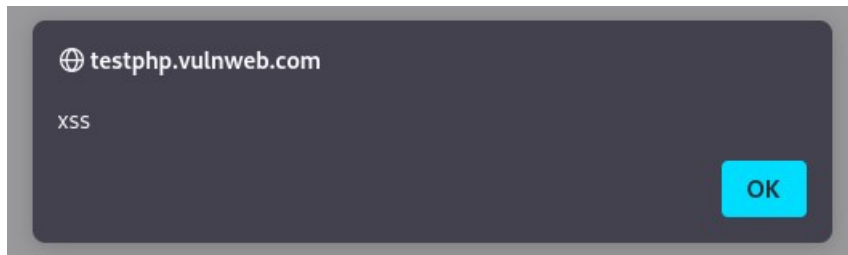
<http://testphp.vulnweb.com/listproducts.php?cat=1#> adresinde bulunan herhangi bir postere yorum yapılır.

URL	http://testphp.vulnweb.com/comment.php?pid=1
HTTP Talep Türü	GET
Payload	<script>alert('xss')</script>



The screenshot shows a web form with two input fields. The first field, labeled 'Name', contains the text '<script>alert('xss')</script>'. The second field, labeled 'Comment', contains the text 'hffhth'. Below the 'Comment' field is a 'Submit' button.

“name” alanına ilgili payload yazılarak XSS açığı tespit edilir.

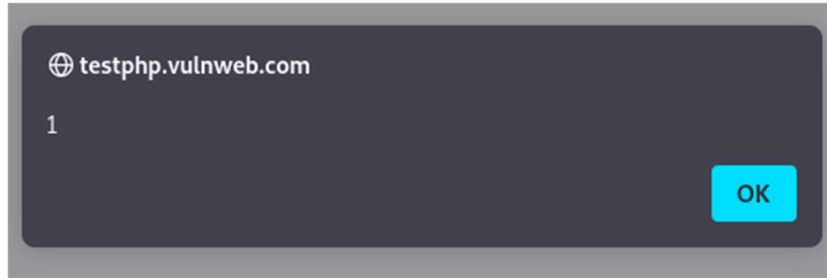


4) XSS

Önem Derecesi	Kritik
Açıklığın Etkisi	Yetersiz Erişim, Bilgi İfşası
Erişim Noktası	İnternet
Bulgu Kategorisi	Web
Bulgu Sebebi	Yapılandırma Eksiği

<http://testphp.vulnweb.com/listproducts.php?cat=1> adresindeki 1 yerine `<script>alert(1)</script>` ifadesi eklenir.

URL	http://testphp.vulnweb.com/listproducts.php?cat=1
HTTP Talep Türü	GET
Payload	<code><script>alert(1)</script></code>



5) XSS

Önem Derecesi	Yüksek
Açıklığın Etkisi	Yetersiz Erişim, Bilgi İfşası
Erişim Noktası	İnternet
Bulgu Kategorisi	Web
Bulgu Sebebi	Yapılandırma Eksiği

<http://testphp.vulnweb.com/guestbook.php> adresinde bulunan mesaj alanına ilgili payload yazılır.

URL	http://testphp.vulnweb.com/guestbook.php
HTTP Talep Türü	GET
Payload	<code><script>alert("test")</script></code>

Our guestbook

test	10.27.2022, 1:37 pm
	
<code><script>alert("test")</script></code>	
<input type="button" value="add message"/>	

