Access control vulnerabilities and privilege escalation

LAB 61 Unprotected admin functionality

Quick fuzzing of the website reveals presence of /robots.txt file. Here are the contents of the file:

```
User-agent: *
Disallow: /administrator-panel
```

I directed to /administrator-panel and got access to admin table:

Users

wiener - Delete
carlos - Delete

Now, I can delete user 'carlos':

Congratulations, you solved the lab!

User deleted successfully!

Users

wiener - Delete

LAB 62 Unprotected admin functionality with unpredictable URL

Page source code:

```
                        <p>Not solved</p>
                        <span class=lab-status-icon></span>
                    </div>
                </div>
            </div>
        </section>
    </div>
    <div theme="ecommerce">
        <section class="maincontainer">
            <div class="container">
                <header class="navigation-header">
                    <section class="top-links">
                        <a href=/>Home</a><p>|</p>
                        <script>
var isAdmin = false;
if (isAdmin) {
   var topLinksTag = document.getElementsByClassName("top-links")[0];
   var adminPanelTag = document.createElement('a');
   adminPanelTag.setAttribute('href', '/admin-3161wg');
   adminPanelTag.innerText = 'Admin panel';
   topLinksTag.append(adminPanelTag);
   var pTag = document.createElement('p');
   pTag.innerText = '|';
   topLinksTag.appendChild(pTag);
}
</script>
                        <a href="/my-account">My account</a><p>|</p>
                    </section>
                </header>
                <header class="notification-header">
                </header>
                <section class="ecoms-pageheader">
                    <img src="/resources/images/shop.svg">
                </section>
                <section class="container-list-tiles">
                    <div>
                        <img src="/image/productcatalog/products/36.jpg">
                        <h3>Caution Sign</h3>
                        <img src="/resources/images/rating2.png">
                        $18.60
                        <a class="button" href="/product?productId=1">View details</a>
                    </div>
                    <div>
                        <img src="/image/productcatalog/products/28.jpg">
                        <h3>Vintage Neck Defender</h3>
```

It reveals an URL obfuscated admin page /admin-3161wg:

Users

wiener - Delete
carlos - Delete

Deleting ‘carlos’ user:

Congratulations, you solved the lab!

User deleted successfully!

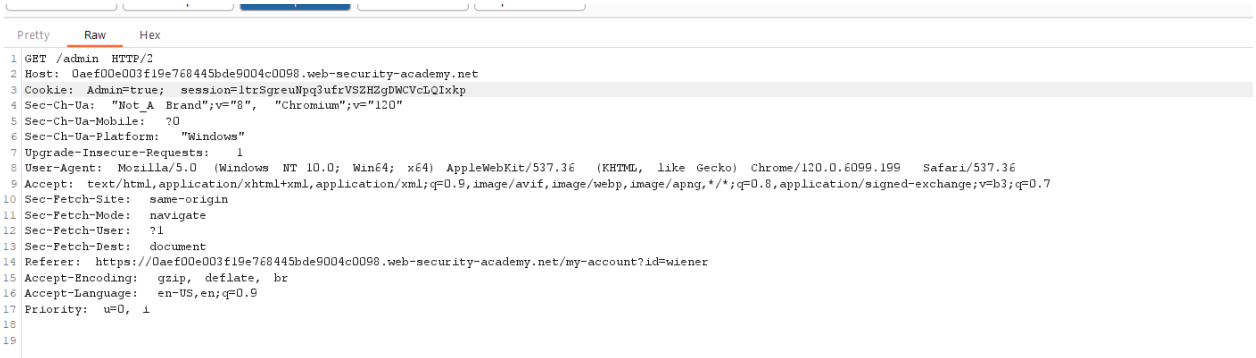
Users

wiener - Delete

LAB 63 User role controlled by request parameter

In this lab, I noticed Admin cookie to be set during log in:

I intercepted the request using Burp Interceptor and changed cookie to be true:



I did it on every request, since any action on website checks the admin cookie, directing o /admin requires cookie change as well. Finally, Admin panel is available:

Users

wiener - Delete
carlos - Delete

After ‘carlos’ deletion:

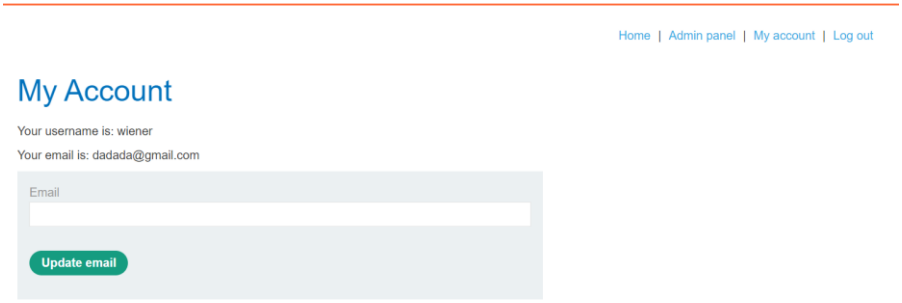
Congratulations, you solved the lab!

LAB 64 [User role can be modified in user profile]

Changing account email request contains JSON piece of code:

```
Pretty  Raw  Hex
1 POST /my-account/change-email HTTP/2
2 Host: 0a8e008e04a995c28313999000950073.web-security-academy.net
3 Cookie: session=31yuGFUuBXrSkIGp9LnZixprhq8JhsIB
4 Content-Length: 28
5 Sec-Ch-Ua: "Not_A Brand";v="8", "Chromium";v="120"
6 Sec-Ch-Ua-Platform: "Windows"
7 Sec-Ch-Ua-Mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.199 Safari/537.36
9 Content-Type: text/plain;charset=UTF-8
10 Accept: */*
11 Origin: https://0a8e008e04a995c28313999000950073.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://0a8e008e04a995c28313999000950073.web-security-academy.net/my-account?id=wiener
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: en-US,en;q=0.9
18 Priority: u=1, i
19
20 {
   "email":"dadada@gmail.com"
}
```

In lab description, it was mentioned that admin panel is available to users with roleid:2, therefore, I will add “roleid”:2 into json:



Having changed the email with my injection, I have admin panel access now. Now, final step of the task – deletion of user carlos: