



YAVUZLAR

Web Security & Development Team

Restoran Uygulaması Web Güvenliđi Raporu

Bu belge Yavuzlar içerisinde geliştirilen Restoran uygulamasının zafiyet raporunu
içermektedir

Eren Ersoyluođlu
Yavuzlar 5. Takım



İçindekiler

Giriş.....	2
Kapsam	2
Kullanılan Hesaplar	2
Risk Seviyesi Tanımları	2
Rapor Özeti	3
Zafiyet Tablosu	3
Bulunan Zafiyetler	4
SQL Veritabanı Table ve Column keşifi:.....	4
Kullanıcılar arası veri manipulasyonu	5
Dosya Yükleme Zafiyeti	19



Giriş

Bu rapor Yavuzlar bünyesinde geliştirilen Restoran uygulamasının güvenlik analizini barındırmaktadır.

Kapsam

Bu rapor ve güvenlik testinin kapsamında olan uygulama aşağıda paylaşılan github repository' sinde bulunmaktadır:

<https://github.com/1Xnes/yavuzlar/tree/main/hafta3odev>

Kullanılan Hesaplar

Kullanıcı Adı	Yetki
User	Yetkisiz, normal kullanıcı
User1	Yetkisiz, normal kullanıcı
'@@version	Yetkisiz, normal kullanıcı
Company	Restoran yönetimine sahip kullanıcı
Company2	Restoran yönetimine sahip kullanıcı
Admin	Şirket ve Kullanıcı yönetimine sahip kullanıcı

Risk Seviyesi Tanımları

Risk Seviyesi	Tanım
Kritik	Kritik risk seviyesi bulunan zafiyetler, sisteme ve kullanıcılara kolaylıkla zarar verebilen zafiyetlerdir. Bulunduğu anda müdahale edilmek zorundadır.
Yüksek	Yüksek risk seviyesi bulunan zafiyetler, kullanılması daha da zor olsada sisteme ve kullanıcılara zarar verebilen zafiyetlerdir.
Orta	Orta risk seviyesi bulunan zafiyetler, kullanıcı ve sisteme verdiği hasar daha az olsada sisteme erişim ve veri bütünlüğünü tehdit edebilir.
Düşük	Düşük risk seviyesi bulunan zafiyetler, sistemde erişim engellemesi sağlamayan veya sisteme daha az zarar türde zafiyetler.
Bilgi	Bilgi derecesi zafiyetler sisteme etkisi bulunmayan sadece saldırganın bilgi toplamasını sağlayan zafiyetlerdir.



Rapor Özeti

Yapılan incelemeler sonucu uygulama üzerinde 1 Kritik , 1 Orta ve 1 Bilgi seviyesinde açığı olduğu bulundu. Bulunan bu zafiyetler hem sistem için hemde kullanıcı için büyük risk oluşturup veri bütünlüğü konusunda risk oluşturacak yapıdadırlar.

Zafiyet Tablosu

Risk Seviyesi	CVSS Puanı	Zafiyet İsmi	Zafiyetin etkisi
Kritik	9.1	Dosya yükleme	KontROLSÜZ olarak yüklenen dosyalar sistemin bütünlüğünü tehlikeye atmaktadır.
Orta	5.3	Kullanıcılar Arası Veri Manipulasyonu	Kullanıcılara özel olması gereken verilerin kaynak kodu üzerinden rahatça erişebilmesi ve değişiklik yapabilmesi sonucu kullanıcı veri bütünlüğü tehlikeye atılmaktadır.
Bilgi	0.0	SQL Veritabanı Table ve Column keşifi	Sistemin döndüğü hata mesajlarının kapatılmaması sonucu gizli olması gereken verinin kullanıcıya sunulması.

Risk Seviyesi / Kapsam	Kritik	Yüksek	Orta	Düşük	Bilgi	Toplam
Veri Tabanı Sistemleri					1	1
Web Uygulamaları	1		1			2
Toplam	1		1		1	3



Bulunan Zafiyetler

SQL Veritabanı Table ve Column keşifi:

Seviye: Bilgi

CVSS Skoru: 0.0

Restoran uygulaması üzerinde gönderilen POST requestler Burp Suite uygulaması ile yakalandı, istekler incelendi ve gönderilen veri değiştirildi.

Request

POST /add_to_cart.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:130.0) Gecko/20100101 Firefox/130.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 50
Origin: http://localhost
DNT: 1
Sec-OPC: 1
Connection: Keep-Alive
Referer: http://localhost/customer_restaurant_menu.php?id=2
Cookie: phpMyAdmin=c70c5c441da47b7460aab8af5986a6c1; pma_lang=en; PHPSESSID=4b4d82860791e20d3b30a25be3292e1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
food_id=&quantity=1

Response

HTTP/1.1 200 OK
Date: Mon, 30 Sep 2024 10:52:23 GMT
Server: Apache/2.4.56 (Debian)
X-Powered-By: PHP/8.0.30
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 448
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

Fatal error

Uncaught PDOException: SQLSTATE[HY000]: General error: 1366 Incorrect integer value: '' for column 'food_id' at row 1 in /var/www/src/includes/functions.php:641

Stack trace:

#0 /var/www/src/includes/functions.php(641): PDOStatement->execute(Array)
#1 /var/www/html/add_to_cart.php(22): addToCart(Object(PDO), 5, '', '1', '')
#2 {main}
thrown in /var/www/src/includes/functions.php
on line 641

Veri yapısı veritabanının beklediği formata uymazasa SQL tarafınan hata mesajı döndü ve hata mesajı incelendiğinde veritabanında bulunan Table ve Column isimlerinin açıkça paylaşıldığı gözlemlendi.

