Zafiyet Raporu

# 1 ) Remote Code Execution

|  |
| --- |
| Zafiyet Adı |
| Remote Code Execution |
|  |
| Zafiyet Açıklaması |
| <http://127.0.0.1/login.php> adresine gidilir ve giriş yapılır. Ardından <http://127.0.0.1/customer_profile.php> adresine gidilir. Profil resmi seçin butonuna tıklanır ve test.jpg dosyası sistemi yüklenir ve istek BurpSuite proxy aracı ile yakalanır ve isteğe sağ tıklanıp “send to repeater” seçeneği seçilir.    Görsel - 1 Dosya Yükleme İsteği  Dosya uzantısı .php ile değiştirilir ve Content-Disposition: form-data; name="update\_profile\_picture" Header’ının altına “<?php $value = system("cat /etc/passwd"); echo $value; ?> bu payload yazılır. Ardından istek gönderilir. İstek üzerinden dönen Response üzerinden yüklenen dosyanın konumu bulunur. Bulunan konuma (<http://127.0.0.1/uploads/profile_pictures/66fee6c82b28b_test.php>) istek atılır. Böyle başarıyla sunucu üzerinde uzaktan kod yürütülür.    Görsel - 2 Elde edilen Kullanıcı şifreleri |
| Çözüm Önerisi |
| Dosya Türü Kontrolü:   * Yüklemeye izin verilen dosya türlerini sınırlayın. Sadece belirli dosya türlerine (örneğin, .jpg, .png, .pdf) izin verin. * Dosya uzantılarını kontrol etmek yeterli değildir; dosya içeriğini de doğrulamak için MIME türü kontrolü yapın.   Dosya Boyutu Sınırlaması:   * Yüklenen dosyaların boyutunu sınırlayın. Belirli bir boyutun üzerinde dosya yüklemeyi engelleyin.   Dosya İsimleri Kontrolü:   * Yüklenen dosyaların isimlerini güvenli hale getirin. Dosya isimlerindeki özel karakterleri temizleyin ve dosya isimlerini standart bir formatta düzenleyin. * Aynı dosya ismi ile yüklenmeleri durumunda yeni isimler verin. |
| Zafiyetin Doğurabileceği Sonuçlar |
| * Tam Kontrol: Saldırgan, hedef sistemde tam kontrol sağlayabilir. Bu, dosya sistemine erişim, sistem ayarlarını değiştirme ve yazılımları yükleme veya kaldırma anlamına gelir. * Veri Hırsızlığı: RCE zafiyeti sayesinde, saldırgan hassas verilere (şifreler, kişisel bilgiler, finansal veriler vb.) erişebilir ve bunları çalabilir. * Zarar Verme: Saldırgan, hedef sistemde kötü amaçlı yazılımlar, virüsler veya truva atları yükleyerek sistemin işleyişini bozabilir. * Ağ İçin Tehdit: Hedef sistemin yanı sıra, RCE zafiyetleri, diğer bağlı sistemlere (ağdaki diğer cihazlar, sunucular vb.) de zarar verebilir veya erişim sağlayabilir. * Veri Bütünlüğünün İhlali: Saldırgan, verileri değiştirebilir veya silebilir, bu da veri bütünlüğünü ciddi şekilde etkileyebilir. * Hizmet Durdurma: Saldırgan, sistem kaynaklarını aşırı şekilde kullanarak hedef sistemin hizmet dışı kalmasına neden olabilir (DoS/DDoS saldırıları). * Sistem İzleme: Saldırgan, hedef sistemde gizlice izleme yaparak kullanıcıların etkinliklerini gözlemleyebilir. |
| CVSS |
| 8.8 |
| 1 |

