Module 10 Assignment_2

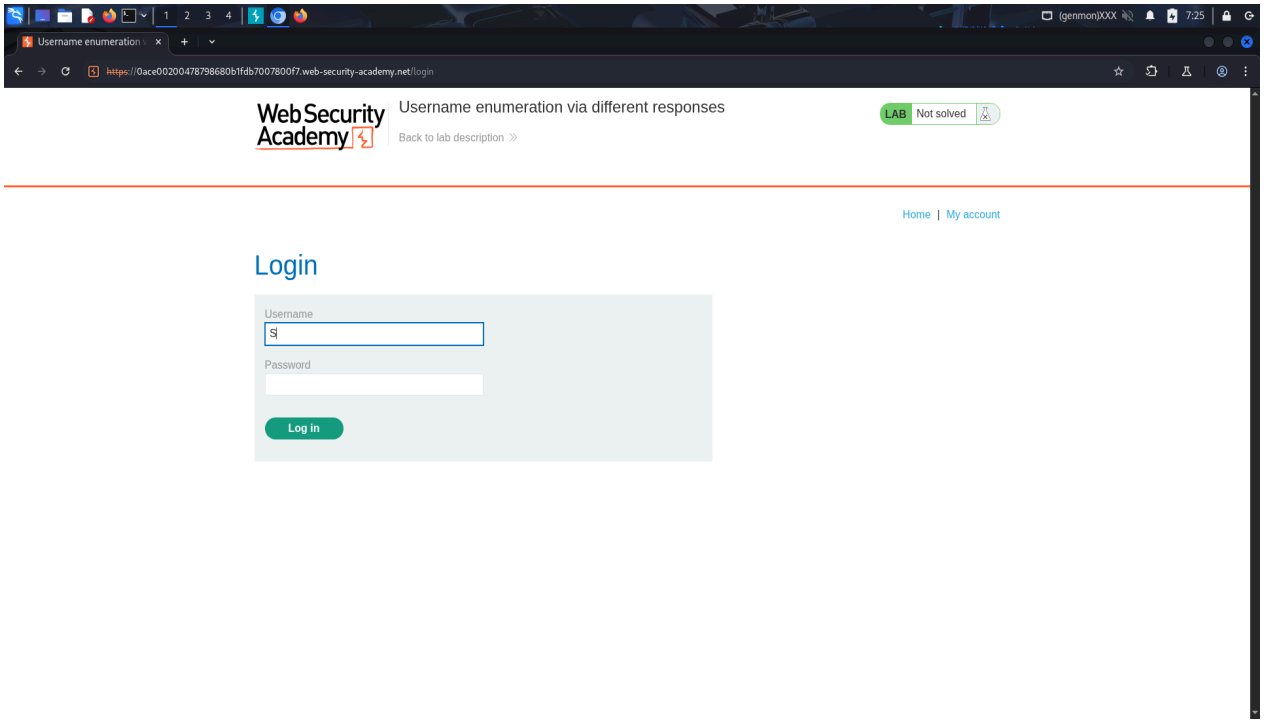
Topic: Web Security Lab Solutions: PortSwigger Platform

Lab 1:Username enumeration via different responses

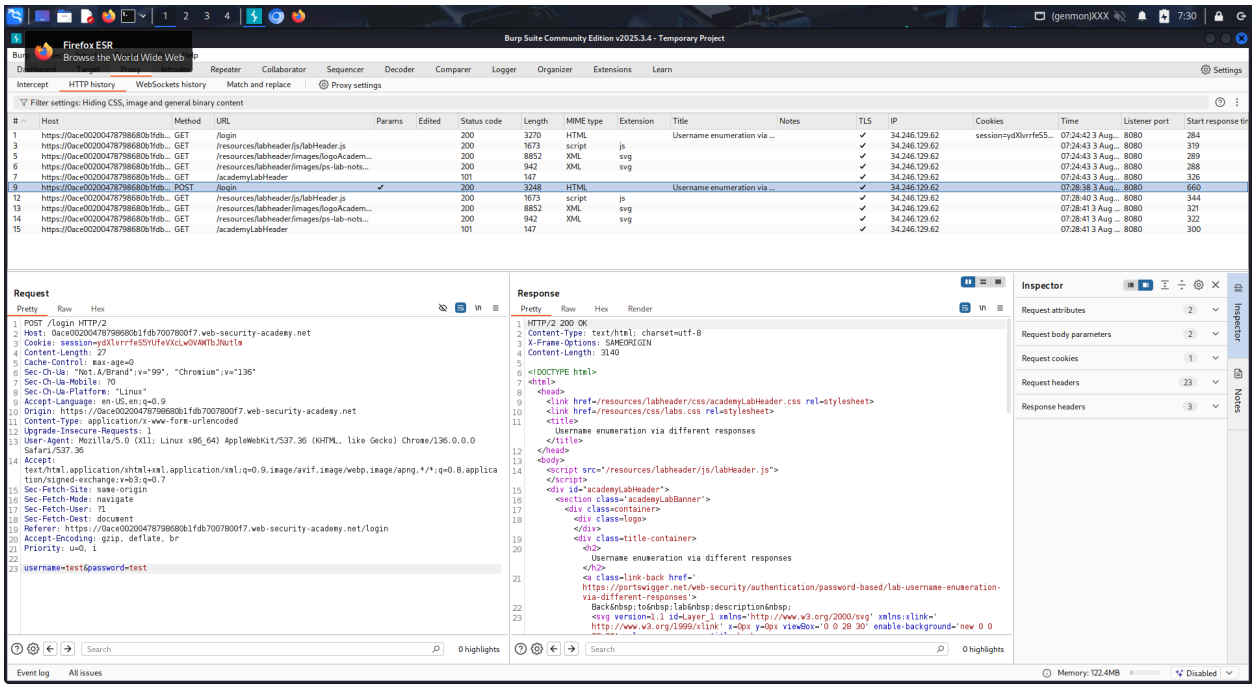
This report describes the analysis and exploitation of a web authentication vulnerability where different server responses can be used to enumerate valid usernames. The lab is part of the PortSwigger Web Security Academy's training on password-based authentication flaws.

