



YAVUZLAR

RESTORANT SİTESİ PENTEST RAPORU

ÖZGÜL AFRA SU

İçindekiler

1. Giriş	2
2. Test Kapsamı	2
3. Yöntemoloji.....	2
4. Bulunan Açıklar.....	3
4.1. Gereksiz Veri Tabanı Yükleme.....	3
4.2.Local File Inclusion (LFI) Açığı	5
4.3. Yetkisiz Veri Değişikliği	7
4.4. Boş Kupon Ekleme Açığı.....	9
5. Sonuçlar ve Öneriler	10

1. Giriş

Bu rapor, Yavuzlar takımının gönüllü olarak geliştirdiği yemek sistemi projesinin güvenlik testlerini içermektedir. Testler, sistemin güvenlik açıklarını belirlemek ve bu açıkların kapatılması için öneriler sunmak amacıyla gerçekleştirilmiştir.

2. Test Kapsamı

Test Edilen Uygulama

<https://github.com/1Xnes/yavuzlar/tree/main/hafta3odev>

3. Yöntemoloji

Testler, manuel inceleme ve kullanıcı etkileşimleri ile gerçekleştirilmiştir. Belirli araçlar kullanılmamıştır, ancak tarayıcı üzerinde geliştirici araçları ile incelemeler yapılmıştır.

4. Bulunan Açıklar

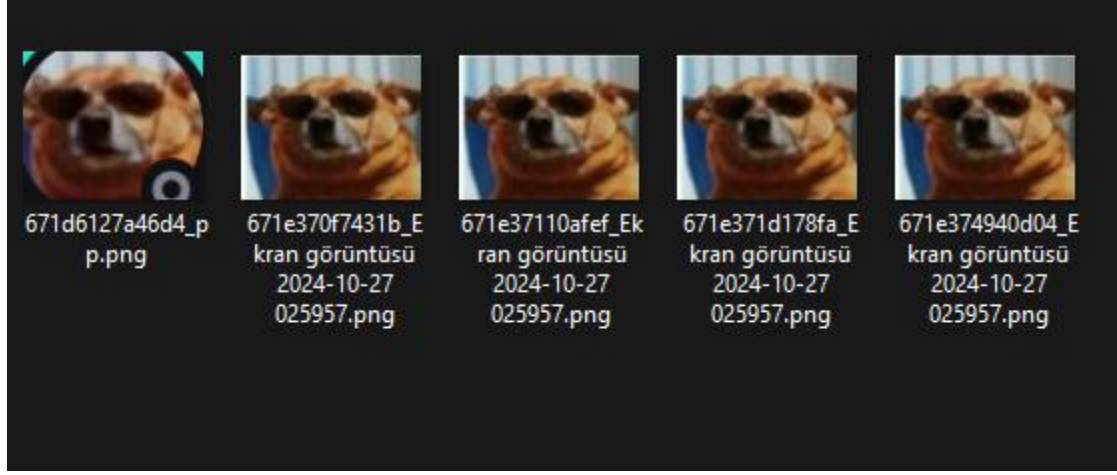
4.1. Gereksiz Veri Tabanı Yüklemesi

- **Zafiyetin Nerede Oluştı:** customer_profile.php
- **Zafiyetin Doğurabileceği Sonuçlar:** Gereksiz veri tabanı yüklemesi, sistem performansını olumsuz etkileyebilir.
- **Zafiyetin Kapatılması İçin Öneriler:** Profil fotoğrafı yalnızca değiştiğinde güncellenmeli, aksi takdirde mevcut fotoğraf kullanılmalıdır.
- **CVSS Puanı:** 4.0 (Orta)

The screenshot displays a user profile interface with the following elements:

- PROFIL** (Profile) header in purple.
- A green success message: **Profil resmi başarıyla güncellendi.** (Profile picture successfully updated).
- Profil Bilgileri** (Profile Information) section with input fields for Ad (afra), Soyad (su), and Kullanıcı Adı (farfara).
- A button labeled **PROFİLİ GÜNCELLE** (Update Profile).
- Profil Resmi** (Profile Picture) section with a profile picture icon and a button labeled **Dosya Seç** (Select File).
- A button labeled **PROFİL RESMİNİ GÜNCELLE** (Update Profile Picture).
- Şifre Değiştir** (Change Password) section with a button labeled **ŞİFRE DEĞİŞTİR** (Change Password).
- Bakiye** (Balance) section showing **Mevcut Bakiye: 5,000.00 TL** (Current Balance: 5,000.00 TL).
- An input field for **Eklenecek Miktar (TL):** (Amount to be added (TL):) with a button labeled **BAKİYE EKLE** (Add Balance).
- A button labeled **ANA SAYFAYA DÖN** (Return to Home Page).

