YAVUZLAR

RESTORANT SİTESİ PENTEST RAPORU

ÖZGÜL AFRA SU

İçindekiler

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

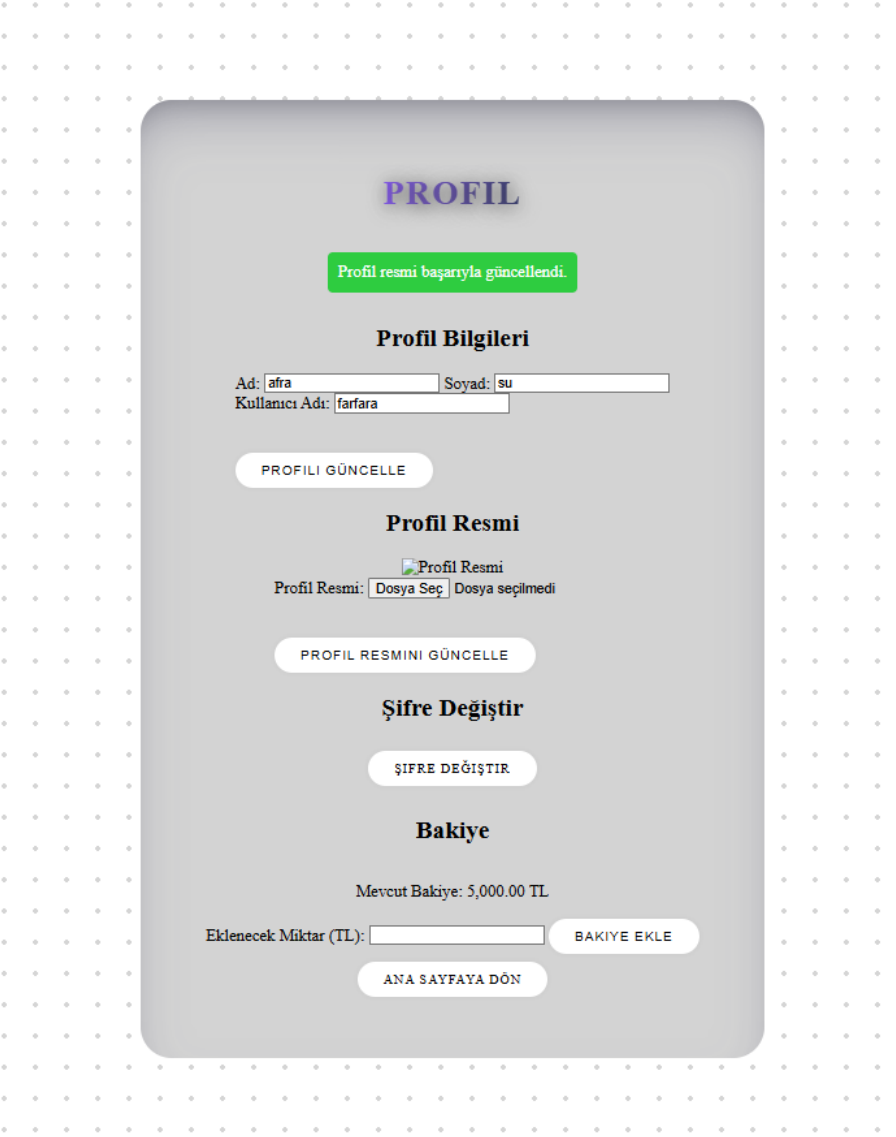
3. Yöntemoloji

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

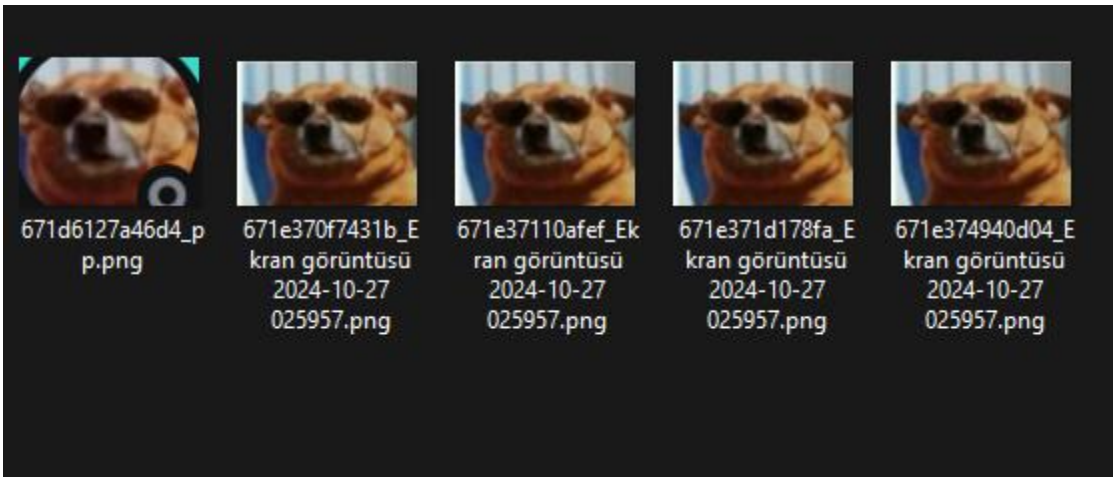
4. Bulunan Açıklar

4.1. Gereksiz Veri Tabanı Yüklemesi

- **Zafiyetin Nerede Oluştu**: 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)



Profil resmi eklendikten sonra sayfa yenilendi.



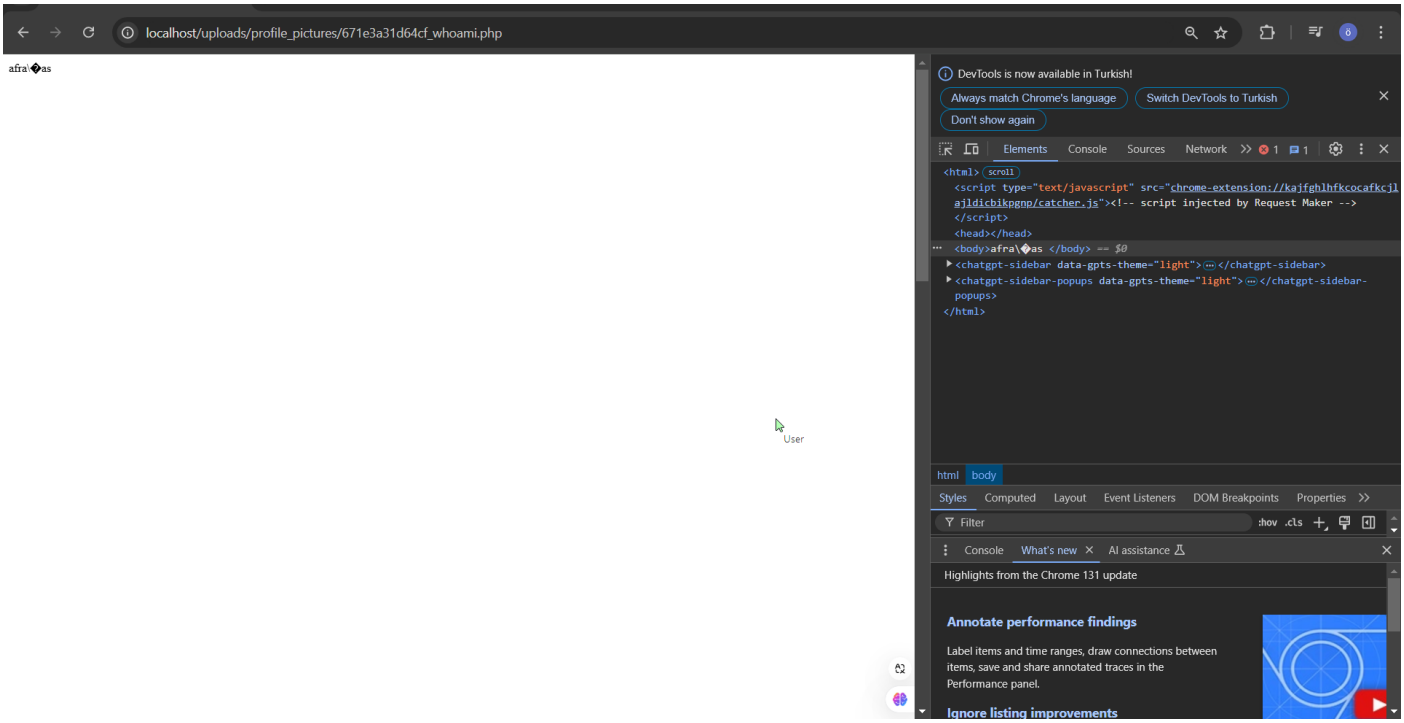
		id	user_id	photo_path	created_at
☐	Düzenle Kopyala Sil	1	2	/uploads/profile_pictures/671d2d7c93cf5_deneme.txt	2024-10-26 20:57:16
☐	Düzenle Kopyala Sil	2	2	/uploads/profile_pictures/671d2db0a4455_deneme.txt	2024-10-26 20:58:08
☐	Düzenle Kopyala Sil	3	2	/uploads/profile_pictures/671d2de0770b6_deneme.txt	2024-10-26 20:58:56
☐	Düzenle Kopyala Sil	4	2	/uploads/profile_pictures/671d30e5dc8d0_deneme.txt	2024-10-26 21:11:49
☐	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 Oluştu**: 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)