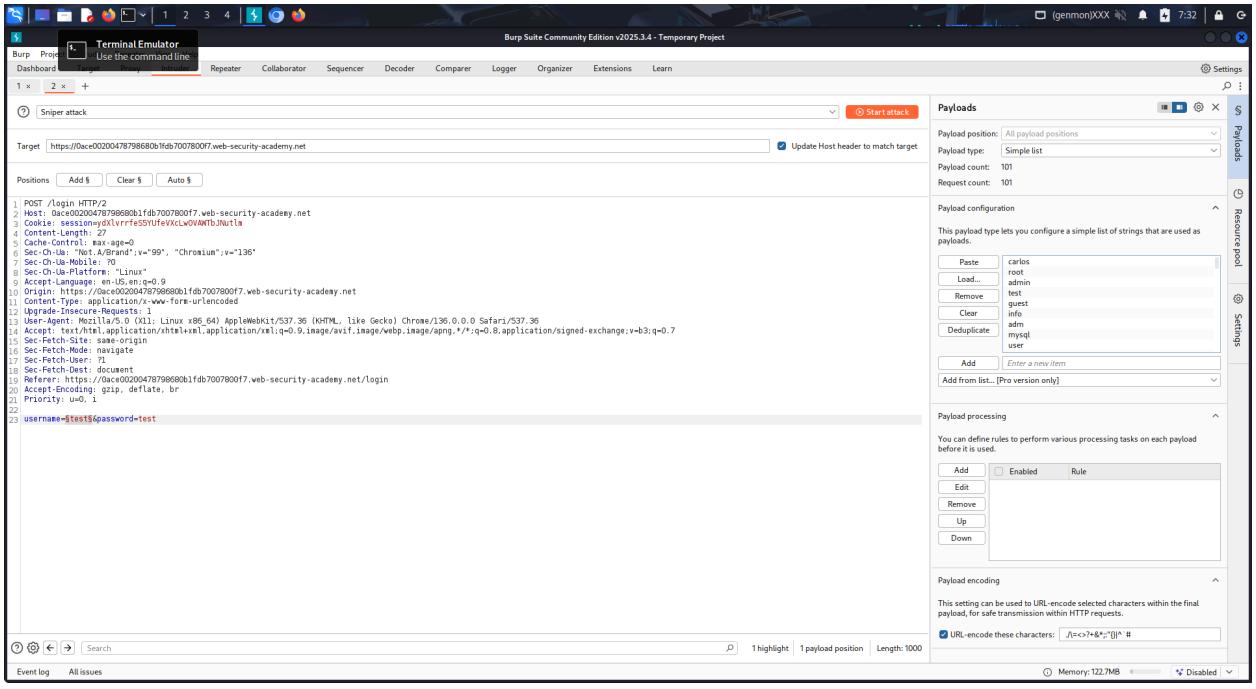
Steps to Solve the Lab:

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.

