

**Restaurant\_App**

**Web Uygulaması Testi Raporu**

**Barış**

**Güray Dağ**

**Ayberk İlbaş**

**Alpaslan Tiryakioğlu**

**Yavuzlar Takımı iota Ekibi**

**İçindekiler**

[**Uyarı** 3](#_Toc178965908)

[**Kapsam** 3](#_Toc178965909)

[**Test Ekibi** 4](#_Toc178965910)

[**Genel Değerlendirme** 4](#_Toc178965911)

[**Sızma testi türleri** 4](#_Toc178965912)

[**Risk Derecelendirme** 5](#_Toc178965913)

[**Teknik Bilgiler** 6](#_Toc178965914)

[**Kullanılan** **Araçlar** 6](#_Toc178965915)

[**Bulgular** 7](#_Toc178965916)

[File Upload 7](#_Toc178965917)

[File Upload 8](#_Toc178965918)

[File Upload 9](#_Toc178965919)

[File Upload 10](#_Toc178965920)

[File Upload 11](#_Toc178965921)

[File Upload 12](#_Toc178965922)

[File Upload 13](#_Toc178965923)

[File Upload 14](#_Toc178965924)

[File Upload 15](#_Toc178965925)

[File Upload 16](#_Toc178965926)

[File Upload 17](#_Toc178965927)

[**Önlemler** 18](#_Toc178965928)

## **Uyarı**

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

Bu rapor Yılmaz Üstüntaş’a 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 İçinde yer alan çözüm önerilerine konu hakkında fikir verme amaçlı yer verilmiştir. Çözüm önerilerinin uygulanması sebebi ile çıkabilecek problemlerden raporu hazırlayan firma sorumlu tutulamaz. Önerilerde sunulan değişikliklerden gerçekleştirilmeden önce konu hakkında uzman kişilerden destek alınması tavsiye edilir.

## **Kapsam**

Bu test; tek hedef tek, domain tek, IP adresinde gerçekleştirilmiştir. Başka herhangi bir makine ile bağlantısı bulunmamaktadır.

|  |  |
| --- | --- |
| **IP ADRESİ** | **Açıklama** |
| localhost | Apache 2.4.62 |

## **Test Ekibi**

|  |
| --- |
| Alpaslan Tiryakioğlu |
| Ayberk İlbaş |
| Güray Dağ |
| Barış |

## **Genel Değerlendirme**

Testini gerçekleştirdiğim web uygulamasında File Upload zafiyeti keşfedilmiştir. Temelde önem ve risk derecesi yüksektir. Bu zafiyetin çıkış sebebi sunucu tarafına dosya yüklemesi yapılırken yeterli kontrollerin yapılmamasından kaynaklanmaktadır.

Raporun devamında gelecek olan bulgu kartlarında daha detaylı zafiyet bilgilerine ve çözüm önerilerine yer vermiş olacağız.

## **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 ağ'daki 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 teşti 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** |
| Acil | 5 | Acil öneme sahip açıklıklar, niteliksiz saldırganlar tarafından uzaktan gerçekleştirilen ve sistemin tamamen ele geçirilmesi ile sonuçlanan ataklara sebep olan açıklıklardır. Depolanmış XSS, SQL enjeksiyonu ve RFI/LFI, ayrıca müşteri bilgisi ifşasına yol açabilecek açıklık vektörleri bu kategoriye girerler. |
| Kritik | 4 | Kritik öneme sahip açıklıklar, nitelikli saldırganlar tarafından uzaktan gerçekleştirilen ve sistemin tamamen ele geçirilmesi ile sonuçlanan ataklara sebep olan açıklıklardır. Ayrıca yansıtılan ve DOM tabanlı açıklık vektörleri bu kategoriye girer. |
| Yüksek | 3 | Yüksek öneme sahip açıklıklar, uzaktan gerçekleştirilen ve kısıtlı hak yükseltilmesi (mesela, yönetici hakları olmayan bir işletim sistemi kullanıcısı veya e- posta sahteciliği) veya hizmet dışı kalma ile sonuçlanan, ayrıca yerel ağdan ya da sunucu üzerinden gerçekleştirilen ve hak yükseltmeyi sağlayan ataklara sebep olan açıklıkları içermektedir. |
| Orta | 2 | Orta öneme sahip açıklıklar, yerel ağdan veya sunucu üzerinden gerçekleştirilen ve hizmet dışı bırakılma ile sonuçlanan ataklara sebep olan açıklıkları içermektedir. |
| Düşük | 1 | Düşük öneme sahip açıklıklar İse etkilerinin tam olarak belirlenemediği ve literatürdeki en İyi sıkılaştırma yöntemlerinin (best practices) izlenmemesinden kaynaklanan eksikliklerdir. |