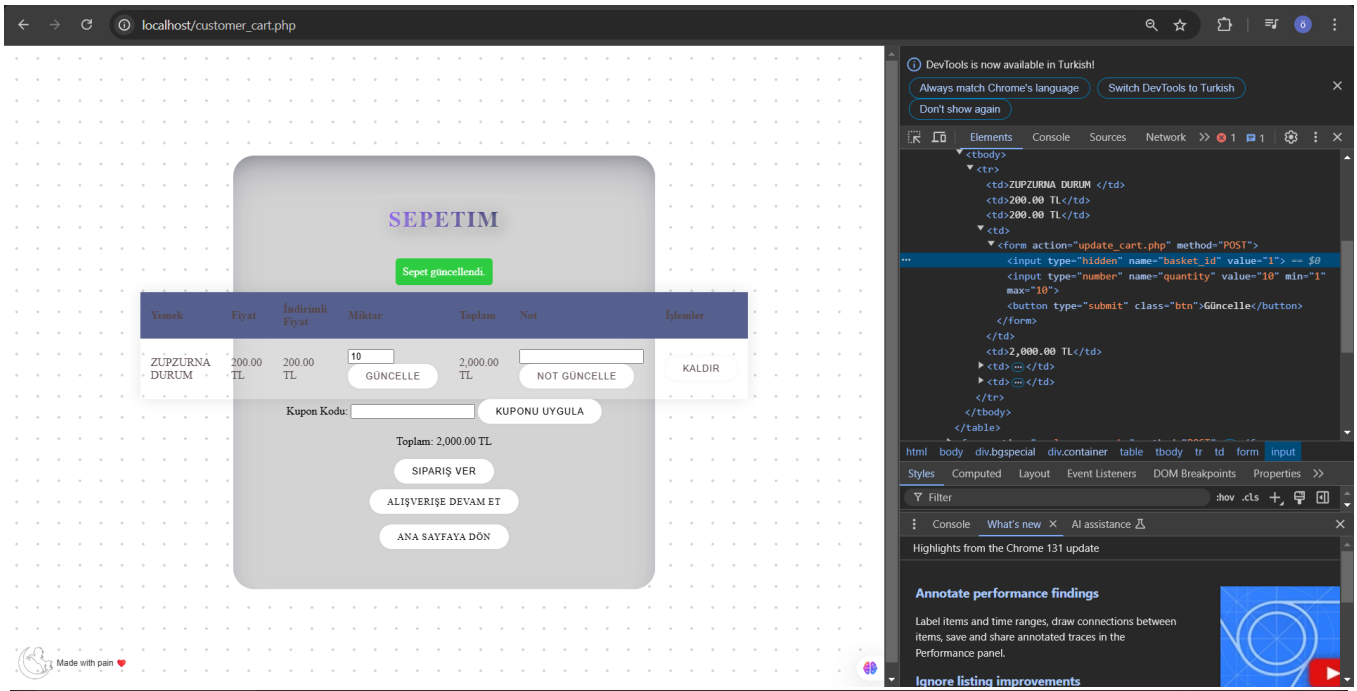
Sisteme txt uzantılı dosya eklenebilme olasılığı test edildi ve olumlu sonuç alındı.