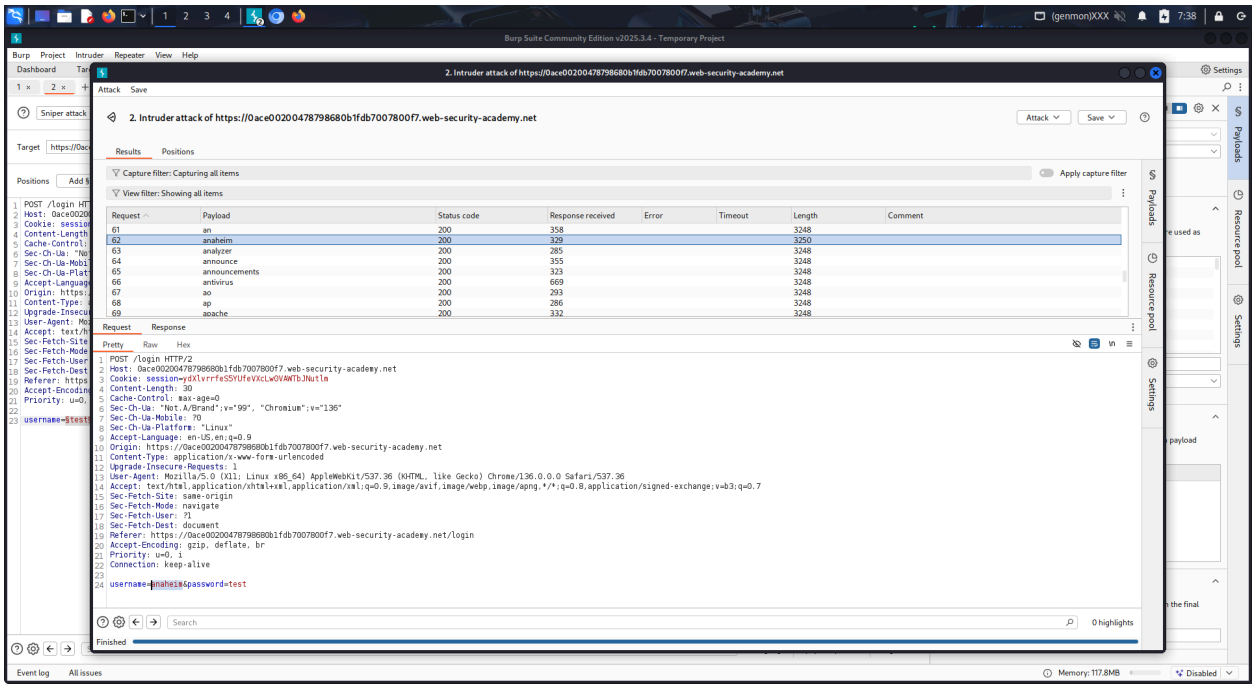


Then the step by step screenshots I had done to solve this lab

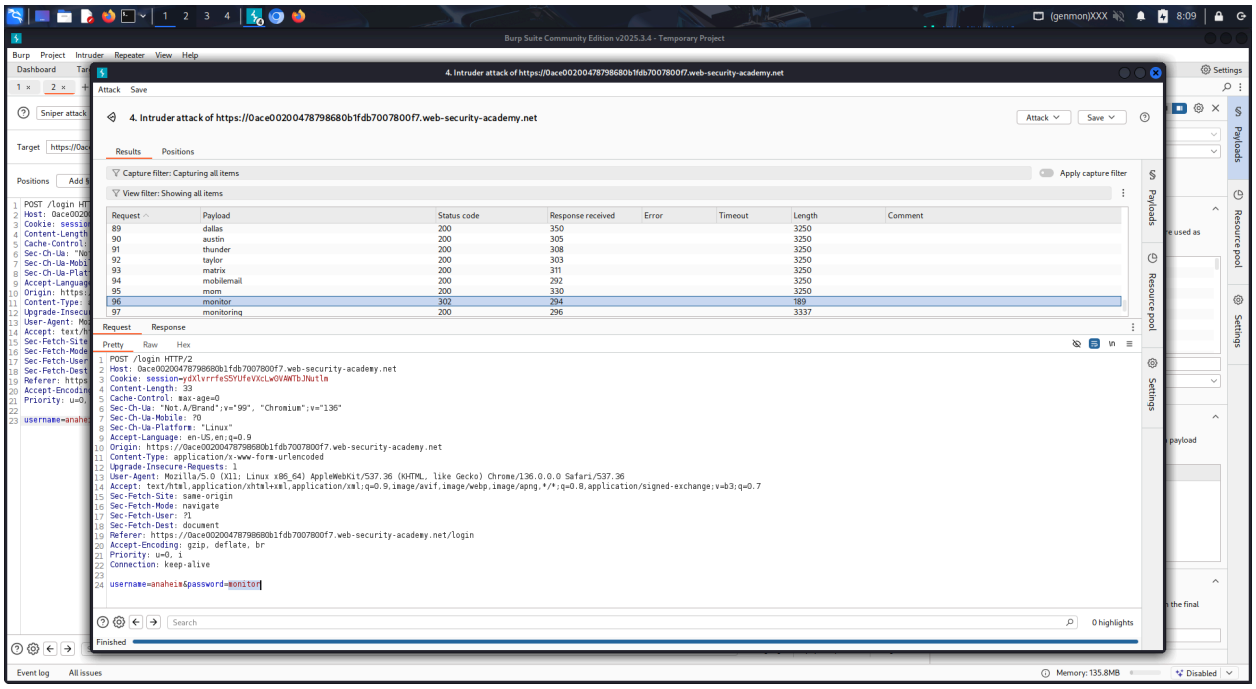

Firefox ESR
Browse the World Wide Web
Burp Suite Community Edition v2025.3.4 - Temporary Project
Request
Response
Inspector


Terminal Emulator
Use the command line
Burp Suite Community Edition v2025.3.4 - Temporary Project
Payloads

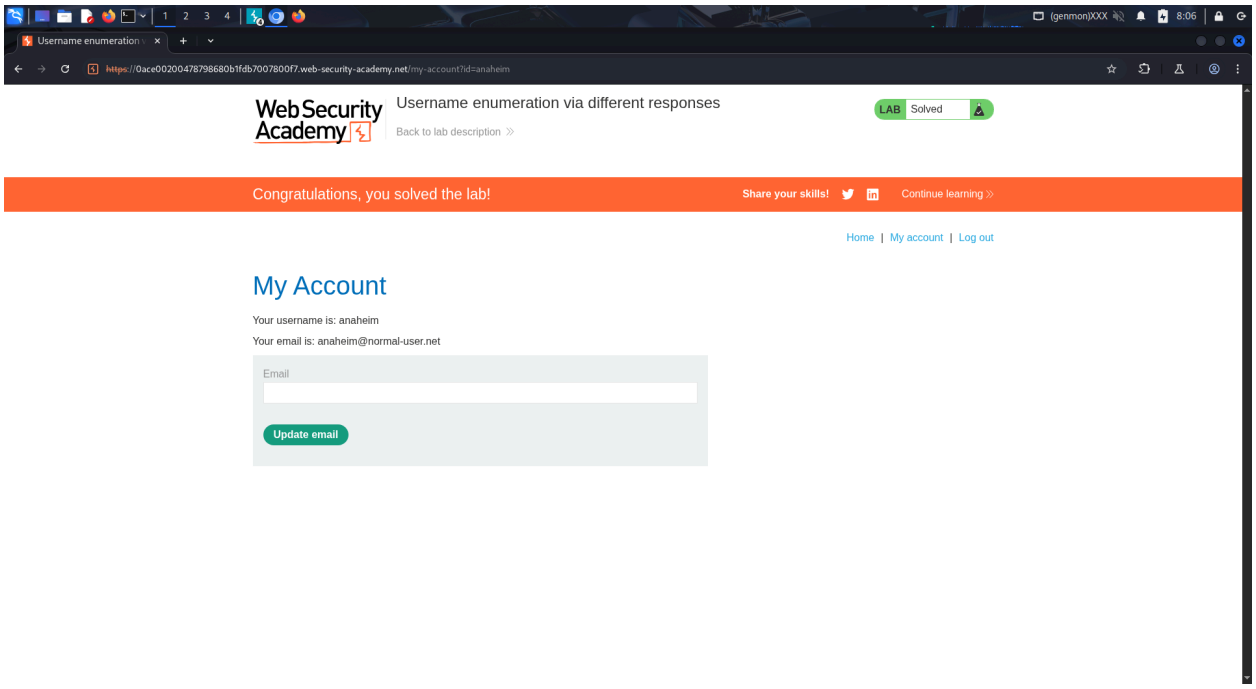
The correct username found.



