

Yavuzlar 1.Takım

Restoran Sitesi Pentest

Rapor Başlığı:	Restoran Sitesi Sızma Testi Raporu
Yazan:	Tuğba CAN, Yılmaz ÜSTÜNTAŞ
Test Ekibi:	Tuğba CAN, Yılmaz ÜSTÜNTAŞ, Yavuz Selim YILMAZ
Kontrol Eden:	Melike Sena ÇAKIR

İçindekiler Tablosu

ÖZET	3
Bulunan Zafiyetler	4
Zafiyet Adı: Broken Access Control	4
Zafiyet Adı: IDOR	5
Zafiyet Adı: Privilege Escalation, IDOR	6
Zafiyet Adı: XSS	8

ÖZET

Bu rapor, Yavuzlar 1.Takım tarafından “Restoran” sitesi üzerindeki güvenlik açıklarını ortaya çıkarmak amacı ile 02.10.2024 – 06.10.2024 tarihleri arasında gerçekleştirilen güvenlik testleri çalışmalarının sonuçlarını içermektedir.

Tetsler, localhost ile gerçekleşmiş olup 2 kritik, 2 orta olmak üzere toplam 4 farklı güvenlik açığı tespit edilmiştir. Açıkların detayları raporun devamında verilmiştir.

Testler sonucunda en büyük güvenlik eksikliği, **"Broken Access Control"** olarak belirlenmiştir. Bu güvenlik eksikliği herhangi bir yetkilendirme olmamasından ya da bozuk yetkilendirme sistemi olmasından kaynaklanıyor, “adminpanel.php” gibi kritik bir sayfaya giriş yapmadan sadece url üzerinden yazarak erişebiliyoruz. Bu önem taşıyan zafiyetin önlenmesi için düzgün oturum yapılandırması örnek;

```
session_start();

if (!isset($_SESSION['user_role']) || $_SESSION['user_role'] != 'admin') {

    header("Location: login.php");

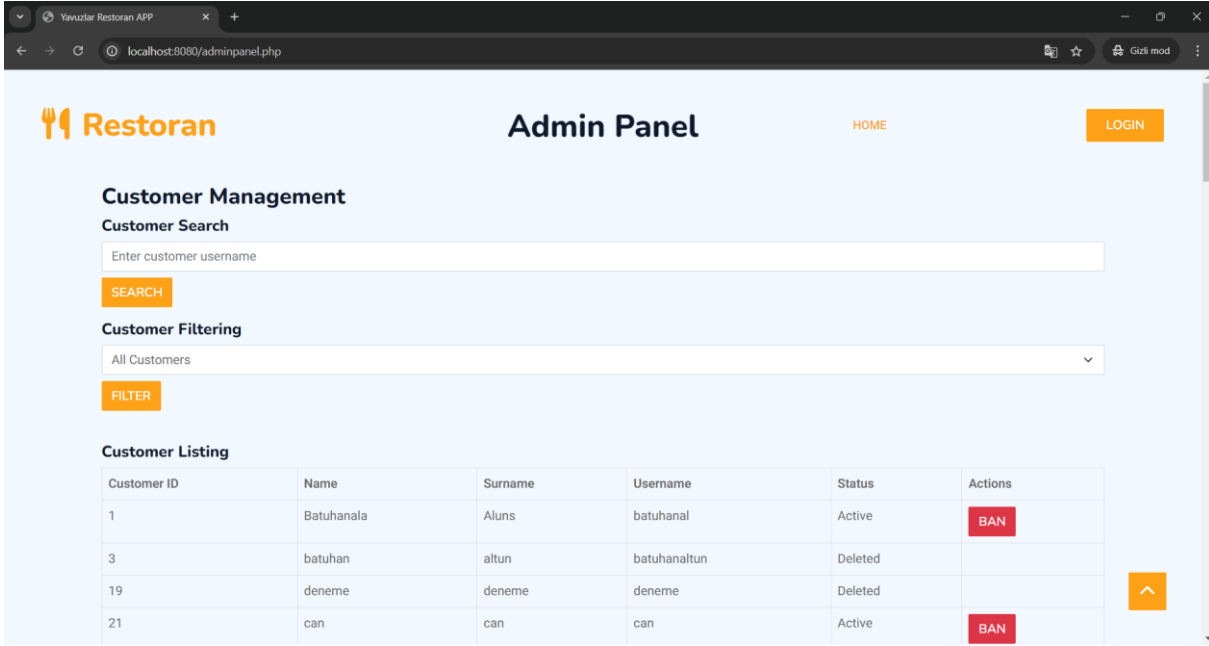
    exit();

}
```

