Case Study Background

We have been hired as cybersecurity consulting team by SafeCart Solutions, a mid-sized e-commerce firm. The organization recently noticed abnormal access attempts and traffic surges directed at its public-facing online application. Although no hack has been proven, internal IT suspects probing behavior to discover weakness. SafeCart Solutions conducts a rigorous penetration test to analyze the resilience of its systems and identify and solve any security holes before they are exploited by hostile actors.

Company Background

SafeChart Solutions is a growing online retail firm that provides personalized health and fitness items via a unique web application. The platform facilitates client registration, payment processing, order tracking and administrative tasks. Recently, system logs indicated unsuccessful login attempts and abnormal server activity, raising concerns in the IT department.

To retain consumer trust and regulatory compliance, the firm has hired our team to conduct a controlled, ethical white-box penetration test to identify possible hazards and provide practical remedial strategies.

Objectives

- Test the security Safecart Solution's online system through a simulated cyberhack(penetration test)
- Identify any weakness or vulnerabilities that hacker might tyr to exploit
- Analyze unusual access attempts and traffic surges to understand potential threats
- Provider clear recommendation to fix the security issues found
- Help SafeCart Solutions strengthen its defense and prevent future cyberattacks

SCOPE

- Penetration Testing
  Perfom controlled, ethical hacking to simulate real-word attacks and uncover security weakness

- Vulnerability Identifications
  Detect and document any security gaps that could be exploited by attackers

- Reporting and Recommendations
  Provide a detailed report of finding with practical steps to fix vulnerbilities and improve overall cybersecurity

- Assesment of Public-Facing Systems
  Focus on the company's main online appplication and any systems accesible from the internet.

- Traffic and Access Analysis
  Review logs and pattern related to abnormal traffic access attempts to identify possible probing behaviour

Tools and Techniques

ATTACK	TOOLS	ASSIGN TO	PLATFORM
SQL INJECTION	SQLMAP	DANISH	DVWA
BROKEN ACCESS CONTROL	BURP SUITE	IKHWAN	OWASP Juice Shop
CROSS-SITE SCRIPTING (XSS)	OWASP ZAP	SYARIFUDDIN	XSS Game by Google

JUSTIFICATION:

SQL INJECTION

For this project, we used SQLMap as our primary tool to test for SQL Injection. SQLMap is a free and powerful tool that automates the process of identifying and exploiting SQL injection vulnerabilities. It can identify several forms of SQL injection, including error based, time based and boolean based.

We use SQLMap because:

- It is easy to use and works well with test environments like DVWA or OWASP Juice Shop.
- It can quickly find weaknesses and even show what data could be stolen.
- It supports many database systems like MySQL, PostgreSQL, and more.

BROKEN ACCESS CONTROL

We are testing for Broken Access Control using Burp Suite. Burp Suite is a popular web security testing tool for intercepting, modifying, and replaying HTTP requests. This makes it extremely useful for determining if people can access areas of a website that they should not be able to.

We use Burp Suite because:

- It lets us manually test access control by changing user roles, session tokens, or IDs in requests.
- We can intercept and modify parameters, such as URLs or cookies, to check if unauthorized access is allowed.
- It gives us full control to inspect the request and response, helping us understand how the system handles access permissions.

CROSS-SITE SCRIPTING (XSS)

We are testing for Cross-Site Scripting (XSS) vulnerabilities with OWASP ZAP. This tool is intended to assist in the detection of security flaws in online applications, with a particular emphasis on XSS prevention.

We chose OWASP ZAP because:

- It can automatically scan input fields to test if the application reflects or executes harmful scripts.
- It supports active and passive scanning, allowing us to test both user-visible and hidden areas of the application.
- The tool can inject XSS payloads and show whether they are executed in the browser, which helps confirm the vulnerability.

TEAM ROLES

Name	Tasks/Roles
 MUHAMMAD DANISH MIRZA BIN IBRAHIM	**LEAD TESTER AND RESEARCHER** • Investigate cybersecurity threats and analyze the system for security weaknesses. • Select and suggest suitable penetration testing tools and payloads to aid in the vulnerability testing process.