Then the password found



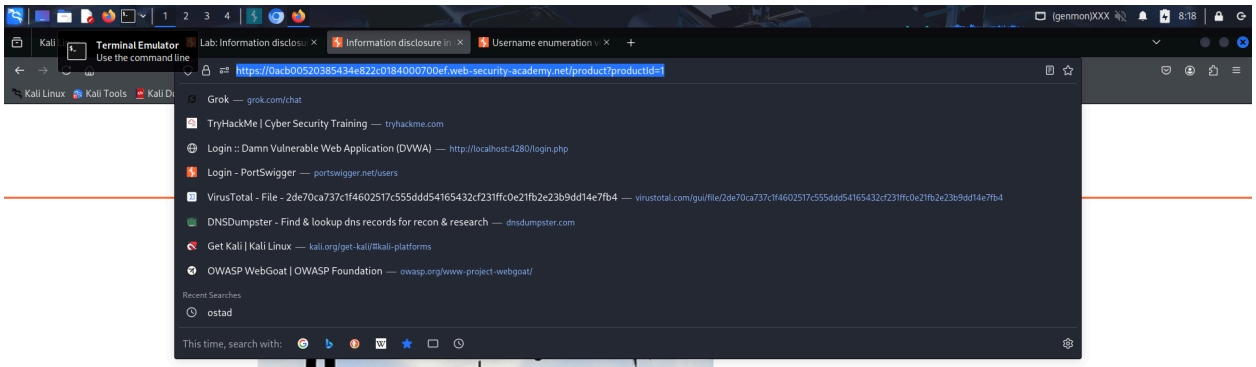
Finally successfully log in the account

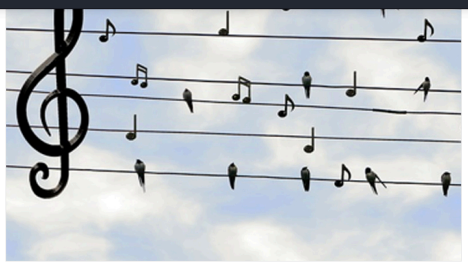


Lab 2: Information disclosure in error messages

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.