# 2) Remote Code Execution

|  |
| --- |
| Zafiyet Adı |
| Remote Code Execution |
|  |
| Zafiyet Açıklaması |
| <http://127.0.0.1/login.php> adresine gidilir ve firma giriş yapılır. Ardından <http://127.0.0.1/company_add_restaurant.php> adresine gidilir. Restaurant resmi seçin butonuna tıklanır ve test.jpg dosyası sistemi yüklenir ve istek BurpSuite proxy aracı ile yakalanır ve isteğe sağ tıklanıp “send to repeater” seçeneği seçilir.    Görsel - 3 Dosya Yükleme İsteği  Dosya uzantısı .php ile değiştirilir ve Content-Disposition: form-data; name="update\_profile\_picture" Header’ının altına “<?php $value = system("whoami"); echo $value; ?> bu payload yazılır. Ardından istek gönderilir. Sistemden çıkış yapılır ve <http://127.0.0.1/login.php> adresine gidilir ve müşteri giriş yapılır. <http://127.0.0.1/customer_restaurants.php> adresine gidilip seçilen restauran’ın <img> etiketi içinde yüklenen dosyanın konumu bulunur. Bulunan konuma (<http://127.0.0.1/uploads/restaurant_images/66fee861dc801_test.php> ) istek atılır. Böyle başarıyla sunucu üzerinde uzaktan kod yürütülür.    Görsel - 4 Elde Edilen Komutun Response’u |
| Çözüm Önerisi |
| Dosya Türü Kontrolü:   * Yüklemeye izin verilen dosya türlerini sınırlayın. Sadece belirli dosya türlerine (örneğin, .jpg, .png, .pdf) izin verin. * Dosya uzantılarını kontrol etmek yeterli değildir; dosya içeriğini de doğrulamak için MIME türü kontrolü yapın.   Dosya Boyutu Sınırlaması:   * Yüklenen dosyaların boyutunu sınırlayın. Belirli bir boyutun üzerinde dosya yüklemeyi engelleyin.   Dosya İsimleri Kontrolü:   * Yüklenen dosyaların isimlerini güvenli hale getirin. Dosya isimlerindeki özel karakterleri temizleyin ve dosya isimlerini standart bir formatta düzenleyin. * Aynı dosya ismi ile yüklenmeleri durumunda yeni isimler verin. |
| Zafiyetin Doğurabileceği Sonuçlar |
| * Tam Kontrol: Saldırgan, hedef sistemde tam kontrol sağlayabilir. Bu, dosya sistemine erişim, sistem ayarlarını değiştirme ve yazılımları yükleme veya kaldırma anlamına gelir. * Veri Hırsızlığı: RCE zafiyeti sayesinde, saldırgan hassas verilere (şifreler, kişisel bilgiler, finansal veriler vb.) erişebilir ve bunları çalabilir. * Zarar Verme: Saldırgan, hedef sistemde kötü amaçlı yazılımlar, virüsler veya truva atları yükleyerek sistemin işleyişini bozabilir. * Ağ İçin Tehdit: Hedef sistemin yanı sıra, RCE zafiyetleri, diğer bağlı sistemlere (ağdaki diğer cihazlar, sunucular vb.) de zarar verebilir veya erişim sağlayabilir. * Veri Bütünlüğünün İhlali: Saldırgan, verileri değiştirebilir veya silebilir, bu da veri bütünlüğünü ciddi şekilde etkileyebilir. * Hizmet Durdurma: Saldırgan, sistem kaynaklarını aşırı şekilde kullanarak hedef sistemin hizmet dışı kalmasına neden olabilir (DoS/DDoS saldırıları). * Sistem İzleme: Saldırgan, hedef sistemde gizlice izleme yaparak kullanıcıların etkinliklerini gözlemleyebilir. |
| CVSS |
| 7.2 |
| 2 |