Bunun gibi bir oturum rol doğruluğunu kontrol ederek bu güvenlik açıklığının önüne geçilebilir. Genel olarak çoğu zafiyetin önüne geçebilmek için düzenli güvenlik testleri yapılmalı böylece olası zafiyetler tespit edilebilir ve önceden önlem alınabilir.

Zafiyet Adı: Broken Access Control

CVSS: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N **9.0 (Critical)**



Şekil 1 -Admin Paneline Yetkisiz Erişim

Siteye giren herkes “<http://localhost:8080/adminpanel.php>” adresine login olmadan erişebiliyor. Herhangi denetim bulunmuyor.

Broken Access Control zafiyeti, kullanıcıların yetkileri dışında verilere veya işlemlere erişim sağlayabildiği bir güvenlik açığıdır. Bu zafiyet, sistemdeki yetki denetimlerinin yetersiz veya yanlış uygulanmasından kaynaklanır. OWASP 2023'te bu tür zafiyet, en kritik web uygulama güvenlik riskleri arasında yer alır.

Zafiyetinin Doğurabileceği Sonuçlar:

Yetkisiz Veri Erişimi: Kullanıcılar, erişim izni olmayan verilere ulaşabilir. Örneğin, başka bir kullanıcının özel bilgilerini görüntüleyebilir veya değiştirebilir.

Yetkisiz İşlem Yapma: Düşük seviyeli kullanıcılar, yüksek yetkiye sahip kullanıcıların yapabileceği işlemleri gerçekleştirebilir.

Veri Manipülasyonu: Yetkisiz kullanıcılar verileri değiştirebilir, silebilir veya sistemde önemli bilgileri güncelleyebilir.

Sistem Kontrolünün Ele Geçirilmesi: Bir saldırgan, yüksek yetkili hesapları ele geçirip tüm sistemi kontrol edebilir, bu da sistemin çökmesine veya kötüye kullanılmasına neden olabilir.


Zafiyetinin Kapatılması İçin Öneriler:

- Sunucu taraflı erişim denetimleri uygulanmalı
- Role-Based Access Control (RBAC) kullanılmalı
- IDOR gibi zafiyetler önlenmeli
- Güvenli oturum yönetimi sağlanmalı
- Düzenli güvenlik testleri yapılmalı

Zafiyet Adı: IDOR

CVSS: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:C/C:N/I:H/A:N **5.9 (Medium)**

Your Profile Information



Dosya Seç Dosya seçilmedi

Role:
user

First Name: Selami Last Name: Çakır

Username selami

Your Balance is 5000.00\$

Şekil 2-Bakiye Yükleme

```
23 -----WebKitFormBoundaryTSc27Zj1lvwh3Yfs
24 Content-Disposition: form-data; name="balance"
25
26 3000
27 -----WebKitFormBoundaryTSc27Zj1lvwh3Yfs
28 Content-Disposition: form-data; name="balance_user_id"
29
30 15
31 -----WebKitFormBoundaryTSc27Zj1lvwh3Yfs--
32
```

Şekil 3-User ID İncelenmesi

Kullanıcı bakiye yüklemesi yaparken burp suite aracı ile inceleyerek “balance_user_id” değerini görüyoruz. Bu değeri değiştirerek farklı kullanıcılara bakiye yüklemesi gerçekleştirebiliyoruz.