 MUHAMMAD IKHWAN BIN OSMAN	**REPORT WRITER** • Prepare and structure the final report, incorporating the introduction, methodology, and results from testing. • Consolidate technical insights into a concise and well-organized summary.
 SYARIFUDDIN BIM AMIR	**DEMO COORDINATOR** • Organize the system demonstration by setting up tools, outlining the presentation flow, and presenting the project clearly during the evaluation. • Coordinate team roles to deliver a smooth and timely demonstration

6.0 RULES OF ENGAGEMENT

The penetration test activities will be conducted only within the bounds of authorized, intentionally vulnerable environments such as DVWA (Damn Vulnerable Web Application) and OWASP Juice Shop. These are expressly set up for safe, legal, and educational purposes in cybersecurity studies. All testing will be conducted during allocated class or lab hours to ensure supervision, coordination, and compliance to academic guidelines. No live systems or third-party infrastructure will be targeted, and no activity will include data destruction, denial-of-service, or anything that might result in

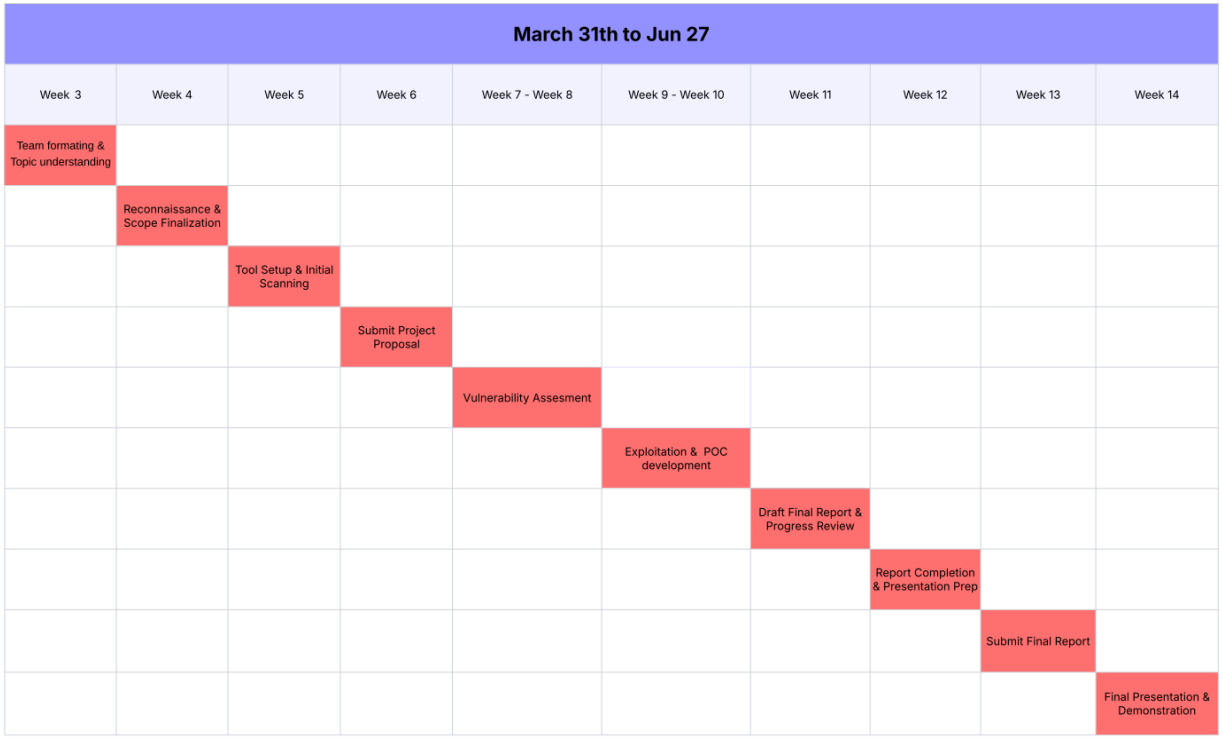
damage or disruption of service. Every action taken will be logged to maintain transparency, reproducibility, and accountability. The deliverables will be a comprehensive penetration testing report and a team presentation of results and recommendations.

7.0 Ethical Considerations

- The penetration test is to be conducted exclusively on publicly available, purposely exposed websites for education and ethical hacking (e.g., DVWA, OWASP Juice Shop.
- Unauthorized access to data, third-party, or private systems will not be attempted.
- All actions and activities are within the scope of ethical hacking and are permissible under the test environment acceptable use policies.
- The aim of this project is purely academic and intended to develop safe and responsible cybersecurity practices.

8.0 TIMELINE

Gantt Chart Of Timeline Group Project ITT320



Week	Milestone	Responsible Members
Week 3	Team Formation & Topic Understanding	All
Week 4	Reconnaissance & Scope Finalization	Lead Tester, Researcher
Week 5	Tool Setup & Initial Scanning	Lead Tester
Week 6	Submit Project Proposal	All
Week 7–8	Vulnerability Assessment	Lead Tester, Researcher
Week 9–10	Exploitation & Proof of Concept Development	Lead Tester
Week 11	Draft Final Report & Progress Review	Report Writer, Demo Coordinator
Week 12	Report Completion & Presentation Prep	Report Writer, Demo Coordinator
Week 13	Submit Final Report	All
Week 14	Final Presentation & Demonstration	All