UPSILON

PENTEST RAPORU

RESTORAN

TARİH: 05.10.2024

Gizli Belge

İÇİNDEKİLER

1. Gizlilik Bildirimi

Bu rapor, sızma testi kapsamında elde edilen bulguları içermektedir ve yalnızca yetkilendirilmiş kişiler için tasarlanmıştır. Rapor, tescilli ve gizli bilgiler barındırabilir. Herhangi bir biçimde tamamen veya kısmen çoğaltılması, yeniden dağıtılması veya kullanılması, ilgili tarafların onayını gerektirir. Raporun içeriği, yalnızca belirli yetkilendirilmiş kişilere açıklanabilir ve paylaşılabilir.

2. Feragatname

Bu sızma testi, belirli bir uygulamanın potansiyel güvenlik zayıflıklarını ve açıklarını belirlemek amacıyla gerçekleştirilmiştir. Test sonuçları, belirli bir zaman diliminde elde edilen veriler doğrultusunda hazırlanmıştır ve bu süre sonrasında meydana gelen değişiklikleri yansıtmaz. Rapor, yalnızca testin yapıldığı zaman diliminde geçerli olan bilgileri sunar ve herhangi bir sistem veya uygulama üzerindeki güvenlik durumunu sürekli olarak garanti etmez.

3. Katkıda Bulunanlar

İsim	Soyisim
Gürkan	Zengin
Hüseyin	Ayağa
Sabri	Küçük
Furkan Kağan	Taşkın
Naci	Balcı

4. Risk Puanlama Tablosu

Aşağıdaki tablo, güvenlik açığı ve risk etkisini değerlendirmek için belge boyunca kullanılan önem düzeylerini ve karşılık gelen CVSS puan aralığını tanımlamaktadır.

RİSK	CVSS V3 SKOR ARALIĞI	TANIMLAR
Kritik	9.0-10.0	**Zafiyet:** • Zafiyet basittir. • Sistem düzeyinde tehlikelerle sonuçlanır. **Alınacak Aksiyon:** • Hemen düzeltilmeli.
Yüksek	7.0-8.9	**Zafiyet**: • İstismar etmek daha zordur. Daha farklı bilgiler gerektirebilir. • Veri kaybına veya kesintiye neden olabilir. **Alınacak Aksiyon**: • Mümkün olan en kısa sürede düzeltilmeli.
Orta	4.0-6.9	**Zafiyet:** • Zafiyet var ancak istismar edilemeyebilir. • Güvenlik açığını istismar etmek için ekstra adımlar gerektirebilir. **Alınacak Aksiyon:** • Yüksek öncelikli sorunlardan sonra düzeltilmeli.
Düşük	0.1-3.9	**Zafiyet:** • Zafiyetler istismar edilemez. • Yine de bu Zafiyetin kapatılması saldırı yüzeyini azaltacaktır. **Alınacak Aksiyon:** • Bir sonraki bakım sürecinde düzeltin.
Bilgi	N/A	• Zafiyet bulunmamaktadır. • Test sırasında gözlemlenen noktalar, güçlü kontroller ve ek belgeler hakkında ek bilgiler sağlanmıştır.

5. Zafiyet Bilgilendirme Tablosu

Aşağıdaki tablo, bulunan zafiyetleri ve önerilen düzeltmeleri göstermektedir:

BULGULAR	CVSS 3.0 SKORU	ÖNERİLER
Insecure Direct Object References (IDOR)	**6.5**	Fiyat hesaplamaları yalnızca sunucu tarafında yapılmalı, istemci tarafında gelen değerler sadece gösterim amacıyla kullanılmalı.
Broken Access Control (BAC)	**9.1**	Kullanıcı rollerini ve erişim izinlerini net bir şekilde tanımlayın.
Stored Cross-Site Scripting (XSS)	**7.2**	Kullanıcıdan alınan tüm verileri sunucu tarafında doğrulayın ve temizleyin.
Business Logic	**5.3**	Yıldız puanı gibi kritik parametreler, backend tarafından uygun bir şekilde doğrulanmalı ve geçersiz değerler reddedilmelidir.
Insecure Direct Object References (IDOR)	**6.5**	Kullanıcıların yalnızca kendi bakiyelerine erişim izni olmalı; diğer kullanıcıların bakiyeleri için yetki kontrolü yapılmalıdır.