Zafiyetin bulunduğu url “http://localhost:8080/profile.php”

IDOR , web uygulamalarında kullanıcıların, yetkili olmadıkları nesnelere (örneğin, dosyalara, veri kayıtlarına veya diğer kaynaklara) doğrudan erişim sağlamasına izin veren bir güvenlik açığıdır. Bu zafiyet, genellikle uygulamanın, kullanıcı yetkilerini yeterince kontrol etmemesi sonucu oluşur.

Zafiyetinin Doğurabileceği Sonuçlar:

Yetkisiz Veri Erişimi: Saldırganlar, yetkili olmadıkları kullanıcıların bilgilerine (örneğin, kişisel bilgiler, finansal veriler) erişebilirler.

Veri Sızıntısı: Hassas verilerin (şifreler, kişisel bilgiler, sağlık kayıtları) sızması, ciddi güvenlik ihlallerine neden olabilir.

Zafiyetinin Kapatılması İçin Öneriler:

- Sunucu Tarafı Erişim Denetimi Uygulanmalı
- Kullanıcı ID'si Gizlenmeli
- Yetkilendirme Kontrolü Eklenmeli
- Parametre Manipülasyonunu Önlemek İçin Token Kullanımı

Zafiyet Adı: Privilege Escalation, IDOR

CVSS: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N **9.0 (Critical)**

```
-----WebKitFormBoundaryUUHnEWBQAYW6redH
Content-Disposition: form-data; name="role"

admin
-----WebKitFormBoundaryUUHnEWBQAYW6redH
Content-Disposition: form-data; name="fname"

ali
-----WebKitFormBoundaryUUHnEWBQAYW6redH
Content-Disposition: form-data; name="surname"

ali
-----WebKitFormBoundaryUUHnEWBQAYW6redH
Content-Disposition: form-data; name="username"

ali
-----WebKitFormBoundaryUUHnEWBQAYW6redH
Content-Disposition: form-data; name="passwd"

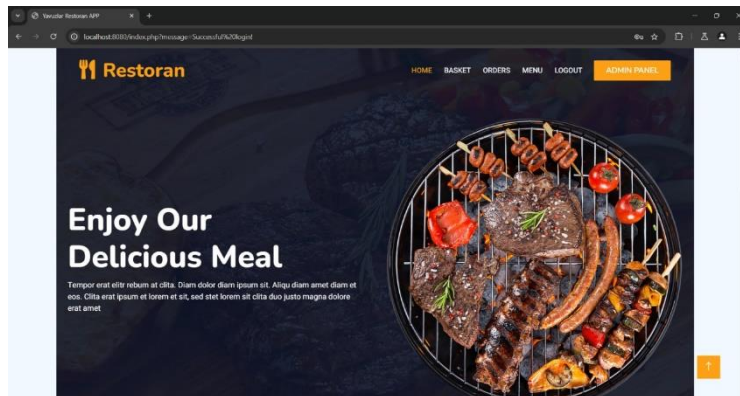
ali
-----WebKitFormBoundaryUUHnEWBQAYW6redH--
```

Şekil 4-Register.php request

Response					
	Pretty	Raw	Hex	Render	Hackvortor
1	HTTP/1.1 200 OK				
2	Date: Sat, 05 Oct 2024 19:34:56 GMT				
3	Server: Apache/2.4.62 (Debian)				
4	X-Powered-By: PHP/8.1.30				
5	Expires: Thu, 19 Nov 1981 08:52:00 GMT				
6	Cache-Control: no-store, no-cache, must-revalidate				
7	Pragma: no-cache				
8	Vary: Accept-Encoding				
9	Content-Length: 478				
10	Keep-Alive: timeout=5, max=100				
11	Connection: Keep-Alive				
12	Content-Type: text/html; charset=UTF-8				
13					

Şekil 5-Register.php Response

Register.php de kullanıcı kayıt ederken burp suite ile izliyoruz ve burp suite üzerinden istekteki rol kısmını admin olarak değiştirerek yeni bir admin kullanıcısı kayıt ediyoruz.