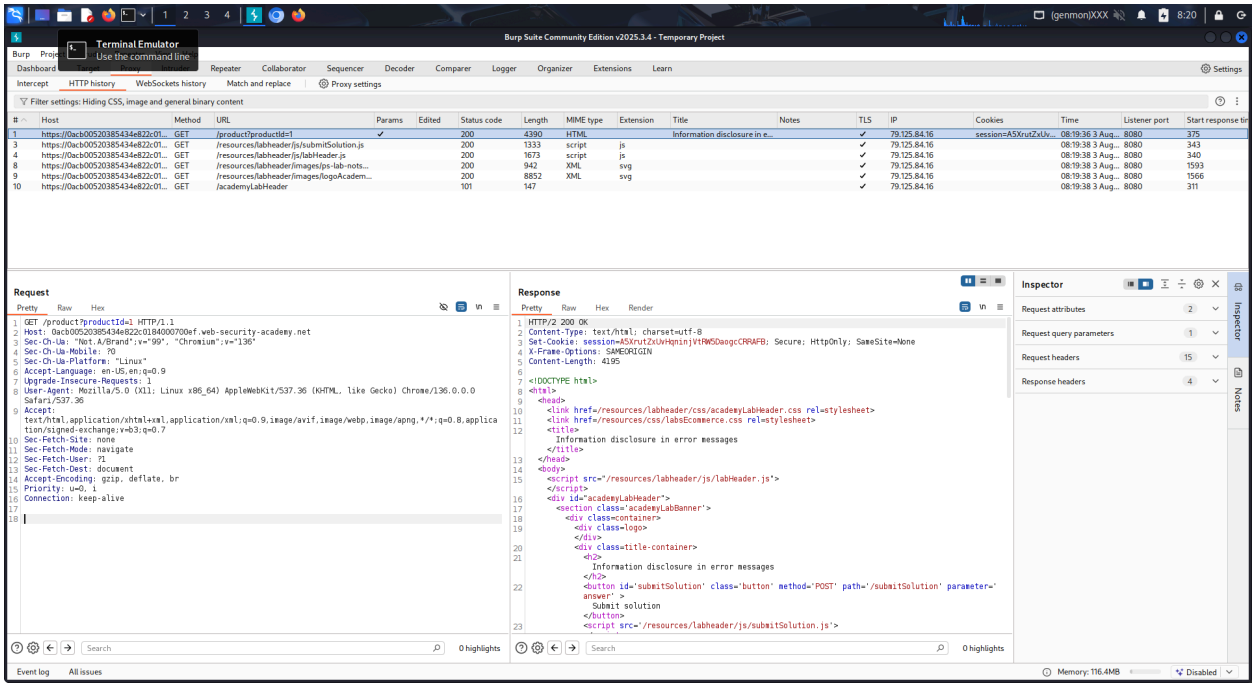


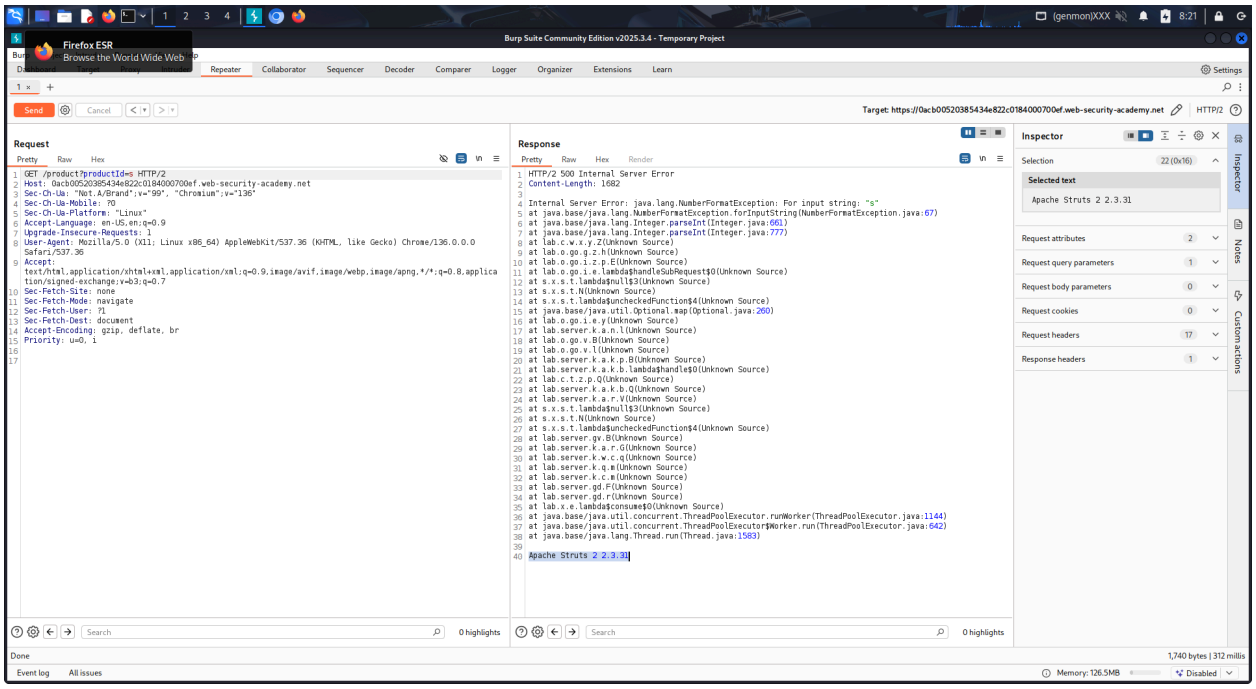
Description:

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

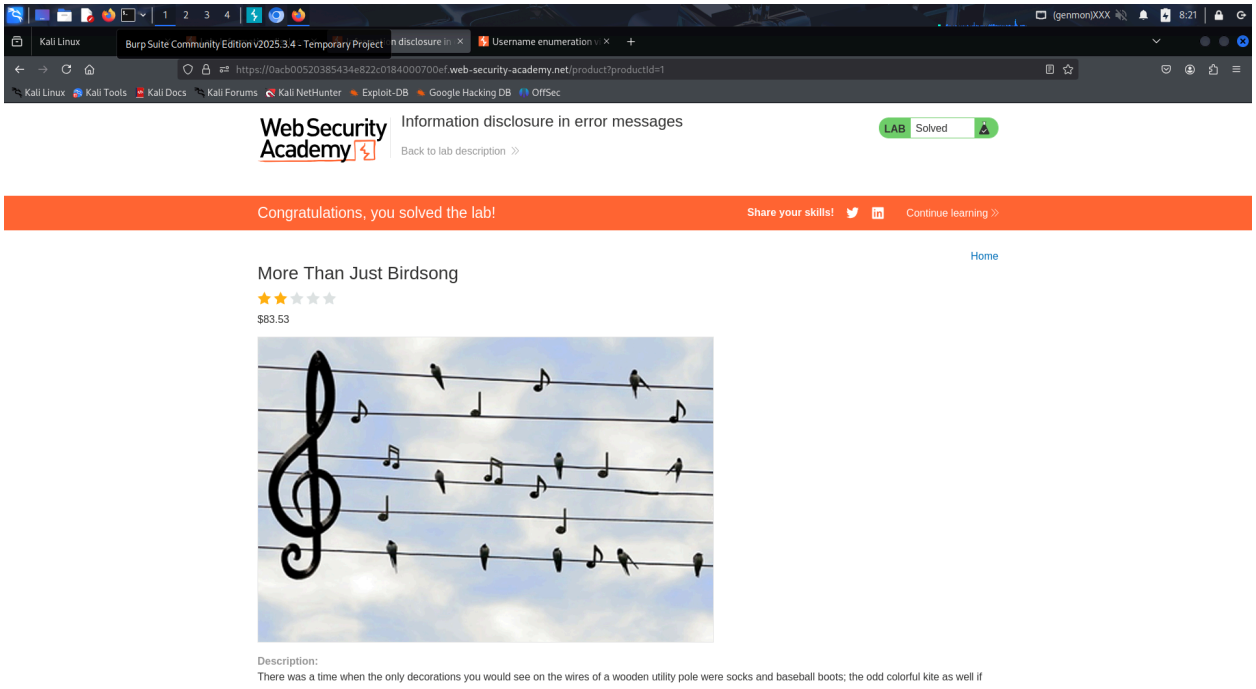
We have come up with a more desirable way to liven up those ugly overhead wires. Our collection of musical notes are made from electro resistant materials

