RESTORAN SİTESİ PENTEST

Restoran Sitesinde Pentest Çalışması Yaparak Bulunan Açıkları Ele Alacağız.

1. Girdi Doğrulama (Input Validation)

Bulunduğu Yer: Yemekler Sayfasında Bulunan Sepete Ekle İşleminde.

Oluştuğu Yer: Adet Kısmına Site Üzerinden Sadece Sayı Girilebilmekte. Fakat Eğer Burpsuite Üzerinden İsteği Yakalayıp Repeater İle Miktar Değerini Bir Harf ile Değiştirirsek Sepet Ekleme İşlemi Başarıyla Gerçekleşmekte. Buda Demek Oluyor ki Ko Kısmında Sayı Olup Olmadığı Kontrol Edilmediğini Gösteriyor.

Doğurabileceği Sonuçlar : Eğer Başka Gerekli Önlemler Yoksa Çeşitli SQL Injection, Command Injection, Cross-Site Scripting vb Zaafiyet Sömürüleri Deniyerek Sisteme Zarar Verilebilir Süistimal Edilebilir Fakat Bu Sitede Zarar Verilebilecek Bir Başka Zaafiyet Görülmedi O Bölümde.

Kapatılması İçin Öneriler:

1. Whitelist Kullanılabilir Örneğin Sadece 1-10000 Sayıları Kabul Etmesi Sağlanabilir.
2. Backend Kod Kısmında. Veri Türünün Doğruluğu Kontrol Edilebilir. Yani Girilen Girdinin Sayı Olup Olmadığını Kontrol Edilebilir. Bu Sayede Sayı Girilmediyse Engelleyebilir.

CVSS:

Saldırı Vektörü (Attack Vector – AV): **Ağ (Network – N)**

- Bu Açık İnternet Üzerindeki Bir Sitede Gerçekleşiyor. Saldırgan Site Üzerinden Zafiyeti İstismar Edebiliyor.

Saldırı Karmaşıklığı (Attack Complexity – AC): **Düşük (Low – L)**

- Saldırgan Sadece BurpSuite Gibi Bir Araç İle İsteği Düzenleyip Uygulamaya Yollaması yeterli. Ekstra Bir Bilgi veya Özel Bir Yetki vb İhtiyaç Yok.

Yetkilendirme (Privileges Required – PR): **Düşük (Low – L)**

- Saldırganın Giriş Yapmış Olması Yeterli. Bunun İçinde Kayıt Olma Sayfasıda Bulunmaktadır. Bu Yüzden Düşük Düzeyde Yetki Gerekiyor.

Kullanıcı Etkileşimi (User Interaction – UI): **Gerekli (Required – R)**

- Bu Saldırı Giriş Yapmış Bir Kullanıcı Tarafından Yapılmalıdır, Bu Sebeple Kullanıcı Etkileşimi Gereklidir.

Etkilenen Bileşenlerin Kapsamı (Scope – S): **Değişmez (Unchanged – U)**

- Güvenlik Açığı, Doğrudan Sitenin kendi İçinde ve Başka Sisteme Etki Etmiyor.

Gizlilik Etkisi (Confidentiality Impact – C): **Yok (None – N)**

- Bu Açık Gizli Bilgilere Erişim Sağlamıyor. Sadece Sepete Eklenen ÜSrünler etkileniyor.

Bütünlük Etkisi (Integrity Impact – I): **Düşük (Low – L)**

- Kullanıcının Sepete Ekleme Eşlemi Manipüle Edilebiliyor ve Sitenin İşleyişi Yanlış Sonuçlar Doğurabiliyor. Örneğin Hatalı Miktarda Ürün Eklenebilir Bu da Finansal Kayba Yol Açabilir.

Kullanılabilirlik Etkisi (Availability Impact – A): **Yok (None – N)**

- Bu Zafiyet Sitenin Kullanılabilirliğini Direk Etkilemiyor. Sepet İşlemi Çalışmaya Devam Ediyor.

CVSS Temel Puanı Hesaplaması:

CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:N

Zayıflığın Yayılma Hızı (Temporal Score): 3.5 **Çevresel Skor (Environmental Score):** 3.5

1. Dosya Yükleme Zafiyeti (File Upload Vulnerability)

Bulunduğu Yer: Kullanıcı Ayarlar Sayfasında Fotoğraf Yükleme İşleminde.