## **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** |
| Nmap | Aktif keşif, port taraması |
| Burp Suite | HTTP paket analizi ve manipülasyonu |
| Wappalyzer | Pasif keşif, bilgi toplama |
| Sqlmap | SQLi zafiyetini sömürmek için otomatize araç |

## **Bulgular**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Bulgu Adı | | | | |
| File Upload | | | | |
| Bulgu Kodu | | | | |
| FILE\_UPLOAD1 | | | | |
| Önem Derecesi | **Erişim Noktası** | **Kullanıcı Profili** | **Durum** | **CVSS** |
| Yüksek | İnternet | Anonim | Giderilmedi | 8.8 High |
| Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H | | | | |
| Bulgunun Tespit Edildiği Bileşen/Bileşenler | | | | |
| <http://0.0.0.0:8080/add-company.php>  <http://0.0.0.0:8080/scripts/add-company-query.php> | | | | |
| Zafiyetin Etkisi | | | | |
| **Web sunucusunda uzaktan kod yürütme, web shell yüklenmesi gibi durumlara yol açabilir.** | | | | |
| Zafiyetin Açıklaması | | | | |
| Admin sayfası üzerindeki firma ekleme sayfasında bulunan logo yükleme alanlarında yetersiz kontrolden kaynaklı .php uzantılı dosyalar yüklenebilmekte ve uzaktan kod yürütmek mümkün hale gelmektedir. | | | | |
| Çözüm Önerisi | | | | |
| Yüklenen dosyaların içerik ve uzantılarına dair sıkı doğrulama yapılmalı | | | | |
| Referans | | | | |
| <https://portswigger.net/web-security/file-upload> | | | | |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Bulgu Adı | | | | | | | |
| File Upload | | | | | | | |
| Bulgu Kodu | | | | | | | |
| FILE\_UPLOAD2 | | | | | | | |
| Önem Derecesi | **Erişim Noktası** | | **Kullanıcı Profili** | | **Durum** | | **CVSS** |
| Yüksek | İnternet | | Anonim | | Giderilmedi | | 8.8 High |
| Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H | | | | | | | |
| Önem Derecesi | | **Erişim Noktası** | | **Kullanıcı Profili** | | **Durum** | |
| Yüksek | | İnternet | | Anonim | | Giderilmedi | |
| Bulgunun Tespit Edildiği Bileşen/Bileşenler | | | | | | | |
| [http://0.0.0.0:8080/update-company.php?c\_id=11](http://0.0.0.0:8080/add-company.php)  [http://0.0.0.0:8080/scripts/update-company-query.php](http://0.0.0.0:8080/scripts/add-company-query.php) | | | | | | | |
| Zafiyetin Etkisi | | | | | | | |
| **Web sunucusunda uzaktan kod yürütme, web shell yüklenmesi gibi durumlara yol açabilir.** | | | | | | | |
| Zafiyetin Açıklaması | | | | | | | |
| Admin sayfası üzerindeki firma güncelleme sayfasında bulunan logo yükleme alanlarında yetersiz kontrolden kaynaklı .php uzantılı dosyalar yüklenebilmekte ve uzaktan kod yürütmek mümkün hale gelmektedir. | | | | | | | |
| Çözüm Önerisi | | | | | | | |
| Yüklenen dosyaların içerik ve uzantılarına dair sıkı doğrulama yapılmalı | | | | | | | |
| Referans | | | | | | | |
| <https://portswigger.net/web-security/file-upload> | | | | | | | |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Bulgu Adı | | | | | | | |
| File Upload | | | | | | | |
| Bulgu Kodu | | | | | | | |
| FILE\_UPLOAD3 | | | | | | | |
| Önem Derecesi | **Erişim Noktası** | | **Kullanıcı Profili** | | **Durum** | | **CVSS** |
| Yüksek | İnternet | | Anonim | | Giderilmedi | | 8.8 High |
| Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H | | | | | | | |
| Önem Derecesi | | **Erişim Noktası** | | **Kullanıcı Profili** | | **Durum** | |
| Yüksek | | İnternet | | Anonim | | Giderilmedi | |
| Bulgunun Tespit Edildiği Bileşen/Bileşenler | | | | | | | |
| <http://0.0.0.0:8080/register.php>  <http://0.0.0.0:8080/scripts/add-company-query.php> | | | | | | | |
| Zafiyetin Etkisi | | | | | | | |
| **Web sunucusunda uzaktan kod yürütme, web shell yüklenmesi gibi durumlara yol açabilir.** | | | | | | | |
| Zafiyetin Açıklaması | | | | | | | |
