Yavuzlar Restoran Uygulaması Güvenlik Testi

Yönetici Özeti

Yavuzlar Restoran Uygulaması için gerçekleştirilen penetrasyon testi, uygulamanın güvenlik açıklarını belirlemek ve potansiyel tehditleri değerlendirmek amacıyla yapılmıştır. Testin kapsamı, uygulamanın kullanıcı arayüzü, yönetici paneli, kullanıcı profili ve dosya yükleme mekanizmaları gibi kritik bileşenlerini içermektedir. Elde edilen bulgular, güvenlik açıklarının varlığını ve bunların olası etkilerini ortaya koymaktadır.

Yapılan testler sonucunda dört ana güvenlik açığı tespit edilmiştir. İlk olarak, oturum yönetimi ile ilgili ciddi bir zaafiyet gözlemlenmiştir. Yetkisiz kullanıcıların yönetici paneline erişim sağlayabilmesi, sistemin güvenliğini zayıflatmaktadır. Bu açık, CVSS 3.0 puanı 9.8 olarak değerlendirilmiştir ve Unauthenticated Access kategorisine girmektedir.

İkinci bulgu, kullanıcı profili bölümünde bulunan XSS (Cross-site Scripting) açığıdır. Kullanıcılar, profil bilgilerine zararlı kod ekleyerek uygulamanın farklı yerlerinde bu kodun çalışmasına neden olabilmektedir. Bu durum, kullanıcı verilerinin güvenliğini tehdit etmektedir.

Üçüncü bulgu, şirket panelinde de mevcut olan XSS açığıdır. Restoran ve yemek ekleme ekranlarında aynı zararlı yüklerin kullanılabilmesi, yönetici düzeyindeki işlemleri tehlikeye atmaktadır.

Son olarak, dosya yükleme mekanizmasındaki zafiyet, kötü niyetli dosyaların sisteme yüklenmesine olanak tanımaktadır. Kullanıcıların yüklediği dosyaların uzantı kontrolü yapılmasına rağmen, çeşitli yöntemlerle bu engelin aşılması mümkün olmaktadır.

Bu bulgular, Yavuzlar Restoran Uygulaması'nın güvenliğini ciddi şekilde tehdit etmekte ve acil düzeltmeler gerektirmektedir.

Test Kapsamı

Yavuzlar Restoran Uygulaması için gerçekleştirilen penetrasyon testinin kapsamı, uygulamanın çeşitli bileşenlerine yönelik kapsamlı bir inceleme yapılmasını içermektedir. Test süresince aşağıdaki alanlar üzerinde yoğunlaşılmıştır:

1. **Oturum Yönetimi**: Uygulamanın oturum yönetimi mekanizmaları, kullanıcıların yetkilendirilmesi ve erişim kontrolü açısından kritik bir öneme sahiptir. Test sırasında, oturum açma süreçlerinin güvenliği ve bu süreçlerdeki potansiyel zaafiyetler incelenmiştir. Özellikle, yönetici paneline yetkisiz erişim gibi durumlar detaylı bir şekilde analiz edilmiştir.

2. **Kullanıcı Profili**: Kullanıcıların kendi profillerine yüklediği bilgilerin güvenliği üzerinde durulmuştur. XSS (Cross-site Scripting) açıları, kullanıcıların profil bilgilerine zararlı kod ekleyerek diğer kullanıcıların verilerini tehdit etme potansiyeli açısından değerlendirilmiştir.

3. **Şirket Paneli**: Restoran ekleme ve yemek ekleme işlemleri gibi yönetici düzeyindeki işlevlerin güvenliğine yönelik testler gerçekleştirilmiştir. Kullanıcıların bu işlemler sırasında gerçekleştirebilecekleri potansiyel saldırı senaryoları göz önünde bulundurulmuştur.

4. **Dosya Yükleme Mekanizmaları**: Uygulamanın dosya yükleme özellikleri, kötü niyetli dosyaların sisteme yüklenmesini engelleyici önlemler açısından incelenmiştir. Yükleme süreçlerinde dosya uzantı kontrollerinin nasıl yapıldığı ve bu kontrollerin aşılabileceği yöntemler detaylandırılmıştır.

