

## **Module 10 Assignment\_2**

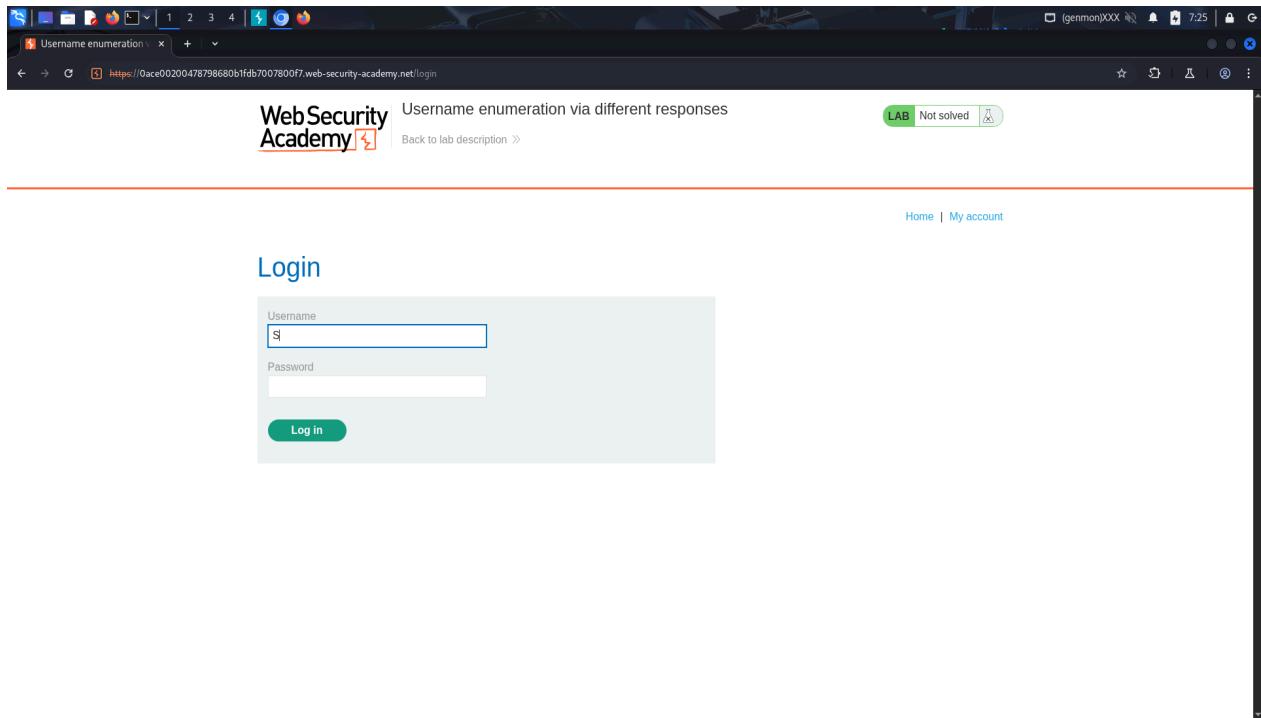
### **Topic: Web Security Lab Solutions: PortSwigger Platform**

#### **Lab 1:Username enumeration via different responses**

This report describes the analysis and exploitation of a web authentication vulnerability where different server responses can be used to enumerate valid usernames. The lab is part of the PortSwigger Web Security Academy's training on password-based authentication flaws.

#### **Steps to Solve the Lab:**

First I had ran the URL in BurpSuite and the log in page had came. Then I tried to log in the website in different username and password.



Then the step by step screenshots I had done to solve this lab

The screenshot shows the Burp Suite interface with the following details:

- Terminal Emulator:** A black box highlights the terminal window where "Sniper attack" is selected.
- Target:** https://0ace00200478798860bfdb7007800f7.web-security-academy.net
- Payloads:** A list of payloads is shown, including "carles", "root", "admin", "test", "guest", "info", "adm", "mysql", and "user".
- Payload processing:** Rules can be defined for payload processing.
- Payload encoding:** URL-encoding options are available.

