

**A REPORT
ON
Vulnerability Assessment and
Penetration Testing**

Submitted by

Mr. Yashwanth.R - 20241CCS3001

Under the guidance of,
**Mr. Girish Kumar B C
Dr. Sharmasth Vali Y**

*in partial fulfillment for the award of the
degree of*

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE AND ENGINEERING (CYBER SECURITY)

AT



**PRESIDENCY UNIVERSITY
BENGALURU**

OCTOBER 2025

PRESIDENCY UNIVERSITY

PRESIDENCY SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

CERTIFICATE

This is to certify that the report of **CSE7000 – Internship** on “**Vulnerability Assessment and Penetration Testing**” being submitted by “**Yashwanth.R**” bearing roll number “**20241CCS3001**” in partial fulfillment of the requirement for the award of the degree of Bachelor of Technology in Computer Science and Engineering (Cyber Security) is a bonafide work carried out under our supervision.

Mr. R Girish Kumar B C
Assistant Professor
PSCS
Presidency University

Dr. Sharmasth Vali Y
Assistant Professor
PSCS
Presidency University

Dr. Sharmasth Vali Y
Internship Program
Coordinate PSCS
Presidency University

Dr. Anandaraj S P
HoD
PSCS
Presidency University

Dr. Shakkeera L
Associate Dean
PSCS
Presidency University

Dr. Duraipandian N
Dean – PSCS & PSIS
Presidency University

PRESIDENCY UNIVERSITY

PRESIDENCY SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

DECLARATION

I hereby declare that the work, which is being presented in the report entitled **“Vulnerability Assessment and Penetration Testing”** in partial fulfillment for the award of Degree of **Bachelor of Technology in Computer Science and Engineering (Cyber Security)**, is a record of my own investigations carried under the guidance of **Mr. Girish Kumar B C, Assistant Professors and Dr. Sharmasth Vali Y, Assistant Professors**, Presidency School of Computer Science and Engineering, Presidency University, Bengaluru.

I have not submitted the matter presented in this report anywhere for the award of any other Degree.

Name:Yashwanth.R

Roll No:20241CCS3001

Signature of the Student:

INTERNSHIP COMPLETION CERTIFICATE



ACKNOWLEDGEMENT

First of all, I indebted to the **GOD ALMIGHTY** for giving me an opportunity to excel in our efforts to complete this internship on time.

I express sincere thanks to our respected Dean **Dr. Duraipandian N**, Presidency School of Computer Science and Engineering & Presidency School of Information Science, Presidency University for getting us permission to undergo the internship.

I express heartfelt gratitude to our beloved Associate Dean **Dr. Shakkeera L**, Presidency School of Computer Science and Engineering, Presidency University, and **Dr. Anandaraj S P**, Head of the Department, Presidency School of Computer Science and Engineering, Presidency University, for rendering timely help in completing this internship successfully.

I am greatly indebted to my reviewers **Mr. Girish Kumar B C**, Assistant Professor and **Dr. Sharmasth Vali Y**, Assistant Professor, Presidency School of Computer Science and Engineering, Presidency University for their inspirational guidance, and valuable suggestions and for providing a chance to express technical capabilities in every respect for the completion of the internship work.

I would like to convey gratitude and heartfelt thanks to the Internship Coordinator **Dr. Md Ziaur Rahman** and Program Internship Coordinator **Dr. Sharmasth Vali Y**. I also thank my family and friends for the strong support and inspiration they have provided us in bringing out this internship.

Yashwanth.R(20241CCS3001)

ABSTRACT

This report details the one-month practical training completed at **CENERGYIS INFOTECH PVT LTD [ZINGHR]** from July 1, 2025, to July 31, 2025, as a mandatory component of the B.Tech CSE (Cybersecurity) program. The internship was conducted within the **Product Development** department, where the intern served as a **Penetration Testing Intern**. ZingHR is a global Human Capital Management (HCM) solutions provider headquartered in Mumbai, specializing in a cloud-based platform that manages the entire "Hire to Rehire" employee lifecycle.

The primary goal was to bridge academic theory with real-world application, specifically by applying theoretical security concepts to practical scenarios. Key activities included hands-on experience with industry-standard **penetration testing tools** and methodologies. The intern developed proficiency in using **Burp Suite** for web application security testing, **Nmap** for network scanning, and **Metasploit** for vulnerability exploitation. This work involved identifying and exploiting common web vulnerabilities like **SQL Injection** and **Cross-Site Scripting (XSS)**.

The experience profoundly enhanced the intern's professional capabilities, improving **teamwork and communication skills** through collaboration with development and QA teams, and strengthening **problem-solving** and **time management**. The internship successfully reinforced concepts from academic coursework, particularly **Ethical Hacking** and **Network Security**, and solidified a clear career path in the **offensive security** industry. This training was an invaluable, transformative experience that confirmed the intern's aspirations and provided a robust foundation for future professional endeavors.