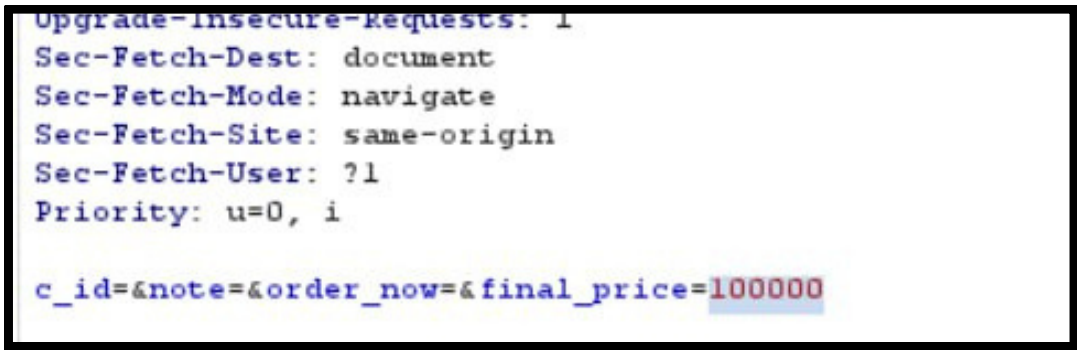
6. Bulunan Zafiyetler

6.1. Insecure Direct Object References (IDOR)

CVSS Skoru: 6.5 (Orta)

AÇIKLAMA:	Sepet işlemleri sırasında, siparişin oluşturulma aşamasında istemci tarafından gönderilen toplam fiyat bilgisinin sunucu tarafında doğrulanmadan işlenmesi nedeniyle bir güvenlik açığı oluşmaktadır.
YÖNTEM:	Manuel
ARAÇLAR:	
REFERANS:	Insecure Direct Object References

Kanıt



Sipariş oluşturma işlemin için gönderilen HTTP paketi içerisinde final_price adında bir parametre mevcut. Bu parametredeki 10000 değerini 5 ile değiştirerek sipariş oluşturabildik.

Zafiyetin Doğurabileceği Sonuçlar:

- Kullanıcılar, toplam fiyatı manipüle ederek haksız kazanç sağlayabilirler.
- Şirketin finansal kaybına yol açar ve uygulamanın güvenliği zedelenir.
- Suistimal edildikçe şirketin itibarı zarar görebilir.

Zafiyetin Kapatılması İçin Öneriler:

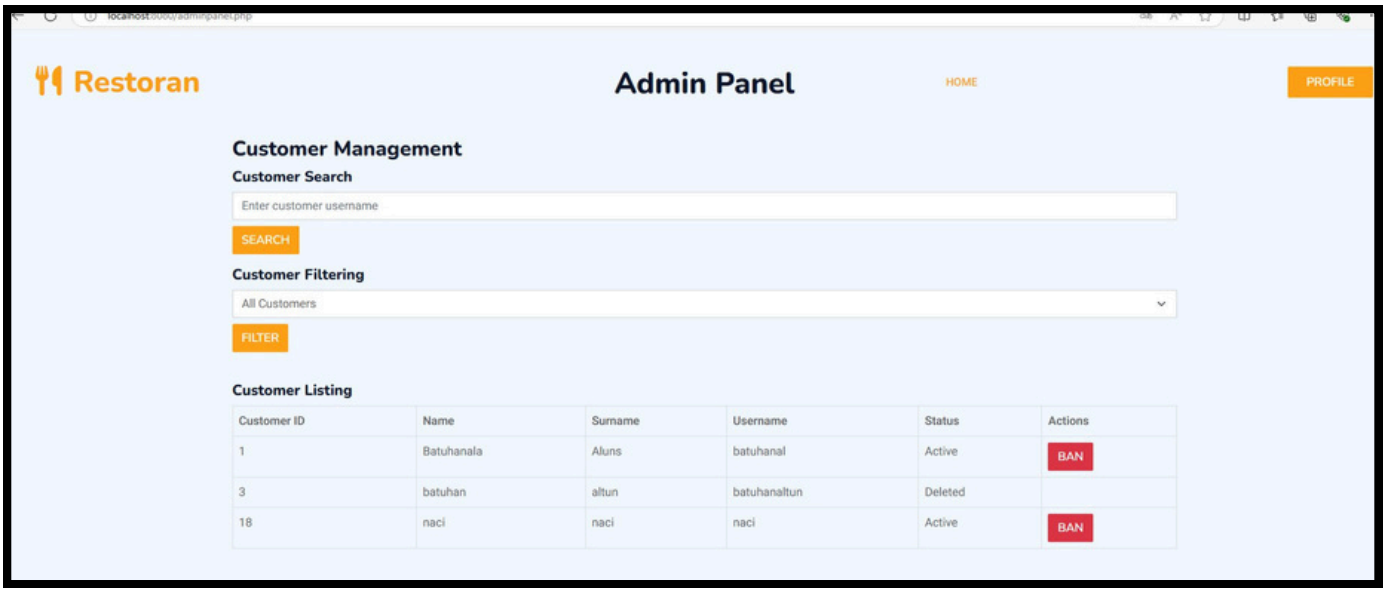
- Fiyat hesaplamaları yalnızca sunucu tarafında yapılmalı, istemci tarafında gelen değerler sadece gösterim amacıyla kullanılmalı.
- Sunucuya gönderilen fiyat bilgilerinin ve parametrelerin geçerliliği sunucu tarafında doğrulanmalı.
- Girdi doğrulama ve güvenlik kontrolleri artırılmalı.

6.2. Broken Access Control (BAC)

CVSS Skoru: 9.1 (Kritik)

AÇIKLAMA:	Kullanıcı, adminpanel.php gibi bir sayfaya URL değiştirerek erişim sağlayabiliyor. Normalde yalnızca yetkili kullanıcıların erişmesi gereken bu sayfaya, yetkisiz bir kullanıcı (örneğin, "user" rolündeki bir kullanıcı erişim sağlayabiliyor.
YÖNTEM:	Manuel
ARAÇLAR:	
REFERANS:	Broken Access Control

Kanıt



Zafiyetin Doğurabileceği Sonuçlar:

- Yetkisiz Erişim: Yetkisiz kullanıcılar, yönetimsel işlemleri gerçekleştirebilir. Bu, hassas verilerin sızdırılmasına veya kötüye kullanılmasına neden olabilir.
- Veri Manipülasyonu: Yetkisiz kullanıcılar, veri silme, ekleme veya güncelleme işlemleri gerçekleştirebilir.
- Sistem Güvenliği: Yönetim paneline erişim, sistemin güvenliğini tehlikeye atar, bu da daha ciddi güvenlik ihlallerine yol açabilir.

Zafiyetin Kapatılması İçin Öneriler:

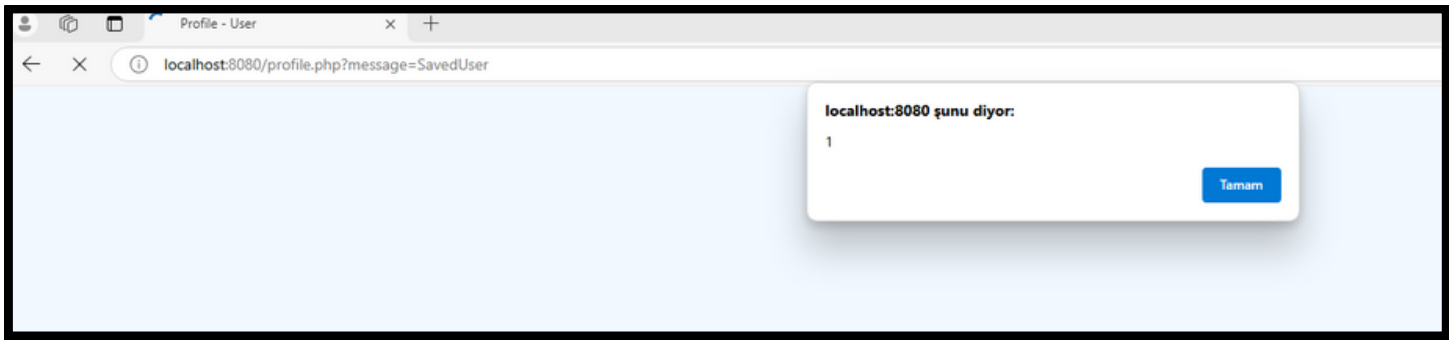
- Rol Tabanlı Erişim Kontrolü (RBAC) Uygulama: Kullanıcı rollerini ve erişim izinlerini net bir şekilde tanımlayın. Sadece yetkili kullanıcıların erişebileceği sayfaları kontrol edin.
- Sunucu Tarafında Kontrol: Kullanıcıların erişim haklarını her istekte sunucu tarafında kontrol edin. Örneğin, oturum açmış kullanıcının rolünü kontrol ederek, bu kullanıcıya uygun sayfalara erişim izni verin.

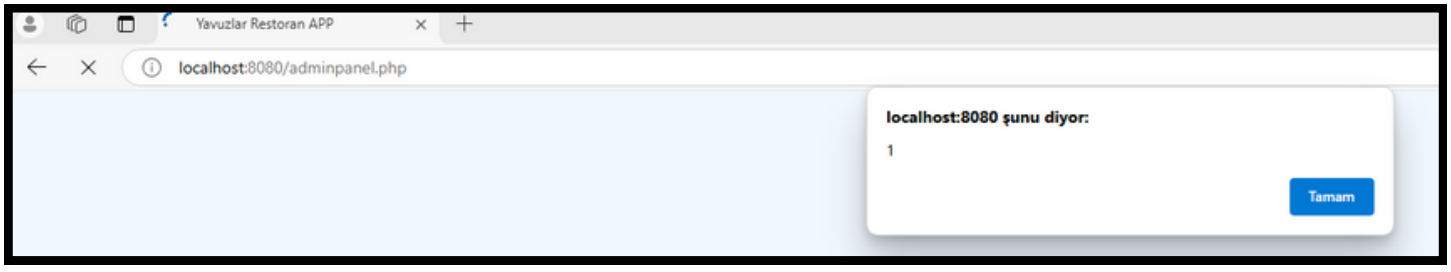
6.3. Stored Cross-Site Scripting (XSS)

CVSS Skoru: 6.1 (Orta)

AÇIKLAMA:	User panelde değişilen kullanıcı ismi admin panelde de görüldüğünden tehlikeli xss sonuçları meydana geliyor. Ayrıyetten Admin panelinde oluşturulan diğer verilerde xss içeriyor.
YÖNTEM:	Manuel
ARAÇLAR:	
REFERANS:	Cross-Site Scripting (XSS)

Kanıt





Zafiyetin Doğurabileceği Sonuçlar:

- Kullanıcı Verilerinin Sızdırılması: Kötü niyetli bir kullanıcı, zararlı JavaScript kodunu enjekte ederek, oturum bilgileri gibi hassas kullanıcı verilerini çalabilir.
- Oturum Ele Geçirme: XSS saldırıları, kullanıcıların oturumlarının ele geçirilmesine neden olabilir, bu da kötü niyetli kullanıcıların diğer kullanıcıların hesaplarına erişmesine yol açar.
- Veri Manipülasyonu: Kötü amaçlı scriptler aracılığıyla, uygulamanın işleyişi manipüle edilebilir. Bu, kullanıcılar arasında güveni sarsabilir ve veri bütünlüğünü tehlikeye atabilir.