| Kayıt olma sayfasında profil fotoğrafı yükleme alanında file upload zafiyeti keşfedilmiştir. | | | | | | | |
| Çözüm Önerisi | | | | | | | |
| Yüklenen dosyaların içerik ve uzantılarına dair sıkı doğrulama yapılmalı | | | | | | | |
| Referans | | | | | | | |
| <https://portswigger.net/web-security/file-upload> | | | | | | | |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Bulgu Adı | | | | | | | |
| File Upload | | | | | | | |
| Bulgu Kodu | | | | | | | |
| FILE\_UPLOAD4 | | | | | | | |
| Önem Derecesi | **Erişim Noktası** | | **Kullanıcı Profili** | | **Durum** | | **CVSS** |
| Yüksek | İnternet | | Anonim | | Giderilmedi | | 8.8 High |
| Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H | | | | | | | |
| Önem Derecesi | | **Erişim Noktası** | | **Kullanıcı Profili** | | **Durum** | |
| Yüksek | | İnternet | | Anonim | | Giderilmedi | |
| Bulgunun Tespit Edildiği Bileşen/Bileşenler | | | | | | | |
| <http://0.0.0.0:8080/profile.php>  <http://0.0.0.0:8080/scripts/update-profile-query.php> | | | | | | | |
| Zafiyetin Etkisi | | | | | | | |
| **Web sunucusunda uzaktan kod yürütme, web shell yüklenmesi gibi durumlara yol açabilir.** | | | | | | | |
| Zafiyetin Açıklaması | | | | | | | |
| Kullanıcının profil güncelleme ekranındaki profil fotoğrafı yükleme alanında file upload zafiyeti tespit edilmiştir.  metin, ekran görüntüsü, yazılım, multimedya yazılımı içeren bir resim  Açıklama otomatik olarak oluşturuldu | | | | | | | |
| Çözüm Önerisi | | | | | | | |
| Yüklenen dosyaların içerik ve uzantılarına dair sıkı doğrulama yapılmalı | | | | | | | |
| Referans | | | | | | | |
| <https://portswigger.net/web-security/file-upload> | | | | | | | |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Bulgu Adı | | | | | | | |
| File Upload | | | | | | | |
| Bulgu Kodu | | | | | | | |
| FILE\_UPLOAD5 | | | | | | | |
| Önem Derecesi | **Erişim Noktası** | | **Kullanıcı Profili** | | **Durum** | | **CVSS** |
| Yüksek | İnternet | | Anonim | | Giderilmedi | | 8.8 High |
| Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H | | | | | | | |
| Önem Derecesi | | **Erişim Noktası** | | **Kullanıcı Profili** | | **Durum** | |
| Yüksek | | İnternet | | Anonim | | Giderilmedi | |
| Bulgunun Tespit Edildiği Bileşen/Bileşenler | | | | | | | |
| <http://0.0.0.0:8080/profile.php>  <http://0.0.0.0:8080/scripts/update-profile-query.php> | | | | | | | |
| Zafiyetin Etkisi | | | | | | | |
| **Web sunucusunda uzaktan kod yürütme, web shell yüklenmesi gibi durumlara yol açabilir.** | | | | | | | |
| Zafiyetin Açıklaması | | | | | | | |
| Firma hesabına giriş yaptıktan sonra şirket profili güncelleme ekranındaki logo yükleme alanında file upload zafiyeti keşfedilmiştir. | | | | | | | |
| Çözüm Önerisi | | | | | | | |
| Yüklenen dosyaların içerik ve uzantılarına dair sıkı doğrulama yapılmalı | | | | | | | |
| Referans | | | | | | | |
| <https://portswigger.net/web-security/file-upload> | | | | | | | |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Bulgu Adı | | | | | | | |
| File Upload | | | | | | | |
| Bulgu Kodu | | | | | | | |
| FILE\_UPLOAD6 | | | | | | | |
| Önem Derecesi | **Erişim Noktası** | | **Kullanıcı Profili** | | **Durum** | | **CVSS** |
| Yüksek | İnternet | | Anonim | | Giderilmedi | | 8.8 High |
| Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H | | | | | | | |
| Önem Derecesi | | **Erişim Noktası** | | **Kullanıcı Profili** | | **Durum** | |
| Yüksek | | İnternet | | Anonim | | Giderilmedi | |
| Bulgunun Tespit Edildiği Bileşen/Bileşenler | | | | | | | |
| <http://0.0.0.0:8080/update-company.php>  <http://0.0.0.0:8080/scripts/update-company-query.php> | | | | | | | |
