

## 1. Tespit Edilen Açıklar

### 1.1. Giriş Ekranında SQL Injection Zafiyeti

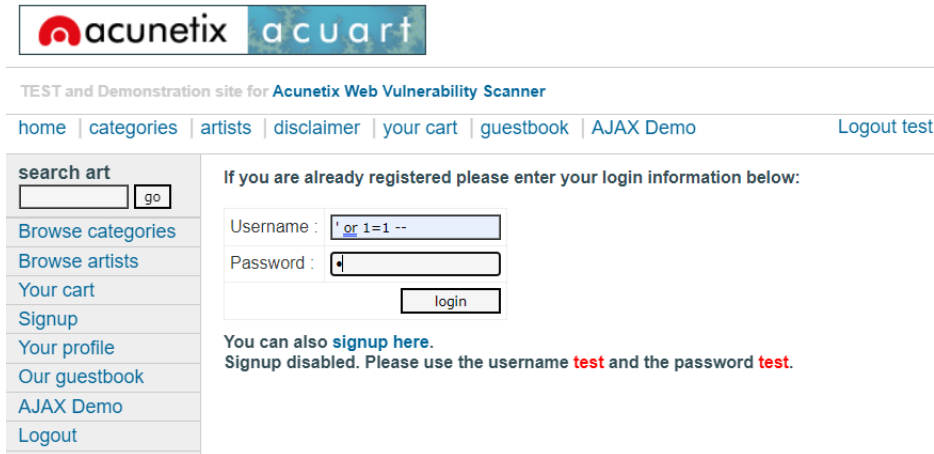
SQL Injection zafiyeti, web sitesinde herkese açık olarak sunulan giriş, iletişim gibi formlarda etkilidir. Kodlaması yanlış ya da eksik yapılan formlarda girilen bir metnin veya sorgu dizisinin, saldırgan tarafından veri tabanına yetkisiz erişim imkânı sağlayan bir güvenlik açığıdır.

Bulgu 1:

Url	<a href="http://testphp.vulnweb.com/login.php">http://testphp.vulnweb.com/login.php</a>
Http Talep türü	GET
Parametre	
Payload	or 1=1 --

Tablo 1.1

Tabloda belirtilen bilgiler doğrultusunda giriş ekranında “Username” ve “Password” alanına yukardaki payload değeri yazıldığında herhangi bir GET veya POST isteğinde bulunulmadan aşağıdaki ekran görüntülerinde olduğu gibi direkt olarak sisteme giriş yapabiliyoruz.



acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo | Logout test

search art  go

Browse categories

Browse artists

Your cart

Signup

Your profile

Our guestbook

AJAX Demo

Logout

If you are already registered please enter your login information below:

Username :

Password :

login

You can also [signup here](#).

Signup disabled. Please use the username **test** and the password **test**.

#### Şekil-1 Giriş Sayfasında Bulunan SQL Injection Zafiyeti

Şekil-1’de görüldüğü üzere giriş sayfasındaki Username kısmına tabloda verilen payloadı yazdığımızda Şekil-2’deki anasayfaya yönlendirme yapılıyor.

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo Logout test

search art  go

Browse categories  
Browse artists  
Your cart  
Signup  
Your profile  
Our guestbook  
AJAX Demo  
Logout

Links  
Security art  
PHP scanner  
PHP vuln help  
Fractal Explorer

**javascript:alert(document.domain)E (test)**

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

Name: javascript:alert(document.domain)E  
Credit card number: 1234-5678-2300-9000  
E-Mail: -1 OR 1=1)) and ifnull(unicode(substr(/{  
Phone number: 2323345  
Address: 21 street  
update

You have 0 items in your cart. You visualize you cart [here](#).

Şekil-2 SQL Injection Zafiyeti Kullanılarak Girilen Kullanıcı Anasayfası

Bu zafiyeti kullanarak girildiğinde kullanıcının tüm bilgilerinin saldırgan tarafından görülebildiği ve değiştirilebildiği tespit edilmiştir.

