Application Testing Automation

Tanuwijaya, Richard Valent
Supervised by Prof. Lin, Fangzhen

THE DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
計算機科學及工程學系

Background

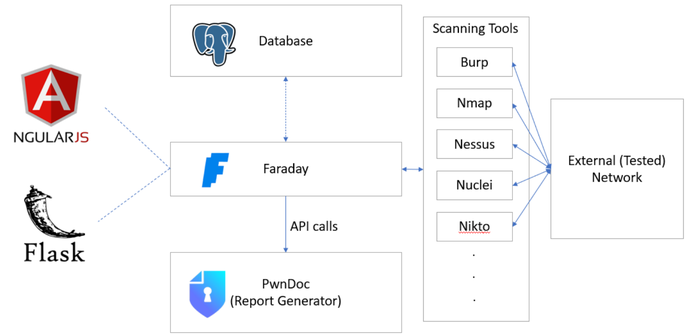
Faraday is a centralized vulnerability management system that consolidates and manages vulnerability data in one platform. It offers seamless integration with multiple vulnerability scanners.

PwnDoc is a platform designed for creating penetration testing reports. It enables professional report generation with customizable templates and stores past vulnerabilities for easy retrieval.

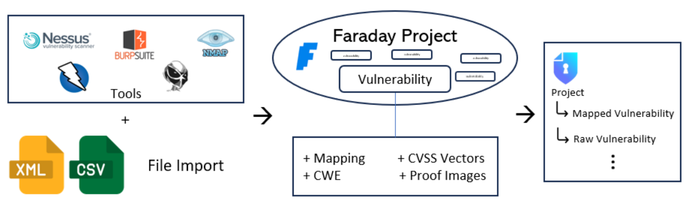
Objectives

1. Integrate more vulnerability scanners to Faraday
2. Match vulnerabilities scanned in Faraday to PwnDoc vulnerability templates.
3. Facilitate easy referencing for penetration testers.
4. Predict CVSS scores to assist penetration testers in their assessments.
5. Enable users to save and submit proof images from Faraday to PwnDoc.

System Architecture

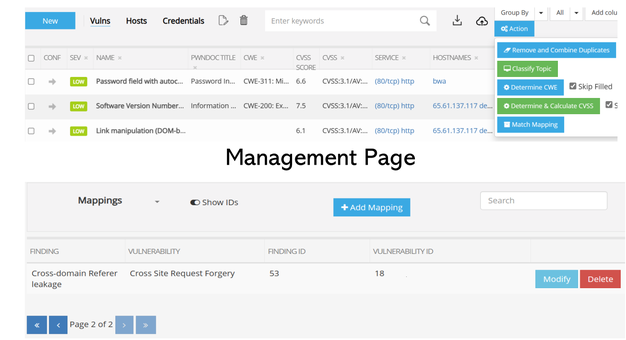


Workflow

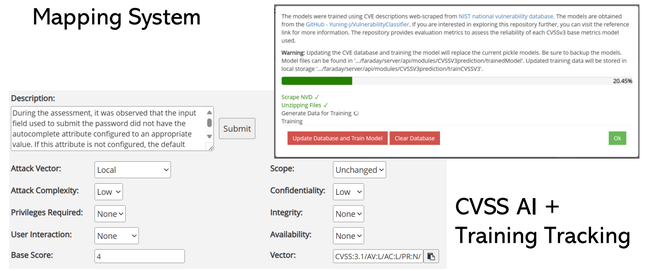


Procedures:
- Scan or import vulnerabilities
- Confirm found vulnerabilities (while pentesting)
- Update necessary information using AI(s) in Faraday
- Export to PwnDoc with templated vulnerabilities or raw Faraday information

User Interfaces Designs



Management Page



Mapping System

CVSS AI + Training Tracking

Conclusion

The enhancements made to Faraday and integration with PwnDoc allows a more streamlined process of scanning, managing vulnerabilities, and reporting. AI are implemented to help employees with other related information.