| Zafiyetin Etkisi | | | | | | | |
| **Web sunucusunda uzaktan kod yürütme, web shell yüklenmesi gibi durumlara yol açabilir.** | | | | | | | |
| Zafiyetin Açıklaması | | | | | | | |
| Firma hesabı içerisinde şirketin haricinde yemek firmasının logosunun güncellendiği alanda file upload zafiyeti keşfedilmiştir. | | | | | | | |
| Çözüm Önerisi | | | | | | | |
| Yüklenen dosyaların içerik ve uzantılarına dair sıkı doğrulama yapılmalı | | | | | | | |
| Referans | | | | | | | |
| <https://portswigger.net/web-security/file-upload> | | | | | | | |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Bulgu Adı | | | | | | | |
| File Upload | | | | | | | |
| Bulgu Kodu | | | | | | | |
| FILE\_UPLOAD7 | | | | | | | |
| Önem Derecesi | **Erişim Noktası** | | **Kullanıcı Profili** | | **Durum** | | **CVSS** |
| Yüksek | İnternet | | Anonim | | Giderilmedi | | 8.8 High |
| Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H | | | | | | | |
| Önem Derecesi | | **Erişim Noktası** | | **Kullanıcı Profili** | | **Durum** | |
| Yüksek | | İnternet | | Anonim | | Giderilmedi | |
| Bulgunun Tespit Edildiği Bileşen/Bileşenler | | | | | | | |
| <http://0.0.0.0:8080/add-food.php>  <http://0.0.0.0:8080/scripts/add-food-query.php> | | | | | | | |
| Zafiyetin Etkisi | | | | | | | |
| **Web sunucusunda uzaktan kod yürütme, web shell yüklenmesi gibi durumlara yol açabilir.** | | | | | | | |
| Zafiyetin Açıklaması | | | | | | | |
| Firma hesabı içerisinde restoranın yemek ekleme sayfasında yemek resmi yükleme alanında file uplaod zafiyeti keşfedilmiştir. | | | | | | | |
| Çözüm Önerisi | | | | | | | |
| Yüklenen dosyaların içerik ve uzantılarına dair sıkı doğrulama yapılmalı | | | | | | | |
| Referans | | | | | | | |
| <https://portswigger.net/web-security/file-upload> | | | | | | | |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Bulgu Adı | | | | | | | |
| File Upload | | | | | | | |
| Bulgu Kodu | | | | | | | |
| FILE\_UPLOAD8 | | | | | | | |
| Önem Derecesi | **Erişim Noktası** | | **Kullanıcı Profili** | | **Durum** | | **CVSS** |
| Yüksek | İnternet | | Anonim | | Giderilmedi | | 8.8 High |
| Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H | | | | | | | |
| Önem Derecesi | | **Erişim Noktası** | | **Kullanıcı Profili** | | **Durum** | |
| Yüksek | | İnternet | | Anonim | | Giderilmedi | |
| Bulgunun Tespit Edildiği Bileşen/Bileşenler | | | | | | | |
| <http://0.0.0.0:8080/update-food.php>  <http://0.0.0.0:8080/scripts/update-food-query.php> | | | | | | | |
| Zafiyetin Etkisi | | | | | | | |
| **Web sunucusunda uzaktan kod yürütme, web shell yüklenmesi gibi durumlara yol açabilir.** | | | | | | | |
| Zafiyetin Açıklaması | | | | | | | |
| Firma hesabı içerisinde restoranın eklediği yemeği güncelleme sayfasında yemek resmi yükleme alanında file uplaod zafiyeti keşfedilmiştir. | | | | | | | |
| Çözüm Önerisi | | | | | | | |
| Yüklenen dosyaların içerik ve uzantılarına dair sıkı doğrulama yapılmalı | | | | | | | |
| Referans | | | | | | | |
| <https://portswigger.net/web-security/file-upload> | | | | | | | |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Bulgu Adı | | | | | | | |
| File Upload | | | | | | | |
| Bulgu Kodu | | | | | | | |
| FILE\_UPLOAD9 | | | | | | | |
| Önem Derecesi | **Erişim Noktası** | | **Kullanıcı Profili** | | **Durum** | | **CVSS** |
| Yüksek | İnternet | | Anonim | | Giderilmedi | | 8.8 High |
| Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H | | | | | | | |
| Önem Derecesi | | **Erişim Noktası** | | **Kullanıcı Profili** | | **Durum** | |
| Yüksek | | İnternet | | Anonim | | Giderilmedi | |
| Bulgunun Tespit Edildiği Bileşen/Bileşenler | | | | | | | |
