Cybersecurity DVWA & Ethical Hacking Labs

IEEE-Style Project Documentation and Case Study

Muhammad Haider Abbas | MSc Computer Science & Technology | Ulster University Birmingham Campus



Figure 1. Project visual identity used in the portfolio website.

Abstract

Cybersecurity DVWA & Ethical Hacking Labs is documented as a professional portfolio case study by Muhammad Haider Abbas. The project demonstrates practical capability in Cybersecurity through a structured problem-solution design, implementation direction, testing plan and future development roadmap. The report explains the business or academic motivation, system requirements, architecture, workflow, quality considerations and expected professional value of the project. It is prepared for use as downloadable portfolio evidence for recruiters, clients and academic reviewers.

Keywords: Cybersecurity, Practical Labs, Security Learner, DVWA, Burp Suite, OWASP, Security

I. Project Profile

Field	Details
Project Title	Cybersecurity DVWA & Ethical Hacking Labs
Category	Cybersecurity
Year	2026
Role	Security Learner
Status	Practical Labs
Tools	DVWA, Burp Suite, OWASP testing workflow
Portfolio Slug	dvwa-ethical-hacking-labs

II. Introduction and Problem Context

This document presents the technical and professional documentation for Cybersecurity DVWA & Ethical Hacking Labs. The project is positioned as a practical labs in the Cybersecurity category. The work highlights the author's ability to combine technical implementation, documentation discipline and outcome-focused project thinking. The project summary is: Hands-on cybersecurity labs using DVWA, Burp Suite, OWASP concepts and professional reporting practice.

A. Problem Statement

Security concepts are easier to understand when tested in legal, controlled lab environments.

B. Proposed Solution

DVWA-style workflows are used to practise vulnerability testing, evidence capture and mitigation thinking.

III. Aim and Objectives

To practise and document web application security testing in a legal, controlled vulnerable lab environment.

- Set up DVWA-style vulnerable application testing safely.
- Use Burp Suite and browser tools to inspect requests.
- Practise common OWASP-style vulnerability categories.
- Capture evidence and write professional mitigation notes.
- Improve secure development awareness.

IV. Requirements Analysis

ID	Requirement	Type	Priority
FR-01	Local lab environment	Functional / project requirement	Required
FR-02	DVWA target	Functional / project requirement	Required
FR-03	Burp Suite proxy	Functional / project requirement	Required
FR-04	OWASP vulnerability categories	Functional / project requirement	Required
FR-05	Evidence screenshots direction	Functional / project requirement	Required
FR-06	Risk and remediation notes	Functional / project requirement	Required
NFR-01	Usability and clear portfolio presentation	Non-functional	Required
NFR-02	Maintainability and future extensibility	Non-functional	Required
NFR-03	Professional documentation and evidence quality	Non-functional	Required

V. System Architecture

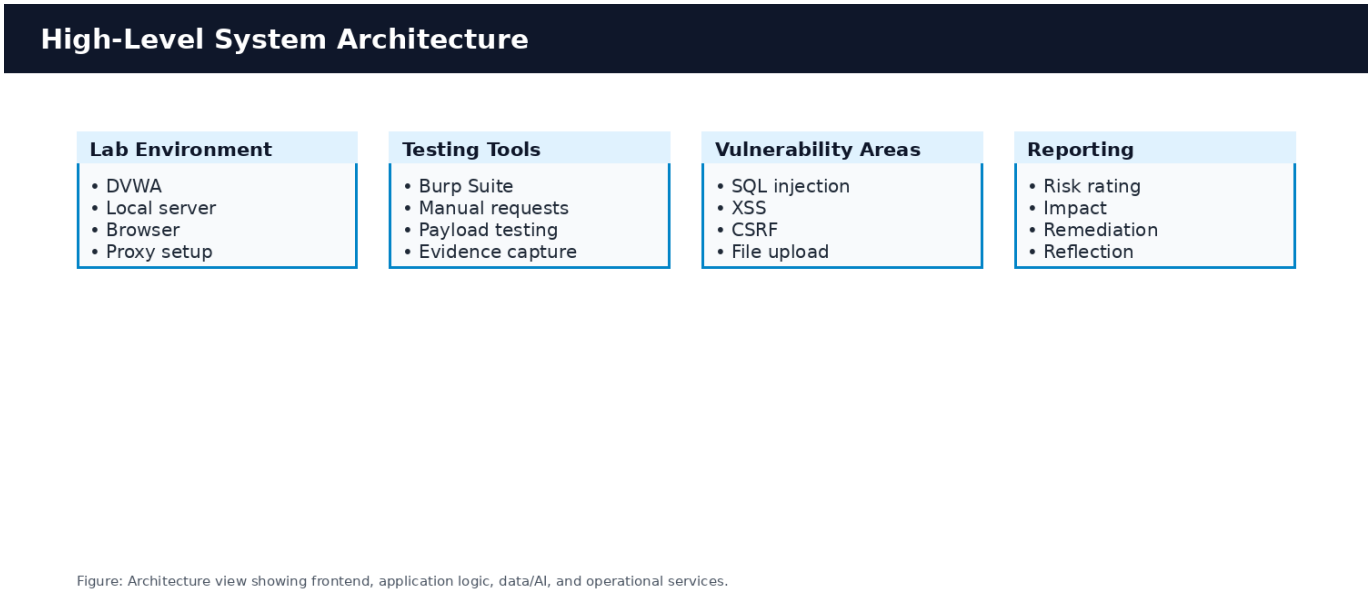


Figure: Architecture view showing frontend, application logic, data/AI, and operational services.