# 3) Remote Code Execution

|  |
| --- |
| Zafiyet Adı |
| Remote Code Execution |
|  |
| Zafiyet Açıklaması |
| <http://127.0.0.1/login.php> adresine gidilir ve firma giriş yapılır. Ardından <http://127.0.0.1/company_add_food.php> adresine gidilir. Yemek resmi seçin butonuna tıklanır ve test.jpg dosyası sistemi yüklenir ve istek BurpSuite proxy aracı ile yakalanır ve isteğe sağ tıklanıp “send to repeater” seçeneği seçilir.    Görsel - 5 Dosya Yükleme İsteği  Dosya uzantısı .php ile değiştirilir ve Content-Disposition: form-data; name="update\_profile\_picture" Header’ının altına “<?php $value = system("whoami"); echo $value; ?> bu payload yazılır. Ardından istek gönderilir. Sistemden çıkış yapılır ve <http://127.0.0.1/login.php> adresine gidilir ve müşteri giriş yapılır. <http://127.0.0.1/customer_food_search.php> adresine gidilip seçilen restauran’ın <img> etiketi içinde yüklenen dosyanın konumu bulunur. Bulunan konuma (<http://127.0.0.1/uploads/food_images/66fee8b7bec0b_test.php> ) istek atılır. Böyle başarıyla sunucu üzerinde uzaktan kod yürütülür.    Görsel - 6 Elde Edilen Komutun Response’u |
| Çözüm Önerisi |
| Dosya Türü Kontrolü:   * Yüklemeye izin verilen dosya türlerini sınırlayın. Sadece belirli dosya türlerine (örneğin, .jpg, .png, .pdf) izin verin. * Dosya uzantılarını kontrol etmek yeterli değildir; dosya içeriğini de doğrulamak için MIME türü kontrolü yapın.   Dosya Boyutu Sınırlaması:   * Yüklenen dosyaların boyutunu sınırlayın. Belirli bir boyutun üzerinde dosya yüklemeyi engelleyin.   Dosya İsimleri Kontrolü:   * Yüklenen dosyaların isimlerini güvenli hale getirin. Dosya isimlerindeki özel karakterleri temizleyin ve dosya isimlerini standart bir formatta düzenleyin. * Aynı dosya ismi ile yüklenmeleri durumunda yeni isimler verin. |
| Zafiyetin Doğurabileceği Sonuçlar |
| * Tam Kontrol: Saldırgan, hedef sistemde tam kontrol sağlayabilir. Bu, dosya sistemine erişim, sistem ayarlarını değiştirme ve yazılımları yükleme veya kaldırma anlamına gelir. * Veri Hırsızlığı: RCE zafiyeti sayesinde, saldırgan hassas verilere (şifreler, kişisel bilgiler, finansal veriler vb.) erişebilir ve bunları çalabilir. * Zarar Verme: Saldırgan, hedef sistemde kötü amaçlı yazılımlar, virüsler veya truva atları yükleyerek sistemin işleyişini bozabilir. * Ağ İçin Tehdit: Hedef sistemin yanı sıra, RCE zafiyetleri, diğer bağlı sistemlere (ağdaki diğer cihazlar, sunucular vb.) de zarar verebilir veya erişim sağlayabilir. * Veri Bütünlüğünün İhlali: Saldırgan, verileri değiştirebilir veya silebilir, bu da veri bütünlüğünü ciddi şekilde etkileyebilir. * Hizmet Durdurma: Saldırgan, sistem kaynaklarını aşırı şekilde kullanarak hedef sistemin hizmet dışı kalmasına neden olabilir (DoS/DDoS saldırıları). * Sistem İzleme: Saldırgan, hedef sistemde gizlice izleme yaparak kullanıcıların etkinliklerini gözlemleyebilir. |
| CVSS |
| 7.2 |
| 3 |

# 4 ) Remote Code Execution

|  |
| --- |
| Zafiyet Adı |
| Remote Code Execution |
|  |
| Zafiyet Açıklaması |
| <http://127.0.0.1/login.php> adresine gidilir ve firma giriş yapılır. Ardından <http://127.0.0.1/company_edit_food.php?id=2> adresine gidilir. Yemek resmi seçin butonuna tıklanır ve test.jpg dosyası sistemi yüklenir ve istek BurpSuite proxy aracı ile yakalanır ve isteğe sağ tıklanıp “send to repeater” seçeneği seçilir.    Görsel - 7 Dosya Yükleme İsteği  Dosya uzantısı .php ile değiştirilir ve Content-Disposition: form-data; name="update\_profile\_picture" Header’ının altına “<?php $value = system("whoami"); echo $value; ?> bu payload yazılır. Ardından istek gönderilir. Sistemden çıkış yapılır ve <http://127.0.0.1/login.php> adresine gidilir ve müşteri giriş yapılır. <http://127.0.0.1/customer_food_search.php> adresine gidilip seçilen restauran’ın <img> etiketi içinde yüklenen dosyanın konumu bulunur. Bulunan konuma (<http://127.0.0.1/uploads/food_images/66ffc9e65e6d4_test.php> ) istek atılır. Böyle başarıyla sunucu üzerinde uzaktan kod yürütülür.    Görsel - 8 Elde Edilen Komutun Response’u |
| Çözüm Önerisi |
| Dosya Türü Kontrolü:   * Yüklemeye izin verilen dosya türlerini sınırlayın. Sadece belirli dosya türlerine (örneğin, .jpg, .png, .pdf) izin verin. * Dosya uzantılarını kontrol etmek yeterli değildir; dosya içeriğini de doğrulamak için MIME türü kontrolü yapın.   Dosya Boyutu Sınırlaması:   * Yüklenen dosyaların boyutunu sınırlayın. Belirli bir boyutun üzerinde dosya yüklemeyi engelleyin.   Dosya İsimleri Kontrolü:   * Yüklenen dosyaların isimlerini güvenli hale getirin. Dosya isimlerindeki özel karakterleri temizleyin ve dosya isimlerini standart bir formatta düzenleyin. * Aynı dosya ismi ile yüklenmeleri durumunda yeni isimler verin. |
| Zafiyetin Doğurabileceği Sonuçlar |
| * Tam Kontrol: Saldırgan, hedef sistemde tam kontrol sağlayabilir. Bu, dosya sistemine erişim, sistem ayarlarını değiştirme ve yazılımları yükleme veya kaldırma anlamına gelir. * Veri Hırsızlığı: RCE zafiyeti sayesinde, saldırgan hassas verilere (şifreler, kişisel bilgiler, finansal veriler vb.) erişebilir ve bunları çalabilir. * Zarar Verme: Saldırgan, hedef sistemde kötü amaçlı yazılımlar, virüsler veya truva atları yükleyerek sistemin işleyişini bozabilir. * Ağ İçin Tehdit: Hedef sistemin yanı sıra, RCE zafiyetleri, diğer bağlı sistemlere (ağdaki diğer cihazlar, sunucular vb.) de zarar verebilir veya erişim sağlayabilir. * Veri Bütünlüğünün İhlali: Saldırgan, verileri değiştirebilir veya silebilir, bu da veri bütünlüğünü ciddi şekilde etkileyebilir. * Hizmet Durdurma: Saldırgan, sistem kaynaklarını aşırı şekilde kullanarak hedef sistemin hizmet dışı kalmasına neden olabilir (DoS/DDoS saldırıları). * Sistem İzleme: Saldırgan, hedef sistemde gizlice izleme yaparak kullanıcıların etkinliklerini gözlemleyebilir. |
| CVSS |
| 7.2 |
| 3 |