Zafiyetin Kapatılması İçin Öneriler:

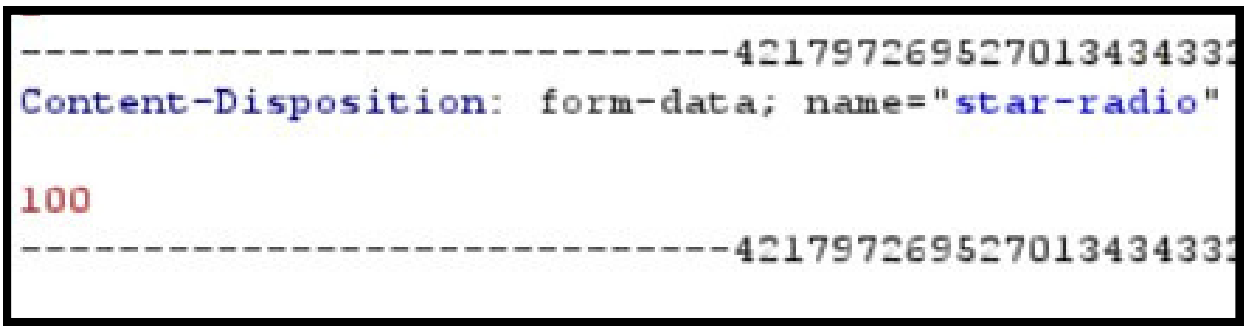
- Web uygulamalarını korumak için bir WAF kullanarak, kötü niyetli trafiği tespit edip engelleyebilirsiniz. WAF, uygulama katmanında gelen istekleri analiz ederek, XSS gibi yaygın saldırıları filtreleyebilir ve zararlı içeriklerin sunucuya ulaşmasını önleyebilir.
- Kullanıcıdan alınan tüm verileri sunucu tarafında doğrulayın ve temizleyin. HTML özel karakterlerini uygun şekilde escape ederek zararlı kodların çalışmasını engelleyin
- Kullanıcıdan gelen verileri temizlemek için HTML temizleme (cleaning) fonksiyonları kullanın. Örneğin, htmlspecialchars() veya strip_tags() gibi PHP fonksiyonları ile kullanıcıdan alınan verilerden zararlı içerikleri ayıklayabilirsiniz.
- Uygulamanıza bir CSP ekleyerek, yalnızca güvenilir kaynaklardan gelen içeriklerin yüklenmesine izin verin. Bu, kötü niyetli scriptlerin çalışmasını sınırlayarak XSS saldırılarına karşı bir koruma katmanı sağlar.

6.4. Business Logic

CVSS Skoru: 5.3 (Orta)

AÇIKLAMA:	Sitede bir restorana yıldızlı yorum yapılırken, HTTP paketindeki star-radio parametresi kontrol edilmediğinden kullanıcılar, 10 üzerinden istedikleri sayıda yıldız vererek restoranın ortalama puanını haksız şekilde yükseltebiliyor.
YÖNTEM:	Manuel
ARAÇLAR:	
REFERANS:	Business Logic

Kanıt



Bir restorana yorum yaparken giden HTTP paketimizdeki star-radio parametresinin değerini 100 yaptık ve yorumumuz 100 yıldızlı olarak kaydedildi.