Introduction

Internships serve as a crucial bridge between academic learning and professional application, allowing students to experience firsthand the realities of their chosen field. This report presents a comprehensive account of my one-month internship at ZingHR (Cnergyis Infotech Pvt. Ltd.), undertaken from 1st July 2025 to 31st July 2025 as part of the B.Tech in Computer Science and Engineering (Cybersecurity) program at Presidency University. The primary objective of this internship was to gain practical exposure to cybersecurity practices within a corporate setting, understand the functioning of real-world security operations, and apply the theoretical concepts acquired during my academic coursework.

During my tenure at ZingHR, I was assigned to the Product Development Department, where I had the opportunity to explore the technical, analytical, and strategic aspects of penetration testing and web application security. Working in this department enabled me to understand how cybersecurity integrates with the broader product development lifecycle—ensuring that innovative HR solutions remain secure, reliable, and compliant with industry standards.

The internship provided me with exposure to several professional dimensions: understanding corporate culture, engaging in collaborative problem-solving, and developing essential technical skills relevant to the cybersecurity domain. Furthermore, it allowed me to observe the interaction between cross-functional teams, emphasizing the importance of communication, coordination, and documentation in real-world IT environments.

Through this experience, I sought to achieve the following key objectives:

Practical Application: To apply cybersecurity principles and penetration testing methodologies to assess and enhance product security.

Skill Development: To strengthen my technical and professional competencies, particularly in ethical hacking, vulnerability assessment, and

risk management.

Industry Exposure: To gain insights into modern HR technology platforms and understand the security challenges faced by organizations in a digital ecosystem.

Professional Growth: To develop adaptability, teamwork, and effective communication within a dynamic organizational framework.

Overall, this internship served as a transformative learning experience—enhancing my technical proficiency, shaping my professional outlook, and providing a deeper understanding of how cybersecurity plays an integral role in modern software development and enterprise operations.

OBJECTIVE

The primary objective of this internship was to bridge the gap between theoretical knowledge and its real-world application by gaining practical exposure in the field of cybersecurity, specifically focusing on penetration testing and web application security. The internship aimed to provide hands-on experience in identifying, analyzing, and mitigating security vulnerabilities within enterprise systems, while also enhancing professional and interpersonal skills essential for a successful career in the cybersecurity domain.

The specific objectives of the internship were as follows:

1.Application of Academic Knowledge: To apply the cybersecurity principles, ethical hacking techniques, and network defense mechanisms learned during academic coursework to real-world security assessments and testing scenarios.

2.Technical Skill Enhancement: To develop practical expertise in using

industry-standard tools such as Burp Suite, Nmap, and Metasploit for vulnerability scanning, exploitation, and reporting.

3.Understanding Corporate Security Practices: To gain insights into the functioning of security operations within a corporate environment, including policy implementation, compliance standards, and secure software development practices.

4.Problem-Solving and Analytical Development: To cultivate a systematic approach to identifying vulnerabilities, analyzing potential risks, and formulating effective solutions aligned with organizational goals.

5.Professional Growth and Team Collaboration: To enhance communication, teamwork, and time management skills by working collaboratively within the Product Development team and engaging with professionals across departments.

6.Career Orientation: To explore and understand the roles, responsibilities, and challenges of a cybersecurity professional, thereby strengthening my commitment and direction toward a career in offensive security and ethical hacking.

WORK PROGRESS

During my internship at ZingHR (Cnergyis Infotech Pvt. Ltd.), my role centered on penetration testing and web application security within the Product Development Department. The internship, held from 1st July 2025 to 31st July 2025, followed a structured progression that allowed me to gradually transition from foundational learning to independent security testing and reporting. Each week introduced new technical challenges, hands-on tasks, and collaborative learning experiences that strengthened both my technical and professional competencies.

Week 1: Orientation and Environment Setup

The first week was dedicated to familiarization with the company's structure, workflow, and the foundational concepts of security testing.

- Attended onboarding and orientation sessions to understand ZingHR's product architecture, security framework, and development processes.
 - Gained insights into the Human Capital Management (HCM) platform and how cybersecurity integrates into its modules.
 - Set up a virtual testing environment using Kali Linux, configured with penetration testing tools such as Burp Suite, Nmap, and OWASP ZAP.
 - Installed and configured the Damn Vulnerable Web Application (DVWA) on the Kali Linux environment to practice and understand common web vulnerabilities in a controlled setup.
 - Reviewed internal security guidelines, SDLC documentation, and ZingHR's approach to maintaining product integrity and data protection.
-

Week 2: Web Application Analysis and Reconnaissance

In the second week, my focus shifted toward understanding web application architecture and conducting reconnaissance activities.

- Explored ZingHR's web-based modules related to employee management, payroll, and performance systems to understand their functional workflow.
- Practiced reconnaissance and information gathering techniques using Nmap and WHOIS to identify open ports, services, and underlying technologies.
- Utilized DVWA to simulate reconnaissance and enumeration exercises, testing various approaches to identify system information and vulnerabilities.
- Reviewed OWASP Top 10 vulnerabilities and began mapping these to potential risks in corporate web applications.
- Collaborated with developers and QA team members to understand real-world challenges in securing web-based HR systems.

Week 3: Vulnerability Assessment and Exploitation

The third week was highly practical and focused on testing, analysis, and vulnerability exploitation.