The terminal session shows the following command history:

```
1 POST /login HTTP/2
2 Host: 0ace00200478798860bfdb7007800f7.web-security-academy.net
3 Cookie: session=0ydlvrfrfSSYUfexVxLw0WnTbNutm
4 Content-Type: application/x-www-form-urlencoded
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Not/A/Brand";v="99", "Chromium";v="136"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Linux"
9 Accept-Language: en-US,en;q=0.9
10 Upgrade-Insecure-Requests: 1
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36
12 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
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-User: ?0
15 Sec-Fetch-Dest: document
16 Referer: https://0ace00200478798860bfdb7007800f7.web-security-academy.net/login
17 Content-Type: application/x-www-form-urlencoded
18 Priority: uod, i
19
20
21
22
23 username=test&password=test
```

## The correct username found.

Burp Suite Community Edition v2025.3.4 - Temporary Project

2. Intruder attack of https://Oace00200478798680b1fdb7007800f7.web-security-academy.net

Attack Save

Results Positions

Capture filter: Capturing all items

View filter: Showing all items

Request Payload Status code Response received Error Timeout Length Comment

|  |   |  |  |  |  |  |  |
|--|---|--|--|--|--|--|--|
| 1 POST /login HTTP/1.1   | Host: Oace00200478798680b1fdb7007800f7.web-security-academy.net |  |  |  |  |  |  |
| 2 Host: Oace00200478798680b1fdb7007800f7.web-security-academy.net  |   |  |  |  |  |  |  |
| 3 Cookie: session=dXlrrFe5YUfeVklwGVNTbJuUmln  |   |  |  |  |  |  |  |
| 4 Content-Length: 23   |   |  |  |  |  |  |  |
| 5 Cache-Control: No-Cache  |   |  |  |  |  |  |  |
| 6 Sec-CD-Url: "/"  |   |  |  |  |  |  |  |
| 7 Sec-CD-Url-Mobi: "/"   |   |  |  |  |  |  |  |
| 8 Sec-CD-Url-Plat: "/"   |   |  |  |  |  |  |  |
| 9 Accept-Language: en-US,en;q=0.9  |   |  |  |  |  |  |  |
| 10 Content-Type: application/x-www-form-urlencoded   |   |  |  |  |  |  |  |
| 11 Accept-Encoding: gzip, deflate, br  |   |  |  |  |  |  |  |
| 12 Priority: u=0, i=100  |   |  |  |  |  |  |  |
| 13 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36             |   |  |  |  |  |  |  |
| 14 Accept: */*   |   |  |  |  |  |  |  |
| 15 Sec-Patch-Site: "/"   |   |  |  |  |  |  |  |
| 16 Sec-Patch-Mode: "same-origin"   |   |  |  |  |  |  |  |
| 17 Sec-Patch-User-Agent: "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36" |   |  |  |  |  |  |  |
| 18 Sec-Patch-Dest: document  |   |  |  |  |  |  |  |
| 19 Referer: https://Oace00200478798680b1fdb7007800f7.web-security-academy.net/login  |   |  |  |  |  |  |  |
| 20 Accept-Charset: "ISO-8859-1,utf-8;q=0.7,*;q=0.7"  |   |  |  |  |  |  |  |
| 21 Priority: u=0, i=1  |   |  |  |  |  |  |  |
| 22 Connection: keep-alive  |   |  |  |  |  |  |  |
| 23 username=anheis&password=test   |   |  |  |  |  |  |  |
| 24   |   |  |  |  |  |  |  |

Pretty Raw Hex

Request Payload Status code Response received Error Timeout Length Comment

|  |   |  |  |  |  |  |  |
|--|---|--|--|--|--|--|--|
| 1 POST /login HTTP/1.1   | Host: Oace00200478798680b1fdb7007800f7.web-security-academy.net |  |  |  |  |  |  |
| 2 Host: Oace00200478798680b1fdb7007800f7.web-security-academy.net  |   |  |  |  |  |  |  |
| 3 Cookie: session=dXlrrFe5YUfeVklwGVNTbJuUmln  |   |  |  |  |  |  |  |
| 4 Content-Length: 23   |   |  |  |  |  |  |  |
| 5 Cache-Control: No-Cache  |   |  |  |  |  |  |  |
| 6 Sec-CD-Url: "/"  |   |  |  |  |  |  |  |
| 7 Sec-CD-Url-Mobi: "/"   |   |  |  |  |  |  |  |
| 8 Sec-CD-Url-Plat: "/"   |   |  |  |  |  |  |  |
| 9 Accept-Language: en-US,en;q=0.9  |   |  |  |  |  |  |  |
| 10 Content-Type: application/x-www-form-urlencoded   |   |  |  |  |  |  |  |
| 11 Accept-Encoding: gzip, deflate, br  |   |  |  |  |  |  |  |
| 12 Priority: u=0, i=100  |   |  |  |  |  |  |  |
| 13 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36             |   |  |  |  |  |  |  |
| 14 Accept: */*   |   |  |  |  |  |  |  |
| 15 Sec-Patch-Site: "/"   |   |  |  |  |  |  |  |
| 16 Sec-Patch-Mode: "same-origin"   |   |  |  |  |  |  |  |
| 17 Sec-Patch-User-Agent: "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36" |   |  |  |  |  |  |  |
| 18 Sec-Patch-Dest: document  |   |  |  |  |  |  |  |
| 19 Referer: https://Oace00200478798680b1fdb7007800f7.web-security-academy.net/login  |   |  |  |  |  |  |  |
| 20 Accept-Charset: "ISO-8859-1,utf-8;q=0.7,*;q=0.7"  |   |  |  |  |  |  |  |
| 21 Priority: u=0, i=1  |   |  |  |  |  |  |  |
| 22 Connection: keep-alive  |   |  |  |  |  |  |  |
| 23 username=anheis&password=test   |   |  |  |  |  |  |  |
| 24   |   |  |  |  |  |  |  |

Pretty Raw Hex

Event log All issues

Memory: 117.8MB Disabled

## Then the password found

Burp Suite Community Edition v2025.3.4 - Temporary Project

4. Intruder attack of https://Oace00200478798680b1fdb7007800f7.web-security-academy.net

Attack Save

Results Positions

Capture filter: Capturing all items

View filter: Showing all items

Request Payload Status code Response received Error Timeout Length Comment

|  |   |  |  |  |  |  |  |
|--|---|--|--|--|--|--|--|
| 1 POST /login HTTP/1.1   | Host: Oace00200478798680b1fdb7007800f7.web-security-academy.net |  |  |  |  |  |  |
| 2 Host: Oace00200478798680b1fdb7007800f7.web-security-academy.net  |   |  |  |  |  |  |  |
| 3 Cookie: session=dXlrrFe5YUfeVklwGVNTbJuUmln  |   |  |  |  |  |  |  |
| 4 Content-Length: 23   |   |  |  |  |  |  |  |
| 5 Cache-Control: No-Cache  |   |  |  |  |  |  |  |
| 6 Sec-CD-Url: "/"  |   |  |  |  |  |  |  |
| 7 Sec-CD-Url-Mobi: "/"   |   |  |  |  |  |  |  |
| 8 Sec-CD-Url-Plat: "/"   |   |  |  |  |  |  |  |
| 9 Accept-Language: en-US,en;q=0.9  |   |  |  |  |  |  |  |
| 10 Content-Type: application/x-www-form-urlencoded   |   |  |  |  |  |  |  |
| 11 Accept-Encoding: gzip, deflate, br  |   |  |  |  |  |  |  |
| 12 Priority: u=0, i=100  |   |  |  |  |  |  |  |
| 13 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36             |   |  |  |  |  |  |  |
| 14 Accept: */*   |   |  |  |  |  |  |  |
| 15 Sec-Patch-Site: "/"   |   |  |  |  |  |  |  |
| 16 Sec-Patch-Mode: "same-origin"   |   |  |  |  |  |  |  |
| 17 Sec-Patch-User-Agent: "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36" |   |  |  |  |  |  |  |
| 18 Sec-Patch-Dest: document  |   |  |  |  |  |  |  |
| 19 Referer: https://Oace00200478798680b1fdb7007800f7.web-security-academy.net/login  |   |  |  |  |  |  |  |
| 20 Accept-Charset: "ISO-8859-1,utf-8;q=0.7,*;q=0.7"  |   |  |  |  |  |  |  |
| 21 Priority: u=0, i=1  |   |  |  |  |  |  |  |
| 22 Connection: keep-alive  |   |  |  |  |  |  |  |
| 23 username=anheis&password=000000   |   |  |  |  |  |  |  |
| 24   |   |  |  |  |  |  |  |