Yavuzlar 5. Takım



Request				Response			
Pretty	Raw	Hex	Hackvortor	Pretty	Raw	Hex	Hackvortor
<pre>1 POST /add_to_cart.php HTTP/1.1 2 Host: localhost 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:130.0) Gecko/20100101 Firefox/130.0 4 Accept: 5 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8 6 Accept-Language: en-US,en;q=0.5 7 Accept-Encoding: gzip, deflate, br 8 Content-Type: application/x-www-form-urlencoded 9 Content-Length: 21 10 Origin: http://localhost 11 DNT: 1 12 Sec-GPC: 1 13 Connection: Keep-Alive 14 Referer: http://localhost/customer_restaurant_menu.php?id=2 15 Cookie: phpMyAdmin=c70c5c44ida47b7460aab8af5956a6c1; pma_lang=en; PHPSESSID=4b4d826860791e20d3b30a28be3292e1 16 Upgrade-Insecure-Requests: 1 17 Sec-Fetch-Dest: document 18 Sec-Fetch-Mode: navigate 19 Sec-Fetch-Site: same-origin 20 Sec-Fetch-User: ?1 21 Priority: u=0, i 22 food_id=99&quantity=1</pre>				<pre>1 HTTP/1.1 200 OK 2 Date: Mon, 30 Sep 2024 10:59:04 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 Vary: Accept-Encoding 9 Content-Length: 584 10 Keep-Alive: timeout=5, max=100 11 Connection: Keep-Alive 12 Content-Type: text/html; charset=UTF-8 13 14
 15
 16 Fatal error 17 : Uncaught PDOException: SQLSTATE[23000]: Integrity constraint violation: 1452 Cannot add 18 or update a child row: a foreign key constraint fails ('yemek_yonetim_sistemi'.basket', 19 CONSTRAINT basket_ibfk_2 FOREIGN KEY ('food_id') REFERENCES food ('id')) in 20 /var/www/src/includes/functions.php:641 21 Stack trace: 22 #0 /var/www/src/includes/functions.php(641): PDOStatement->execute(Array) 23 #1 /var/www/html/add_to_cart.php(22): addToCart(Object(PDO), 5, '99', '1', '') 24 #2 (main) 25 thrown in
 26 /var/www/src/includes/functions.php 27 28 </br> 29 on line
 30 641 31 </br> 32
</pre>			
0 highlights				0 highlights			

Kullanıcılar arası veri manipulasyonu

Seviye: Orta

CVSS Skoru: 5.3

Restoran uygulamasına müşteri hesabı 'User' ile giriş yapıldı ve kullanıcı sepetine ürün ekledi.

Yavuzlar 5. Takım

5



GİRİŞ YAP

GİRİŞ YAP

ANA SAYFA



SEPETİM

Yemek	Fiyat	İndirimli Fiyat	Miktar	Toplam	Not	İşlemler
asdasdas	200.00 TL	200.00 TL	1 <input type="text" value="1"/>	200.00 TL	<input type="text"/>	<input type="button" value="KALDIR"/>
			<input type="button" value="GÜNCELLE"/>		<input type="button" value="NOT GÜNCELLE"/>	
asdasdas	200.00 TL	200.00 TL	1 <input type="text" value="1"/>	200.00 TL	qweqweqwe	<input type="button" value="KALDIR"/>
			<input type="button" value="GÜNCELLE"/>		<input type="button" value="NOT GÜNCELLE"/>	

Kupon Kodu:

Toplam: 400.00 TL

Sepet sayfasının kaynak kodları incelendi, kaynak kodları arasında sepet ürünlerinin id'si gizli bir şekilde tutulduğu görüldü.



```
Search HTML
<td>200.00 TL</td>
<td>200.00 TL</td>
▼ <td>
  ▼ <form action="update_cart.php" method="POST">
    <input type="hidden" name="basket_id" value="1">
    <input type="number" name="quantity" value="1" min="1" max="10">
    <button class="btn" type="submit">Güncelle</button>
  </form>
</td>
<td>200.00 TL</td>
▼ <td>
  ▼ <form action="update_cart_note.php" method="POST">
    <input type="hidden" name="basket_id" value="1">
    <input type="text" name="note" value="qweqweqwe">
    <button class="btn" type="submit">Not Güncelle</button>
  </form>
</td>
▼ <td>
  ▼ <form action="remove_from_cart.php" method="POST">
    <input type="hidden" name="basket_id" value="1">
    <button class="btn" type="submit">Kaldır</button>
  </form>
</td>
</tr>
</tbody>
```

'user' kullanıcılarından çıkış yapılarak yeni bir müşteri kullanıcıya "@@version" giriş yapıldı ve bu kullanıcısında sepetine ürün eklendi.