Oluştuğu Yer: Fotoğraf Yükleme Esnasında Site Sadece Belli Uzantılar Kabul Ediyor gif, jpeg, jpg, png vb. Fakat Saldırgan Dosya Uzantısını .gif.php Gibi Çift Uzantılı Yaparak Kontrolü Atlatabiliyor.

Doğurabileceği Sonuçlar: Saldırgan Bu Sayede Shell vb Zararlı Dosya Yükleyerek Komut Sunucu Üzerinde Komutlar Çalıştırılabilir. Hatta Mysql Dump Shell vb Sheller Kullanarak Veritabanı İçindeki Verilere de Ulaşıp Çekilebilir.

Kapatılması İçin Öneriler:

1. Yüklenen Dosyanın Sadece Uzantısına değil, MIME Türünede Bakılarak Doğrulama Yapılabilir. Bu Sayede Dosyanın İçeriği de Kontrol Edilebilir.
2. Yüklenen Dosyaların Uzantıları Sadece İstemci Tarafında Değil, Sunucu Tarafında da Kontrol Edilmelidir. Çift Uzantılı Dosyalar Engellenmelidir.
3. Yüklenen Dosyalar Sunucuya Kaydedilmeden Önce Farklı Bir Adla Yeniden Adlandırılabilir.
4. Yüklenen Dosyaların Çalıştırılabilir Olmasına İzin verilmemeli. Örneğin Yüklenen Dosyalar Url Üzerinden Direk Çalıştıracağı Bir Dizine Değil Sadece Görüntülenebileceği Bir Dizine Kaydedilmelidir.
5.

CVSS:

Saldırı Vektörü (Attack Vector – AV): **Ağ (Network – N)**

- Bu Açık İnternet Üzerindeki Bir Sitede Gerçekleşiyor. Saldırgan Site Üzerinden Dosya Yükleyerek Zafiyeti İstismar Edebiliyor.

Saldırı Karmaşıklığı (Attack Complexity – AC): **Düşük (Low – L)**

- Saldırgan Yalnızca Uzantıyı Manipüle Edip Dosya Yükleyerek Açığı İstismar Edebilir. Ekstra Bilgiye veya Özel Bir Yetkiye İhtiyaç Yok. Saldırgan Direk Yeni Hesap Açıp Açığı İstismar Edebilir.

Yetkilendirme (Privileges Required – PR): **Düşük (Low – L)**

- Saldırganın Giriş Yapmış Olması Yeterli. Bunun İçinde Kayıt Olma Sayfasıda Bulunmaktadır. Bu Yüzden Düşük Düzeyde Yetki Gerekiyor.

Kullanıcı Etkileşimi (User Interaction – UI): **Gerekli (Required – R)**

- Bu Saldırı Giriş Yapmış Bir Kullanıcı Tarafından Yapılmalıdır, Bu Sebeple Kullanıcı Etkileşimi Gereklidir.

Etkilenen Bileşenlerin Kapsamı (Scope – S): **Değişmez (Unchanged – U)**

- Güvenlik Açığı, Doğrudan Sitenin kendi İçinde ve Başka Sisteme Etki Etmiyor.

Gizlilik Etkisi (Confidentiality Impact – C): **Yok (None – H)**

- Bu Açık Saldırganın Sunucuya Shell Yükleyerek Sunucu Üzerindeki Veritabanındaki veya Dosyalardaki Gizli Verilere Erişmesine Olanak Tanıyabilir. Bu Gizlilik Açısından Ciddi Bir Risktir.

Bütünlük Etkisi (Integrity Impact – I): **Düşük (Low – H)**

- Saldırganın Sunucu Üzerinde Zararlı Kod Çalıştırarak Sistemin Bozabileceği ve Kritik Dosyaları Değiştirebileceği Silebileceği Düşünülmektedir.

Kullanılabilirlik Etkisi (Availability Impact – A): **Yok (None – H)**

- Saldırgan Sunucuda Kötü Amaçlı Kod Çalıştırarak Sistemin Çökmesine veya Hizmet Dışı Kalmasına Neden Olabilir.

CVSS Temel Puanı Hesaplaması:

CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H

Zayıflığın Yayılma Hızı (Temporal Score): 8.0 **Çevresel Skor (Environmental Score):** 8.0