Profil resmi eklendikten sonra sayfa yenilendi.



				id	user_id	photo_path	created_at
<input type="checkbox"/>	Düzenle	Kopyala	Sil	1	2	/uploads/profile_pictures/671d2d7c93cf5_deneme.txt	2024-10-26 20:57:16
<input type="checkbox"/>	Düzenle	Kopyala	Sil	2	2	/uploads/profile_pictures/671d2db0a4455_deneme.txt	2024-10-26 20:58:08
<input type="checkbox"/>	Düzenle	Kopyala	Sil	3	2	/uploads/profile_pictures/671d2de0770b6_deneme.txt	2024-10-26 20:58:56
<input type="checkbox"/>	Düzenle	Kopyala	Sil	4	2	/uploads/profile_pictures/671d30e5dc8d0_deneme.txt	2024-10-26 21:11:49
<input type="checkbox"/>	Düzenle	Kopyala	Sil	5	2	/uploads/profile_pictures/671d30ee6386f_whoami.php	2024-10-26 21:11:58

Veri tabanı ve profil fotoğraflarının tutulduğu klasör kontrol edildiğinde sayfa yenilenme sayısı kadar profil fotoğrafı kaydı yapıldığı görüldü.

4.2. Local File Inclusion (LFI) Açığı

- **Zafiyetin Nerede Oluştı:** customer_profile.php
- **Zafiyetin Doğurabileceği Sonuçlar:** Saldırganlar, sunucu üzerinde yetkisiz dosyalar çalıştırarak sistemin kontrolünü ele geçirebilir.
- **Zafiyetin Kapatılması İçin Öneriler:** Yüklenen dosyaların türü kontrol edilmeli ve yalnızca belirli dosya uzantılarına izin verilmelidir.
- **CVSS Puanı:** 7.5 (Yüksek)



PROFIL

Profil Bilgileri

Ad: Soyad:
Kullanıcı Adı:

PROFİLİ GÜNCELLE

Profil Resmi

Profil Resmi: deneme.txt

PROFİL RESMİNİ GÜNCELLE

Şifre Değiştir

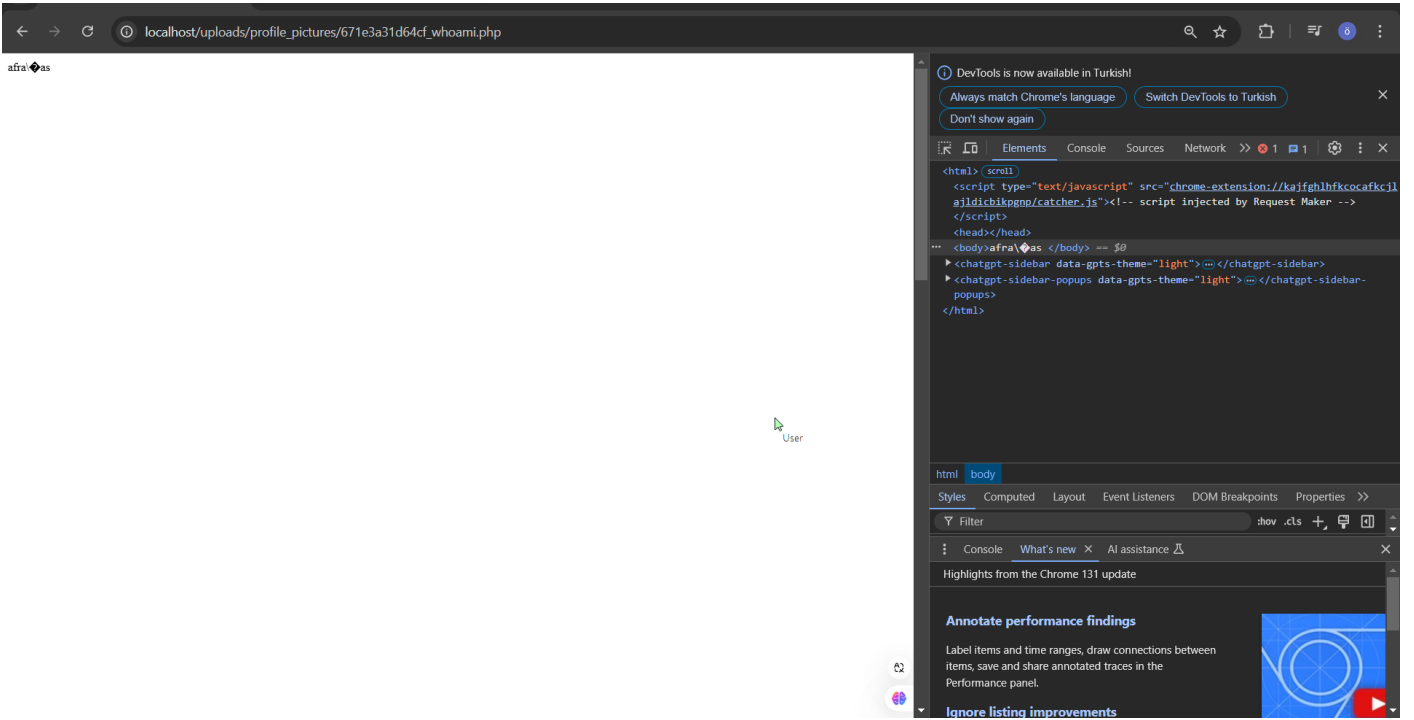


PROFIL

Profil resmi başarıyla güncellendi.

Profil Bilgileri

Sisteme txt uzantılı dosya eklenebilme olasılığı test edildi ve olumlu sonuç alındı.



Sisteme "whoami" adında basit bir php shell dosyası yüklendi ve bu dosya çalıştırılarak sistemdeki bilgisayar kullanıcısının ismi elde edildi.

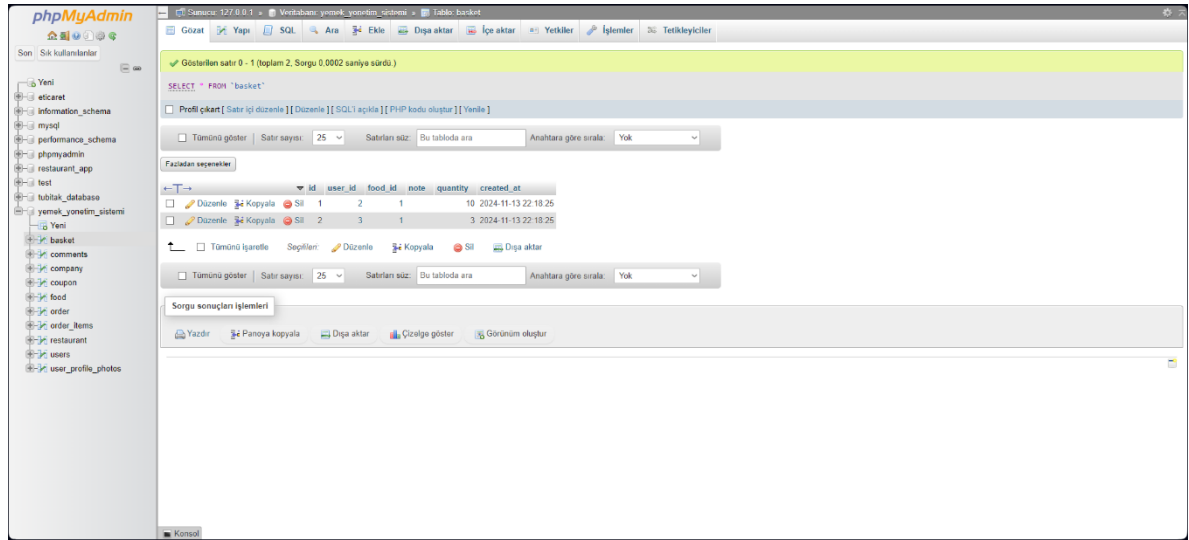
4.3. Yetkisiz Veri Değişikliği

- **Zafiyetin Nerede Oluştu:** customer_chart.php
- **Zafiyetin Doğurabileceği Sonuçlar:** Kullanıcıların sepetlerinde yetkisiz değişiklikler yapılabilir.
- **Zafiyetin Kapatılması İçin Öneriler:** Sunucu tarafında veri doğrulama yapılmalı ve kullanıcıların yalnızca kendi sepetleri üzerinde değişiklik yapmalarına izin verilmelidir.
- **CVSS Puanı:** 5.0 (Orta)

The image displays two screenshots of a web application running on localhost/customer_cart.php. The application is titled "SEPETİM" (My Cart) and features a shopping cart interface. The cart contains one item, "ZUPZURNA DURUM", with a price of 200.00 TL and a quantity of 10. The total amount is 2,000.00 TL. The interface includes buttons for "Sepet güncellendi.", "GÜNCELLE", "NOT GÜNCELLE", "KALDIR", "KUPONU UYGULA", "SİPARİŞ VER", "ALİŞVERİŞE DEVAM ET", and "ANA SAYFAYA DÖN".