Şekil 6-Başarılı Admin girişi

Privilege Escalation , bir saldırganın, sisteme veya uygulamaya erişim sağladıktan sonra, başlangıçta sahip olduğu kullanıcı haklarını (örneğin, normal kullanıcı veya misafir) daha yüksek yetkilere yükseltme sürecidir. Bu tür bir saldırı, güvenlik açıkları veya yanlış yapılandırmalar aracılığıyla gerçekleştirilebilir.

Zafiyetinin Doğurabileceği Sonuçlar:

Tam Sistem Kontrolü: Saldırgan, yönetici veya süper kullanıcı yetkileri elde ederek sistem üzerinde tam kontrol sağlayabilir.

Veri İhlalleri: Hassas verilere erişim sağlanması, kullanıcı bilgileri, finansal veriler ve diğer kritik bilgilerin sızmasına yol açabilir.

Zararlı Yazılım Yayılımı: Yükseltilmiş yetkilerle, saldırı sistemde zararlı yazılımlar kurabilir veya mevcut olanları değiştirebilir.

Hizmet Kesintisi: Saldırgan, sistemdeki kritik bileşenleri değiştirebilir veya silebilir, bu da hizmet kesintilerine yol açabilir.

İtibar Kaybı: Veri ihlalleri ve güvenlik açıkları, kuruluşun itibarına ciddi zararlar verebilir ve müşteri güvenini sarsabilir.

Zafiyetinin Kapatılması İçin Öneriler:

Rol alanı kullanıcıdan gelen istekte bulunmamalı, sunucuda sabit bir şekilde ayarlanmalıdır.

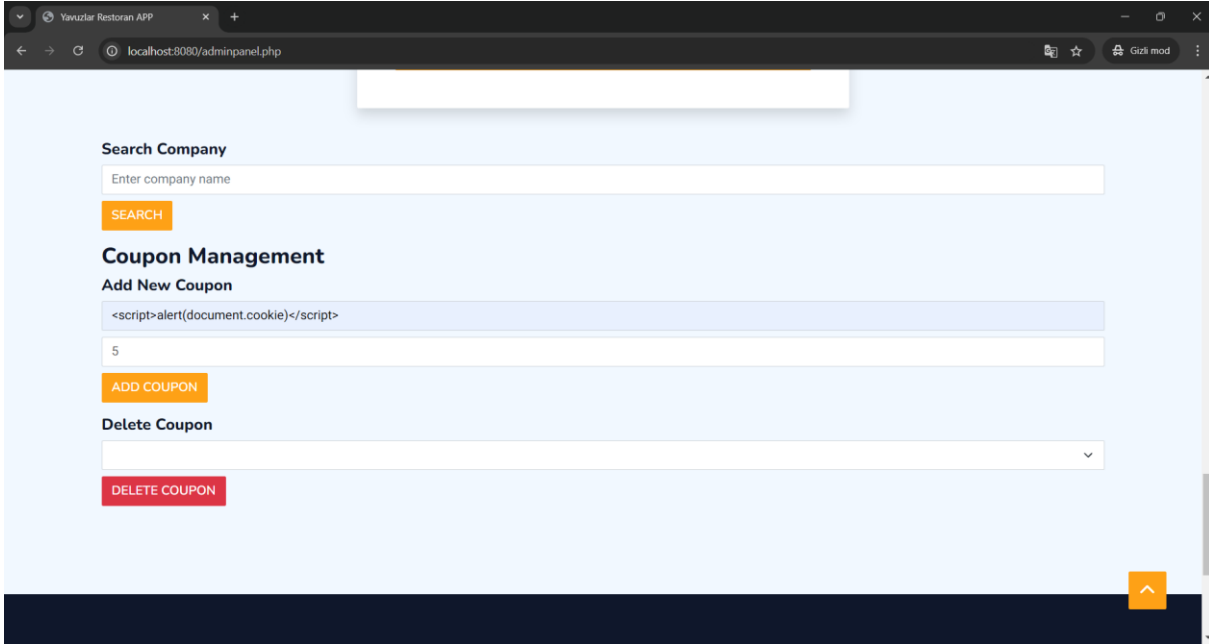
Kullanıcı rolü sadece admin yetkisine sahip kişiler tarafından atanmalı ve kullanıcı oturumu sunucu tarafında doğrulanmalıdır.