# 5 ) Remote Code Execution

|  |
| --- |
| Zafiyet Adı |
| Remote Code Execution |
|  |
| Zafiyet Açıklaması |
| <http://127.0.0.1/login.php> adresine gidilir ve firma giriş yapılır. Ardından <http://127.0.0.1/company_edit_restaurant.php?id=1> adresine gidilir. Restaurant resmi seçin butonuna tıklanır ve test.jpg dosyası sistemi yüklenir ve istek BurpSuite proxy aracı ile yakalanır ve isteğe sağ tıklanıp “send to repeater” seçeneği seçilir.    Görsel - 9 Dosya Yükleme İsteği  Dosya uzantısı .php ile değiştirilir ve Content-Disposition: form-data; name="update\_profile\_picture" Header’ının altına “<?php $value = system("whoami"); echo $value; ?> bu payload yazılır. Ardından istek gönderilir. Sistemden çıkış yapılır ve <http://127.0.0.1/login.php> adresine gidilir ve müşteri giriş yapılır. <http://127.0.0.1/customer_restaurants.php> adresine gidilip seçilen restauran’ın <img> etiketi içinde yüklenen dosyanın konumu bulunur. Bulunan konuma (<http://127.0.0.1/uploads/restaurant_images/66fee861dc801_test.php> ) istek atılır. Böyle başarıyla sunucu üzerinde uzaktan kod yürütülür.  metin, ekran görüntüsü, yazı tipi içeren bir resim  Açıklama otomatik olarak oluşturuldu  Görsel - 10 Elde Edilen Komutun Response’u |
| Çözüm Önerisi |
| Dosya Türü Kontrolü:   * Yüklemeye izin verilen dosya türlerini sınırlayın. Sadece belirli dosya türlerine (örneğin, .jpg, .png, .pdf) izin verin. * Dosya uzantılarını kontrol etmek yeterli değildir; dosya içeriğini de doğrulamak için MIME türü kontrolü yapın.   Dosya Boyutu Sınırlaması:   * Yüklenen dosyaların boyutunu sınırlayın. Belirli bir boyutun üzerinde dosya yüklemeyi engelleyin.   Dosya İsimleri Kontrolü:   * Yüklenen dosyaların isimlerini güvenli hale getirin. Dosya isimlerindeki özel karakterleri temizleyin ve dosya isimlerini standart bir formatta düzenleyin. * Aynı dosya ismi ile yüklenmeleri durumunda yeni isimler verin. |
| Zafiyetin Doğurabileceği Sonuçlar |
| * Tam Kontrol: Saldırgan, hedef sistemde tam kontrol sağlayabilir. Bu, dosya sistemine erişim, sistem ayarlarını değiştirme ve yazılımları yükleme veya kaldırma anlamına gelir. * Veri Hırsızlığı: RCE zafiyeti sayesinde, saldırgan hassas verilere (şifreler, kişisel bilgiler, finansal veriler vb.) erişebilir ve bunları çalabilir. * Zarar Verme: Saldırgan, hedef sistemde kötü amaçlı yazılımlar, virüsler veya truva atları yükleyerek sistemin işleyişini bozabilir. * Ağ İçin Tehdit: Hedef sistemin yanı sıra, RCE zafiyetleri, diğer bağlı sistemlere (ağdaki diğer cihazlar, sunucular vb.) de zarar verebilir veya erişim sağlayabilir. * Veri Bütünlüğünün İhlali: Saldırgan, verileri değiştirebilir veya silebilir, bu da veri bütünlüğünü ciddi şekilde etkileyebilir. * Hizmet Durdurma: Saldırgan, sistem kaynaklarını aşırı şekilde kullanarak hedef sistemin hizmet dışı kalmasına neden olabilir (DoS/DDoS saldırıları). * Sistem İzleme: Saldırgan, hedef sistemde gizlice izleme yaparak kullanıcıların etkinliklerini gözlemleyebilir. |
| CVSS |
| 7.2 |
| 3 |