Bu testler, Yavuzlar Restoran Uygulaması'nın güvenlik açıklarını ortaya koymayı ve potansiyel tehditleri değerlendirmeyi amaçlamaktadır. Analiz edilen özellikler, uygulamanın genel güvenlik durumu hakkında önemli bilgiler sunmaktadır.

Metodoloji

Penetrasyon testi sırasında izlenen metodoloji, sistemin güvenlik açıklarını tespit etmek ve değerlendirmek amacıyla sistematik bir yaklaşım içermektedir. Test sürecinde aşağıdaki adımlar ve kullanılan araçlar detaylı bir şekilde ele alınmıştır.

1. Bilgi Toplama

Bu aşamada, hedef uygulama hakkında mümkün olduğunca fazla bilgi toplanır. Hedefin yapısı, kullanılan teknolojiler ve potansiyel zafiyetlerin bulunduğu alanlar hakkında genel bir anlayış geliştirilir. Tek bir uygulama üzerinde olduğu için yalnızca web tarayıcısı üzerinden keşif yapılmıştır.

2. Tarama

Bilgi toplama aşamasından sonra, sistemin zayıf noktalarını belirlemek için tarama işlemleri gerçekleştirilir. Bu aşamada, Burp Suite veya sqlmap gibi zafiyet tarayıcıları kullanılarak belirli güvenlik açıkları tespit edilmeye çalışılır. Tarama sonuçları, potansiyel tehditlerin belirlenmesine yardımcı olur.

3. Saldırı Simülasyonu

Bu aşamada, tespit edilen zafiyetlerin kötüye kullanılması amaçlanır. Burp Suite ve Metasploit gibi araçlar kullanılarak, XSS, SQL Injection ve dosya yükleme gibi açıklar üzerinde testler gerçekleştirilir. Bu aşamanın amacı, zafiyetlerin gerçek hayatta nasıl istismar edilebileceğini anlamaktır.

4. Raporlama

Son aşamada, tüm test sürecinin sonuçları ve bulgular raporlanır. Rapor, tespit edilen zayıf noktalar, bunların potansiyel etkileri ve önerilen düzeltme adımlarını içermektedir. Bu aşama, uygulamanın güvenlik durumunu iyileştirmek için kritik bir öneme sahiptir.

Her bir aşama, uygulamanın genel güvenlik durumu hakkında önemli bilgiler sunarak, güvenlik açıklarının hızlı bir şekilde düzeltilmesine olanak tanır. Bu sistematik yaklaşım, Yavuzlar Restoran Uygulaması'nın güvenliğini artırmak için gereklidir.

Zaafiyet Değerlendirmesi

Yavuzlar Restoran Uygulaması'nda tespit edilen güvenlik açıklarının detaylı değerlendirmesi aşağıda sunulmuştur. Her bir açık için etki derecelerini belirten CVSS skorları ve kategorileri ile birlikte açıklamalar yer almaktadır.

1. Oturum Yönetimi - CVSS: 9.8 (Kritik)

Kategori: Unauthenticated Access
Oturum yönetimi mekanizmasındaki zafiyet, yetkisiz kullanıcıların admin paneline erişim sağlamasına olanak tanımaktadır. Kullanıcı rolü kontrol edilmeden yapılan bu işlem, sistemin güvenliğini ciddi şekilde tehdit etmektedir. Sorunun çözümü için oturum kontrolünün doğru bir şekilde yapılması gerekmektedir.

2. Kullanıcı Profili XSS - CVSS: 6.1 (Orta)

Kategori: Cross-site Scripting (XSS)
Kullanıcılar, profil bilgilerine zararlı kod ekleyerek uygulamanın diğer bölümlerinde bu kodun çalışmasına neden olabilmektedir. Bu durum, kullanıcı verilerinin güvenliğini tehdit etmekte ve kötü niyetli kullanıcıların diğer profillere zarar vermesine yol açabilmektedir. Girdi filtreleme ve sanitize işlemleri ile bu açık kapatılmalıdır.

