Web Application Pen-Testing

AY 2022/2023

Week 3.2 Practical

OWASP Top 10 - 2021

A01:2021-Broken Access Control

Part 2

Horizontal Privilege Escalation

(User 🡪 Other User)

Insecure direct object references (IDOR)

Access control vulnerabilities in multi-step processes

Referer-based access control

Directory traversal

Document Version: 1

Tools covered:

* Enumeration Tools: OWASP ZAP
* Exploitation Tools: ZAP, Burp Suite

Table of Contents

[1 Setup 3](#_Toc118279051)

[1.1. Start and Login to Kali Linux VM with NAT enabled 3](#_Toc118279052)

[1.2. Enabling Kali Linux Web Browser Proxy Settings 4](#_Toc118279053)

[1.3. Login to WebSecurity Academy 5](#_Toc118279054)

[2 Horizontal privilege escalation 6](#_Toc118279055)

[2.1. Lab 1: User ID controlled by request parameter 6](#_Toc118279056)

[3 Homework 14](#_Toc118279057)

[3.1. Horizontal privilege escalation 14](#_Toc118279058)

[**3.1.1.** **User ID controlled by request parameter, with unpredictable user IDs** 14](#_Toc118279059)

[**3.1.2.** **User ID controlled by request parameter with data leakage in redirect** 14](#_Toc118279060)

[3.2. Insecure Direct Object References (IDOR) 14](#_Toc118279061)

[3.3. Access control vulnerabilities in multi-step processes 15](#_Toc118279062)

[3.4. Referer-based access control 15](#_Toc118279063)

[3.5. Directory traversal 16](#_Toc118279064)

# Horizontal privilege escalation

Horizontal privilege escalation arises when a user can gain access to resources belonging to another user, instead of their own resources of that type. For **example**, if an employee should only be able to access their own employment and payroll records but can in fact also access the records of other employees, then this is horizontal privilege escalation.

## Lab 1: User ID controlled by request parameter

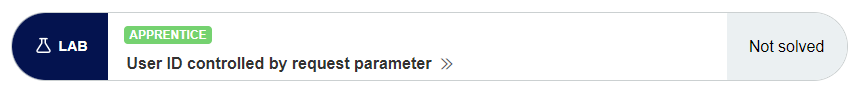
**NOTE: Read through all the steps below, before proceeding to do the lab**

A user might ordinarily access their own account page using a URL like the following:

https://insecure-website.com/myaccount?id=123

Now, if an attacker modifies the id parameter value to that of another user, then the attacker might gain access to another user's account page, with associated data and functions.

Click on the link “User ID controlled by request parameter”. This lab has a horizontal privilege escalation vulnerability on the user account page. To solve the lab, obtain the API key for the user carlos and submit it as the solution. You can log in to your own account using the following credentials: wiener:peter



#### Launch Burp Suite

Before you launch Burp Suite, make sure that **OWASP ZAP is not running (Quit/Terminate OWASP ZAP)**. Click on Kali Linux logo at the top left corner of the Desktop, and search for “burp”. Click on “Burp Suite Community Edition” to launch the Burp Suite

#### Prepping Up Burp Suite

Add the following rule in the “Intercept Server Responses” under the Burp Proxy “Options”, to enable Burp Proxy to also intercept webserver responses with HTTP Status Code 302. Don’t forget to “Save options” as shown below to your Desktop, so that you don’t have to repeat this procedure. The next time you launch the Burp Suite use the “Load options” and select the file you saved on the desktop.

|  |  |
| --- | --- |
| Graphical user interface, text  Description automatically generated | Graphical user interface, text, application  Description automatically generated |

Click on “Proxy” tab 🡪 “Intercept” tab. Click on the button “Intercept is on” to toggle it to “Intercept is off”. With this setting Burp Suite will not be intercepting requests and responses between the Kali Linux Web Browser and a webserver. With “Intercept is off” Burp Suite will be in listener mode, where it will just listen and record all the requests and responses made between the Kali Linux Web Browser and a webserver

|  |  |
| --- | --- |
| Graphical user interface, text, application, email  Description automatically generated | Graphical user interface, text, application, email  Description automatically generated |

Right click on “Access the lab” and select “Open Link in New Tab”. This would allow you to come back to this tab in case you want to refer to the “Solution” or “Community Solutions” for this particular Lab.

Graphical user interface, text, email, website

Description automatically generated

Add this website to Burp Suite scope. **Make sure you are adding the right website into the scope, by verifying the address in the** **Kali Linux Web Browser’s address bar**.