Figure 2. High-level architecture or production pipeline for the project.

The architecture separates user-facing presentation, project logic, data or model processing, and operational output. This structure makes the project easier to explain, test and extend inside a professional portfolio environment.

VI. Workflow Design

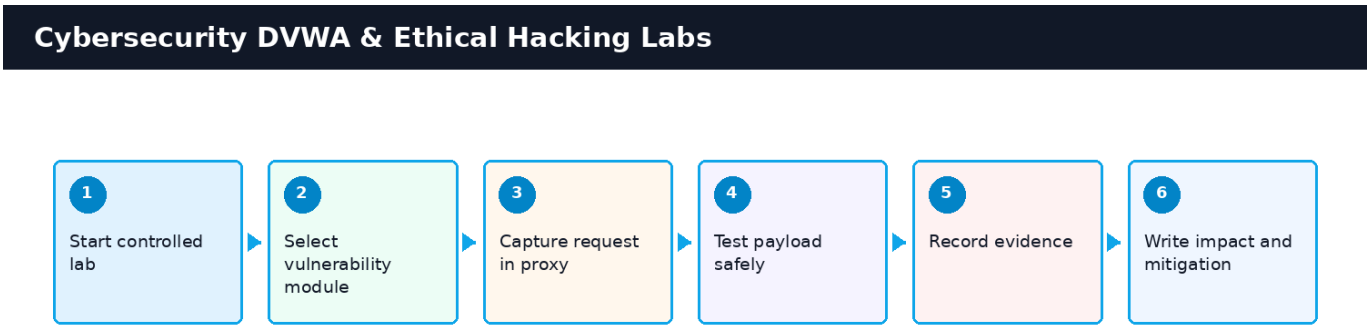


Figure: Generated project workflow / architecture artefact for portfolio documentation.

Figure 3. Project workflow from input or user action to final output.

VII. Data, Components and Implementation View

Component	Layer	Responsibilities	Notes
C-01	Lab Environment	DVWA, Local server, Browser, Proxy setup	Core component group
C-02	Testing Tools	Burp Suite, Manual requests, Payload testing, Evidence capture	Core component group
C-03	Vulnerability Areas	SQL injection, XSS, CSRF, File upload	Core component group
C-04	Reporting	Risk rating, Impact, Remediation, Reflection	Core component group

Implementation should be documented through screenshots, code snippets, database schema extracts, test outputs or demonstration media when available. For deployed or live systems, screenshots and logs should be attached as appendices to increase evidence strength.

VIII. Testing and Validation Strategy

Test Area	Test Method	Expected Result
Lab access	Open DVWA locally	Login/dashboard works
Proxy setup	Intercept test request	Request visible in Burp
Vulnerability test	Run safe payload	Expected lab behaviour observed
Report quality	Write finding	Risk/impact/fix included

The testing strategy focuses on validating the main user or system journey, confirming that core requirements behave as expected, and recording limitations clearly. This supports honest portfolio evidence and avoids overclaiming features that are still prototypes.

IX. Security, Ethics and Professional Considerations

- Operate only in legal, owned or intentionally vulnerable lab environments.
- Separate evidence gathering from harmful real-world exploitation.
- Write remediation-focused reports rather than exploit-only notes.

X. Results, Outcome and Future Work

A. Outcome

A practical cybersecurity learning portfolio section.

B. Future Enhancements

Add full write-ups, remediation steps and lab videos.

Roadmap Stage	Enhancement Direction
Short term	Add missing screenshots, demo links and downloadable supporting files.
Medium term	Connect live/source URLs and replace placeholder evidence with real artefacts.
Long term	Use analytics, user feedback or formal evaluation results to strengthen the project case study.

XI. References

[1] DigiNinja, "Damn Vulnerable Web Application (DVWA)," https://github.com/digininja/DVWA

[2] OWASP Foundation, "OWASP Top 10," https://owasp.org/www-project-top-ten/

[3] PortSwigger, "Burp Suite," https://portswigger.net/burp

Appendix A. Portfolio Download Mapping

Item	Value
Recommended PDF path	docs/dvwa-ethical-hacking-labs-project-documentation.pdf
Recommended Word path	docs/dvwa-ethical-hacking-labs-project-documentation.docx
Admin field: Documentation	docs/dvwa-ethical-hacking-labs-project-documentation.pdf
Admin field: Extra Project File	docs/dvwa-ethical-hacking-labs-project-documentation.docx