3. Şirket Paneli XSS - CVSS: 6.1 (Orta)

Kategori: Cross-site Scripting (XSS)
Restoran ve yemek ekleme ekranlarında benzer bir XSS açığı mevcuttur. Kullanıcıların bu ekranlarda zararlı kodları çalıştırabilmesi, yönetici düzeyindeki işlemleri tehlikeye atmaktadır. Bu durum, uygulamanın genel güvenliğini sarsmakta ve gerekli düzeltmeler yapılmadığı takdirde ciddi sonuçlar doğurabilir.

4. Dosya Yükleme - CVSS: 7.5 (Yüksek)

Kategori: File Upload
Dosya yükleme mekanizmasındaki zafiyet, kötü niyetli dosyaların sisteme yüklenmesine izin vermektedir. Uygulama, yüklenen dosyaların uzantılarını kontrol etmesine rağmen çeşitli yöntemlerle bu engelin aşılması mümkündür. Bu durum, sisteme arka kapı açma potansiyeli taşıyan kritik bir güvenlik açığıdır. Yükleme işlemleri sırasında daha sıkı kontroller ve filtreleme mekanizmaları uygulanmalıdır.

Bulgular ve Öneriler

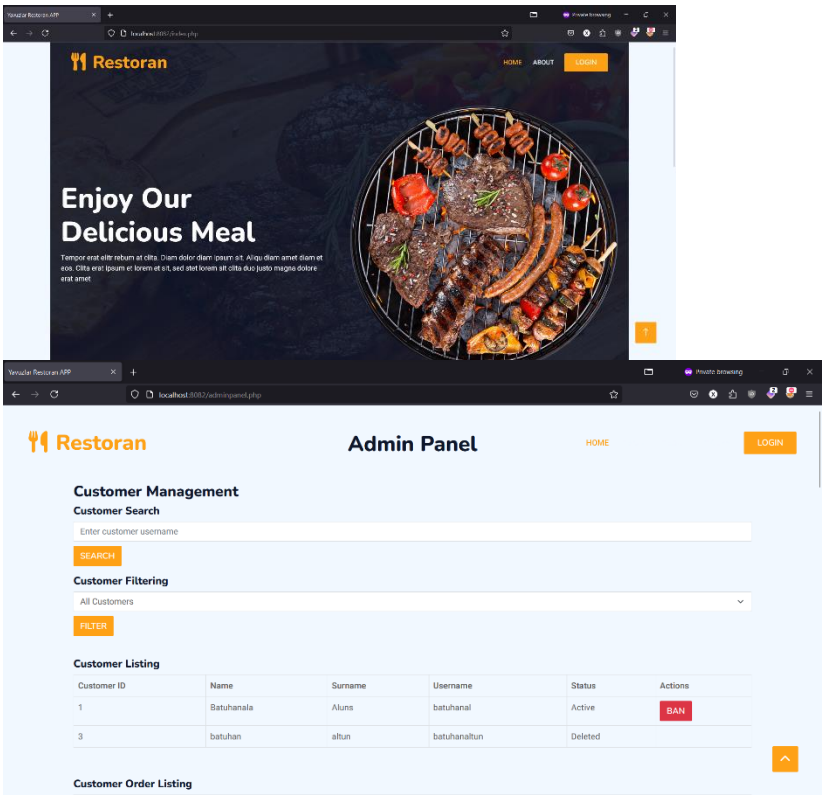
Gerçekleştirilen penetrasyon testi sonucunda elde edilen güvenlik açıkları ve bu açıkların çözüm yolları aşağıda sıralanmıştır.

1. Oturum Yönetimi - CVSS: 9.8 (Kritik)

Bulgu: Yetkisiz kullanıcıların admin paneline erişim sağlaması, sistemin güvenliğini tehdit etmektedir. Kullanıcı rolü kontrolü yapılmadan oturum açılabilmesi, ciddi bir güvenlik açığı yaratmaktadır.

Uygulanış: Hiçbir şey yapmadan direk olarak adres çubuğundan http://localhost:8080/adminpanel.php adresine giriş yapabiliyoruz.