Pretty Raw Hex

Request Payload Status code Response received Error Timeout Length Comment

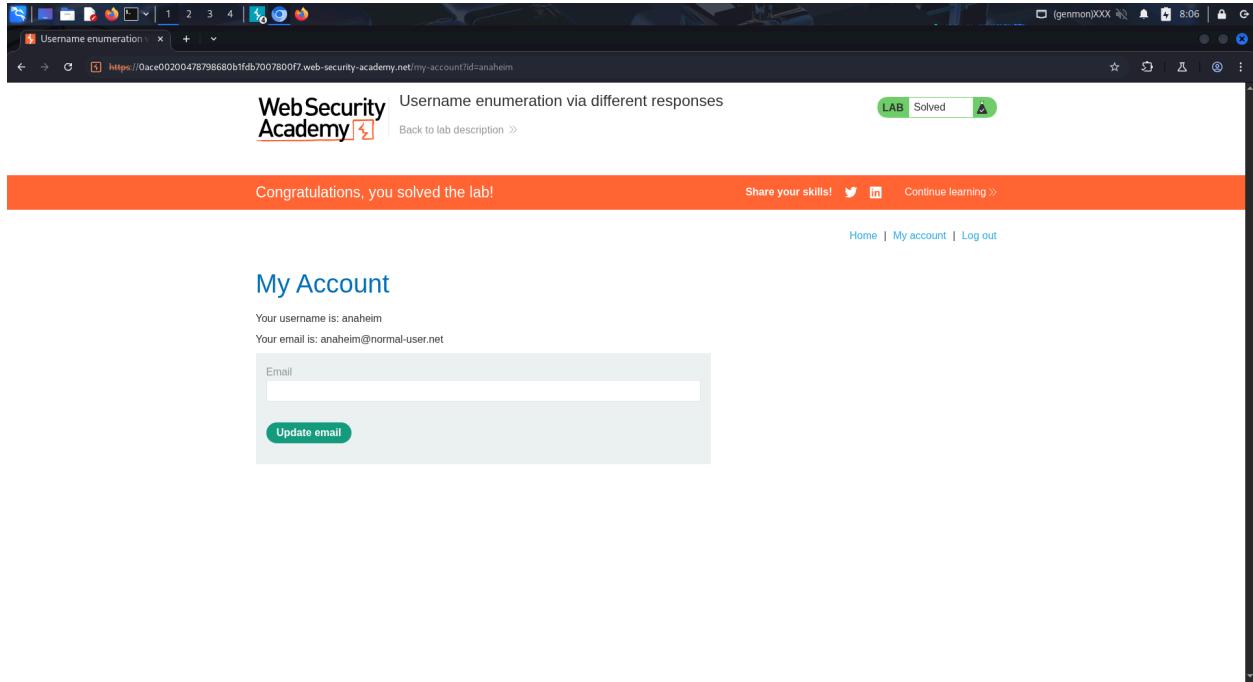
|  |   |  |  |  |  |  |  |
|--|---|--|--|--|--|--|--|
| 1 POST /login HTTP/1.1   | Host: Oace00200478798680b1fdb7007800f7.web-security-academy.net |  |  |  |  |  |  |
| 2 Host: Oace00200478798680b1fdb7007800f7.web-security-academy.net  |   |  |  |  |  |  |  |
| 3 Cookie: session=dXlrrFe5YUfeVklwGVNTbJuUmln  |   |  |  |  |  |  |  |
| 4 Content-Length: 23   |   |  |  |  |  |  |  |
| 5 Cache-Control: No-Cache  |   |  |  |  |  |  |  |
| 6 Sec-CD-Url: "/"  |   |  |  |  |  |  |  |
| 7 Sec-CD-Url-Mobi: "/"   |   |  |  |  |  |  |  |
| 8 Sec-CD-Url-Plat: "/"   |   |  |  |  |  |  |  |
| 9 Accept-Language: en-US,en;q=0.9  |   |  |  |  |  |  |  |
| 10 Content-Type: application/x-www-form-urlencoded   |   |  |  |  |  |  |  |
| 11 Accept-Encoding: gzip, deflate, br  |   |  |  |  |  |  |  |
| 12 Priority: u=0, i=100  |   |  |  |  |  |  |  |
| 13 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36             |   |  |  |  |  |  |  |
| 14 Accept: */*   |   |  |  |  |  |  |  |
| 15 Sec-Patch-Site: "/"   |   |  |  |  |  |  |  |
| 16 Sec-Patch-Mode: "same-origin"   |   |  |  |  |  |  |  |
| 17 Sec-Patch-User-Agent: "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36" |   |  |  |  |  |  |  |
| 18 Sec-Patch-Dest: document  |   |  |  |  |  |  |  |
| 19 Referer: https://Oace00200478798680b1fdb7007800f7.web-security-academy.net/login  |   |  |  |  |  |  |  |
| 20 Accept-Charset: "ISO-8859-1,utf-8;q=0.7,*;q=0.7"  |   |  |  |  |  |  |  |
| 21 Priority: u=0, i=1  |   |  |  |  |  |  |  |
| 22 Connection: keep-alive  |   |  |  |  |  |  |  |
| 23 username=anheis&password=000000   |   |  |  |  |  |  |  |
| 24   |   |  |  |  |  |  |  |