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo Logout test

search art  go

Browse categories  
Browse artists  
Your cart  
Signup  
Your profile  
Our guestbook  
AJAX Demo  
Logout

Links  
Security art  
PHP scanner  
PHP vuln help  
Fractal Explorer

**A (test)**

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

Name: A  
Credit card number: 1234-5678-2300-9000  
E-Mail: email@email.com  
Phone number: 554545  
Address: 21 street  
update

Şekil-3 Bilgileri Değiştirilmiş Kullanıcı

## 1.2. Yansıtılan Siteler Arası Script Çalıştırma/ XSS (OWASP-DV-001)

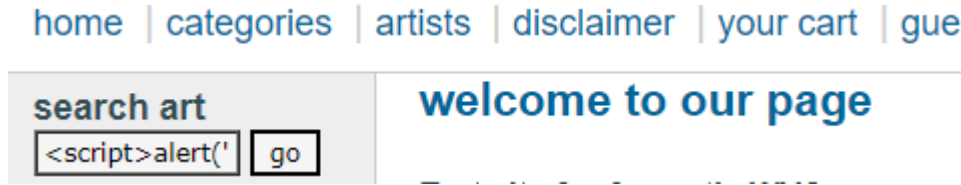
Depolanan Siteler Arası Script Çalıştırma (XSS), siteler arası komut dosyası çalıştırma saldırısı, bir saldırganın, iyi ve güvenilir olarak görülen bir web sayfasının içeriğine, genellikle istemci tarafı komut dosyası biçiminde kötü amaçlı kod enjekte etmesiyle oluşur. Kötü amaçlı komut dosyası genellikle, JavaScript ve HTML olan istemci tarafı programlama dillerinde yazılır.

Bulgu 1:

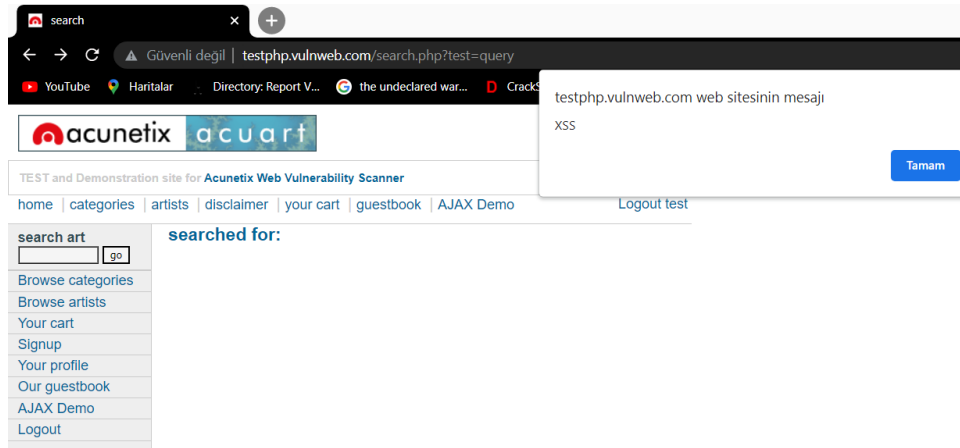
Url	http://testphp.vulnweb.com/
Http Talep türü	GET
Parametre	
Payload	<script>alert('XSS')</script>

Tablo 1.2

Sitedeki arama kısmına Tablo 1.2’de gösterilen payload yazıldığında sistem yanıt vermeyip saldırgan tarafından yazılan komut dosyasını çalıştırır. Böylece saldırgan XSS zafiyetini kullanarak web sitesini kullanılamaz hale getirebilir.



Şekil-4 Arama Kısımına JavaScript Kodu Yazılan Sayfa



Şekil-5 XSS ile Çalıştırılmış Komut

Bulgu 2:

Url	http://testphp.vulnweb.com/guestbook.php
Http Talep türü	GET
Parametre	
Payload	<script>alert('XSS')</script>


Tablo 1.3

search art  
 go

[Browse categories](#)  
[Browse artists](#)  
[Your cart](#)  
[Signup](#)  
[Your profile](#)  
[Our guestbook](#)  
[AJAX Demo](#)  
[Logout](#)

