VulneraAI

A fusion of "Vulnerability" and "AI" for automated bug detection and fixation

Department of CSE,
Green University Of Bangladesh

Team Information

Md.Robiul Islam → 222002068
Ashrafun Nahar Arifa → 222002066
Md. Mahmudul Hasan Rifat → 222002048
Md. Nayem Ibne Nur → 221002256

Abstract

VulneraAI is an AI-driven vulnerability scanning system that automates threat detection for domains and IPs. It combines port scanning, service enumeration, and OS fingerprinting with machine learning and signature-based analysis. The tool generates actionable reports with risk scores, enabling efficient and scalable security assessments. VulneraAI enhances detection accuracy while minimizing false positives.

Introduction

- AI-Powered Vulnerability Scanner
- Real-World Threat Intelligence
- Professional Reporting & Analytics
- Modern Dark Cybersecurity UI
- Lightweight & Scalable Architecture
- Enterprise-Grade Security & Validation

Problem Domain

- Modern networks are increasingly complex.
- Vulnerabilities are harder to detect manually.
- Traditional scanners give many false positives.
- Manual assessments are slow and not scalable.
- Existing tools lack smart threat prioritization.
- AI-powered solutions are in high demand.

Motivations

- Rising cyber threats demand proactive defense.
- Manual scanning is inefficient and error-prone.
- Existing tools lack AI-based threat analysis.
- Security teams need faster risk detection.
- Real-time scanning boosts incident response.
- AI improves accuracy and reduces false positives.

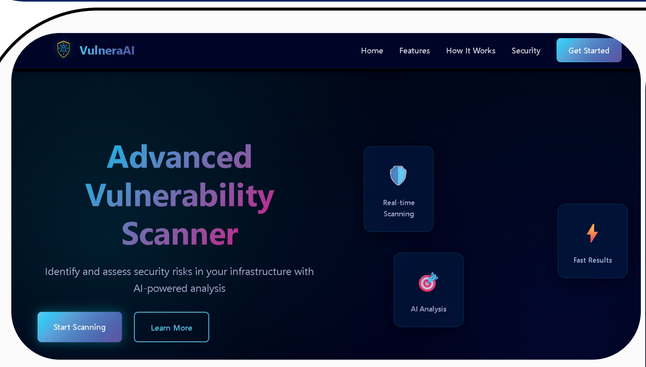
Objectives

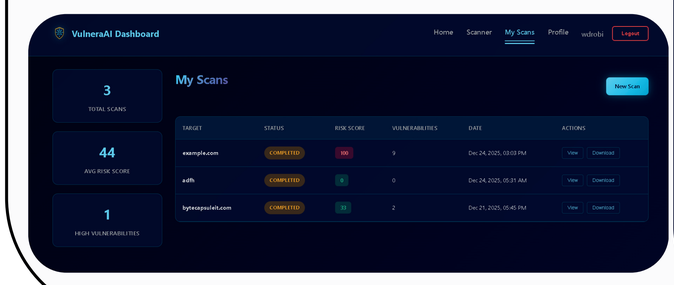
- Develop an AI-powered scanning tool.
- Automate vulnerability detection tasks.
- Integrate port, service, and OS scanning.
- Apply ML for risk classification.
- Generate actionable security reports.
- Minimize false positives in output.