Pretty Raw Hex

Event log All issues

Memory: 135.8MB Disabled

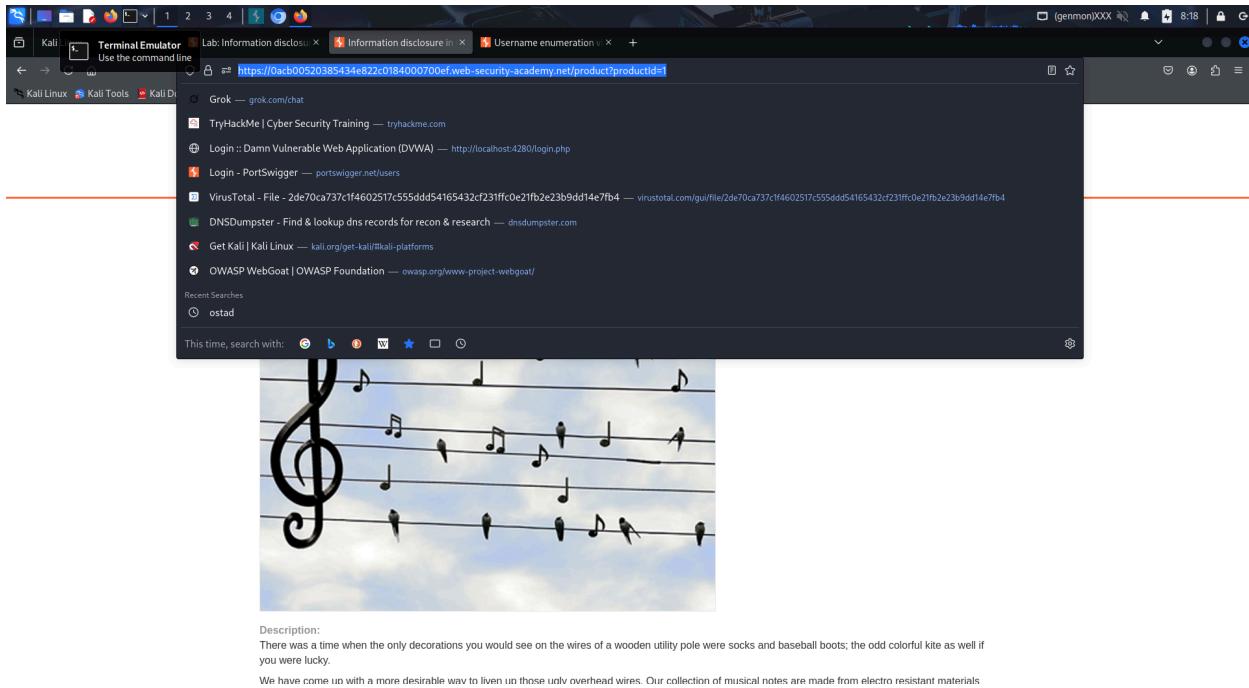
Finally successfully log in the account



## Lab 2: Information disclosure in error messages

This report discusses a vulnerability where sensitive internal information is disclosed via detailed error messages. The lab provided by PortSwigger demonstrates how such messages can reveal file paths, stack traces, or system-level data, which could assist attackers in further exploiting the system.

First I had ran the product page url in BurpSuite.



Description:

There was a time when the only decorations you would see on the wires of a wooden utility pole were socks and baseball bats; the odd colorful kite as well if you were lucky.

We have come up with a more desirable way to liven up those ugly overhead wires. Our collection of musical notes are made from electro resistant materials

Then I follow the steps to solve the lab.