Our guestbook

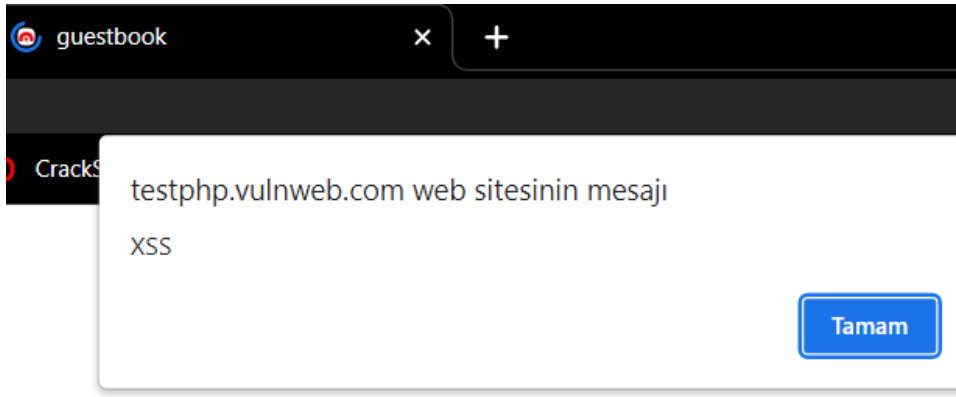
test10.26.2022, 8:23 pm



```
<script>alert('XSS')</script>
```

add message

Şekil-6 Mesaj Kısımına JavaScript Kodu Yazılan Sayfa



Şekil-7 Şekil-5 XSS ile Çalıştırılmış Komut ve Ulaşılmayan Sayfa

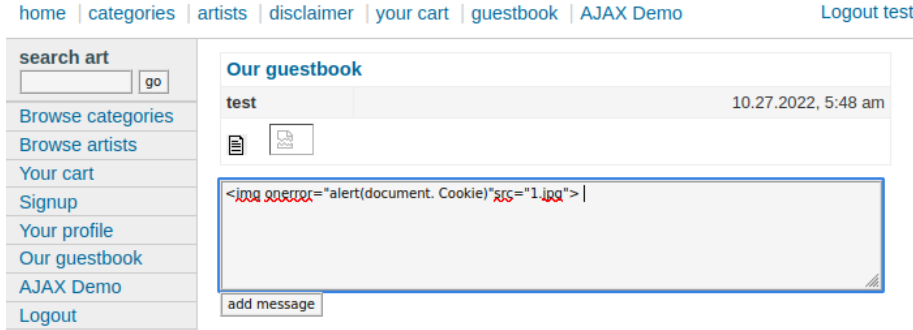
### 1.3. Depolanan Siteler Arası Script Çalıştırma/XSS

Bulgu 1:

Url	http://testphp.vulnweb.com/guestbook.php
Http Talep türü	GET
Parametre	
Payload	

Tablo 1.4

Siteler arası script çalıştırma zafiyeti olarak bilinen XSS, kötü niyetli kişilerin bu site üzerinden diğer kullanıcılara istemci tarafında çalışmak üzere kod (genellikle JavaScript ve html) gönderip kötü amaçlarla çalıştırmalarına imkân tanımaktadır. XSS zafiyetleri uygulamalarda dışarıdan alınan bilgiler için yeterli girdi ve çıktı denetimi yapılmadığı durumlarda ortaya çıkar ve art niyetli bir kullanıcı istediği gibi javascript kodu çalıştırarak hedef aldığı kişilere ait oturum bilgilerini çalabilir, hedef aldığı kişilerin browserini istediği gibi yönlendirebilir.