- Conducted vulnerability scanning using Burp Suite and OWASP ZAP to detect issues such as SQL Injection, Cross-Site Scripting (XSS), and Broken Authentication within internal testing environments.
- Practiced exploitation techniques using DVWA, applying different levels of security configurations to understand how attacks vary in complexity and impact.
- Performed manual testing to verify automated findings and evaluate real exploitation potential.
- Collaborated with senior cybersecurity professionals to prioritize

vulnerabilities based on severity, impact, and likelihood.

- Began drafting detailed vulnerability reports, outlining the description, impact, and remediation suggestions for each identified issue.

Week 4: Reporting, Review, and Documentation

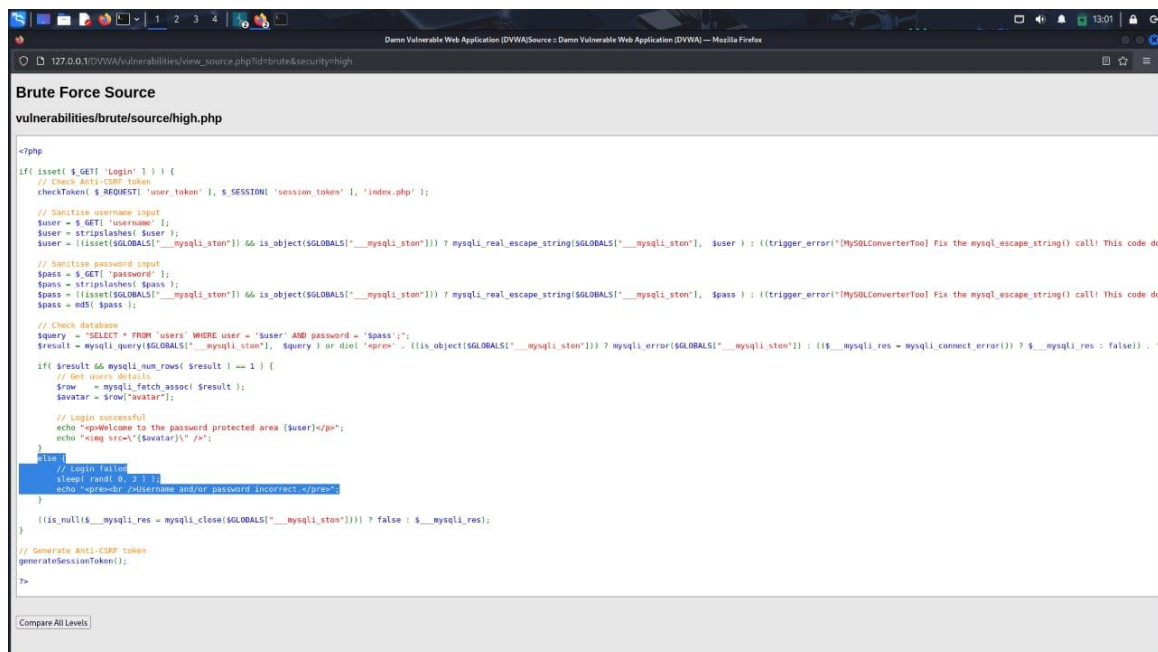
The final week was devoted to report preparation, verification, and knowledge consolidation.

- Compiled a comprehensive penetration testing report, documenting methodologies, testing tools, identified vulnerabilities, and recommended mitigation measures.
- Presented findings to the Product Development and QA teams, participating in discussions about remediation and secure coding improvements.
- Conducted re-testing after developers implemented fixes to ensure closure of reported vulnerabilities.
- Summarized the learning process from DVWA exercises to real-world applications, emphasizing how controlled practice enhanced testing accuracy.
- Prepared the final documentation and submitted the internship report for academic and organizational review.

RESULTS

The practical implementation using DVWA on Kali Linux successfully enhanced my understanding of web application vulnerabilities and exploitation techniques. Through hands-on testing, I identified and analyzed issues such as SQL Injection, Cross-Site Scripting (XSS), and Command Injection. Each vulnerability was explored across different security levels to understand varying defense mechanisms. This exercise improved my ability to detect, exploit, and document vulnerabilities effectively. It also strengthened my analytical thinking and problem-solving skills in real-time attack scenarios. Overall, the project provided a strong practical foundation for penetration testing and web application security.