| #  | Host                            | Method | URL  | Params | Edited | Status code | Length | MIME type | Extension | Title                          | Notes | TLS          | IP                    | Cookies           | Time              | Listener port | Start response by |
|----|---------------------------------|--------|--|--------|--------|-------------|--------|-----------|-----------|--------------------------------|-------|--------------|-----------------------|-------------------|-------------------|---------------|-------------------|
| 1  | https://0acb00520385434e8220... | GET    | /product?productId=1                         |        | ✓      | 200         | 4390   | HTML      |           | Information disclosure in e... | ✓     | 79.125.84.16 | session=A5XrutzxUv... | 08:19:36 3 Aug... | 8080              | 375           |                   |
| 3  | https://0acb00520385434e8220... | GET    | /resources/labHeader/js/labHeaderSolution.js |        |        | 200         | 1333   | script    | js        |                                |       | ✓            | 79.125.84.16          |                   | 08:19:38 3 Aug... | 8080          | 343               |
| 4  | https://0acb00520385434e8220... | GET    | /resources/labHeader/js/labHeader.js         |        |        | 200         | 670    | script    | js        |                                |       | ✓            | 79.125.84.16          |                   | 08:19:38 3 Aug... | 8080          | 340               |
| 8  | https://0acb00520385434e8220... | GET    | /resources/labHeader/images/ops/lab-not...   |        |        | 200         | 942    | XML       | svg       |                                |       | ✓            | 79.125.84.16          |                   | 08:19:38 3 Aug... | 8080          | 1593              |
| 9  | https://0acb00520385434e8220... | GET    | /resources/labHeader/images/logoAcadem...    |        |        | 200         | 8852   | XML       | svg       |                                |       | ✓            | 79.125.84.16          |                   | 08:19:38 3 Aug... | 8080          | 1566              |
| 10 | https://0acb00520385434e8220... | GET    | /academyLabHeader                            |        |        | 101         | 147    |           |           |                                |       | ✓            | 79.125.84.16          |                   | 08:19:38 3 Aug... | 8080          | 311               |

Firefox ESR - Browse the World Wide Web

Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Target: https://0acb00520385434e822c0184000700ef.web-security-academy.net

Request Response Inspector

```

1 GET /product?productId= HTTP/2
2 Host: 0acb00520385434e822c0184000700ef.web-security-academy.net
3 Sec-CH-Usr-ID: "Not_Agent";v="99", "Chromium";v="136"
4 Sec-CH-Platform: "Windows"
5 Sec-CH-Platform-Version: "0"
6 Accept-Language: en-US,en;q=0.9
7 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0
8 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: none
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Accept-Encoding: gzip, deflate, br
15 Priority: u0, 1
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40 Apache Struts 2 2.3.31

```

Selected text: Apache Struts 2 2.3.31

Request attributes: 2

Request query parameters: 1

Request body parameters: 0

Request cookies: 0

Request headers: 17

Response headers: 1

Custom actions: 0

Notes: 0

Inspector: Apache Struts 2 2.3.31

Done 0 highlights

Event log All issues

Memory: 126.5MB Disabled

Finally I had solved the lab. The error messages is shown because of string.

Kali Linux - Burp Suite Community Edition V2025.3.4 - Temporary Project

in disclosure in | Username enumeration x +

https://0acb00520385434e822c0184000700ef.web-security-academy.net/product?productId=1

Back to lab description >>

WebSecurity Academy

Information disclosure in error messages

LAB Solved

Congratulations, you solved the lab!