Then I follow the steps to solve the lab.





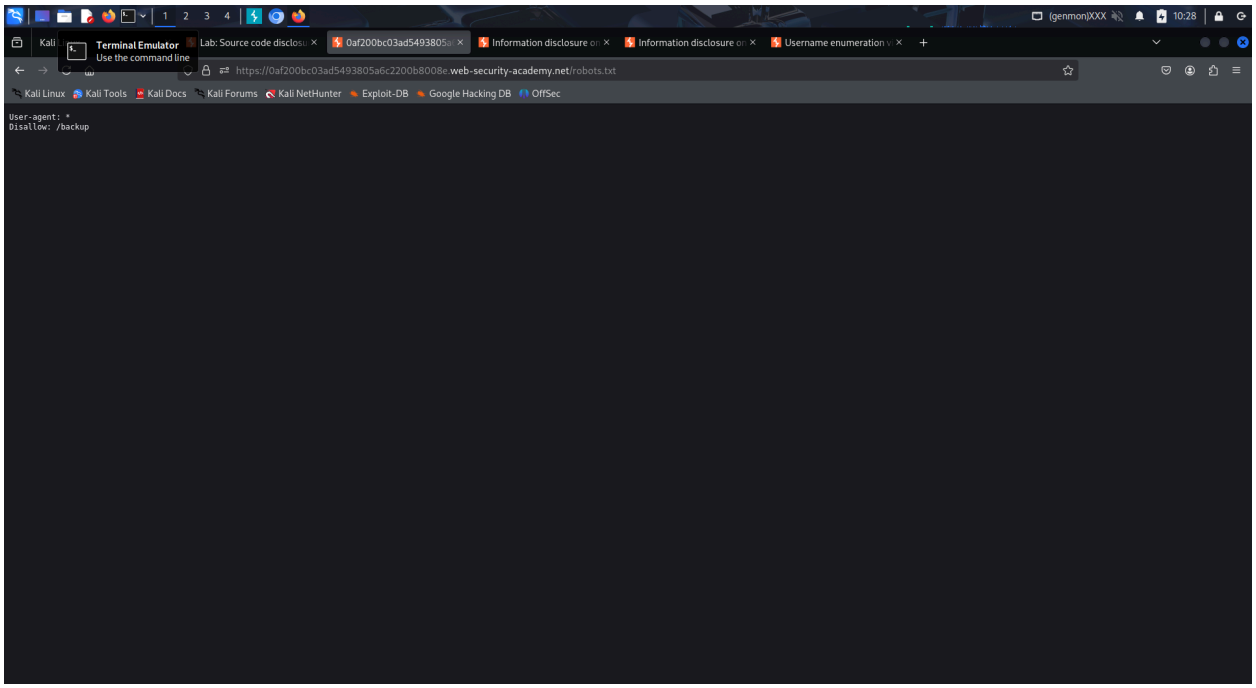
Finally I had solved the lab. The error messages is shown because of string.

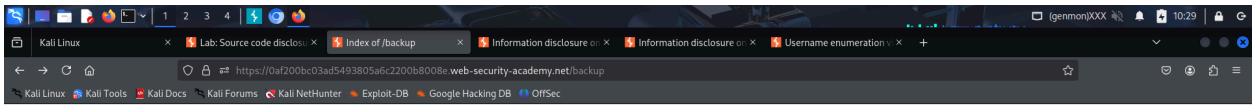


Lab 3: Source code disclosure via backup files

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.