GİRİŞ YAP

GİRİŞ YAP

ANA SAYFA



SEPETİM

Yemek	Fiyat	İndirimli Fiyat	Miktar	Toplam	Not	İşlemler
asdasdas	200.00 TL	200.00 TL	1 <input type="button" value="GÜNCELLE"/>	200.00 TL	<input type="text"/> <input type="button" value="NOT GÜNCELLE"/>	<input type="button" value="KALDIR"/>

Kupon Kodu:

Toplam: 200.00 TL

Yeni giriş yaptığımız kullanıcıda kaynak kodu üzerinden 'basket_id' üzerinde değişiklik yapılarak '1' olarak kayıt edildi.



```
<td>200.00 TL</td>
▼ <td>
  ▼ <form action="update_cart.php" method="POST">
    <input type="hidden" name="basket_id" value="8">
    <input type="number" name="quantity" value="1" min="1" max="10">
    <button class="btn" type="submit">Güncelle</button>
  </form>
</td>
<td>200.00 TL</td>
▼ <td>
  ▼ <form action="update_cart_note.php" method="POST">
    <input type="hidden" name="basket_id" value="8">
    <input type="text" name="note" value="">
    <button class="btn" type="submit">Not Güncelle</button>
  </form>
</td>
▼ <td>
  ▼ <form action="remove_from_cart.php" method="POST">
    <input type="hidden" name="basket_id" value="8">
    <button class="btn" type="submit">Kaldır</button>
  </form>
</td>
</tr>
```

```
<td>200.00 TL</td>
▼ <td>
  ▼ <form action="update_cart.php" method="POST">
    <input type="hidden" name="basket_id" value="8">
    <input type="number" name="quantity" value="1" min="1" max="10">
    <button class="btn" type="submit">Güncelle</button>
  </form>
</td>
<td>200.00 TL</td>
▼ <td>
  ▼ <form action="update_cart_note.php" method="POST">
    <input type="hidden" name="basket_id" value="8">
    <input type="text" name="note" value="">
    <button class="btn" type="submit">Not Güncelle</button>
  </form>
</td>
▼ <td>
  ▼ <form action="remove_from_cart.php" method="POST">
    <input type="hidden" name="basket_id" value="1">
    <button class="btn" type="submit">Kaldır</button>
  </form>
</td>
</tr>
```

"@@version' kullanıcısı üzerinden ürün silinmeye çalışıldığında sepette bulunan ürünün silinmediği görüldü.

Yavuzlar 5. Takım

11



SEPETİM

Ürün sepetten kaldırıldı.

Yemek	Fiyat	İndirimli Fiyat	Miktar	Toplam	Not	İşlemler
asdasdas	200.00 TL	200.00 TL	1	200.00 TL		<div><div>GÜNCELLE</div><div>NOT GÜNCELLE</div><div>KALDIR</div></div>

Kupon Kodu:

KUPONU UYGULA

Toplam: 200.00 TL

SİPARİŞ VER

ALİŞVERİŞE DEVAM ET

ANA SAYFAYA DÖN

'user' kullanıcısına tekrar giriş yapıldı ve sepetsayfasına girildi.

GİRİŞ YAP

GİRİŞ YAP

ANA SAYFA



“@@vesion” kullanıcısında yarılan eyem sonucu ‘user’ kullanıcısının sepetinde bulunan bir ürün silindi.

SEPETİM

Yemek	Fiyat	İndirimli Fiyat	Miktar	Toplam	Not	İşlemler
asdasdas	200.00 TL	200.00 TL	1 <input type="text"/>	200.00 TL	<input type="text"/>	<div>GÜNCELLE</div> <div>NOT GÜNCELLE</div> <div>KALDIR</div>

Kupon Kodu:

KUPONU UYGULA

Toplam: 200.00 TL

SİPARİŞ VER

ALİŞVERİŞE DEVAM ET

ANA SAYFAYA DÖN

Aynı zafiyetin karşılaştığı diğer modüller:

Şirket çalışanı kupon silerken “id” parametresinde değişiklik yaparak yetkisi olmayan bir restorandan kupon siler.



KUPONLAR

Kupon başarıyla eklendi.