Share your skills! Twitter LinkedIn Continue learning >>

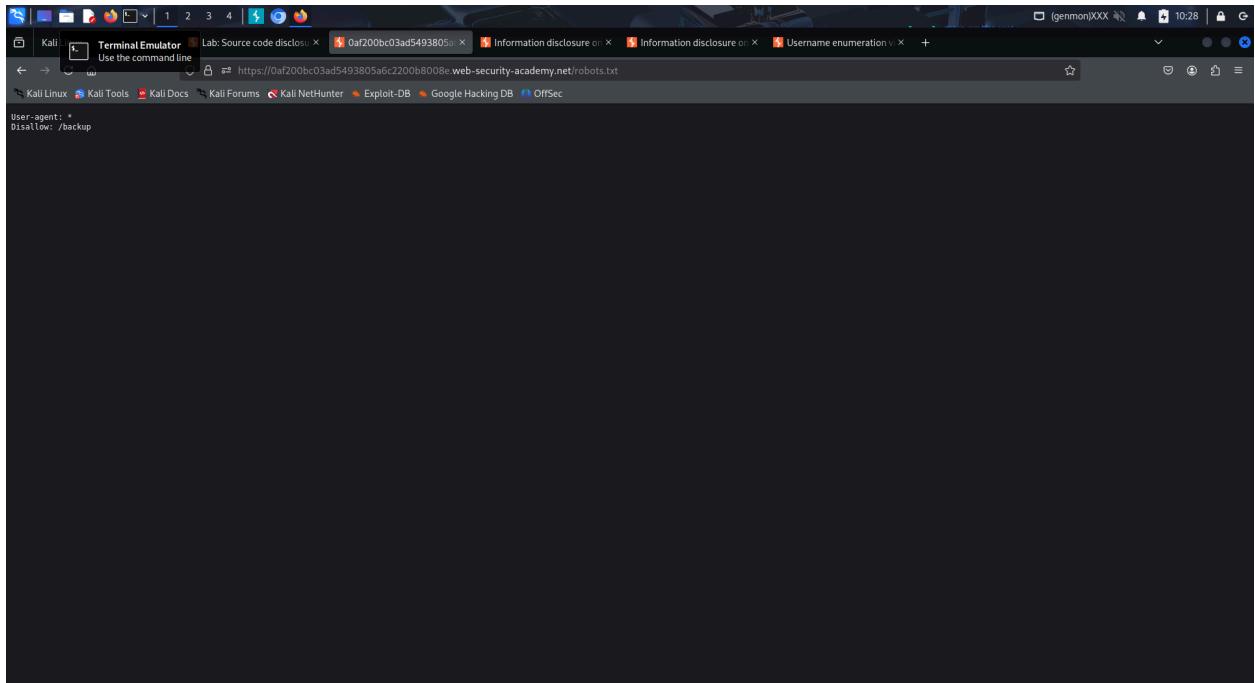


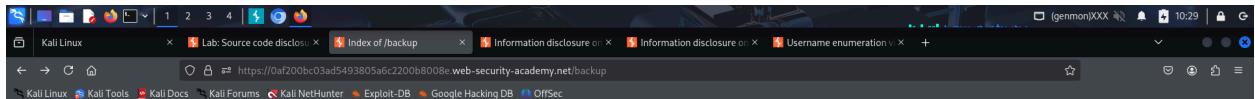
Description:  
There was a time when the only decorations you would see on the wires of a wooden utility pole were socks and baseball bats; the odd colorful kite as well if

## Lab 3: Source code disclosure via backup files

This lab leaks its source code via backup files in a hidden directory. To solve the lab, identify and submit the database password, which is hard-coded in the leaked source code.

Step by step solution with screenshots:





## Index of /backup

| Name                                     | Size  |
|--|-------|
| <a href="#">ProductTemplate.java.hak</a> | 1647B |

A screenshot of a Firefox browser window. The address bar shows the URL: https://0af200bc03ad5493805a6c2200b8008e.web-security-academy.net/backup/ProductTemplate.java.bak. The page content displays the source code of the ProductTemplate.java.bak file:

```
import java.io.ObjectInputStream;
import java.sql.Connection;
import java.sql.DriverManager;
import java.sql.SQLException;
import java.sql.Statement;

public class ProductTemplate implements Serializable
{
    static final long serialVersionUID = 1L;

    private final String id;
    private transient Product product;

    public ProductTemplate(String id)
    {
        this.id = id;
    }

    private void readObject(ObjectInputStream inputStream) throws IOException, ClassNotFoundException
    {
        inputStream.defaultReadObject();

        ConnectionBuilder connectionBuilder = ConnectionBuilder.from(
                "org.postgresql.Driver",
                "postgresql",
                "localhost",
                5432,
                "postgres",
                "postgres",
                "1234567890q1234567890");
        connectionBuilder.withAutoCommit();
    }

    Connection connect = connectionBuilder.connect(30);
    String sql = String.format("SELECT * FROM products WHERE id = '%s' LIMIT 1", id);
    Statement statement = connect.createStatement();
    ResultSet resultSet = statement.executeQuery(sql);
    if (!resultSet.next())
    {
        return;
    }
    product = Product.from(resultSet);
}
catch (SQLException e)
{
    throw new IOException(e);
}

public String getId()
{
    return id;
}

public Product getProduct()
{
    return product;
}
```

Finally solve the lab.

A screenshot of a web browser window showing a completed lab on WebSecurityAcademy. The title of the page is "Source code disclosure via backup files" and the status is "Solved". Below the title, there is a message saying "Congratulations, you solved the lab!" and options to "Share your skills!" and "Continue learning". The main content features a section titled "WE LIKE TO SHOP" with four items: "Fur Babies" (two babies in bunny hats), "Beat the Vacation Traffic" (a pink van on a beach), "The Splash" (a person splashing water), and "WTF? - The adult party game" (a box with batteries). Each item has a star rating, price, and a "View details" button. Below this are four smaller thumbnail images.

## Lab 4: Information disclosure on debug page

This lab contains a debug page that discloses sensitive information about the application.

