Restaurant App

Web Uygulaması Testi Raporu

Güray Dağ

İçindekiler

Uyarı

Bu rapor tamamen test ve öğrenim amacıyla yazılmış bir rapordur. İçerisinde hatalar, yanlışlar bulunabilir.

Bu rapor Gürkan Zengin'e ait olan Restaurant App uygulamasına karşı yapılmış temel sızma testinin sonuç raporudur. Burada yapılanların herhangi bir yasal yükümlülüğü bulunmamaktadır.

Bu sızma testi süresinde test ortamına herhangi bir zarar verilmemiştir. Hizmet reddi saldırıları yapılmamış, işleyiş bozulmamıştır.

Rapor içinde yer alan çözüm önerilerine konu hakkında fikir verme amaçlı yer verilmiştir. Çözüm önerilerinin uygulanması sebebi ile çıkabilecek problemlerden raporu hazırlayan kişi sorumlu tutulamaz. Önerilerde sunulan değişikliklerden gerçekleştirilmeden önce konu hakkında uzman kişilerden destek alınması tavsiye edilir.

Kapsam

Bu test, web uygulamasının doğası gereği yerel makinede, yerel IP adresinde gerçekleştirilmiştir. Web uygulamasının başka herhangi bir makine ile bağlantısı bulunmamaktadır.

IP ADRESİ	Açıklama
localhost	Apache 2.4.62

Test Ekibi

Güray Dağ

Genel Değerlendirme

Test sonucu web uygulamasında herhangi kritik, yüksek veya düşük seviye zafiyet tespit edilmemiştir.

Web uygulamasında IDOR (Insecure Direct Object Reference) zafiyeti tespit edilmiştir. Orta risk seviyesine sahip olan bu zafiyet, sunucu tarafında yeterli kontrollerin yapılmamasından kaynaklanmaktadır.

Raporun devamında bu zafiyetlerle alakalı daha detaylı bilgiler verilecektir.

Sızma Testi Türleri

Belirlenen sistemin veya ağın güvenlik açısından analiz edilmesi ve sistemin güvenlik açıklarının ve güvenlik boşluklarının bulunması, bu açıklardan faydalanılarak sistemlere sızılması. Otomatik tarama araçları ile gerçekleştirilen zafiyet taramaları sızma testinin bir aşamasıdır; ancak sızma testi değildir.

Beyaz Kutu

Beyaz kutu testi, ağdaki tüm sistemlerden bilgi sahibi olarak yapılan sızma testi türüdür. Test uzmanının dışarıdan ya da içeriden ağa girmeye ve zarar vermeye çalışmasının simülasyonudur.

Siyah Kutu

Siyah kutu testi saldırı yapılacak ağ hakkında hiçbir bilgi sahibi olmadan dışarıdan ağa ulaşmaya çalışan saldırganın verebileceği zararın boyutlarının algılanmasını sağlar.

Gri Kutu

Gri kutu testi iç ağda bulunan yetkisiz bir kullanıcının sistemlere verebileceği zararın analiz edilmesini sağlar. Veri çalınması, yetki yükseltme ve ağ paket kaydedicilerine karşı ağ zayıflıkları denetlenir.

Risk Derecelendirme

Seviyesi	Risk puanı	Detay Açıklama
Kritik	5	Kritik güvenlik açıkları, sistemin tamamını tehdit eden çok ciddi riskler taşır. Saldırganlar tarafından kolayca sömürülebilir ve ciddi sonuçlar doğurabilir. Anında müdahale edilmelidir.
Yüksek	4	Yüksek seviyeli güvenlik açıkları, önemli güvenlik riskleri oluşturur ve saldırganların sistemi etkili bir şekilde hedef almasına izin verebilir. Acilen düzeltilmesi gerekir.
Orta	3	Orta seviyeli güvenlik açıkları, kötüye kullanıldığında sınırlı ancak fark edilebilir zararlara yol açabilir. Bu tür açıklara dikkat edilmeli ve çözülmelidir.
Düşük	2	Düşük seviyeli güvenlik açıkları, sınırlı etkiye sahip olup genellikle sistemin genel güvenliğini ciddi biçimde etkilemez. Ancak yine de düzeltilmelidir.
Hiçbiri	1	Bu, herhangi bir güvenlik riski olmadığını veya güvenlik açığının zararsız veya etkisiz olduğunu gösterir.