# 6) IDOR

|  |
| --- |
| Zafiyet Adı |
| IDOR |
|  |
| Zafiyet Açıklaması |
| <http://127.0.0.1/login.php> adresine gidilir ve admin giriş yapılır. Ardından <http://127.0.0.1/company_add_coupon.php> adresine gidilir. Burada indirim yüzdesi maximum seçilebilecek değer 100 olarak ayarlanmıştır. Kupon ekleme formu doldurulur ve istek BurpSuite proxy aracı ile yakalanır. Yakalanan istek üzerindeki discount= paremetresi 500 değeri ile ve restaurant\_id=1 parametresi 2 değeri ile değiştirilir. Böylece başarıyla %100 üzerinde bir indirim kuponu giriş yapan company’inin restorantları dışında başka herhangi bir restorana eklenir.    Görsel - 11 Yakalanan İstek  metin, ekran görüntüsü, yazı tipi, tasarım içeren bir resim  Açıklama otomatik olarak oluşturuldu  Görsel - 12 Dosya Yükleme İsteği |
| Çözüm Önerisi |
| * Güçlü Doğrulama ve Yetkilendirme Kontrolleri: Güvenli bir kullanıcı doğrulama ve yetkilendirme mekanizması oluşturulmalıdır. Kullanıcıların erişebileceği nesneler, etkili kontrollerle doğrulanmalı ve yetkilendirilmelidir. * Referans Kontrolleri ve Doğrulama: Nesnelere erişim sırasında, referanslar arasında etkili doğrulama yapılmalıdır. Bu, kullanıcının erişim izinlerini sürekli olarak kontrol etmek için önemlidir. * Eşsiz Kimlikler ve Doğrulama Kodları: Güvenli bir referans sistemi oluşturmak adına nesnelere eşsiz kimlikler veya doğrulama kodları eklenmelidir. Bu yöntem, yetkisiz erişimleri önlemeye yardımcı olabilir. |
| Zafiyetin Doğurabileceği Sonuçlar |
| * Yetkisiz Kupon Ekleme : Bir restoran sahibi, IDOR zafiyeti nedeniyle başka restoranların kuponlarını ekleyebilir. Bu, haksız rekabet yaratabilir veya mali kayıplara neden olabilir. * Kuponların Suistimali : Bir kullanıcı, başka restoranlar için geçerli olan kuponları kendine veya başkalarına avantaj sağlamak için kullanabilir. Bu durum, gelir kaybına ve müşteri güveninin sarsılmasına neden olur. * Gelir Kaybı ve İtibar Zedelenmesi :Kupon sisteminde yapılan yetkisiz değişiklikler, işletmeler için büyük mali kayıplara yol açabilir. Ayrıca, sistemin güvenliğinin sorgulanması itibar kaybına neden olabilir. |
| CVSS |
| 4.3 |
| 3 |