YENİ KUPON EKLE

ID	Kupon Adı	İndirim Oranı	Restoran	İşlemler
1	<script>alert('XSS')</script>	10.00 %	Freya Holman	SİL
3	Seth Beasley	77.00 %	Freya Holman	SİL

ANA SAYFAYA DÖN

Footer Image Made with pain

Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application

Search HTML

```
<td>77.00 %</td>
<td>Freya Holman</td>
<td>
  ::before
  <a class="btn" href="company_delete_coupon.php?id=3" onclick="return confirm('Bu kuponu silmek istediğinize emin misiniz?');">SİL</a>
</td>
</tr>
</tbody>
</table>
<p></p>
```

Filter Styles

```
element {
  padding: 10px 25px;
  border-radius: 30px;
  cursor: pointer;
  border: 0;
  background-color: white;
  box-shadow: rgb(0 0 0 / 5%) 0 0 4px;
  letter-spacing: 1px;
  text-transform: uppercase;
  font-size: 13px;
}
```

No changes found.

Changes to CSS in Inspector will appear here.

Şirket çalışanı kupon eklerken “restaurant_id” parametresinde değişiklik yaparak yetkisi olmayan bir restorana kupon atar.

KUPON EKLE

Kupon Adı: bbbb

İndirim Oranı (%): 100

Restoran: company12

KUPON EKLE

KUPON LİSTESİNE DÖN

Footer Image Made with pain

Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application

Search HTML

```
<label for="restaurant_id">Restoran:</label>
  <select id="restaurant_id" name="restaurant_id">
    <option value="1">company11</option>
    <option value="3">company12</option>
  </select>
  <br>
  <br>
  <button class="btn" type="submit">Kupon Ekle</button>
</form>
```

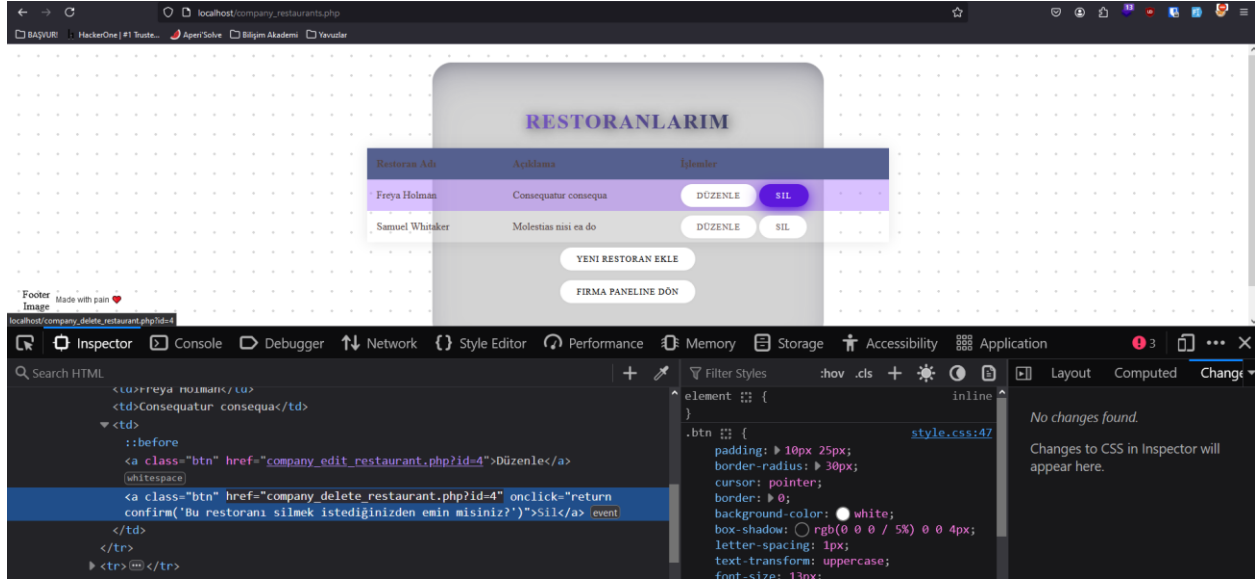
html > body > div.container > form > select#restaurant_id > option