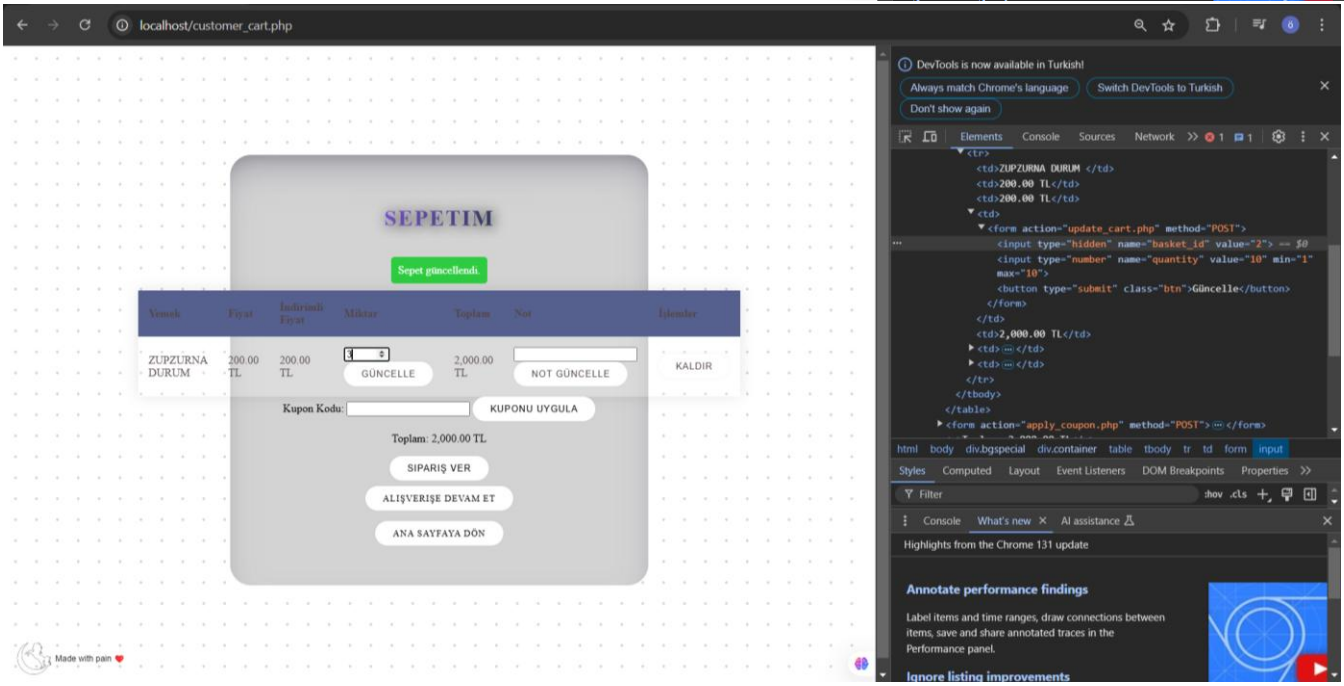


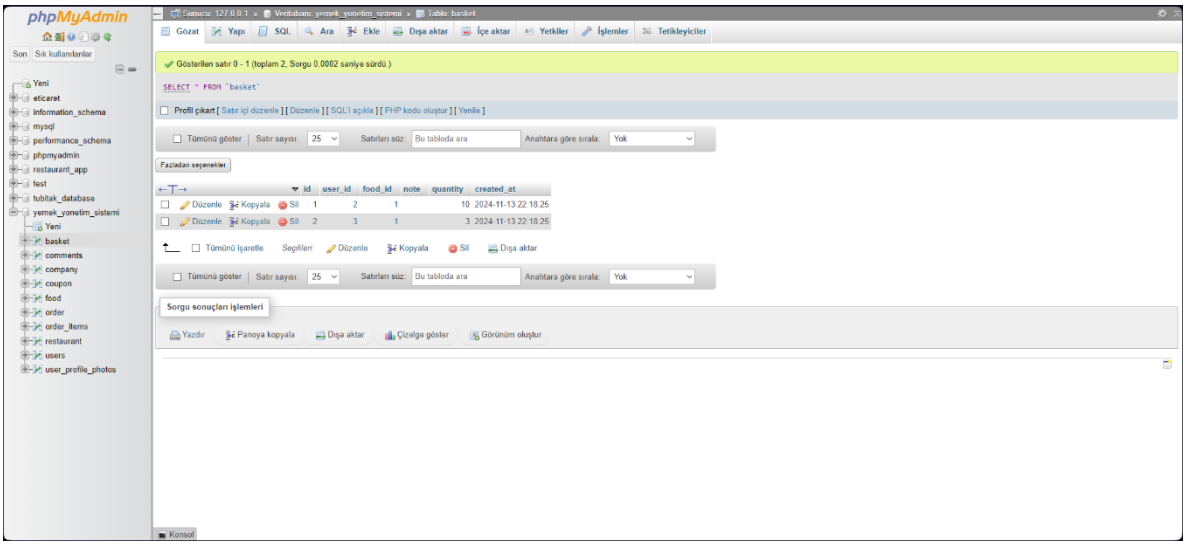
Sisteme "whoami" adında basit bir php shell dosyası yüklendi ve bu dosya çalıştırılarak sistemdeki bilgisayar kullanıcısının ismi elde edildi.