BRUTE FORCE:



```
<?php
if (isset( $GET['Login'] ) ) {
    // Check Anti-CSRF token
    checkToken( $REQUEST['user_token'], $SESSION['session_token'], 'index.php' );

    // Sanitize username input
    $user = $GET['username'];
    $user = stripslashes( $user );
    $user = (isset($GLOBALS['__mysqli_ston']) && is_object($GLOBALS['__mysqli_ston'])) ? mysqli_real_escape_string($GLOBALS['__mysqli_ston'], $user) : ((trigger_error("[MySQLConverterTool] Fix the mysqli_escape_string() call! This code does not work on MySQL 5.0.2 and below") 1));

    // Sanitize password input
    $pass = $GET['password'];
    $pass = stripslashes( $pass );
    $pass = (isset($GLOBALS['__mysqli_ston']) && is_object($GLOBALS['__mysqli_ston'])) ? mysqli_real_escape_string($GLOBALS['__mysqli_ston'], $pass) : ((trigger_error("[MySQLConverterTool] Fix the mysqli_escape_string() call! This code does not work on MySQL 5.0.2 and below") 1));
    $pass = md5( $pass );

    // Check database
    $query = "SELECT * FROM 'users' WHERE user = '$user' AND password = '$pass'";
    $result = mysqli_query($GLOBALS['__mysqli_ston'], $query) or die( "Error: " . (isset($GLOBALS['__mysqli_ston']) ? mysqli_error($GLOBALS['__mysqli_ston']) : (trigger_error("[MySQLConverterTool] Fix the mysqli_error() call! This code does not work on MySQL 5.0.2 and below") 1));

    if ($result && mysqli_num_rows( $result ) == 1 ) {
        // Get users details
        $row = mysqli_fetch_assoc( $result );
        $avatar = $row['avatar'];

        // Login successful
        echo "<p>Welcome to the password protected area {user}</p>";
        echo "<img src='\"$avatar\"' />";
    }
    else {
        // Login failed
        $loop = rand( 0, 2 );
        echo "<p>Error: /Username and/or password incorrect.</p>";
    }

    if (is_null($__mysqli_res = mysqli_close($GLOBALS['__mysqli_ston'])) ? false : $__mysqli_res);
}

// Generate Anti-CSRF token
generateSessionToken();
?>
```

```
Brute Force Source
vulnerabilities/brute/source/high.php

<?php
if (isset($_GET['login'])) {
    // Check Anti-CSRF token
    checkToken($_REQUEST['user_token'], $_SESSION['session_token'], 'index.php');

    // Sanitize username input
    $user = $_GET['username'];
    $user = stripslashes($user);
    $user = (isset($GLOBALS['__mysqli_ston']) && is_object($GLOBALS['__mysqli_ston']) ? mysqli_real_escape_string($GLOBALS['__mysqli_ston'], $user) : ((trigger_error('[MySQLConverterTool] Fix the mysqli_escape_string() call! This code does not work on MySQL < 5.0.10') 2));

    // Sanitize password input
    $pass = $_GET['password'];
    $pass = stripslashes($pass);
    $pass = (isset($GLOBALS['__mysqli_ston']) && is_object($GLOBALS['__mysqli_ston']) ? mysqli_real_escape_string($GLOBALS['__mysqli_ston'], $pass) : ((trigger_error('[MySQLConverterTool] Fix the mysqli_escape_string() call! This code does not work on MySQL < 5.0.10') 2));

    // Check database
    $query = "SELECT * FROM 'users' WHERE user = '$user' AND password = '$pass'";
    $result = mysqli_query($GLOBALS['__mysqli_ston'], $query) or die('mysql_error(' . mysqli_error($GLOBALS['__mysqli_ston']) . ') : (' . $__mysqli_res = mysqli_connect_error() ? $__mysqli_res : false);

    if ($result && mysqli_num_rows($result) == 1) {
        // Get users details
        $row = mysqli_fetch_assoc($result);
        $avatar = $row['avatar'];

        // Login successful
        echo "<h1>Welcome to the password protected area {user}</h1>";
        echo "<img src='\"$avatar\"' />";
    } else {
        // Login failed
        sleep(0.3);
        echo "<p>Invalid username and/or password incorrect.</p>";
    }

    if (isset($_GET['login']) && $__mysqli_res = mysqli_close($GLOBALS['__mysqli_ston'])) ? false : $__mysqli_res;

    // Generate Anti-CSRF token
    generateSessionToken();
}

?>
```

Kali Linux

Vulnerability: Brute Force

Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Authorisation Bypass
Open HTTP Redirect
Cryptography
API

Vulnerability: Brute Force

Login

Username:
Password:

Login

More Information

- <https://www.exploit-db.com/exploits/4048/>
- <https://www.exploit-db.com/exploits/4048/>
- <https://www.exploit-db.com/exploits/4048/>

Inspector

Search HTML

HTML

body > body > div.container > div.main > div.body > div.vulnerable_code_area > form > input