Kanıtlar:



Öneri: Uygulamanın oturum yönetimi eksik olan kısımlarına oturum yönetimi mekanizması eklenmelidir. Bunun için, adminpanel.php dosyasına aşağıdakine benzer kodlar eklenilebilir:

```
return isset($_SESSION['user_role']) && $_SESSION['user_role'] === 'admin';
```

Bu değişiklik, yalnızca admin yetkisine sahip kullanıcıların yönetici paneline erişimini sağlayacaktır.

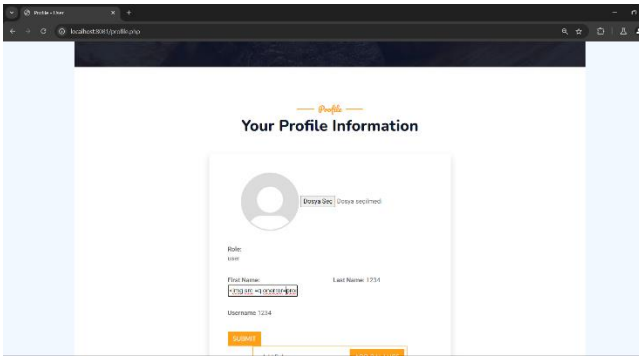
2. Kullanıcı Profili XSS - CVSS: 6.1 (Orta)

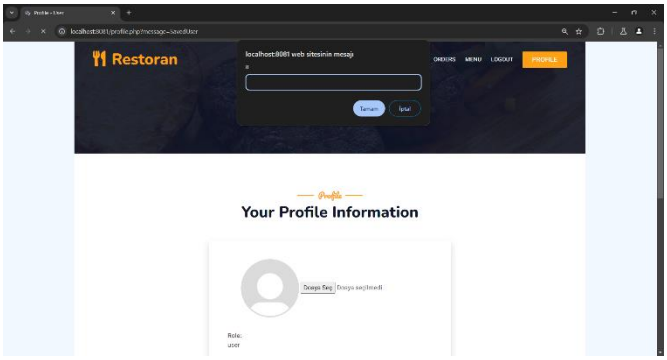
Bulgu: Kullanıcılar, profil bilgilerine zararlı kod ekleyerek uygulamanın diğer bölümlerinde bu kodun çalışmasına neden olabilmektedir. Bu durum, diğer kullanıcıların verilerini tehdit etmektedir.

Kullanılan Payload: <img src =q onerror=prompt(8)>

Uygulanış: Kullanıcı girişi yapıldıktan sonra profil kısmına gelip firstname lastname veya nickname kısımlarından birine payload girilir, kullanıcımızın ismi soyismi veya kullanıcı ismi geçen sayfalarda XSS patlar.

Kanıtlar:





Öneri: Kullanıcıdan alınan girdilerin filtrelenmesi ve sanitize edilmesi gerekmektedir. Kullanıcı profili bölümlerinde, XSS saldırılarına karşı koruma sağlamak için güvenli kod yazım standartlarına uyulmalıdır.