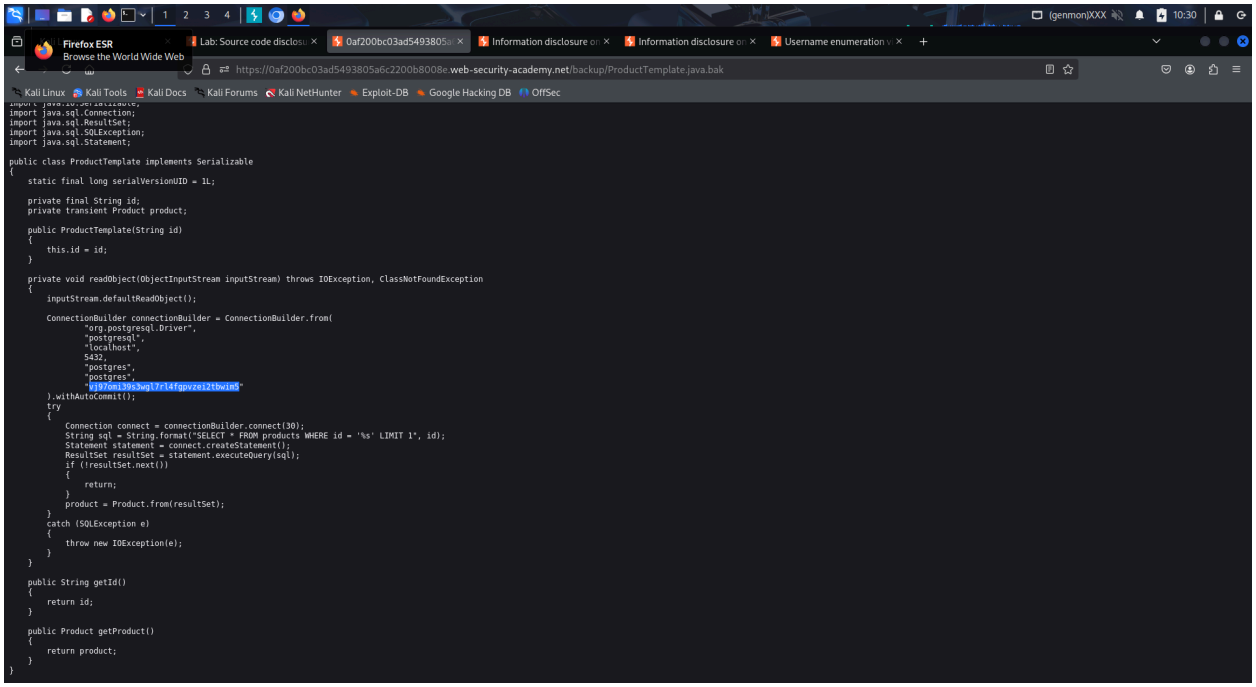
Step by step solution with screenshots:





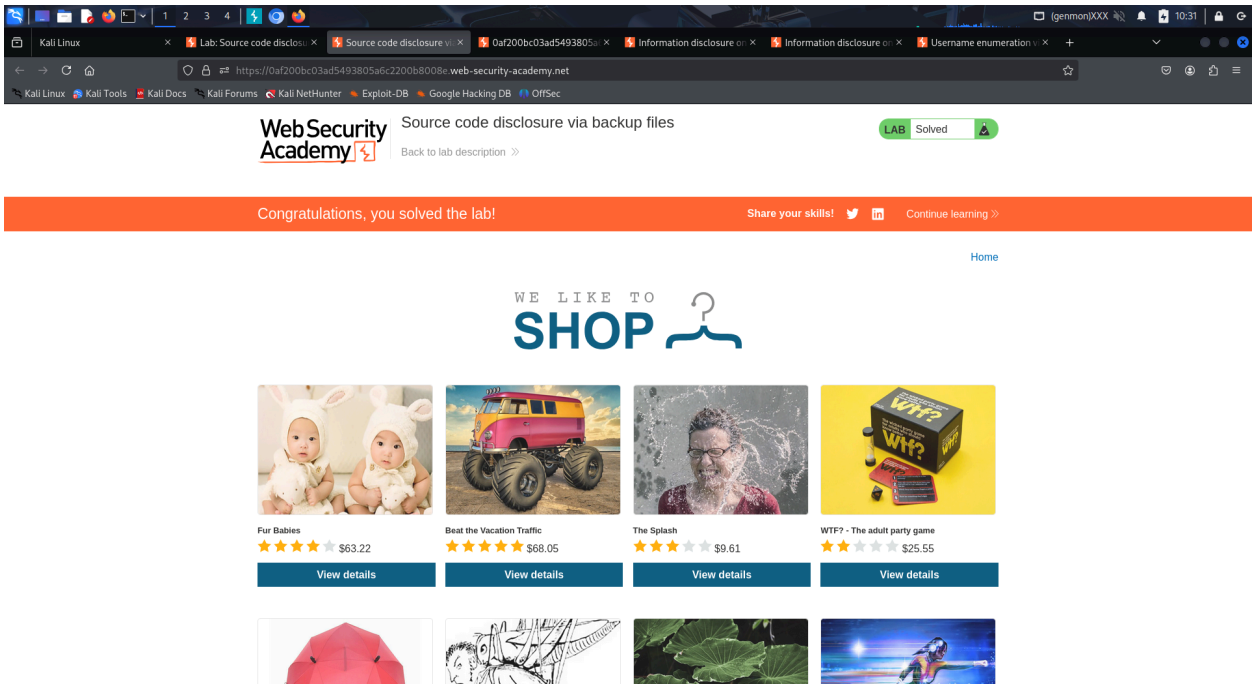
Index of /backup

Name	Size
ProductTemplate.java.bak	1647B




```
import java.sql.Connection;
import java.sql.ResultSet;
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",
                "vj97omi39s3wgl7rl4fgpvzei2tbwim5"
        ).withAutoCommit();
        try
        {
            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;
    }
}
```