The second screenshot shows the same interface with the quantity of the item changed to 2. The DevTools console on the right shows the source code of the application, highlighting the form action for updating the cart. The code snippet is as follows:

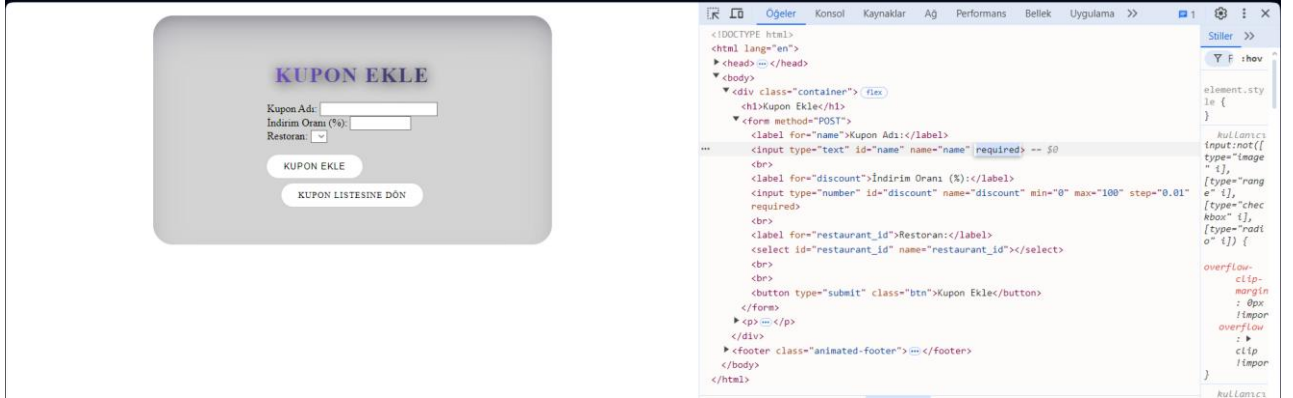
```
<tr>
  <td>ZUPZURNA DURUM </td>
  <td>200.00 TL</td>
  <td>200.00 TL</td>
  <td>
    <input type="text" value="10" />
    <button type="button" class="btn" value="GÜNCELLE" />
    <button type="button" class="btn" value="NOT GÜNCELLE" />
    <button type="button" class="btn" value="KALDIR" />
  </td>
  <td>2,000.00 TL</td>
  <td>
    <input type="text" value="" />
    <button type="button" class="btn" value="KUPONU UYGULA" />
  </td>
  <td>
    <button type="button" class="btn" value="SİPARİŞ VER" />
    <button type="button" class="btn" value="ALİŞVERİŞE DEVAM ET" />
    <button type="button" class="btn" value="ANA SAYFAYA DÖN" />
  </td>
</tr>
</tbody>
</table>
<form action="update_cart.php" method="POST">
  <input type="hidden" name="basket_id" value="1" />
  <input type="text" name="quantity" value="10" min="1" max="10" />
  <button type="submit" class="btn" value="GÜNCELLE" />
</form>
</td>
</tr>
</tbody>
</table>
<form action="apply_coupon.php" method="POST">
  <input type="text" name="coupon_code" value="" />
  <button type="button" class="btn" value="KUPONU UYGULA" />
</form>
</td>
</tr>
</tbody>
</table>
```

Kullanıcı, sepete ürün ekledikten sonra tarayıcıda sağ tıklayıp "incele" seçeneğiyle sayfayı incelediğinde, basket_id value değerini manuel olarak değiştirebildiği görüldü. Bu değişiklik, ilgili basket_id değerine sahip kullanıcının sepetinde de değişiklik yapılmasına olanak tanımakta.

4.4. Boş Kupon Ekleme Açığı

- **Zafiyetin Nerede Oluştu:** company_add_coupon.php
- **Zafiyetin Doğurabileceği Sonuçlar:** Sistemde geçersiz kuponlar oluşturulabilir, bu da kullanıcı deneyimini olumsuz etkileyebilir.
- **Zafiyetin Kapatılması İçin Öneriler:** Form doğrulama kuralları güçlendirilmeli ve boş kupon eklenmesine izin verilmemelidir.
- **CVSS Puanı:** 3.5 (Düşük)



Sayfadaki required parametresi manuel olarak kaldırıldığında boş kupon girişi yapılabildiği gözlemlendi.

5. Sonular ve neriler

Yapılan testler sonucunda, sistemde birkaç gvenlik aıėı tespit edilmiřtir. Bu aıkların kapatılması iin yukarıda belirtilen nerilerin dikkate alınması nemlidir. Projenin gvenliėini artırmak iin dzenli gvenlik testleri yapılması ve gncellemelerin takip edilmesi nerilmektedir.