Teknik Bilgiler

Hedef site hakkında Wappalyzer aracı kullanılarak pasif bilgi toplanmıştır. Debian makinesi üzerinde Apache web sunucusu uygulamasının 2.4.62 sürümünü bulundurduğu, PHP 8.3.12 sürümünü barındırdığı tespit edildi.

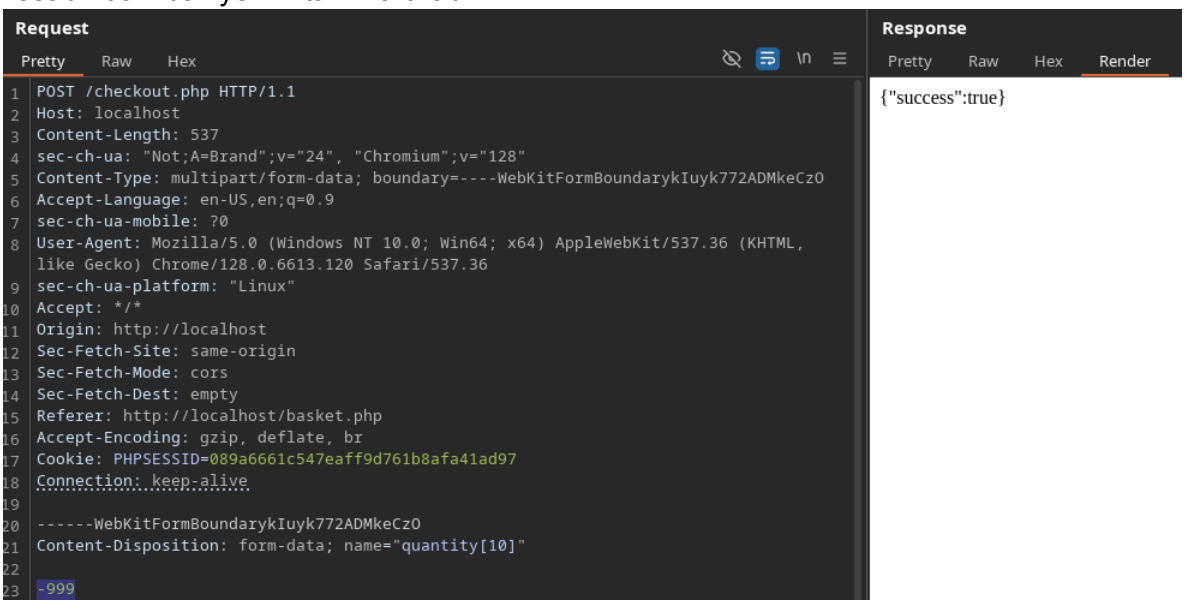
Kullanılan Araçlar

Araç	Amaç
Burp Suite	HTTP paket analizi ve manipülasyonu
Wappalyzer	Pasif keşif, bilgi toplama
Sqlmap	SQLi zafiyetini sömürmek için otomatize araç

Bulgular

Bulgu Adı			
IDOR (Insecure Direct Object Reference)			
Bulgu Kodu			
IDOR_1			
Önem Derecesi	**Erişim Noktası**	**Kullanıcı Profili**	**Durum**
Orta (5.7)	İnternet	Müşteri	Giderilmedi
Bulgunun Tespit Edildiği Bileşen/Bileşenler			
http://localhost/checkout.php			
Zafiyetin Etkisi			
Müşterilerin ücret ödemeden ürün sipariş etmelerine ve ürün tutarı kadar bakiyelerinin otomatik arttırmalarına yol açabilir.			
Zafiyetin Açıklaması			

Bu açığı istismar etmek için, saldırgan gönderilen HTTP isteğinde (örneğin Burp Suite kullanarak) ürün miktarını negatif bir değer ile değiştirebilir. Bu değişikliğin sunucu tarafında herhangi bir kontrolü bulunmuyor. Sonuç olarak, saldırgan negatif miktarda ürün alarak hesabındaki bakiye miktarını artırabilir.