# 7 ) Client-Side Validation Bypass

|  |
| --- |
| Zafiyet Adı |
| Client-Side Validation Bypass |
|  |
| Zafiyet Açıklaması |
| <http://127.0.0.1/login.php> adresine gidilir ve admin giriş yapılır. Ardından <http://127.0.0.1/coupon_add.php> adresine gidilir. Burada indirim yüzdesi maximum seçilebilecek değer 100 olarak ayarlanmıştır. Kupon ekleme formu doldurulur ve istek BurpSuite proxy aracı ile yakalanır. Yakalanan istek üzerindeki discount= paremetresi 500 değeri ile değiştirilir. Böylece başarıyla %100 üzerinde bir indirim kuponu eklenir.  metin, ekran görüntüsü, yazı tipi, tasarım içeren bir resim  Açıklama otomatik olarak oluşturuldu  Görsel - 13 Dosya Yükleme İsteği |
| Çözüm Önerisi |
| * Sunucu tarafında giriş doğrulama ve sınırlandırma yapılmalı. * Beklenmeyen girişlere karşı ek güvenlik önlemleri (rate limiting, input sanitization gibi) uygulanmalıdır. |
| Zafiyetin Doğurabileceği Sonuçlar |
| * İş Mantığı İhlalleri :Sunucuya normalde izin verilmeyen değerler gönderilerek, uygulamanın iş mantığı bozulabilir. Örneğin, bir kullanıcı normalde 100 birim üzerinde sipariş veremiyorken, bu kısıt bypass edilerek büyük miktarlarda sipariş oluşturulabilir. Bu, stok yönetiminde hatalara veya sistemde beklenmedik davranışlara neden olabilir. * Finansal Kayıplar : Fiyat, miktar ya da indirim gibi değerlerin sunucu tarafında doğrulanmaması, finansal kayıplara yol açabilir. Örneğin, bir indirim kuponunun normalde maksimum %50 değerinde olması gerekirken, bu bypass edilerek %100 indirim yapılabilir. Bu, şirketin gelir kaybına neden olabilir. |
| CVSS |
| 3.5 |
| 3 |

# 8) IDOR

|  |
| --- |
| Zafiyet Adı |
| IDOR |
|  |
| Zafiyet Açıklaması |
| <http://127.0.0.1/login.php> adresine gidilir ve şirket giriş yapılır. Ardından <http://127.0.0.1/company_coupons.php> adresine gidilir. Listelenen kuponlardan herhangi bir tanesinin SİL butonuna tıklanır ve istek burpsuite Proxy aracı ile tutulur. GET /company\_delete\_coupon.php?id=6 HTTP/1.1 yandaki http header’ındaki id=3 paremetresinin değeri 6 yapılır. Böylece başarıyla giriş yapan company’inin restorantları dışında başka herhangi bir restoranın kuponu silinir.    Görsel - 14 Yakalanan İstek    Görsel - 15 Dosya Yükleme İsteği |
| Çözüm Önerisi |
| * Güçlü Doğrulama ve Yetkilendirme Kontrolleri: Güvenli bir kullanıcı doğrulama ve yetkilendirme mekanizması oluşturulmalıdır. Kullanıcıların erişebileceği nesneler, etkili kontrollerle doğrulanmalı ve yetkilendirilmelidir. * Referans Kontrolleri ve Doğrulama: Nesnelere erişim sırasında, referanslar arasında etkili doğrulama yapılmalıdır. Bu, kullanıcının erişim izinlerini sürekli olarak kontrol etmek için önemlidir. * Eşsiz Kimlikler ve Doğrulama Kodları: Güvenli bir referans sistemi oluşturmak adına nesnelere eşsiz kimlikler veya doğrulama kodları eklenmelidir. Bu yöntem, yetkisiz erişimleri önlemeye yardımcı olabilir. |
| Zafiyetin Doğurabileceği Sonuçlar |
| * Yetkisiz Kupon Ekleme ve Silme : Bir restoran sahibi, IDOR zafiyeti nedeniyle başka restoranların kuponlarını ekleyebilir. Bu, haksız rekabet yaratabilir veya mali kayıplara neden olabilir. * Kuponların Suistimali : Bir kullanıcı, başka restoranlar için geçerli olan kuponları kendine veya başkalarına avantaj sağlamak için kullanabilir. Bu durum, gelir kaybına ve müşteri güveninin sarsılmasına neden olur. * Gelir Kaybı ve İtibar Zedelenmesi :Kupon sisteminde yapılan yetkisiz değişiklikler, işletmeler için büyük mali kayıplara yol açabilir. Ayrıca, sistemin güvenliğinin sorgulanması itibar kaybına neden olabilir. |
| CVSS |
| 4.3 |
| 3 |