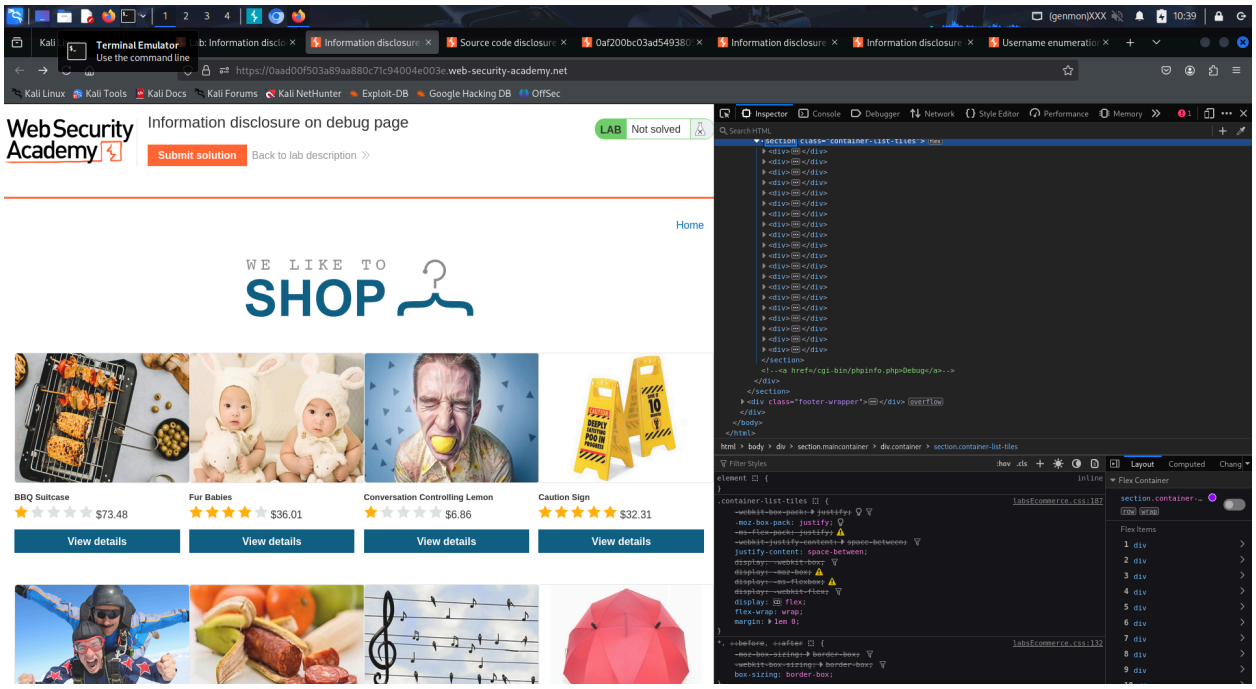
Finally solve the lab.

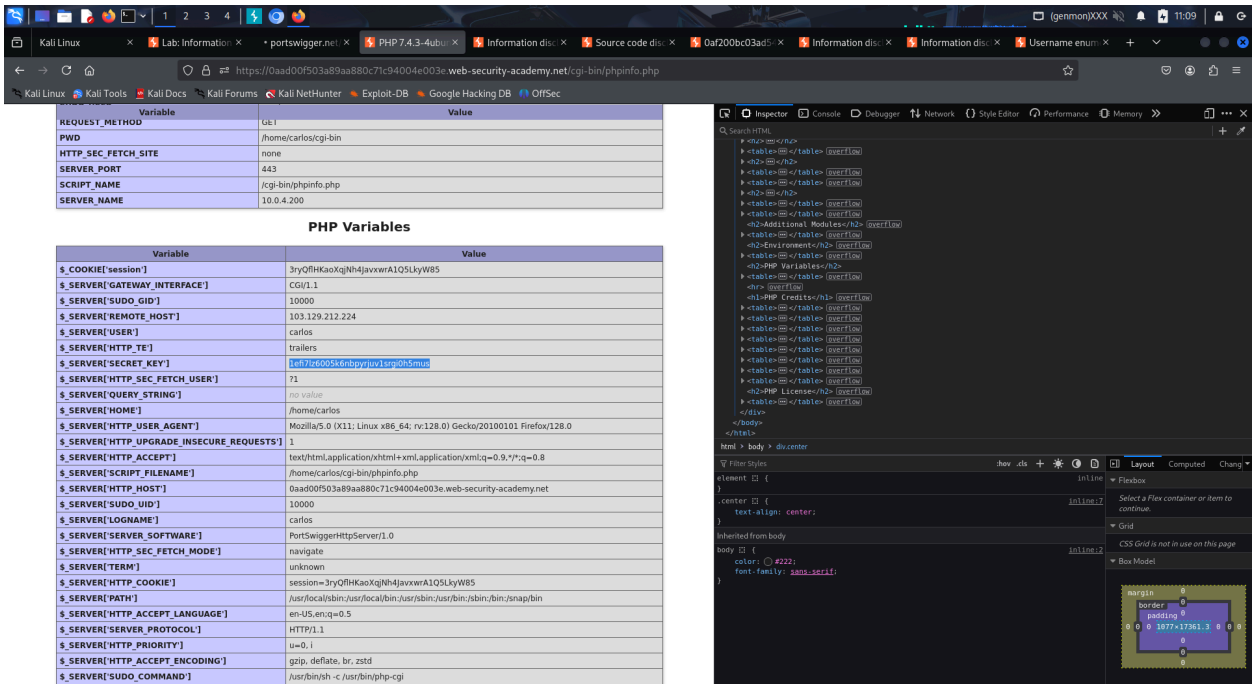


Lab 4: Information disclosure on debug page

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

Step by step solution and screenshots:





Finally solve the lab

0aad00f503a89aa880c71c94004e003e.web-security-academy.net

Sign in

Web Security Academy

Information disclosure on debug page

Back to lab description

LAB Solved

Congratulations, you solved the lab!

Share your skills!

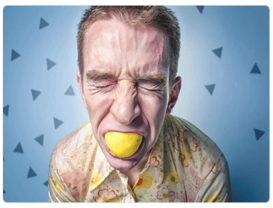
Continue learning

Home

WE LIKE TO SHOP

BBQ Suitcase

Fur Babies



Conversation Controlling Lemon

Caution Sign