| <http://0.0.0.0:8080/add-restaurant.php>  [http://0.0.0.0:8080/scripts/add-restaurant -query.php](http://0.0.0.0:8080/scripts/add-restaurant%20-query.php) | | | | | | | |
| Zafiyetin Etkisi | | | | | | | |
| **Web sunucusunda uzaktan kod yürütme, web shell yüklenmesi gibi durumlara yol açabilir.** | | | | | | | |
| Zafiyetin Açıklaması | | | | | | | |
| Firma hesabı içerisinde restoran ekleme sayfasında restoran logosu alanında file upload zafiyeti tespit edilmiştir. | | | | | | | |
| Çözüm Önerisi | | | | | | | |
| Yüklenen dosyaların içerik ve uzantılarına dair sıkı doğrulama yapılmalı | | | | | | | |
| Referans | | | | | | | |
| <https://portswigger.net/web-security/file-upload> | | | | | | | |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Bulgu Adı | | | | | | | |
| File Upload | | | | | | | |
| Bulgu Kodu | | | | | | | |
| FILE\_UPLOAD10 | | | | | | | |
| Önem Derecesi | **Erişim Noktası** | | **Kullanıcı Profili** | | **Durum** | | **CVSS** |
| Yüksek | İnternet | | Anonim | | Giderilmedi | | 8.8 High |
| Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H | | | | | | | |
| Önem Derecesi | | **Erişim Noktası** | | **Kullanıcı Profili** | | **Durum** | |
| Yüksek | | İnternet | | Anonim | | Giderilmedi | |
| Bulgunun Tespit Edildiği Bileşen/Bileşenler | | | | | | | |
| <http://0.0.0.0:8080/update-restaurant.php>  [http://0.0.0.0:8080/scripts/update-restaurant -query.php](http://0.0.0.0:8080/scripts/update-restaurant%20-query.php) | | | | | | | |
| Zafiyetin Etkisi | | | | | | | |
| **Web sunucusunda uzaktan kod yürütme, web shell yüklenmesi gibi durumlara yol açabilir.** | | | | | | | |
| Zafiyetin Açıklaması | | | | | | | |
| Firma hesabı içerisinde restoran güncelleme sayfasında restoran logosu alanında file upload zafiyeti tespit edilmiştir. | | | | | | | |
| Çözüm Önerisi | | | | | | | |
| Yüklenen dosyaların içerik ve uzantılarına dair sıkı doğrulama yapılmalı | | | | | | | |
| Referans | | | | | | | |
| <https://portswigger.net/web-security/file-upload> | | | | | | | |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Bulgu Adı | | | | | | | |
| File Upload | | | | | | | |
| Bulgu Kodu | | | | | | | |
| FILE\_UPLOAD11 | | | | | | | |
| Önem Derecesi | **Erişim Noktası** | | **Kullanıcı Profili** | | **Durum** | | **CVSS** |
| Yüksek | İnternet | | Anonim | | Giderilmedi | | 8.8 High |
| Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H | | | | | | | |
| Önem Derecesi | | **Erişim Noktası** | | **Kullanıcı Profili** | | **Durum** | |
| Yüksek | | İnternet | | Anonim | | Giderilmedi | |
| Bulgunun Tespit Edildiği Bileşen/Bileşenler | | | | | | | |
| <http://0.0.0.0:8080/update-restaurant.php>  [http://0.0.0.0:8080/scripts/update-restaurant -query.php](http://0.0.0.0:8080/scripts/update-restaurant%20-query.php) | | | | | | | |
| Zafiyetin Etkisi | | | | | | | |
| **Web sunucusunda uzaktan kod yürütme, web shell yüklenmesi gibi durumlara yol açabilir.** | | | | | | | |
| Zafiyetin Açıklaması | | | | | | | |
| Firma hesabı içerisinde restoran güncelleme sayfasında restoran logosu alanında file upload zafiyeti tespit edilmiştir.  metin, ekran görüntüsü, yazılım, multimedya yazılımı içeren bir resim  Açıklama otomatik olarak oluşturuldu | | | | | | | |
| Çözüm Önerisi | | | | | | | |
| Yüklenen dosyaların içerik ve uzantılarına dair sıkı doğrulama yapılmalı | | | | | | | |
| Referans | | | | | | | |
| <https://portswigger.net/web-security/file-upload> | | | | | | | |

## **Önlemler**

* Sunucu tarafında uzantılar kontrol edilmeli ve geçerli formatlara izin verilmeli
* Yüklenen dosyalara erişim kısıtlanmalı, dosya yükleme başarılı olsa bile dosyayı yürütme, çalıştırma fonksiyonları engellenmeli.