## **Step by step solution and screenshots:**

Kali Linux Terminal Emulator Information disclosure Information disclosure Source code disclosure 0fa200bc03ad549380 Information disclosure Information disclosure Username enumeration

https://0aad00f503a89aa80c71c94004e003e.web-security-academy.net

WebSecurity Academy Information disclosure on debug page LAB Not solved Home

WE LIKE TO SHOP

| Product                        | Rating  | Price   |
|--------------------------------|---------|---------|
| BBQ Suitcase                   | ★ ★ ★ ★ | \$73.48 |
| Fur Babies                     | ★★★★★   | \$36.01 |
| Conversation Controlling Lemon | ★ ★ ★ ★ | \$6.86  |
| Caution Sign                   | ★★★★★   | \$32.31 |

View details View details View details View details

Inspector Style Editor Performance Memory

```

section {
    display: flex;
    justify-content: space-between;
    align-items: center;
}

```

Kali Linux Lab: Information portswigger.net PHP 7.4.3-4ubuntu1 Information disclosure Source code disclosure 0fa200bc03ad549380 Information disclosure Information disclosure Username enum

https://0aad00f503a89aa80c71c94004e003e.web-security-academy.net/cgi-bin/phpinfo.php

Variable Value

|                     |                      |
|---------------------|----------------------|
| REQUEST_METHOD      | GET                  |
| PWD                 | /home/carlos/cgi-bin |
| HTTP_SEC_FETCH_SITE | none                 |
| SERVER_PORT         | 443                  |
| SCRIPT_NAME         | /cgi-bin/phpinfo.php |
| SERVER_NAME         | 10.0.4.200           |

PHP Variables

|   |  |
|---|--|
| \$_COOKIE['session']                        | 3ryQfHKAoXqJN4javxrA1Q5LkyW85  |
| \$_SERVER['GATEWAY_INTERFACE']              | CGI/1.1  |
| \$_SERVER['SUDO_GID']                       | 10000  |
| \$_SERVER['REMOTE_HOST']                    | 10.129.212.224   |
| \$_SERVER['USER']                           | carlos   |
| \$_SERVER['HTTP_TE']                        | trailers   |
| \$_SERVER['SECRET_KEY']                     | 1eh7z6005k6nbpvjuvs0hg0h5mus   |
| \$_SERVER['HTTP_SEC_FETCH_USER']            | 71   |
| \$_SERVER['QUERY_STRING']                   | no value   |
| \$_SERVER['HOME']                           | /home/carlos   |
| \$_SERVER['HTTP_USER_AGENT']                | Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0     |
| \$_SERVER['HTTP_UPGRADE_INSECURE_REQUESTS'] | 1  |
| \$_SERVER['HTTP_ACCEPT']                    | text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8            |
| \$_SERVER['SCRIPT_FILENAME']                | /home/carlos/cgi-bin/phpinfo.php   |
| \$_SERVER['HTTP_HOST']                      | 0aad00f503a89aa80c71c94004e003e.web-security-academy.net                   |
| \$_SERVER['SUDO_UID']                       | 10000  |
| \$_SERVER['LOGNAME']                        | carlos   |
| \$_SERVER['SERVER_SOFTWARE']                | PortSwiggerHttpServer/1.0  |
| \$_SERVER['HTTP_SEC_FETCH_MODE']            | navigate   |
| \$_SERVER['TERM']                           | unknown  |
| \$_SERVER['HTTP_COOKIE']                    | session=3ryQfHKAoXqJN4javxrA1Q5LkyW85                                      |
| \$_SERVER['PATH']                           | /usr/local/bin:/usr/local/bin:/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin |
| \$_SERVER['HTTP_ACCEPT_LANGUAGE']           | en-US,en;q=0.5   |
| \$_SERVER['SERVER_PROTOCOL']                | HTTP/1.1   |
| \$_SERVER['HTTP_PRIORITY']                  | u=0,i  |
| \$_SERVER['HTTP_ACCEPT_ENCODING']           | gzip, deflate, br, zstd  |
| \$_SERVER['SUDO_COMMAND']                   | /usr/bin/sh -c /usr/bin/php-cgi  |

Inspector Style Editor Performance Memory

```

body {
    color: #222;
    font-family: sans-serif;
}

```

Finally solve the lab

← → ⌛ 0aad00f503a89aa880c71c94004e003e web-security-academy.net ☆ ⓘ Sign in

**WebSecurity Academy** Information disclosure on debug page

Back to lab description >

LAB Solved 🎉

Congratulations, you solved the lab!

Share your skills! [Twitter](#) [LinkedIn](#) Continue learning >

Home

WE LIKE TO  
**SHOP** 



BBQ Suitcase

▲ ▲ ▲ ▲ ▲



Fur Babies

▲ ▲ ▲ ▲ ▲



Conversation Controlling Lemon

▲ ▲ ▲ ▲ ▲



Caution Sign

▲ ▲ ▲ ▲ ▲