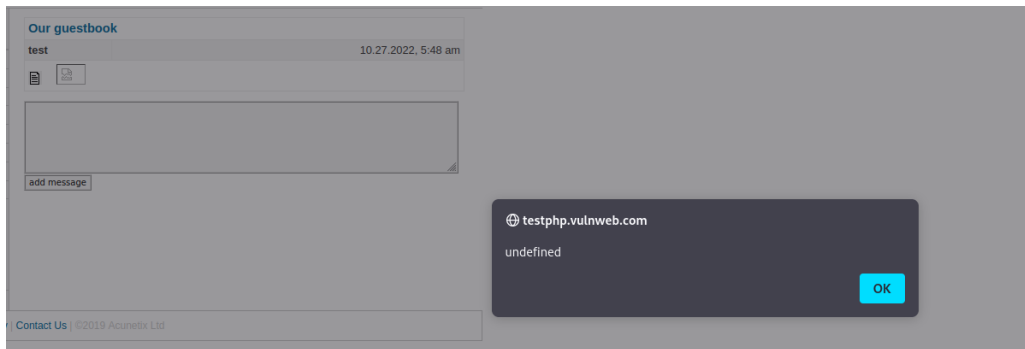
Şekil-8 Payloadın Yazıldığı Mesaj Bölümü

Payload çalıştığı zaman sitenin arka planda çalışan kod kısmı Şekil-9’ da gösterilmiştir. Şekilde görüldüğü üzere payload çalıştığı zaman saldırgan sitede bulunan login cookie kısmını döndürmüştür ve böylece saldırgan kullanıcının bilgilerini ele geçirmiş olur.

```
POST /guestbook.php HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 103
Origin: http://testphp.vulnweb.com
Connection: close
Referer: http://testphp.vulnweb.com/guestbook.php
Cookie: login=test%2Ftest
Upgrade-Insecure-Requests: 1

name=test&text=%3Cimg+onerror%3D%22alert%28document.cookie%29%22src%3D%221.jpg%22%3E&submit=add+message
```

Şekil-9 Payload Çalıştığında Arka Planda Dönen veri

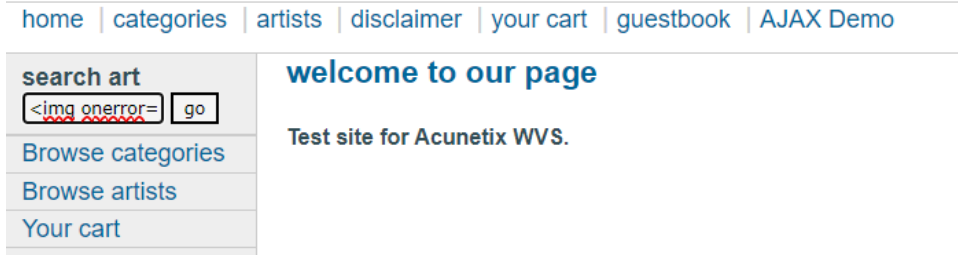


Şekil-10 Payload Çalıştığında Sitede Dönen veri

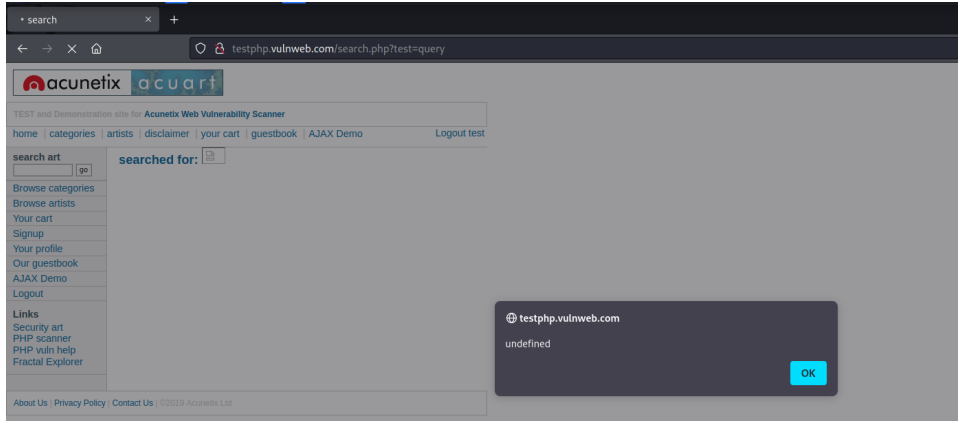
Bulgu 2:

Url	http://testphp.vulnweb.com/
Http Talep türü	GET
Parametre	
Payload	

Tablo 1.5



Şekil-11 XSS Payloadı Yazılan Arama Bölümü



Şekil-12 Payload Çalıştığında Sitede Dönen Veri