element

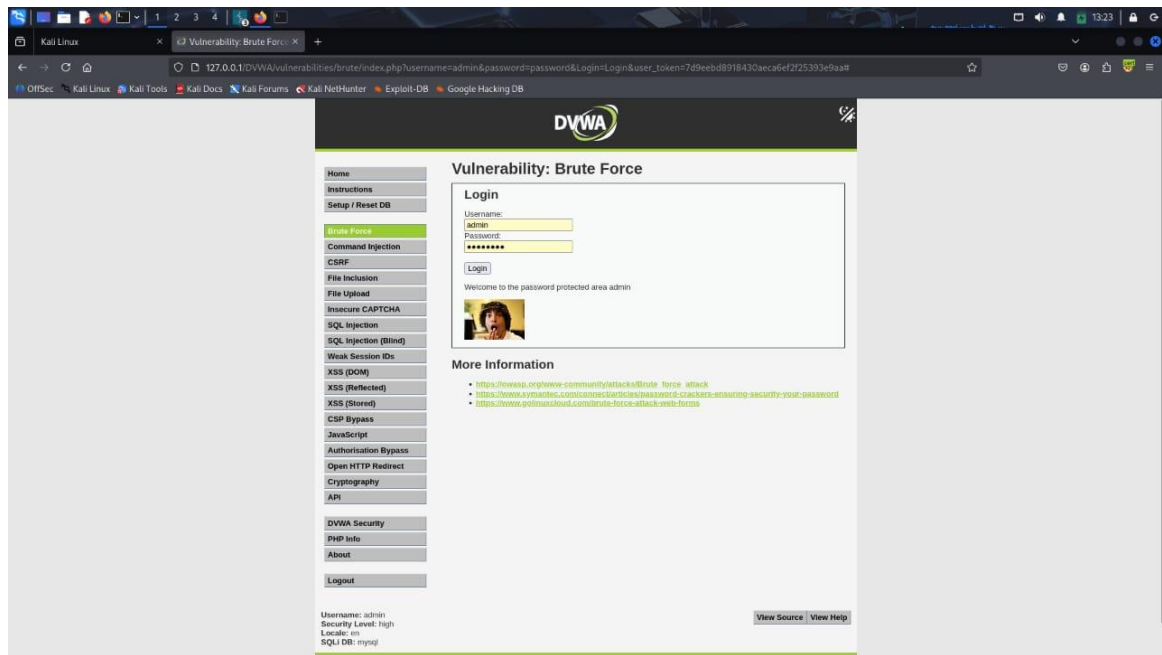
input: username, password

font: 100% Arial, sans-serif

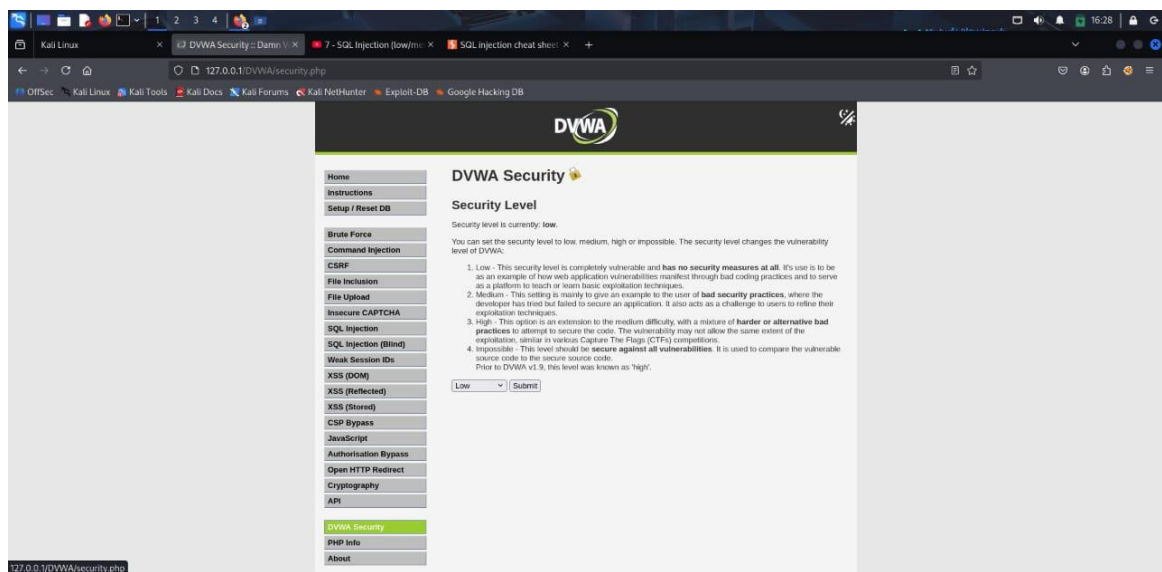
margin: 0; padding: 0;