Şekil 1.1. Zafiyetin Gerçekleştirilmesi

Çözüm Önerisi
Kullanıcı girdilerinin sistem sunucu tarafında doğrulanması ve temizlenmesi gerekir.
Referans
https://portswigger.net/web-security/access-control/idor

Bulgu Adı			
IDOR (Insecure Direct Object Reference)			
Bulgu Kodu			
IDOR_2			
Önem Derecesi	**Erişim Noktası**	**Kullanıcı Profili**	**Durum**
Orta (5.7)	İnternet	Müşteri	Giderilmedi

Bulgunun Tespit Edildiği Bileşen/Bileşenler

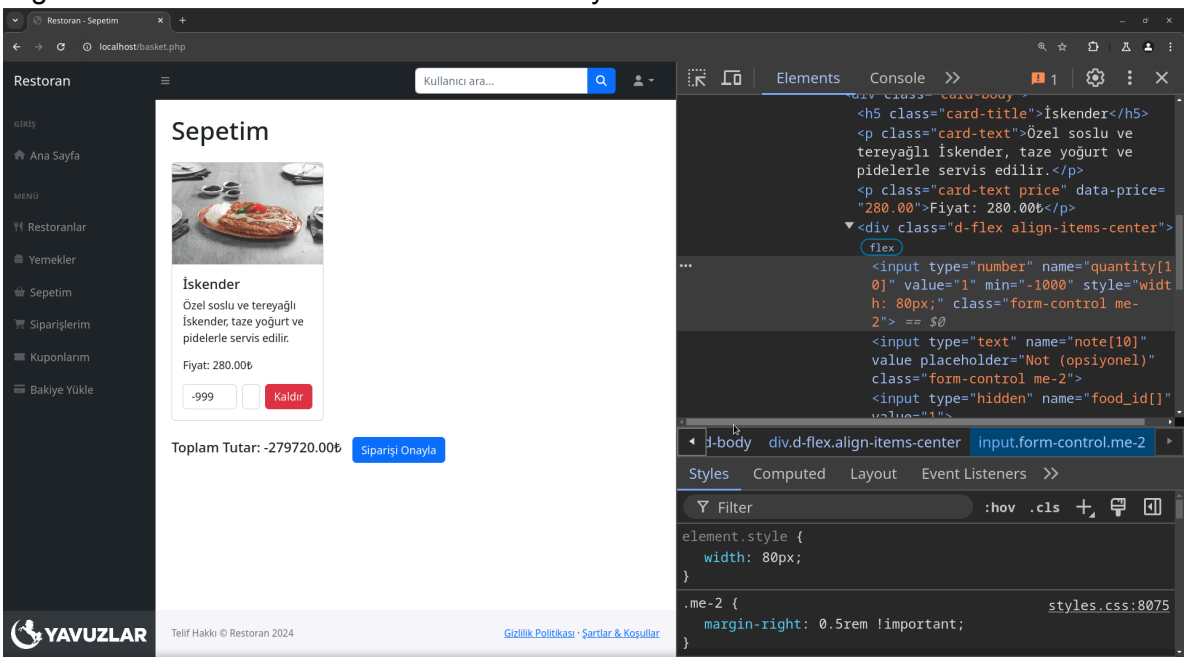
http://localhost/basket.php

Zafiyetin Etkisi

Müşterilerin ücret ödemeden ürün sipariş etmelerine ve ürün tutarı kadar bakiyelerinin otomatik arttırmalarına yol açabilir.

Zafiyetin Açıklaması

Bu açığı istismar etmek için, saldırgan istemci tarafındaki HTML formunda ürün miktarını negatif bir değer ile değiştirebilir. Bu değişiklik, sadece istemci tarafında engellenmeye çalışılmış, sunucu tarafında herhangi bir kontrol bulunmuyor. Sonuç olarak, saldırgan negatif miktarda ürün alarak hesabındaki bakiye miktarını artırabilir.



Şekil 2.1. Zafiyetin Gerçekleştirilmesi

Çözüm Önerisi

Kullanıcı girdilerinin sistem sunucu tarafında doğrulanması ve temizlenmesi gerekir.

Referans

https://portswigger.net/web-security/access-control/idor

Önlemler

- Kullanıcı girdileri sunucu tarafında da kontrol edilmeli, doğrulanmalı ve temizlenmeli.