Zafiyetin Doğurabileceği Sonuçlar:

- Restoranlar, gerçekte almadıkları yüksek puanlar alarak yanıltıcı bir değerlendirme alabilirler.
- Müşteriler, yanıltıcı puanlamalar sonucunda güvenilir restoranları bulmakta zorlanabilir. kullanıcıların hesaplarına erişmesine yol açar.
- Haksız puanlama, diğer restoranların itibarını zedeler ve adil bir rekabet ortamını bozar.
- Restoranların daha yüksek puanlar alması, kullanıcıların beklentilerini yükseltebilir, bu da kötü deneyimlere yol açabilir.
- Haksız yere yüksek puan alan restoranlar, daha fazla müşteri çekebilirken, gerçek değerinin altında kalan restoranlar müşteri kaybedebilir.

Zafiyetin Kapatılması İçin Öneriler:

- Yıldız puanı gibi kritik parametreler, backend tarafından uygun bir şekilde doğrulanmalı ve geçersiz değerler reddedilmelidir.
- Kullanıcıların verebileceği maksimum yıldız sayısı 10 ile sınırlı olmalı ve bu sınırlama sunucu tarafında kontrol edilmelidir.
- Kullanıcı girişleri ve gönderimleri, sunucuya ulaşmadan önce geçerlilik kontrolleri ile denetlenmelidir.
- Puanlama işlemleri ve yorumlar, anormal aktiviteleri tespit etmek için izlenmeli ve loglanmalıdır.
- Kullanıcılar, yanıltıcı yorum veya puanlamaları raporlayabilmeli, böylece yanlışlıklar hızla tespit edilip düzeltilebilir.

6.5. Insecure Direct Object References (IDOR)

CVSS Skoru: 6.5 (Orta)

AÇIKLAMA:	Sitede bakiye yükleme işlemi sırasında, HTTP paketinde yer alan balance_user_id parametresi kontrol edilmediğinden, kullanıcılar kendi bakiyeleri dışında diğer kullanıcıların bakiyelerini de haksız yere değiştirebiliyor.
YÖNTEM:	Manuel
ARAÇLAR:	
REFERANS:	Insecure Direct Object References

Kanıt

```
-----------------------------139999659935850431034524322 92
Content-Disposition: form-data; name="balance"

-1000
-----------------------------139999659935850431034524322 92
Content-Disposition: form-data; name="balance_user_id"

17
-----------------------------139999659935850431034524322 92--
```

Ekran görüntüsündeki HTTP paketinde balance_user_id kısmına farklı bir kullanıcının id'si olan 17 yazıp balance değerini de -1000 olarak değiştirdik ve böylece diğer kullanıcının bakiyesini 1000 azaltmış olduk.

Zafiyetin Doğurabileceği Sonuçlar:

- Kullanıcılar, diğer kullanıcıların bakiyelerini değiştirebilir, bu da haksız avantajlar veya zararlar doğurabilir.
- Kullanıcılar, diğerlerinin bakiyelerine erişim sağlandığını görünce siteye olan güvenlerini kaybedebilir.
- Diğer kullanıcıların bakiyelerinin yanlışlıkla artırılması veya azaltılması, finansal kayıplara yol açabilir.
- Kullanıcılar, hesabına izinsiz müdahale edilmesi durumunda yasal yollara başvurabilir.
- Güvenlik açıkları nedeniyle sitenin itibarı zarar görebilir ve kullanıcı sayısında düşüş yaşanabilir.

Zafiyetin Kapatılması İçin Öneriler:

- Kullanıcıların yalnızca kendi bakiyelerine erişim izni olmalı; diğer kullanıcıların bakiyeleri için yetki kontrolü yapılmalıdır.
- Tüm parametreler sunucu tarafında doğrulanmalı; isteklerin geçerliliği kontrol edilmelidir.
- Farklı kullanıcı rollerine göre yetkilendirme sistemi oluşturulmalı, bu sayede hassas işlemler için ek güvenlik önlemleri alınmalıdır.
- Tüm bakiye değişiklikleri kaydedilmeli ve anormal aktiviteler için izlenmelidir.
- Giriş verileri, sunucuya ulaşmadan önce geçerlilik kontrolleri ile denetlenmelidir.