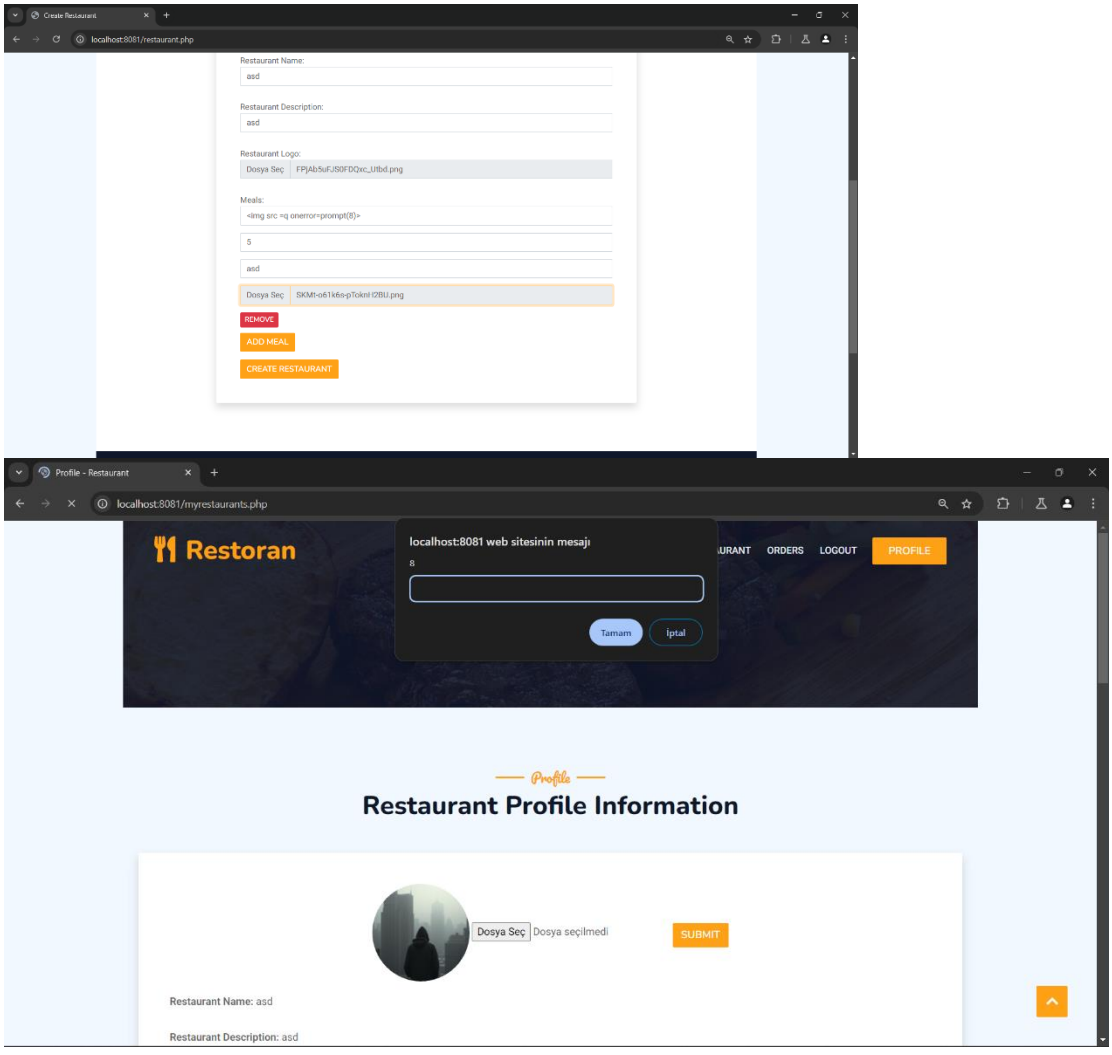
3. Şirket Paneli XSS - CVSS: 6.1 (Orta)

Bulgu: Restoran ve yemek ekleme ekranlarında benzer bir XSS açığı mevcuttur. Kullanıcılar, bu ekranlarda zararlı kodları çalıştırarak yönetici düzeyindeki işlemleri tehlikeye atabilirler.

Kullanılan Payload: <img src =q onerror=prompt(8)>

Uygulanış: Şirket girişi yapıldıktan sonra restoran ekleme ve yemek ekleme ekranında payload girilir, sonra restoran veya yemek isimlerinden hangisi çalıştığına göre XSS açılan ekranda patlar

Kanıtlar:

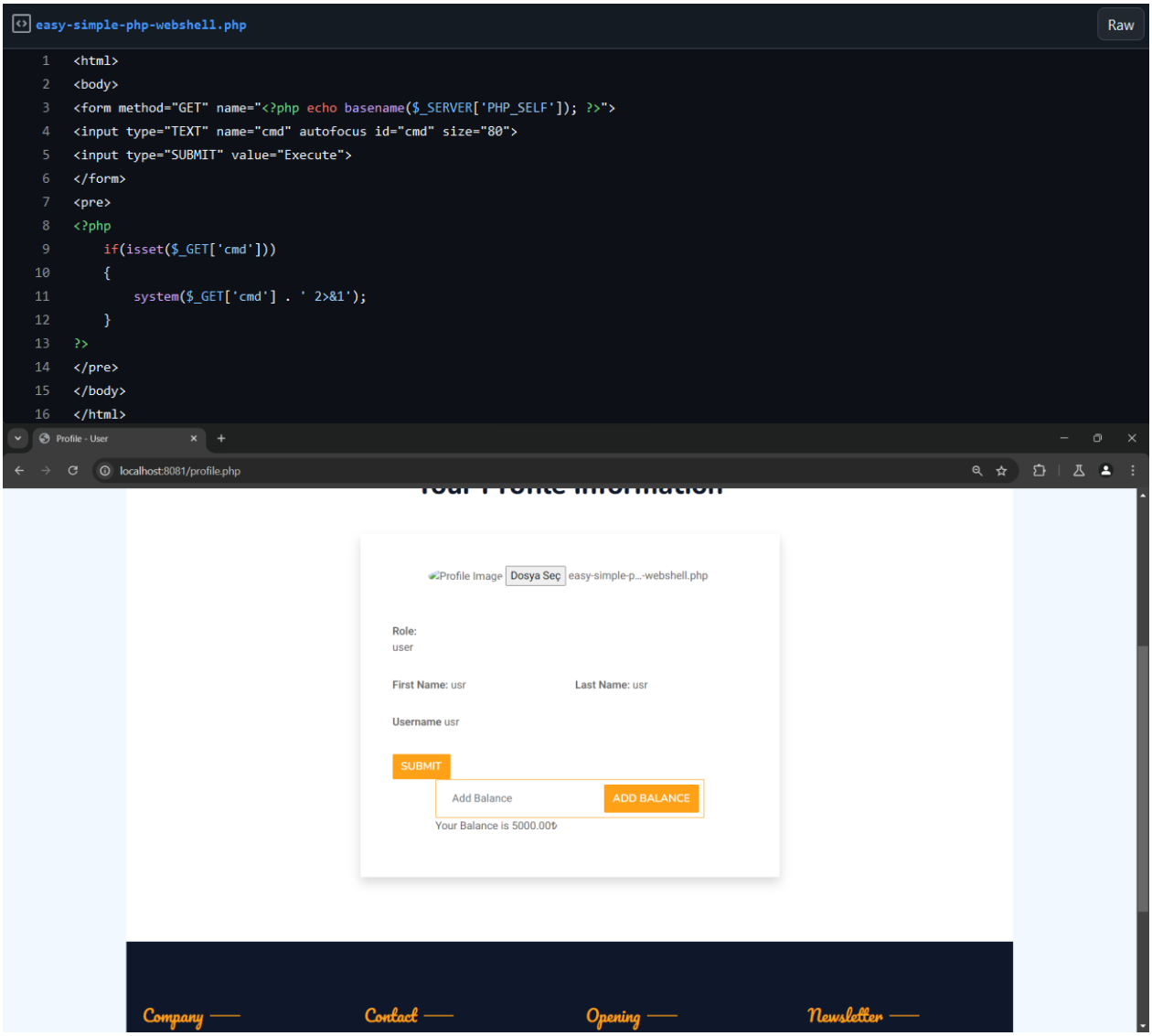


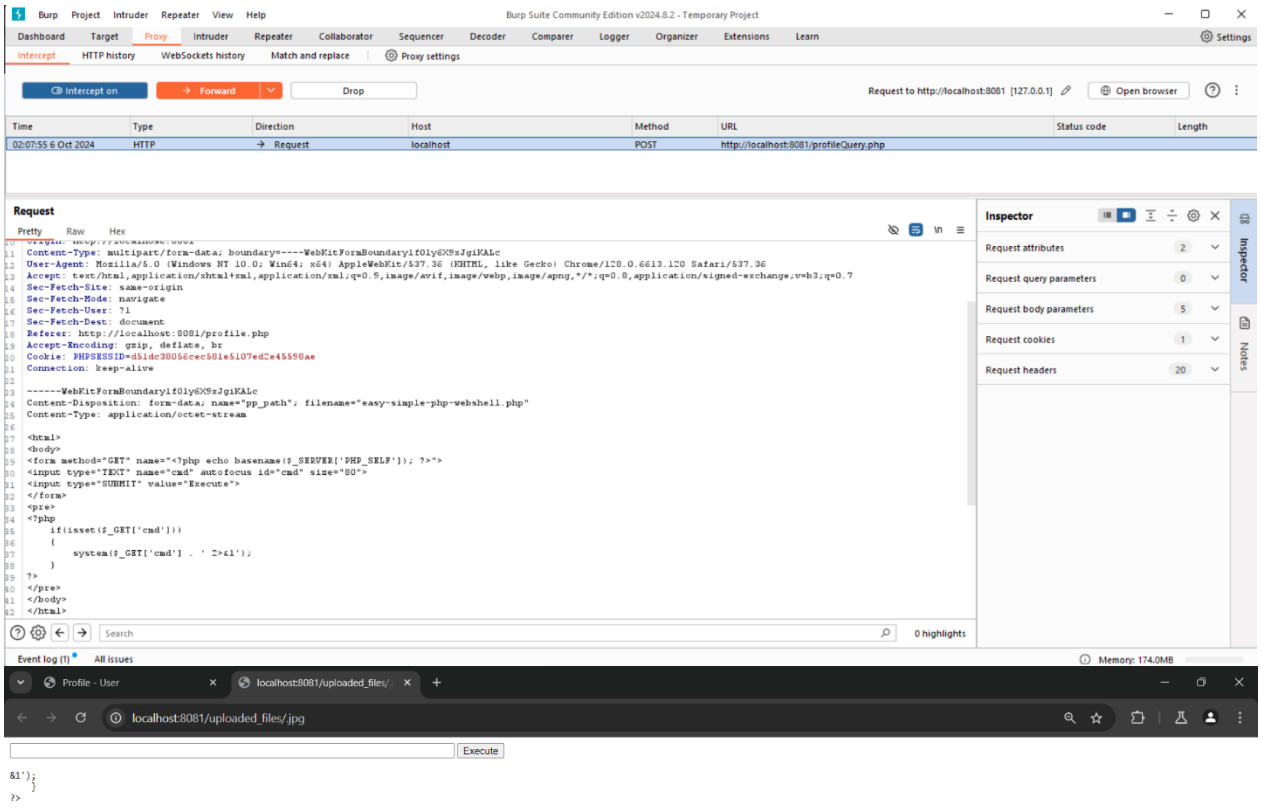
Öneri: Bu ekranlarda da kullanıcı girdileri için filtreleme ve sanitize işlemlerinin yapılması zorunludur. Ayrıca, içerik türü ve uzunluğu gibi kısıtlamalar eklenerek güvenlik artırılmalıdır.

4. Dosya Yükleme - CVSS: 7.5 (Yüksek)

Bulgu: Dosya yükleme mekanizmasındaki zafiyet, kötü niyetli dosyaların sisteme yüklenmesine olanak tanımaktadır. Uzantı kontrolü yapılmasına rağmen, bu engelin aşılması mümkündür. Yaptığımız denemeler sonrası tam olarak çalışan bir shell sağlayamasak da shell sayfasına erişmeyi başardık.

Kanıtlar:





Öneri: Dosya yükleme işlemleri sırasında, sadece belirli dosya türlerinin yüklenmesine izin verilmelidir. Ayrıca, yüklenen dosyaların içeriği üzerinde de kontroller ve tarama yapılmalıdır. Yükleme işlemleri sırasında daha sıkı güvenlik önlemleri alınmalıdır.

İyileştirme Adımları

Yavuzlar Restoran Uygulaması'ndaki güvenlik açıklarının giderilmesi için aşağıdaki iyileştirme adımlarının uygulanması önerilmektedir:

1. Oturum Yönetimi İyileştirmesi

Oturum yönetimi mekanizmasındaki zafiyeti gidermek için, admin paneline erişim kontrolü sağlanmalıdır. Bunun için, adminpanel.php dosyasına aşağıdaki kod eklenmelidir:

```
return isset($_SESSION['user_role']) && $_SESSION['user_role'] === 'admin';
```

Bu değişiklik, yalnızca admin yetkisine sahip kullanıcıların yönetici paneline erişimini sağlayarak, yetkisiz erişim riskini ortadan kaldıracaktır. Ayrıca, kullanıcıların oturum süreleri izlenmeli ve belirli bir süre sonunda otomatik olarak oturumları kapatılmalıdır.