Role alanını kayıt formuna hiç eklemeyin. Kullanıcı kayıt formu yalnızca kullanıcı adı, şifre gibi temel bilgileri içermelidir.

Roller ve yetkiler dikkatlice tanımlanmalı ve bu yetkilere göre erişim kontrolleri sunucu tarafında uygulanmalıdır.

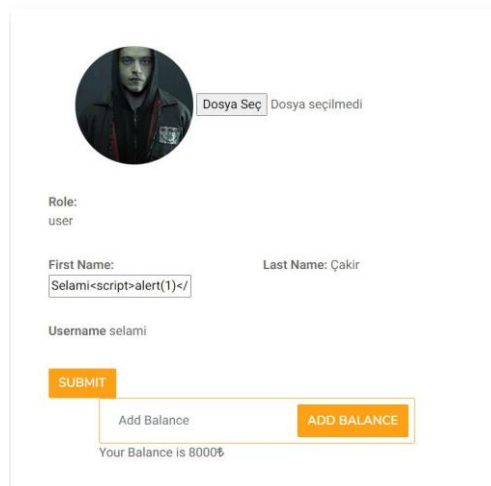
Zafiyet Adı: XSS

CVSS: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:N **6.8 (Medium)**



Şekil 7-XSS Zafiyeti

Sitede admin panel sayfasında “http://localhost:8080/adminpanel.php” kupon eklerken, kullanıcı girdilerinin yeterince doğrulanmaması nedeniyle **XSS** zafiyeti bulunmaktadır. Bu zafiyet, kötü niyetli kullanıcıların zararlı JavaScript kodu ekleyerek, diğer kullanıcıların tarayıcılarında bu kodun çalışmasına neden olabilmektedir, böylece oturum bilgileri çalınabilir veya sistem üzerinde kötü amaçlı işlemler gerçekleştirilebilir.



Şekil 8-Stored XSS

Kullanıcıların profil bilgilerini düzenlediği sayfada “http://localhost:8080/profile.php” stored XSS zafiyeti bulunuyor.

XSS , web uygulamalarında kullanıcıların tarayıcıları üzerinden zararlı kod (genellikle JavaScript) enjekte edilmesine olanak tanıyan bir güvenlik zafiyetidir. Saldırganlar, bu zafiyeti kullanarak kullanıcıların tarayıcılarında kötü niyetli kod çalıştırabilir, bu sayede kullanıcı verilerine erişebilir, oturum bilgilerini çalabilir veya kötü amaçlı içerikler gösterebilir.

Zafiyetinin Doğurabileceği Sonuçlar:

Kötü niyetli içeriklerin kullanıcıya gösterilmesi
Kullanıcıların kötü amaçlı sitelere yönlendirilmesi
Uygulama güvenliğinin zedelenmesi

Zafiyetinin Kapatılması İçin Öneriler:

Kullanıcı girdilerini doğru bir şekilde filtrelemek ve sanitize etmek.
HTML ve JavaScript kodlarına karşı uygun escape mekanizmaları kullanmak.
İçerik Güvenlik Politikası (CSP) uygulamak.
Güvenli kütüphaneler ve çerçeveler kullanmak

<script>alert(document.cookie)</script>	adminpanel.php
<script>alert(1);</script>	profile.php

Burada sitede kullanılan XSS payloadları bunlardır. Eklemediğimiz ama çalışan daha fazla payload bulunuyor.