Graphical user interface, text, application, chat or text message

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Click on “HTTP history” tab, if you notice any records listed in the top pane, right click on the top row record, and click “Clear history”. This would make “HTTP history” tab clear with no previously recorded requests and responses between the Kali Linux Web Browser and a webserver.

Graphical user interface, text, application

Description automatically generated

Click “Yes”

|  |  |
| --- | --- |
| Graphical user interface, text, application  Description automatically generated | Graphical user interface, text, application, email  Description automatically generated |

Click “My account”

Graphical user interface, text, application, website

Description automatically generated

Enter Username: wiener and Password: peter

Graphical user interface, text, application

Description automatically generated

Click on “My account” again

Graphical user interface, text, application

Description automatically generated

You will notice in your Kali Linux Web Browser’s address bar: /my-account?id=wiener

Graphical user interface, text, application, website

Description automatically generated

This is also observed in the Burp Proxy’s HTTP history

Graphical user interface, text, application, email

Description automatically generated

The idea is to change “id” parameter to carlos and see whether carlos’s API Key is revealed. Right click on the Request pane and select “Send to Repeater”.

Graphical user interface, text, application, chat or text message

Description automatically generated

Edit id=wiener to id=carlos and click “Send”

Graphical user interface, text, application, email

Description automatically generated

In the “Response” pane below, click “Render” tab, and you will notice that carlos’s account details are listed along with his API Key.

Graphical user interface, text, application, email

Description automatically generated

In the “Response” pane below, click “Pretty” tab, scroll down until you find Your API Key is:, copy the API Key.

Graphical user interface, text, application, email

Description automatically generated

Go back to the Kali Linux Web Browser and click on the “Submit Solution” button on the top and paste carlos’s API key as shown below, and click “OK”.

Graphical user interface, text

Description automatically generated

You should see a Congratulatory message as below.

Graphical user interface, website

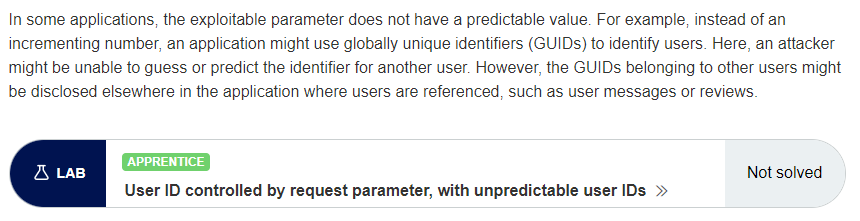
Description automatically generated

# Homework

**Please provide 5 ~ 10 screenshots as evidence of completion for each of the tasks listed below. You may use this document to attach your screenshots and submit it to POLITEMall by Sunday 13th Nov 23:59.**

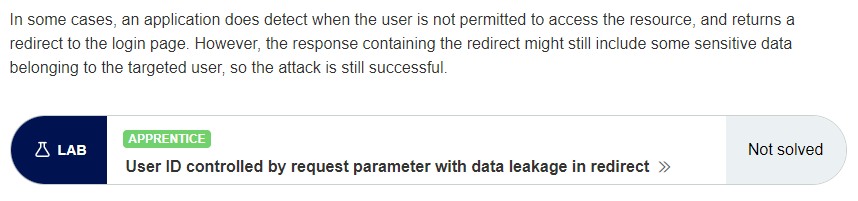
## Horizontal privilege escalation

### **User ID controlled by request parameter, with unpredictable user IDs**



URL: <https://portswigger.net/web-security/access-control/lab-user-id-controlled-by-request-parameter-with-unpredictable-user-ids>

### **User ID controlled by request parameter with data leakage in redirect**



URL: <https://portswigger.net/web-security/access-control/lab-user-id-controlled-by-request-parameter-with-data-leakage-in-redirect>

## Insecure Direct Object References (IDOR)

Graphical user interface, text, application

Description automatically generated

URL: <https://portswigger.net/web-security/access-control/lab-insecure-direct-object-references>

## Access control vulnerabilities in multi-step processes

Graphical user interface, text, application, email

Description automatically generated

URL: <https://portswigger.net/web-security/access-control/lab-multi-step-process-with-no-access-control-on-one-step>

## Referer-based access control

Graphical user interface, text, email

Description automatically generated

URL: <https://portswigger.net/web-security/access-control/lab-referer-based-access-control>

## Directory traversal

URL: <https://portswigger.net/web-security/file-path-traversal>

Attempt any 4 labs under this category.