Filter Styles

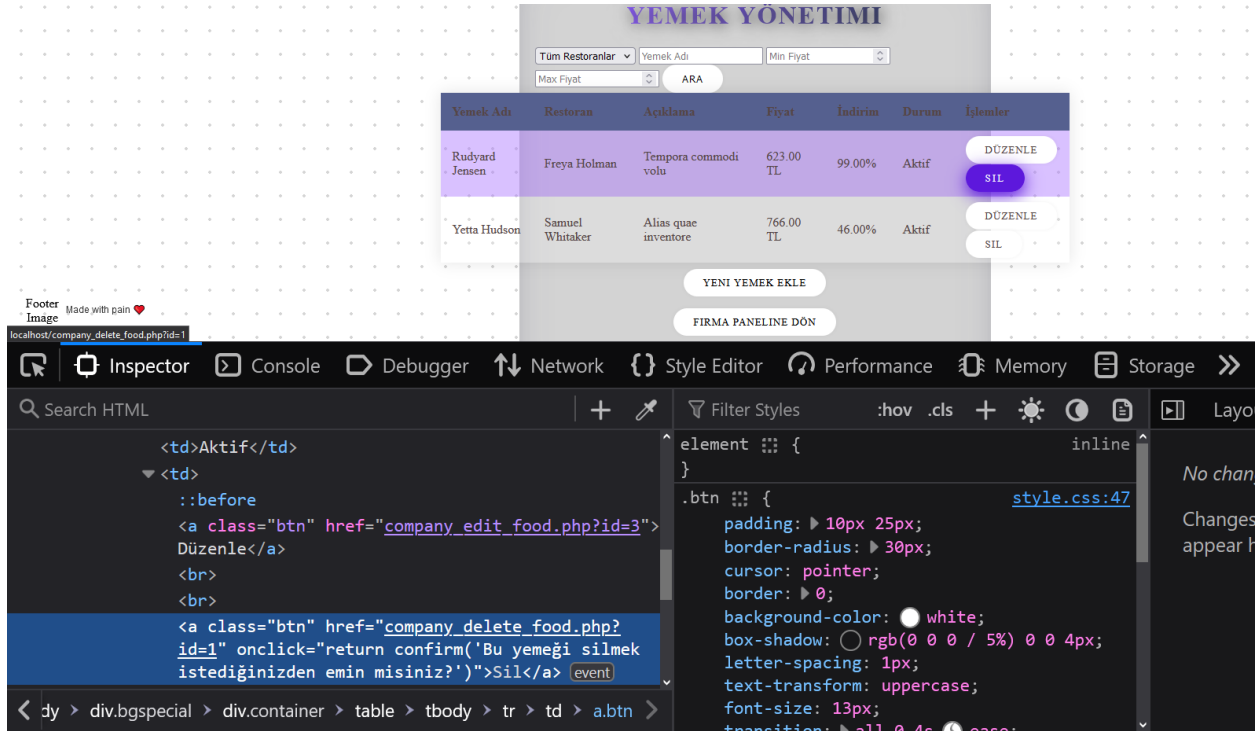
```
element {
}
```



Şirket çalışanı restoran silerken "id" parametresinde değişiklik yaparak yetkisi olmayan bir restoranı siler.



Şirket çalışanı restorandan yemek silerken "id" parametresini değiştirerek yetkisi olmayan restorandan yemek siler.





Şirket çalışanı yemek eklerken “restaurant_id” parametresinde değışiklik yaparak etkisi olmayan bir restorana yemek ekler.



YENİ YEMEK EKLE

Restoran: Freya Holman Yemek Adı: Açıklama:

Fiyat: İndirim (%): 0

Yemek Resmi: Browse... No file selected. YEMEK EKLE

YEMEK LİSTESİNE DÖN

Footer
Image
Made with pain

```
Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application
Search HTML
<form method="POST" enctype="multipart/form-data">
  <label for="restaurant_id">Restoran:</label>
  <select id="restaurant_id" name="restaurant_id" required="">
    <option value="1">Freya Holman</option>
    <option value="3">Samuel Whitaker</option>
  </select>
  <label for="name">Yemek Adı:</label>
  <input id="name" type="text" name="name" required="">
  <label for="description">Açıklama:</label>
  <textarea id="description" name="description"></textarea>
  <label for="price">Fiyat:</label>
  <input type="text" name="price">
  <label for="discount">İndirim (%):</label>
  <input type="text" name="discount">
  <input type="button" value="YEMEK EKLE">
  <input type="button" value="YEMEK LİSTESİNE DÖN">
</form>
```

Bir kullanıcı sepetindeki notu güncellerken "id" parametresini değiştirerek başka bir kullanıcının notunu değiştirir.

Yavuzlar 5. Takım



Two browser screenshots showing the 'SEPETİM' (My Cart) page. The left screenshot shows the cart with a total of 98.20 TL. The right screenshot shows the cart with a total of 529.74 TL. The right screenshot also shows the developer console with a JavaScript error: 'Uncaught SyntaxError: Invalid or unexpected token'.

SEPETİM

Not güncellendi.

Yenek	Fiyat	İndirimli Fiyat	Miktar	Toplam	Not	İşlemler
Troy Spencer	982.00 TL	98.20 TL	1	98.20 TL	88888	GÜNCELLE NOT GÜNCELLE KALDIR

Kupon Kodu: KUPONU UYGULA

Toplam: 98.20 TL

SİPARİŞ VER ALIŞVERİŞE DEVAM ET ANA SAYFAYA DÖN

Footer Image Made with pan

SEPETİM

Not güncellendi.

Yenek	Fiyat	İndirimli Fiyat	Miktar	Toplam	Not	İşlemler
Leo Tanner	135.00 TL	116.10 TL	1	116.10 TL	88888	GÜNCELLE NOT GÜNCELLE KALDIR
Yetta Hudson	766.00 TL	413.64 TL	1	413.64 TL		GÜNCELLE NOT GÜNCELLE KALDIR

Kupon Kodu: KUPONU UYGULA

Toplam: 529.74 TL

SİPARİŞ VER

Footer Image Made with pan

Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility

Q Search HTML

```
<script type="text/javascript">
</script>
<div class="special">
</div>
<div class="container">
</div>
<table>
<thead>
</thead>
<tbody>
<tr>
<td>Leo Tanner</td>
<td>135.00 TL</td>
<td>116.10 TL</td>
<td>1</td>
<td>116.10 TL</td>
<td>88888</td>
<td>GÜNCELLE</td>
<td>NOT GÜNCELLE</td>
<td>KALDIR</td>
</tr>
</tbody>
</table>
<div class="form">
<input type="text" value="Kupon Kodu">
<input type="button" value="KUPONU UYGULA">
</div>
<div class="total">
<div>Toplam: 98.20 TL</div>
<div>SİPARİŞ VER</div>
<div>ALIŞVERİŞE DEVAM ET</div>
<div>ANA SAYFAYA DÖN</div>
</div>
</div>
</div>
```

Activate Windows Go to Settings to activate Windows.

Two browser screenshots showing the 'SEPETİM' (My Cart) page. The left screenshot shows the cart with a total of 98.20 TL. The right screenshot shows the cart with a total of 529.74 TL. The right screenshot also shows the developer console with a JavaScript error: 'Uncaught SyntaxError: Invalid or unexpected token'.

SEPETİM

Not güncellendi.

Yenek	Fiyat	İndirimli Fiyat	Miktar	Toplam	Not	İşlemler
Troy Spencer	982.00 TL	98.20 TL	1	98.20 TL	88888	GÜNCELLE NOT GÜNCELLE KALDIR

Kupon Kodu: KUPONU UYGULA

Toplam: 98.20 TL

SİPARİŞ VER ALIŞVERİŞE DEVAM ET ANA SAYFAYA DÖN

Footer Image Made with pan

SEPETİM

Not güncellendi.

Yenek	Fiyat	İndirimli Fiyat	Miktar	Toplam	Not	İşlemler
Leo Tanner	135.00 TL	116.10 TL	1	116.10 TL	88888	GÜNCELLE NOT GÜNCELLE KALDIR
Yetta Hudson	766.00 TL	413.64 TL	1	413.64 TL		GÜNCELLE NOT GÜNCELLE KALDIR

Kupon Kodu: KUPONU UYGULA

Toplam: 529.74 TL

SİPARİŞ VER

Footer Image Made with pan

Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility

Q Search HTML

```
<script type="text/javascript">
</script>
<div class="special">
</div>
<div class="container">
</div>
<table>
<thead>
</thead>
<tbody>
<tr>
<td>Leo Tanner</td>
<td>135.00 TL</td>
<td>116.10 TL</td>
<td>1</td>
<td>116.10 TL</td>
<td>88888</td>
<td>GÜNCELLE</td>
<td>NOT GÜNCELLE</td>
<td>KALDIR</td>
</tr>
</tbody>
</table>
<div class="form">
<input type="text" value="Kupon Kodu">
<input type="button" value="KUPONU UYGULA">
</div>
<div class="total">
<div>Toplam: 98.20 TL</div>
<div>SİPARİŞ VER</div>
<div>ALIŞVERİŞE DEVAM ET</div>
<div>ANA SAYFAYA DÖN</div>
</div>
</div>
</div>
```

Activate Windows Go to Settings to activate Windows.

Bir kullanıcı sepetindeki ürün miktarını değiştirirken "id" parametresini değiştirerek başka bir kullanıcının sepet ürününü etkiler.



The screenshot shows the 'SEPETİM' (My Cart) page of a web application. The page has a header with the title 'SEPETİM' and a table listing items in the cart. The table has columns: 'Yenik', 'Fiyat', 'İndirimli Fiyat', 'Miktar', 'Toplam', 'Not', and 'İşlemler'. The first item is 'Troy Spencer' with a price of 982.00 TL, a discounted price of 98.20 TL, a quantity of 1, and a total of 98.20 TL. The 'İşlemler' column has buttons for 'GÜNCELLE', 'NOT GÜNCELLE', and 'KALDIR'. Below the table, there is a 'Kupon Kodu' field, a 'KUPONU UYGULA' button, and a 'Toplam: 98.20 TL' label. There are also buttons for 'SİPARİŞ VER', 'ALİŞVERİŞE DEVAM ET', and 'ANA SAYFAYA DÖN'. The footer says 'Made with pain'.

The developer tools show the HTML structure of the page. The table is defined as follows:

Yenik	Fiyat	İndirimli Fiyat	Miktar	Toplam	Not	İşlemler
Troy Spencer	982.00 TL	98.20 TL	1	98.20 TL	bbbbbb	KALDIR

The 'İşlemler' column contains buttons for 'GÜNCELLE', 'NOT GÜNCELLE', and 'KALDIR'. The 'GÜNCELLE' button is highlighted in the screenshot.