# 9) IDOR

|  |
| --- |
| Zafiyet Adı |
| IDOR |
|  |
| Zafiyet Açıklaması |
| <http://127.0.0.1/login.php> adresine gidilir ve şirket giriş yapılır. Ardından <http://127.0.0.1/company_foods.php> adresine gidilir.. Listelenen Yemeklerde herhangi bir tanesinin Düzenle butonuna tıklanır ve istek burpsuite Proxy aracı ile tutulur    Görsel - 16 Yakalanan İstek  Yakalanan istekte Content-Disposition: form-data; name="restaurant\_id" parametresinde 1 değeri 2 ile değiştirilir. Böylece başarıyla başka bir restorana yemek ekleme işlemi gerçekleştirilir. |
| Çözüm Önerisi |
| * Güçlü Doğrulama ve Yetkilendirme Kontrolleri: Güvenli bir kullanıcı doğrulama ve yetkilendirme mekanizması oluşturulmalıdır. Kullanıcıların erişebileceği nesneler, etkili kontrollerle doğrulanmalı ve yetkilendirilmelidir. * Referans Kontrolleri ve Doğrulama: Nesnelere erişim sırasında, referanslar arasında etkili doğrulama yapılmalıdır. Bu, kullanıcının erişim izinlerini sürekli olarak kontrol etmek için önemlidir. * Eşsiz Kimlikler ve Doğrulama Kodları: Güvenli bir referans sistemi oluşturmak adına nesnelere eşsiz kimlikler veya doğrulama kodları eklenmelidir. Bu yöntem, yetkisiz erişimleri önlemeye yardımcı olabilir. |
| Zafiyetin Doğurabileceği Sonuçlar |
| * Yetkisiz Kupon Ekleme : Bir restoran sahibi, IDOR zafiyeti nedeniyle başka restoranların kuponlarını ekleyebilir. Bu, haksız rekabet yaratabilir veya mali kayıplara neden olabilir. * Kuponların Suistimali : Bir kullanıcı, başka restoranlar için geçerli olan kuponları kendine veya başkalarına avantaj sağlamak için kullanabilir. Bu durum, gelir kaybına ve müşteri güveninin sarsılmasına neden olur. * Gelir Kaybı ve İtibar Zedelenmesi :Kupon sisteminde yapılan yetkisiz değişiklikler, işletmeler için büyük mali kayıplara yol açabilir. Ayrıca, sistemin güvenliğinin sorgulanması itibar kaybına neden olabilir. |
| CVSS |
| 4.3 |
| 3 |

# 10) IDOR

|  |
| --- |
| Zafiyet Adı |
| IDOR |
|  |
| Zafiyet Açıklaması |
| <http://127.0.0.1/login.php> adresine gidilir ve kullanıcı giriş yapılır. Ardından <http://127.0.0.1/customer_cart.php> adresine gidilir. Sepetteki listelenen yemeklerde herhangi bir tanesinin Not Güncelle butonuna tıklanır ve istek burpsuite Proxy aracı ile tutulur    Görsel - 17 Yakalanan İstek  Yakalanan istekte basket\_id=4&note=DENEME36 parametreleri sırasıyla 2 ve “TESTBASKET” değerleri ile değiştirilerek başka bir kullanıcının sepetindeki ürünün notu başarıyla değiştirilir. |
| Çözüm Önerisi |
| * Güçlü Doğrulama ve Yetkilendirme Kontrolleri: Güvenli bir kullanıcı doğrulama ve yetkilendirme mekanizması oluşturulmalıdır. Kullanıcıların erişebileceği nesneler, etkili kontrollerle doğrulanmalı ve yetkilendirilmelidir. * Referans Kontrolleri ve Doğrulama: Nesnelere erişim sırasında, referanslar arasında etkili doğrulama yapılmalıdır. Bu, kullanıcının erişim izinlerini sürekli olarak kontrol etmek için önemlidir. * Eşsiz Kimlikler ve Doğrulama Kodları: Güvenli bir referans sistemi oluşturmak adına nesnelere eşsiz kimlikler veya doğrulama kodları eklenmelidir. Bu yöntem, yetkisiz erişimleri önlemeye yardımcı olabilir. |
| Zafiyetin Doğurabileceği Sonuçlar |
| * Yetkisiz Kupon Ekleme : Bir restoran sahibi, IDOR zafiyeti nedeniyle başka restoranların kuponlarını ekleyebilir. Bu, haksız rekabet yaratabilir veya mali kayıplara neden olabilir. * Kuponların Suistimali : Bir kullanıcı, başka restoranlar için geçerli olan kuponları kendine veya başkalarına avantaj sağlamak için kullanabilir. Bu durum, gelir kaybına ve müşteri güveninin sarsılmasına neden olur. * Gelir Kaybı ve İtibar Zedelenmesi :Kupon sisteminde yapılan yetkisiz değişiklikler, işletmeler için büyük mali kayıplara yol açabilir. Ayrıca, sistemin güvenliğinin sorgulanması itibar kaybına neden olabilir. |
| CVSS |
| 4.3 |
| 3 |