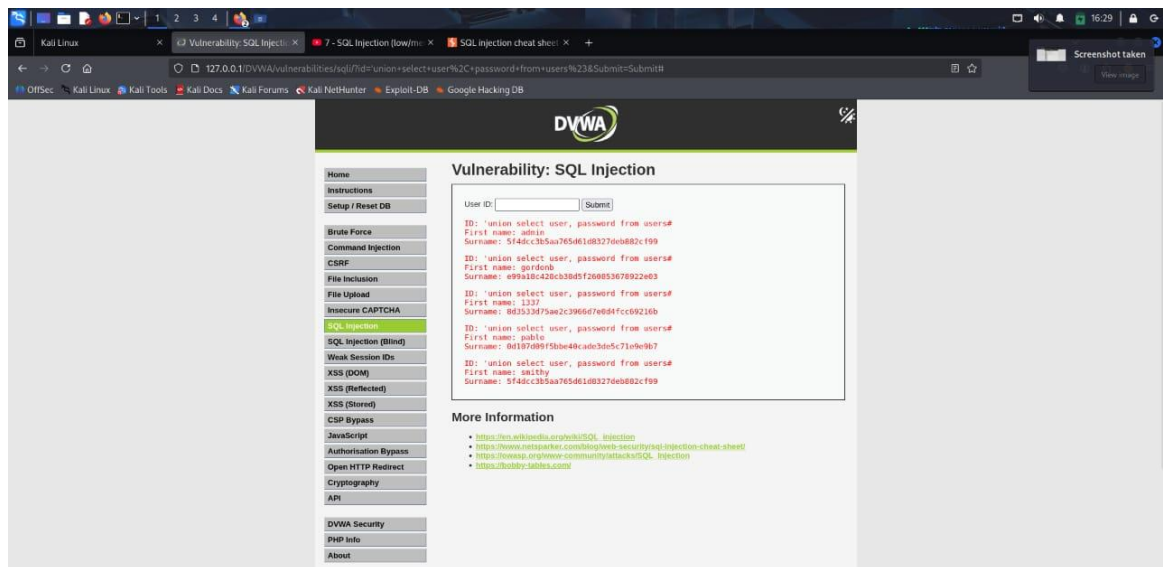
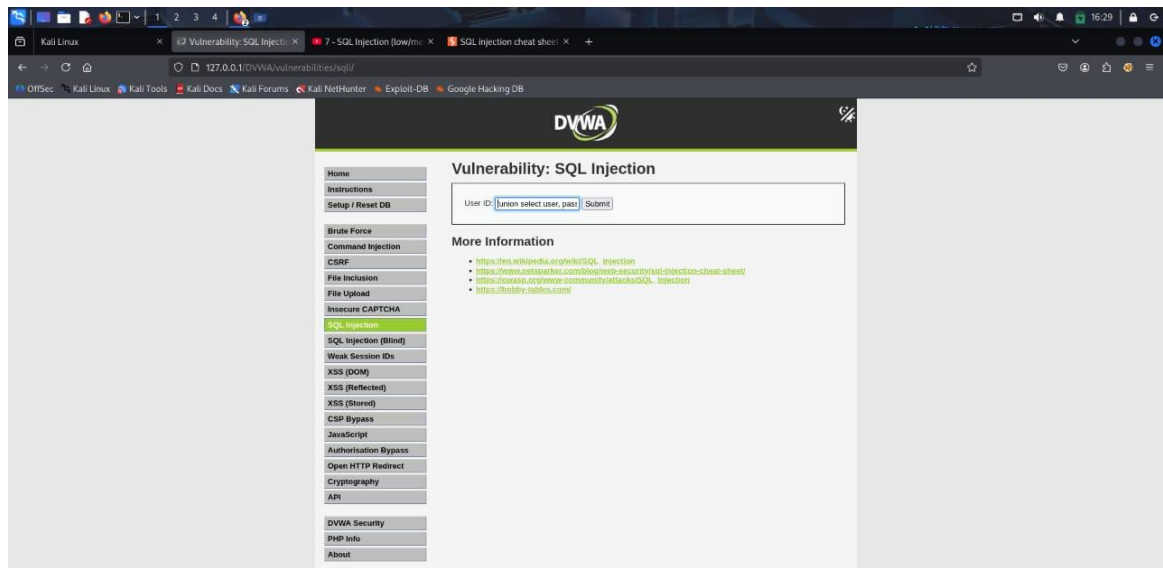
margin: 0; padding: 0;

margin: 0; padding: 0;