The screenshot shows the 'SEPETİM' (My Cart) page of a web application. The page has a header with the title 'SEPETİM' and a table listing items in the cart. The table has columns: 'Yenik', 'Fiyat', 'İndirimli Fiyat', 'Miktar', 'Toplam', 'Not', and 'İşlemler'. The first item is 'Troy Spencer' with a price of 982.00 TL, a discounted price of 98.20 TL, a quantity of 10, and a total of 982.00 TL. The 'İşlemler' column has buttons for 'GÜNCELLE', 'NOT GÜNCELLE', and 'KALDIR'. Below the table, there is a 'Kupon Kodu' field, a 'KUPONU UYGULA' button, and a 'Toplam: 982.00 TL' label. There are also buttons for 'SİPARİŞ VER', 'ALİŞVERİŞE DEVAM ET', and 'ANA SAYFAYA DÖN'. The footer says 'Made with pain'.

The developer tools show the HTML structure of the page. The table is defined as follows:

Yenik	Fiyat	İndirimli Fiyat	Miktar	Toplam	Not	İşlemler
Troy Spencer	982.00 TL	98.20 TL	10	982.00 TL	bbbbbb	KALDIR

The 'İşlemler' column contains buttons for 'GÜNCELLE', 'NOT GÜNCELLE', and 'KALDIR'. The 'GÜNCELLE' button is highlighted in the screenshot.

Dosya Yükleme Zafiyeti

Seviye: Kritik

Yavuzlar 5. Takım

19



CVSS Skoru: 9.1

Restoran uygulamasına müiteri hesabı 'user' ile giriş yapıldı. Profil sayfasına erişildiğinde profil resmi değiştirebildiği keşif edildi. Basit bir png dosyası yüklendi.

PROFIL

Profil resmi başarıyla güncellendi.


Profil Bilgileri

Ad: Soyad:

Kullanıcı Adı:

PROFILI GÜNCELLE

Profil Resmi

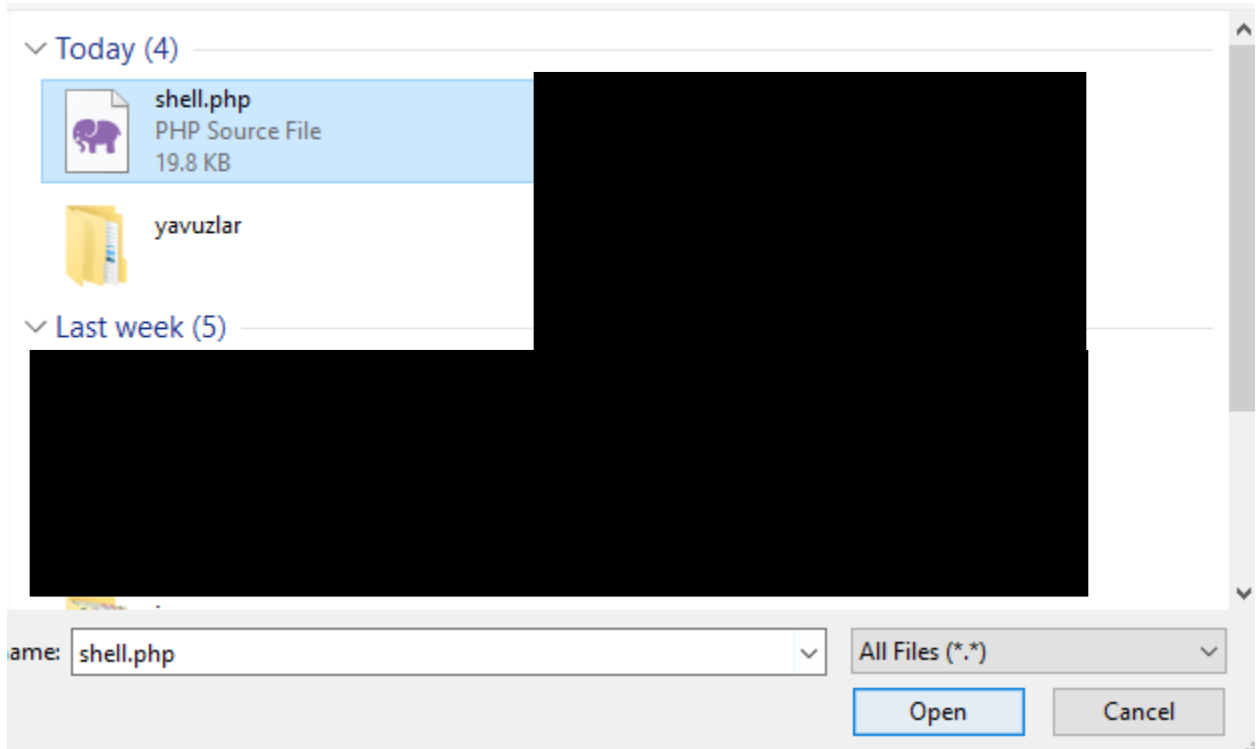


Profil Resmi: No file selected.

2. denemede png dosyası yerine php dosyası seçildi.

Yavuzlar 5. Takım

20





Profil Bilgileri

Ad: Soyad:
Kullanıcı Adı:

PROFİLİ GÜNCELLE

Profil Resmi



Profil Resmi:

Profil resmi güncellendikten sonra tarayıcı üzerinden sayfa incelendiğinde dosyanın sisteme yüklendiği görüldü.



