PenTest-Ont Cybersecurity Ontology

IEEE-Style Project Documentation and Case Study

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

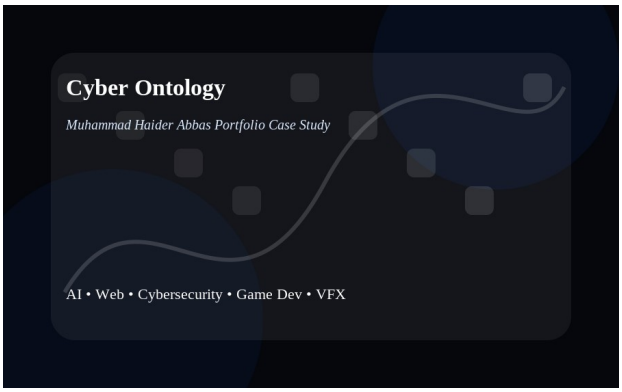


Figure 1. Project visual identity used in the portfolio website.

Abstract

PenTest-Ont Cybersecurity Ontology 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, Academic Project, Security Researcher, OWL, Protégé, SPARQL, Cybersecurity

I. Project Profile

Field	Details
Project Title	PenTest-Ont Cybersecurity Ontology
Category	Cybersecurity
Year	2026
Role	Security Researcher
Status	Academic Project
Tools	OWL, Protégé, SPARQL, Knowledge Graphs
Portfolio Slug	pentest-ont-cybersecurity-ontology

II. Introduction and Problem Context

This document presents the technical and professional documentation for PenTest-Ont Cybersecurity Ontology. The project is positioned as a academic project 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: A cybersecurity ontology modelling tools, techniques, vulnerabilities and penetration testing knowledge.

A. Problem Statement

Cybersecurity knowledge can become fragmented across tools, techniques and vulnerability categories.

B. Proposed Solution

The ontology models relationships between tools, testing techniques, vulnerabilities and reasoning concepts.

III. Aim and Objectives

To model penetration testing knowledge as a structured ontology linking tools, techniques, vulnerabilities, assets and mitigations.

- Define ontology scope and competency questions.
- Build OWL classes and object properties in Protégé.
- Represent relationships between attacks, tools and vulnerabilities.
- Query the knowledge graph using SPARQL.
- Prepare future connection to automated security reports or AI assistants.

IV. Requirements Analysis

ID	Requirement	Type	Priority
FR-01	OWL class hierarchy	Functional / project requirement	Required
FR-02	Object/data properties	Functional / project requirement	Required
FR-03	Tool-vulnerability mapping	Functional / project requirement	Required
FR-04	SPARQL queries	Functional / project requirement	Required
FR-05	Reasoning checks	Functional / project requirement	Required
FR-06	Knowledge graph visualisation	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

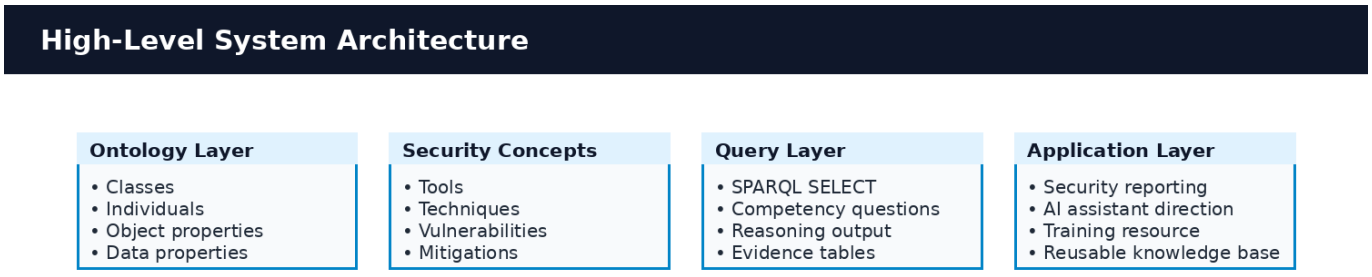


Figure: Architecture view showing frontend, application logic, data/AI, and operational services.

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

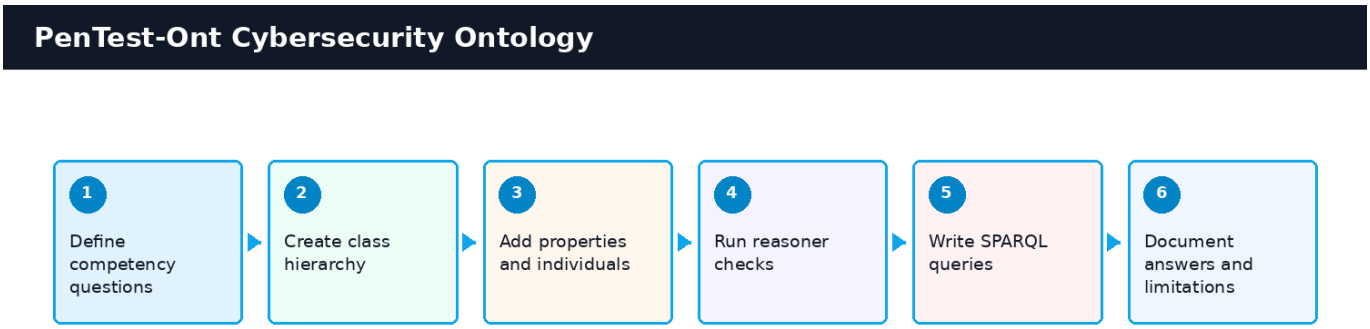


Figure: Generated project workflow / architecture artefact for portfolio documentation.

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

VII. Data, Components and Implementation View

Component	Layer	Responsibilities	Notes
C-01	Ontology Layer	Classes, Individuals, Object properties, Data properties	Core component group
C-02	Security Concepts	Tools, Techniques, Vulnerabilities, Mitigations	Core component group
C-03	Query Layer	SPARQL SELECT, Competency questions, Reasoning output, Evidence tables	Core component group
C-04	Application Layer	Security reporting, AI assistant direction, Training resource, Reusable knowledge base	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
Class hierarchy	Open ontology in Protégé	No structural errors
Reasoner	Run consistency check	Ontology is consistent
SPARQL query	Query tools by vulnerability	Expected rows returned
Documentation	Map competency questions to answers	Coverage is clear

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 unique cybersecurity research project showing structured knowledge modelling.

B. Future Enhancements

Connect ontology to automated security reports and AI assistants.

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] W3C, "OWL 2 Web Ontology Language Document Overview," https://www.w3.org/TR/owl2-overview/

[2] W3C, "SPARQL 1.1 Overview," https://www.w3.org/TR/sparql11-overview/

[3] Stanford Center for Biomedical Informatics Research, "Protégé," https://protege.stanford.edu/

Appendix A. Portfolio Download Mapping

Item	Value
Recommended PDF path	docs/pentest-ont-cybersecurity-ontology-project-documentation.pdf
Recommended Word path	docs/pentest-ont-cybersecurity-ontology-project-documentation.docx
Admin field: Documentation	docs/pentest-ont-cybersecurity-ontology-project-documentation.pdf
Admin field: Extra Project File	docs/pentest-ont-cybersecurity-ontology-project-documentation.docx