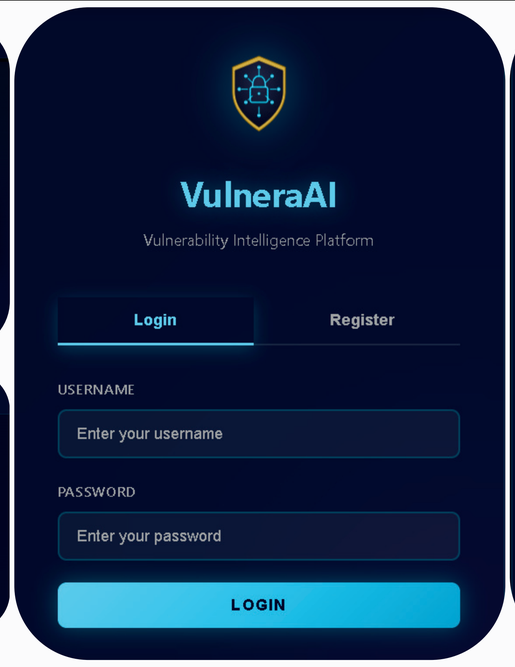
Literature Review

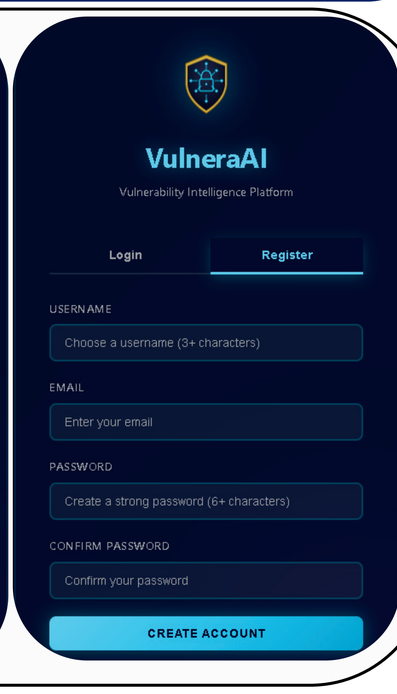
References	Tools	Contributions	Limitations
[1] R. D. Bowes, "Nessus: A Remote Security Scanner," *Tenable Network Security*, 2009.	Nessus Scanner ,Plugin DB	AI-based scoring, adaptive detection	No ML, signature-based only
[2] M. Meier et al., "OpenVAS - Framework for Vulnerability Scanning," Greenbone Networks, 2015.	OpenVAS Engine	ML classification, fast reporting	Rigid scanning rules
[3] G. Lyon, "Nmap Network Scanning," *Insecure.Org*, 2009.	Nmap Toolset	Integrated with AI risk modeling	No threat analysis
[4] S. Kim, "Nikto Web Server Scanner," *CIRT.net*, 2018.	Nikto Web Scanner	Web-specific threat scoring with ML	Outdated databases
[5] H. Moore, "The Metasploit Framework," *Rapid7 Security Labs*, 2011.	Metasploit Framework	Optional AI-assisted correlation	Not designed for passive scanning

Implementation (UI)







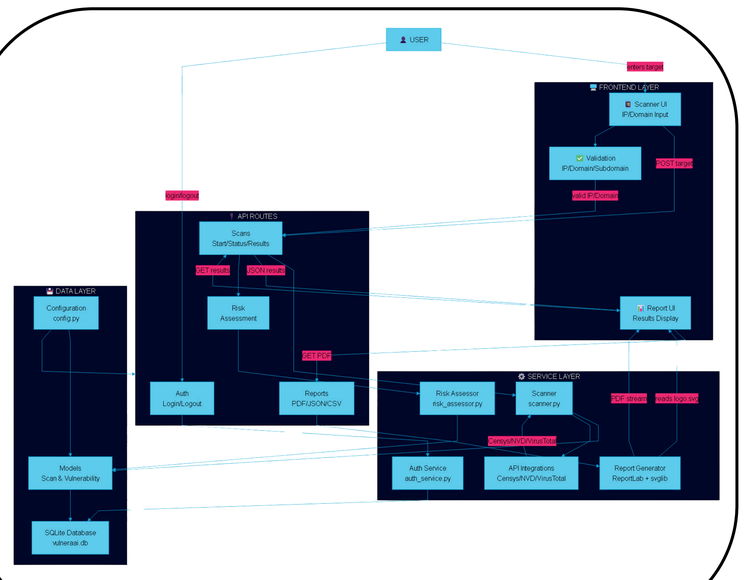


SDLC Model Selection

Priority	Criteria	Waterfall	V-Model	Iterative	Spiral	Agile	DevOps
3	Technological Knowledge	Yes	Yes	Yes	Yes	Yes	Yes
6	Efficiency	No	No	Yes	Yes	Yes	Yes
5	Risk Analysis	No	No	Yes	Yes	Yes	Yes
5	User Testing Ability	No	No	Yes	Yes	Yes	Yes
5	Dependability and Security	No	Yes	Yes	Yes	Yes	Yes
3	Time Consumption	No	No	Yes	Yes	Yes	Yes
4	Flexibility	No	No	Yes	Yes	Yes	Yes
4	Scalability	No	No	Yes	Yes	Yes	Yes
5	Customer Involvement	No	No	Moderate	Moderate	High	High
4	Cost-Effectiveness	Low	Moderate	Moderate	High	Low	High
5	Adaptability to Change	Low	Low	High	Very High	Very High	High
3	Maintenance Complexity	High	High	Moderate	Low	Low	Low
5	Development Speed	Slow	Slow	Moderate	Moderate	High	High
4	Documentation Requirement	High	High	Moderate	High	Low	Low
5	Client Feedback Integration	Low	Low	Moderate	High	Very High	Very High
3	Error Handling	Low	Moderate	High	High	High	High
4	Suitability for Large Projects	High	High	Moderate	Very High	Moderate	High
3	Code Reusability	Low	Low	Moderate	High	High	High
5	Risk Management Efficiency	Low	Low	Moderate	High	Moderate	High
5	Automation Compatibility	Low	Low	Moderate	High	Very High	Very High
3	AI Integration Capability	Low	Low	Moderate	High	Very High	High
Total=89		22	38	64	71	82	85