Made with pain

Profil Bilgileri

Ad: user Soyad: user

Kullanıcı Adı: user

PROFİLİ GÜNCELLE

Profil Resmi

Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application

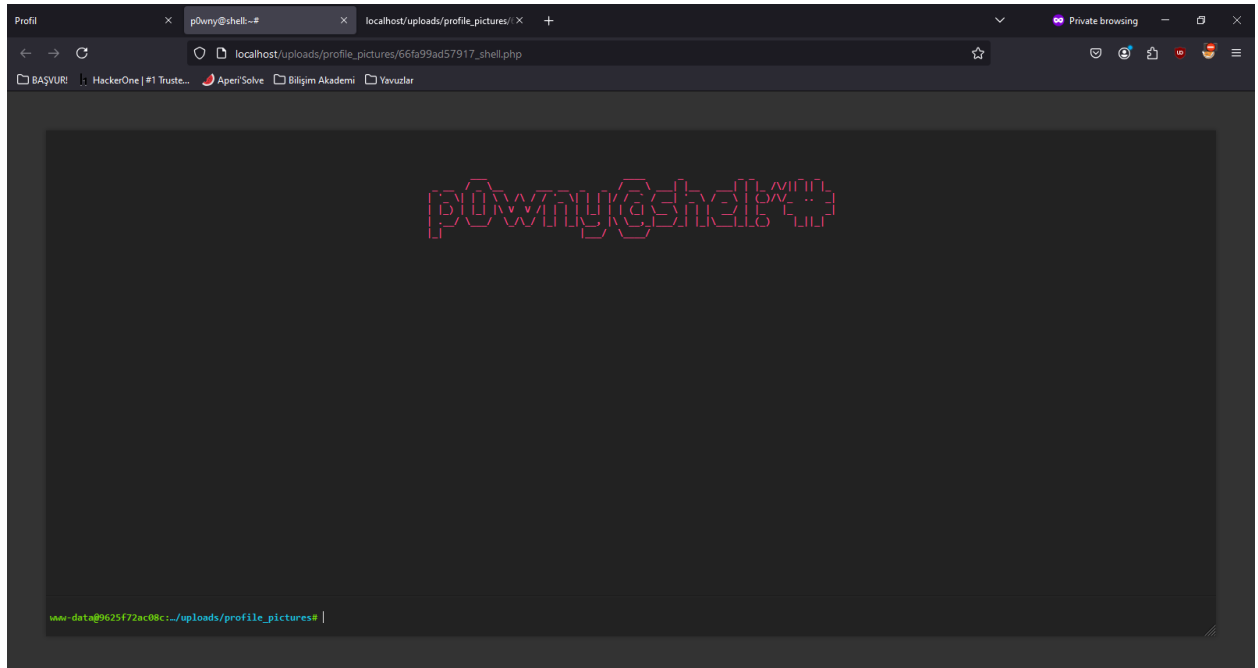
Search HTML

<!DOCTYPE html>
<html lang="en">
<head>
<body>
 <div class="bg-special">
 <div class="container">
 <h1>Profil</h1>
 <p class="success">Profil resmi başarıyla güncellendi.</p>
 <h2>Profil Bilgileri</h2>
 <form method="POST">
 <h2>Profil Resmi</h2>
 <div>

 <form method="POST" enctype="multipart/form-data">
 <h2>Sıfırla</h2>
 <p></p>
 <h2>Bakiye</h2>
 <p>Mevcut Bakiye: 5,200.00 TL</p>
 <form method="POST">
 <p></p>
 </div>
 </div>
 </div>
</body>

Filter Styles show .cls +
element {
 max-width: 200px;
 max-height: 200px;
}

Verilen dizine uygulama üzerinden eriştiğimizde yüklenen php dosyasına erişildi ve sisteme erişmek için gerekli bağlantı kuruldu.





Aynı zafiyetin karşılaştığı diğer platformlar.

Admin şirket çalışanı ekklerken oluşturulan şirketin görselini png/jpeg dışında dosyalar yükler.

KULLANICI EKLE

Şirket ▼

Browse...

Ke0fla.php

KULLANICI EKLE

ADMIN PANELINE DÖN



Şirket çalışanı restoran eklerken restoran resmini png/jpeg dışında dosyalar yükler.

YENİ RESTORAN EKLE

Restoran Adı: Açıklama:

Restoran Resmi: Ke0fla.php

RESTORAN EKLE

RESTORANLARIMA DÖN



Şirket çalışanı yemek eklerken yemek resmini png/jpeg dışında dosyalar yükler.

YENİ YEMEK EKLE

Restoran:	company11 ▾	Yemek Adı:	yemek1	Açıklama:	
	yemek1				
		Fiyat:	11	İndirim (%):	0
Yemek Resmi:	Browse...	Ke0fla.php	YEMEK EKLE		

YEMEK LİSTESİNE DÖN