2. Kullanıcı Profili XSS Önlemleri

Kullanıcı profili bölümünde XSS zaafiyetini önlemek için, kullanıcıdan alınan tüm girdilerin filtrelenmesi ve sanitize edilmesi gerekmektedir. Özellikle first name, last name ve nickname alanları için, aşağıdaki gibi bir kod ile zararlı içerikler temizlenmelidir:

```
$input = htmlspecialchars($input, ENT_QUOTES, 'UTF-8');
```

Bu yöntem, kullanıcıların profil bilgilerine ekleyecekleri zararlı kodların çalışmasını engelleyecek ve veri güvenliğini artıracaktır.

3. Şirket Paneli İçin Güvenlik Güncellemeleri

Şirket panelindeki XSS açıklarının kapatılması için, restoran ve yemek ekleme ekranlarında da benzer filtreleme ve sanitize işlemleri uygulanmalıdır. Özellikle form girdileri üzerinde sıkı kontroller yapılmalı ve içerik türü (örn. metin, sayı) gibi kısıtlamalar eklenmelidir. Ayrıca, bu alanlar için kullanıcıdan alınan verilerin boyut sınırlandırması yapılmalıdır.

4. Dosya Yükleme Güvenliği

Dosya yükleme mekanizmasındaki zafiyetin giderilmesi için, yüklenen dosyaların uzantılarının yanı sıra içeriğinin de kontrol edilmesi gerekmektedir. Yalnızca belirli dosya türlerine (örn. .jpg, .png) izin verilmesinin yanında yüklenen dosyalar güvenlik tarayıcıları kullanılarak incelenmelidir. Ayrıca, yükleme işlemleri sırasında dosya içeriği üzerinde tarama yapılması ve güvenlik duvarı kuralları ile bu dosyaların kontrol edilmesi sağlanmalıdır. Bu şekilde, kötü niyetli dosyaların sisteme yüklenme riski en aza indirilmiş olacaktır.

Sonuç

Yavuzlar Restoran Uygulaması için gerçekleştirilen penetrasyon testi, uygulamanın güvenlik durumunu ciddi şekilde tehdit eden dört ana zafiyetin varlığını ortaya koymuştur. Oturum yönetimindeki ciddi açık, yetkisiz kullanıcıların yönetici paneline erişim sağlamasına olanak tanırken, XSS açıkları, kullanıcı verilerinin güvenliğini tehlikeye atmaktadır. Ayrıca, dosya yükleme mekanizmasındaki zafiyet, kötü niyetli dosyaların sisteme yüklenmesine olanak tanımaktadır.

Test sonuçları, uygulamanın güvenlik düzeyinin acil olarak iyileştirilmesi gerektiğini göstermektedir. Özellikle, oturum yönetimi mekanizmasında yapılacak iyileştirmeler, sadece yetkili kullanıcıların yönetim paneline erişim sağlamasını garanti altına alacaktır. Kullanıcı profilleri ve şirket panelindeki XSS açıklarının kapatılması için, girdi filtreleme ve sanitize işlemlerinin etkin bir şekilde uygulanması şarttır.

Ayrıca, dosya yükleme mekanizmalarında daha sıkı kontrol yöntemlerinin benimsenmesi, sistemin güvenliğini önemli ölçüde artıracaktır. Yüklenen dosyaların içeriği üzerinde tarama yapmak ve yalnızca belirli dosya türlerine izin vermek, bu tür zafiyetlerin önüne geçilmesine yardımcı olacaktır.

Sonuç olarak, Yavuzlar Restoran Uygulaması'nın güvenliğini artırmak için yukarıda belirtilen iyileştirme adımlarının derhal uygulanması kritik öneme sahiptir. Bu sayede, hem kullanıcıların verileri korunacak hem de uygulamanın genel güvenlik durumu iyileştirilecektir.