By integrating Agile's flexibility with DevOps' automation and security- focused principles, the **Hybrid Agile-DevOps** Model ensures that VulneraAI remains an advanced, efficient, and adaptive cybersecurity solution

High Level Architecture



Social Impact

- Promotes cybersecurity awareness.
- Helps protect user data privacy.
- Reduces risk of cybercrime.
- Supports secure digital environments.
- Aids organizations in compliance.
- Enhances trust in online systems.

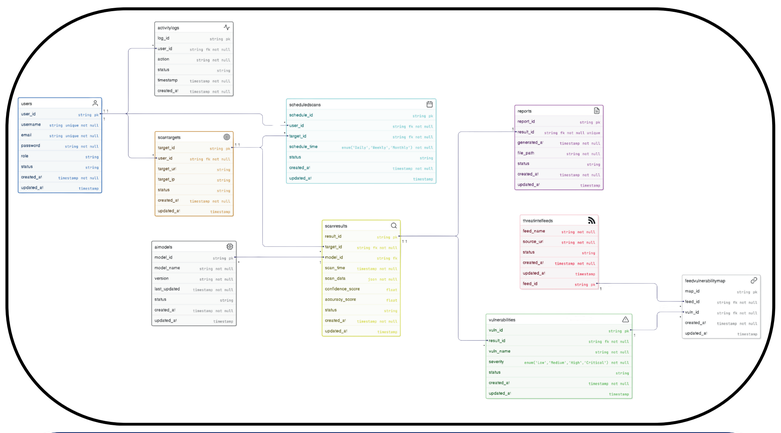
Conclusion

VulneraAI is an AI-powered tool that automates vulnerability detection using smart scanning, fingerprinting, and threat intelligence. It streamlines cybersecurity workflows, provides risk insights, and enhances protection against evolving threats making it a powerful asset for modern digital defense.

Testing

Test ID	Test Case Description	Expected Result	Status
API-001	POST /api/scans/start with valid IP	Returns 201 with scanId	PASS
API-002	POST /api/scans/start with invalid IP	Returns 400 error	PASS
API-003	GET /api/scans/{id}/status during scan	Returns status and progress	PASS
API-004	GET /api/scans/{id}/results with completed scan	Returns vulnerabilities and risk score	PASS
API-005	GET /api/reports/generate?scanId=	Returns PDF stream with correct filename	PASS
API-006	GET /api/risk/{id} aggregate risk	Returns risk score and level	PASS
API-007	POST /api/auth/login with valid credentials	Returns auth token	PASS
API-008	POST /api/auth/login with invalid credentials	Returns 401 unauthorized	PASS

Low-level Architecture (ERD)



Tools and Technology

Category	Technology	Purpose	Key Feature
Frontend	HTML5	Markup & Structure	*Semantic & Accessible*
	CSS3	Styling & Design	*Glass Morphism, Dark Theme*
	JavaScript	Client Logic	*No Framework, Lightweight*
	LocalStorage	Data Persistence	*Session & History*
Backend	Python 3.8+	Server Runtime	*Fast & Scalable*
	Flask 2.2.2	Web Framework	*Lightweight, Modular*
	Flask-CORS	Cross-Origin	*Secure API Comm.*
Database	SQLite	Relational DB	*Lightweight, No Setup*
	JSON	Data Serialization	*Vulnerability Storage*

References

[1] R. D. Bowes, "Nessus: A Remote Security Scanner," Tenable Network Security, 2009. [Online]. Available: https://www.tenable.com
[2] M. Meier, A. Stamer, and T. Holz, "OpenVAS - Framework for Vulnerability Scanning," Greenbone Networks, 2015. [Online]. Available: https://www.openvas.org
[3] G. F. Lyon, "Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning," Insecure.Org, 2009. [Online]. Available: https://nmap.org/book/
[4] S. Kim, "Nikto Web Server Scanner," CIRT.net, 2018. [Online]. Available: https://cirt.net/Nikto2
[5] H. Moore, "The Metasploit Framework," Rapid7 Security Labs, 2011. [Online]. Available: https://www.metasploit.com