

Sızma Testi Raporu

Tarih: 01.03.2025

Test Edilen Sistem: Restoran Yönetim Sistemi

Test Yapan: Güvenlik Ekibi

1. GİZLİLİK BİLDİRİMİ

Bu rapor yalnızca yetkilendirilmiş kişiler tarafından kullanılmak üzere hazırlanmıştır. İçerğinde tespit edilen güvenlik açıkları ve çözüm önerileri bulunmaktadır. Bilgilerin yetkisiz kişilerle paylaşılması yasaktır.

2. RİSK PUANLAMA TABLOSU

Risk Seviyesi	CVSS Puan Aralığı
Düşük	0.1 - 3.9
Orta	4.0 - 6.9
Yüksek	7.0 - 8.9
Kritik	9.0 - 10.0

3.1. Yetkisiz Dosya Yükleme (Unrestricted File Upload)

CVSS Skoru: 9.1 (Kritik)

Sistemde profil resmi yükleme alanında uygun dosya türü denetimi yapılmamaktadır. Kullanıcılar, PHP gibi çalıştırılabilir dosyalar yükleyerek sunucuya sızabilir. Test sırasında `mertshell.php` adlı bir dosya yüklenmiş ve sistemde çalıştırılmıştır.

Sonuçlar:

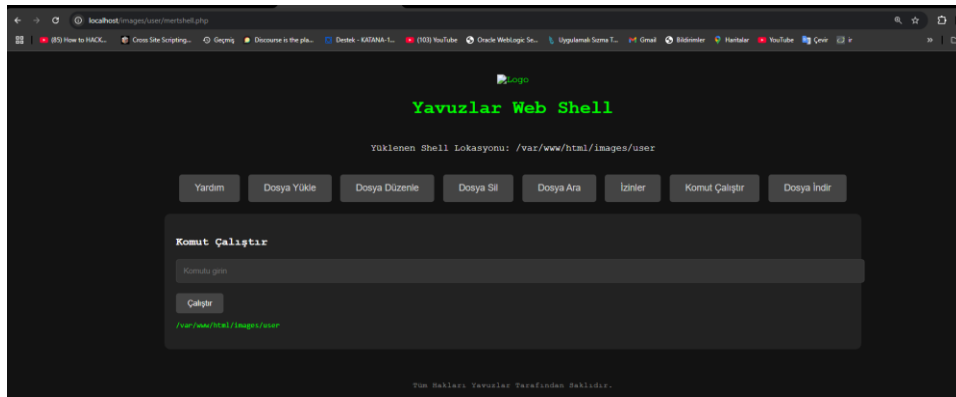
- Yetkisiz kişiler tarafından uzaktan kod çalıştırma (Remote Code Execution - RCE) riski.
- Sistem üzerinde tam kontrol sağlanabilir.

Öneriler:

- Yalnızca belirli dosya türlerinin yüklenmesine izin verilmeli (örneğin `.jpg`, `.png`).
- Yüklenen dosyaların MIME türü doğrulanmalı.
- Sunucu tarafında güvenli dizin kısıtlamaları uygulanmalı.



Yetkisiz Dosya Yükleme Kanıtı



Yetkisiz Shell Erişimi

3.2. Saklı XSS (Stored Cross-Site Scripting - XSS)

CVSS Skoru: 7.2 (Yüksek)

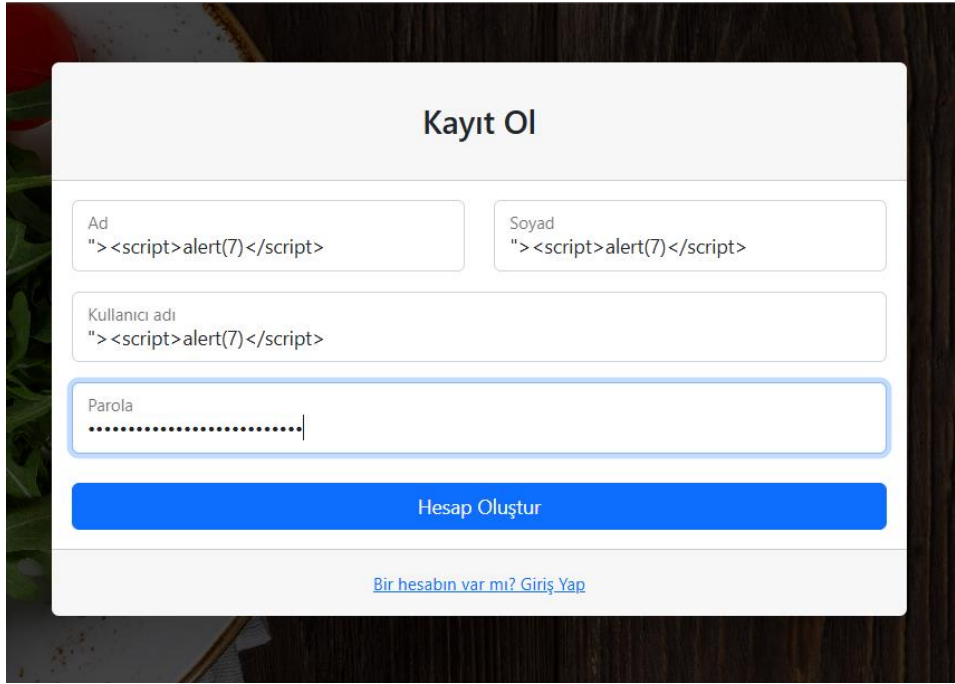
Kayıt ve giriş formundaki `Ad`, `Soyad` ve `Kullanıcı Adı` alanlarında zararlı JavaScript kodlarının kaydedildiği ve çalıştırılabildiği tespit edilmiştir. `<script>alert(7)</script>` gibi kodlar form alanlarına girildiğinde sistem tarafından saklanarak çalıştırılmaktadır.