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)



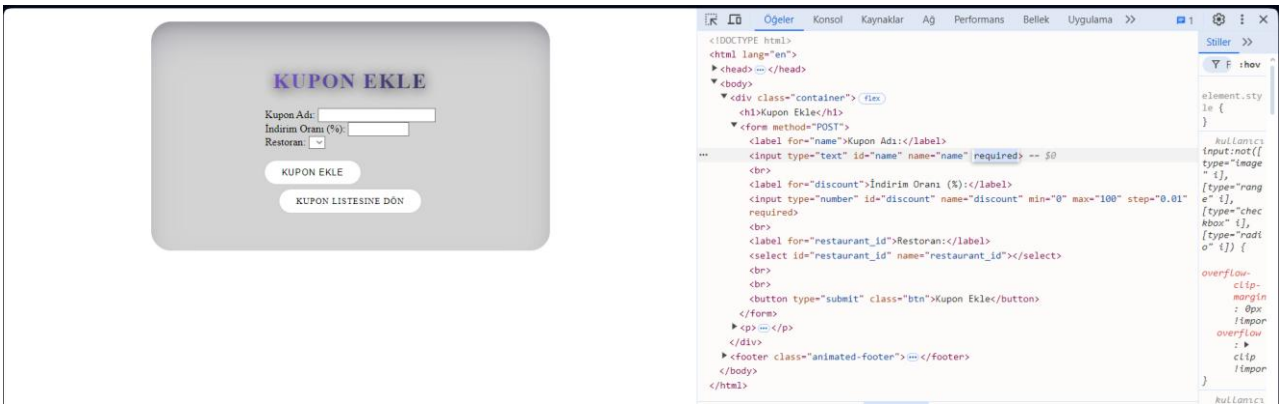


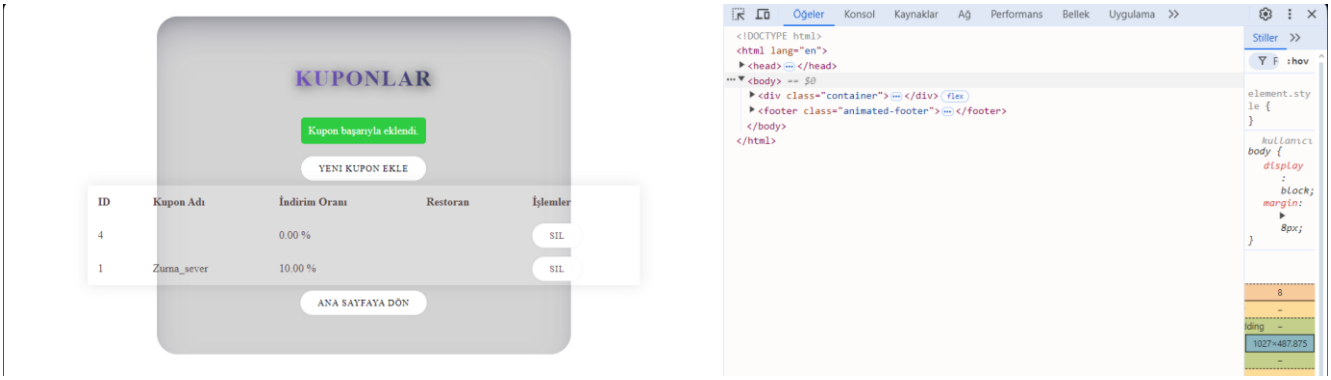


Kullanıcı, sepete ürün ekledikten sonra tarayıcıda sağ tıklayıp "incele" seçeneğiyle sayfayı incelediğinde, basket_id value değerini manuel olarak değiştirebildiği görüldü. Bu değişiklik, ilgili basket_id değerine sahip kullanıcının sepetinde de değişiklik yapılmasına olanak tanımakta.

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. Sonuçlar ve Öneriler

Yapılan testler sonucunda, sistemde birkaç güvenlik açığı tespit edilmiştir. Bu açıkların kapatılması için yukarıda belirtilen önerilerin dikkate alınması önemlidir. Projenin güvenliğini artırmak için düzenli güvenlik testleri yapılması ve güncellemelerin takip edilmesi önerilmektedir.