# 11) IDOR

|  |
| --- |
| Zafiyet Adı |
| IDOR |
|  |
| Zafiyet Açıklaması |
| <http://127.0.0.1/login.php> adresine gidilir ve kullanıcı giriş yapılır. Ardından <http://127.0.0.1/customer_cart.php> adresine gidilir. Sepetteki listelenen yemeklerde herhangi bir tanesinin Kaldır butonuna tıklanır ve istek burpsuite Proxy aracı ile tutulur    Görsel - 17 Yakalanan İstek  Yakalanan istekte basket\_id=4 parametresi 2 değeri ile değiştirilir ve başka bir kullanıcının sepetindeki ürün başarıyla silinir. |
| Çözüm Önerisi |
| * Güçlü Doğrulama ve Yetkilendirme Kontrolleri: Güvenli bir kullanıcı doğrulama ve yetkilendirme mekanizması oluşturulmalıdır. Kullanıcıların erişebileceği nesneler, etkili kontrollerle doğrulanmalı ve yetkilendirilmelidir. * Referans Kontrolleri ve Doğrulama: Nesnelere erişim sırasında, referanslar arasında etkili doğrulama yapılmalıdır. Bu, kullanıcının erişim izinlerini sürekli olarak kontrol etmek için önemlidir. * Eşsiz Kimlikler ve Doğrulama Kodları: Güvenli bir referans sistemi oluşturmak adına nesnelere eşsiz kimlikler veya doğrulama kodları eklenmelidir. Bu yöntem, yetkisiz erişimleri önlemeye yardımcı olabilir. |
| Zafiyetin Doğurabileceği Sonuçlar |
| * Yetkisiz Kupon Ekleme : Bir restoran sahibi, IDOR zafiyeti nedeniyle başka restoranların kuponlarını ekleyebilir. Bu, haksız rekabet yaratabilir veya mali kayıplara neden olabilir. * Kuponların Suistimali : Bir kullanıcı, başka restoranlar için geçerli olan kuponları kendine veya başkalarına avantaj sağlamak için kullanabilir. Bu durum, gelir kaybına ve müşteri güveninin sarsılmasına neden olur. * Gelir Kaybı ve İtibar Zedelenmesi :Kupon sisteminde yapılan yetkisiz değişiklikler, işletmeler için büyük mali kayıplara yol açabilir. Ayrıca, sistemin güvenliğinin sorgulanması itibar kaybına neden olabilir. |
| CVSS |
| 4.3 |
| 3 |

# 12) IDOR

|  |
| --- |
| Zafiyet Adı |
| IDOR |
|  |
| Zafiyet Açıklaması |
| <http://127.0.0.1/login.php> adresine gidilir ve kullanıcı giriş yapılır. Ardından <http://127.0.0.1/customer_cart.php> adresine gidilir. Sepetteki listelenen yemeklerde herhangi bir tanesinin miktarı arttırılıp Güncelle butonuna tıklanır ve istek burpsuite Proxy aracı ile tutulur.    Görsel - 18 Yakalanan İstek  Yakalanan istekte basket\_id=4 parametresi 2 değeri ile değiştirilir ve başka bir kullanıcının sepetindeki ürün miktarı başarıyla değiştirilir. |
| Çözüm Önerisi |
| * Güçlü Doğrulama ve Yetkilendirme Kontrolleri: Güvenli bir kullanıcı doğrulama ve yetkilendirme mekanizması oluşturulmalıdır. Kullanıcıların erişebileceği nesneler, etkili kontrollerle doğrulanmalı ve yetkilendirilmelidir. * Referans Kontrolleri ve Doğrulama: Nesnelere erişim sırasında, referanslar arasında etkili doğrulama yapılmalıdır. Bu, kullanıcının erişim izinlerini sürekli olarak kontrol etmek için önemlidir. * Eşsiz Kimlikler ve Doğrulama Kodları: Güvenli bir referans sistemi oluşturmak adına nesnelere eşsiz kimlikler veya doğrulama kodları eklenmelidir. Bu yöntem, yetkisiz erişimleri önlemeye yardımcı olabilir. |
| Zafiyetin Doğurabileceği Sonuçlar |
| * Yetkisiz Kupon Ekleme : Bir restoran sahibi, IDOR zafiyeti nedeniyle başka restoranların kuponlarını ekleyebilir. Bu, haksız rekabet yaratabilir veya mali kayıplara neden olabilir. * Kuponların Suistimali : Bir kullanıcı, başka restoranlar için geçerli olan kuponları kendine veya başkalarına avantaj sağlamak için kullanabilir. Bu durum, gelir kaybına ve müşteri güveninin sarsılmasına neden olur. * Gelir Kaybı ve İtibar Zedelenmesi :Kupon sisteminde yapılan yetkisiz değişiklikler, işletmeler için büyük mali kayıplara yol açabilir. Ayrıca, sistemin güvenliğinin sorgulanması itibar kaybına neden olabilir. |
| CVSS |
| 4.3 |
| 3 |