Sonuçlar:

- Kullanıcı oturumları ele geçirilebilir.
- Zararlı JavaScript kodları diğer kullanıcılara bulaştırılabilir.

Öneriler:

- Kullanıcı girdileri sunucu tarafında temizlenmeli (Sanitization).
- HTML karakterleri uygun biçimde encode edilmelidir (`<`, `>` gibi).
- İçerik Güvenlik Politikası (CSP) uygulanmalıdır.



The screenshot shows a registration form titled "Kayıt Ol". It contains four input fields: "Ad", "Soyad", "Kullanıcı adı", and "Parola". The "Ad", "Soyad", and "Kullanıcı adı" fields contain the payload "><script>alert(7)</script>". The "Parola" field is empty and has a blue border. Below the fields is a blue button labeled "Hesap Oluştur". At the bottom, there is a link that says "Bir hesabın var mı? Giriş Yap".

Stored XSS Kanıtı - Kayıt Formu

Giriş Yap

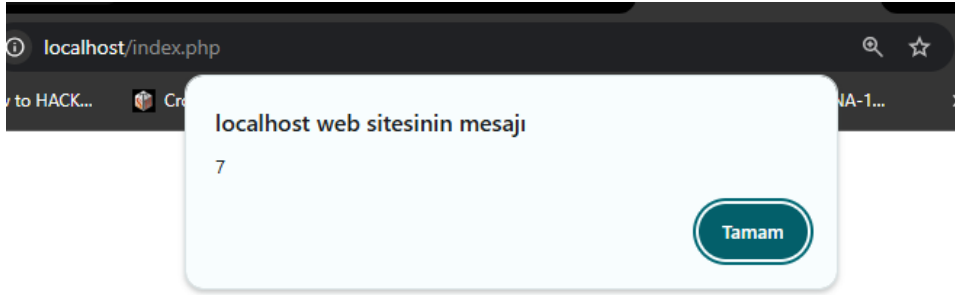
Kullanıcı adı
"> <script>alert(7) </script>

Parola
.....

Giriş Yap

[Bir hesabın yok mu? Kayıt ol!](#)

Stored XSS Kanıtı - Giriş Formu



Stored XSS Kanıtı - Tarayıcı Uyarısı

4. SONUÇ VE ÖNERİLER

Bu testte tespit edilen güvenlik açıkları, sistemin ciddi güvenlik risklerine sahip olduğunu göstermektedir. Sistemde tespit edilen en kritik açıklar şunlardır:

- - Yetkisiz dosya yükleme (Uzaktan kod çalıştırmaya neden olabilir)
- - Saklı XSS (Kullanıcı hesaplarının ele geçirilmesine neden olabilir)

Bu açıkların giderilmesi için aşağıdaki adımlar önerilmektedir:

- - Kullanıcı girişleri sıkı bir şekilde doğrulanmalı ve filtrelenebilir.
- - Dosya yükleme işlemleri sıkı güvenlik politikalarıyla sınırlandırılmalıdır.
- - Web güvenliği konusunda en iyi uygulamalar (OWASP Top 10) takip edilmelidir.

Bu raporun sonuçlarına dayanarak, sistem üzerinde detaylı güvenlik iyileştirmeleri yapılması önerilmektedir. Güvenliğin sürekli olarak sağlanabilmesi için periyodik güvenlik testleri gerçekleştirilmelidir.