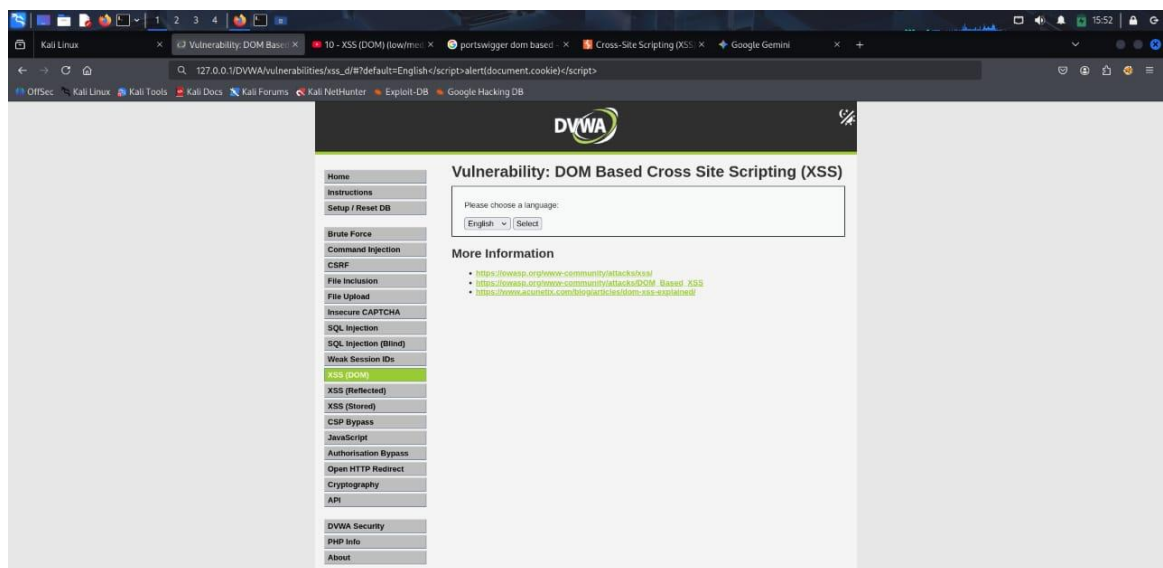
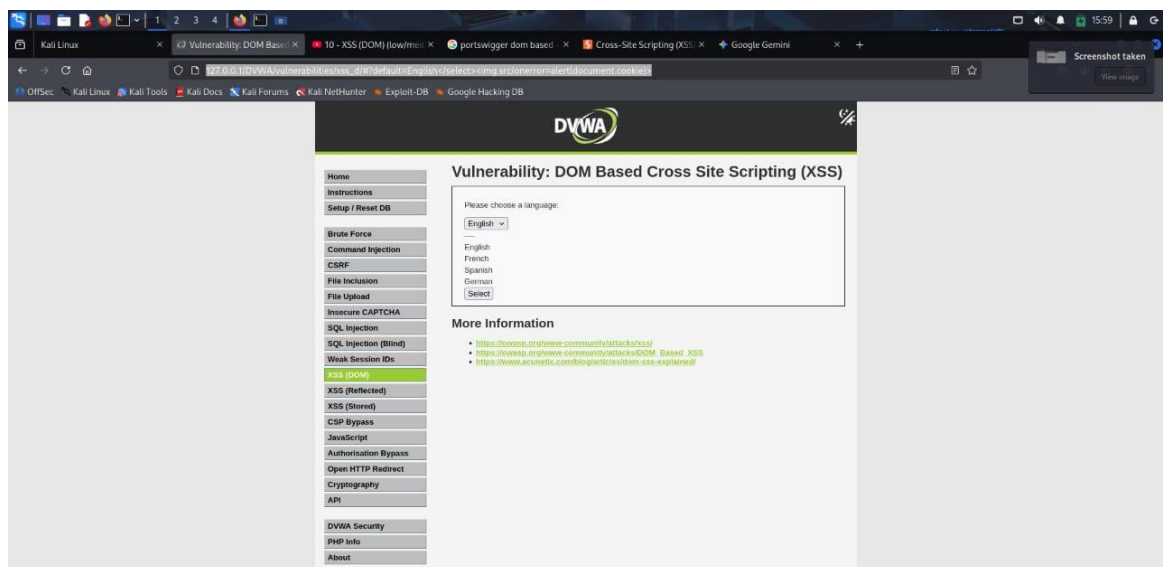
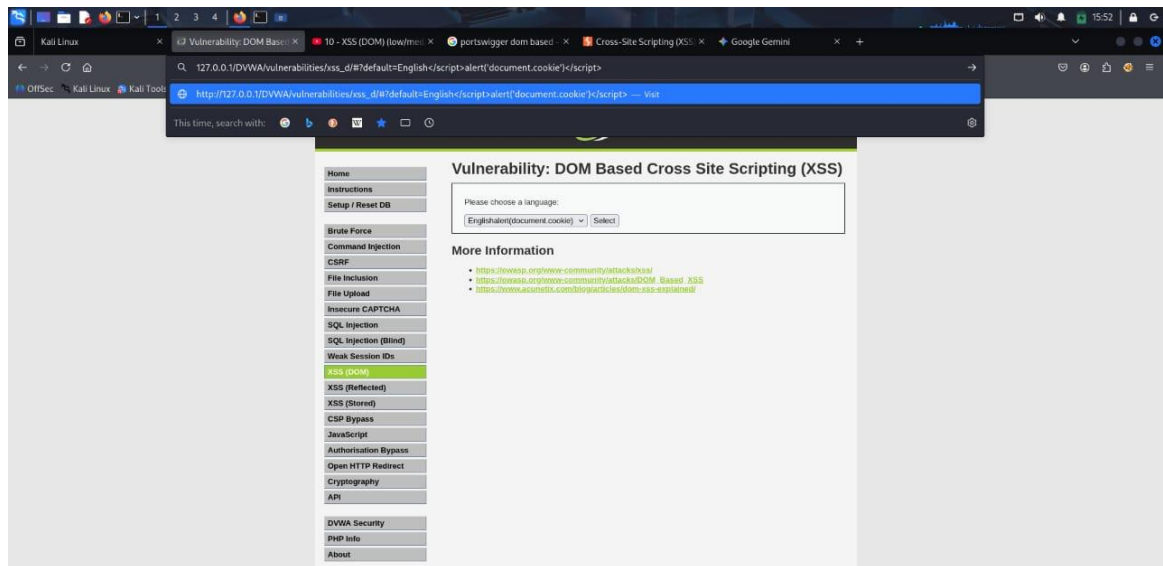
SQL INJECTION:

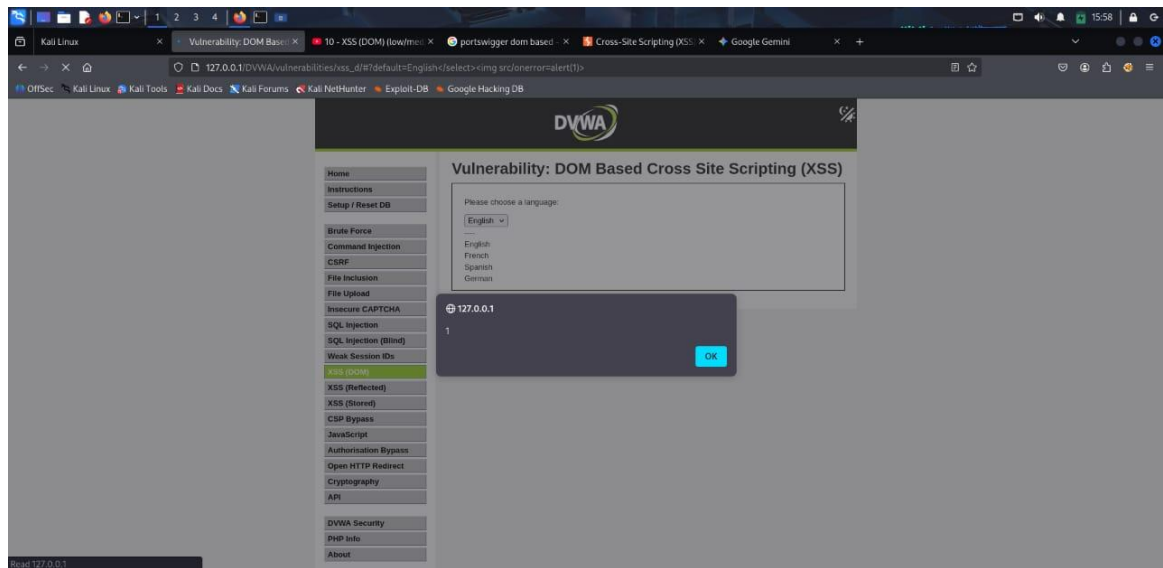




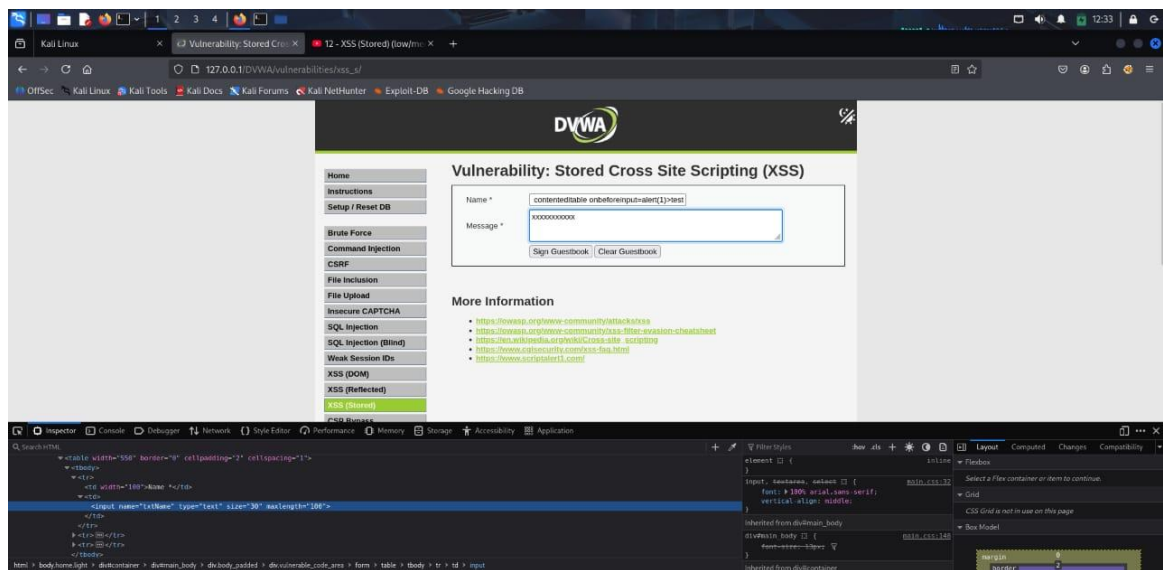
XSS:

DOM:





STORED XSS:



CONCLUSION

The internship at **ZingHR (Cnergyis Infotech Pvt. Ltd.)** provided me with a valuable opportunity to bridge the gap between theoretical knowledge and practical application in the field of **cybersecurity**. Over the course of one month, I gained hands-on experience in **penetration testing, vulnerability assessment, and secure application development**, which deepened my understanding of real-world security challenges in a corporate environment.

Working within the **Product Development Department** allowed me to observe how cybersecurity integrates into every stage of software creation and maintenance. The use of tools such as **Burp Suite, Nmap, and DVWA (Damn Vulnerable Web Application)** enhanced my technical expertise, helping me to identify, exploit, and document vulnerabilities effectively.

These experiences improved not only my technical proficiency but also my analytical, problem-solving, and communication skills.

The internship also strengthened my appreciation for teamwork, collaboration, and the importance of continuous learning in the ever-evolving cybersecurity landscape. It helped me understand how professional security testing contributes directly to building safer and more reliable digital systems.

Overall, this internship was a transformative learning journey that solidified my passion for cybersecurity and ethical hacking. It has equipped me with the technical confidence, professional discipline, and practical insight needed to pursue a successful career in the cybersecurity domain. The experience reaffirmed my goal of becoming a skilled and responsible security professional dedicated to safeguarding digital infrastructures.