International Journal of Interdisciplinary Innovative Research & Development (IJIIRD)
ISSN: 2456-236X
Vol. **11** Special Issue **03** | **2026**

CyberScan Pro: An Automated Vulnerability Scanning and Risk Assessment Framework with Cloud-Based Analytics

Prof. Priyanka L. Fernandes[1], Deeya V. Dorlekar[2], Pranad V. Sawant[3]
[1] *Aisst. Professor, Information Technology, Famt, Maharashtra, India*
[2,3] *Student, Information Technology, Famt, Maharashtra, India*

DOI: 10.5281/zenodo.20630379

ABSTRACT

As more and more applications are being done over the internet, vulnerability has become a serious problem of concern among organizations and developers. Despite the fact that traditional vulnerability scanning tools such as Nessus can scan all types of vulnerabilities, it is resource-consuming, hard to configure, and prohibitive in an academic and small-scale environment (Wongsaard et al., 2025). The paper outlines the design and development of CyberScan Pro, a light weight automated web application vulnerability scanning and risk assessment tool that has been inspired by the Nessus. The identified proposed system focuses on detecting the most frequently used security vulnerabilities which are SQL Injection, Cross-site Scripting (XSS), open ports, insecure headers, and out-of-date servicess (Mdunyelwa et al., 2019) (Amankwah et al., 2020) (Alquwayzani et al., 2024) (Čović, 2024) (Alsaedi et al., 2021). CyberScan Pro is a combination of Linux-based security tools and automated scripts that scan the user submitted URLs. The system is made user friendly, modular and practical with acceptable accuracy. The experimental findings indicate that the system can identify a wide range of vulnerabilities, which makes it a perfect instrument in the academic and small scale analysis of security.

Keyword : *- Web Security, Vulnerability Scanner, Nessus, Penetration Testing, Cybersecurity, Ethical Hacking.*

1. INTRODUCTION

Web applications form an important component of the existing web infrastructure, which offers essential services, such as banking, healthcare, e-commerce, and education. Nevertheless, they have also contributed to the significant increase in the risk of cyber-attacks because of their widespread use. The weaknesses in web applications may lead to serious losses, such as stealing data, unavailability of services, and unauthorized access. Web application security includes vulnerability scanning as an essential component that aids in scanning of the security vulnerability before the hackers exploit them. Very popular are industry standard vulnerability scanning tools such as Nessus, OpenVAS and Qualys. Still, they are resource-heavy, hard to install, and need commercial licenses, which means that they are less accessible to students and small-scale organizations (Aslan et al., 2023) (Swetha et al., 2024) (Jiang et al., 2025). This project will aim at designing and developing a simple automated vulnerability scanning tool based on the Nessus which is specifically created to scan widely exploited vulnerabilities by using open-source tools and scripts.

1.1 Project Background

There have been Several studies conducted on automated vulnerability detection methods for web applications. Conventional vulnerability scanning tools mainly depend on signature-based detection, heuristic evaluation, and rule-based engines. Commercial vulnerability scanning tools such as Nessus have large vulnerability databases that are regularly updated, allowing for the detection of known vulnerabilities in operating systems and applications. However, existing research work has pointed out the drawbacks of high false positives and a lack of flexibility for research purposes (Barchuk & Volkov, 2025). Open-source vulnerability scanning tools such as OWASP ZAP and Nikto are web application-specific but lack centralized analytics and reporting (Swetha et al., 2024). Recent research work has introduced light-weight frameworks that combine multiple open-source scanning tools to achieve better coverage with less complexity.

1.2 Problem Statement

Despite a variety of vulnerability scanning tools on the market, it is lacking light-weight, centralized tools that combine automated scanning, real-time analytics, and reporting within a single framework (Manatova et al., 2022) (Shimizu and Hashimoto, 2025).

1.3 Research Objective

- To develop and establish an automated vulnerability scanning system
- To incorporate vulnerability prioritisation through risk scoring.
- To give real-time log and cloud reporting.
- To compare the effectiveness of the system with the use of existing tools.

1.4 Scope of Work

The study project will focus on the design of a complete vulnerability scanning system of web applications and network services. Automated reconnaissance and detection of the system will focus on the popular weaknesses such as injection attacks, broken authentication, insecure settings, and open services. Active exploitation, real time intrusion prevention, zero-day vulnerability detection and large-scale enterprise benchmarking will not be within the scope of the research. These are pointed out as the future research directions.

1.5 Contributions

- Design of an end-to-end vulnerability scanning framework
- Integration of reconnaissance, detection, scoring, and reporting
- A structured risk scoring model for vulnerability prioritization
- A scalable architecture suitable for academic and real-world use

1.6 Paper Organization

The paper is organized as follows: Section II discusses related work. Section III describes the identification of research gaps. Section IV describes the CyberScan Pro framework. Section V describes the methodology. Sections VI and VII discuss evaluation and results. Section VIII describes the limitations and future work, and conclusions.

2. RELATED WORK

2.1 Traditional Vulnerability Scanning Approaches

The conventional scanning of vulnerabilities was mainly relying on port scanning and signature-based detection. These methods are also less effective with new threats, which is unfortunate since they are only useful with known vulnerabilities and have high false positives.

2.2 Automated Reconnaissance Techniques

Automated reconnaissance enables the systematic discovery of open ports, services and endpoints. Nikto is also famous, but it has simple reporting features with no customization feature (Swetha et al., 2024).

2.3 Risk Scoring Methodologies

Risk scoring systems like CVSS provide severity scores but do not do well to account for the probability of exploitation in real-life attack, which renders them useless in vulnerability prioritization in real-world attacks (Shimizu and Hashimoto, 2025).

2.4 Cloud-Based Reporting in Cybersecurity

The cloud-based security solutions also offer flexibility in data aggregation and real-time analytics. It has been found that interactive analytics dashboard enhances vulnerability management (Manatova et al., 2022) and incident response.

3. IDENTIFIED RESEARCH GAPS

Based on the literature review, the following gaps are identified:

- Limited integration between scanning, analytics, and reporting (Seara & Serrão, 2023)
- Inadequate prioritization of detected vulnerabilities (Swetha et al., 2024)
- Lack of real-time visibility into scan results
- High deployment and operational complexity (Seara & Serrão, 2023)

CyberScan Pro is designed to address these gaps through an integrated, automated framework.

4. CYBERSCAN PRO FRAMEWORK

4.1 Project Overview

CyberScan Pro is a web-based vulnerability scanning and risk assessment framework that automates reconnaissance, vulnerability scanning, risk scoring, and reporting. The framework uses Kali Linux-based scanning scripts and a cloud-based backend for real-time analytics and remediation reporting.

4.2 Overall Architecture

The architecture consists of:

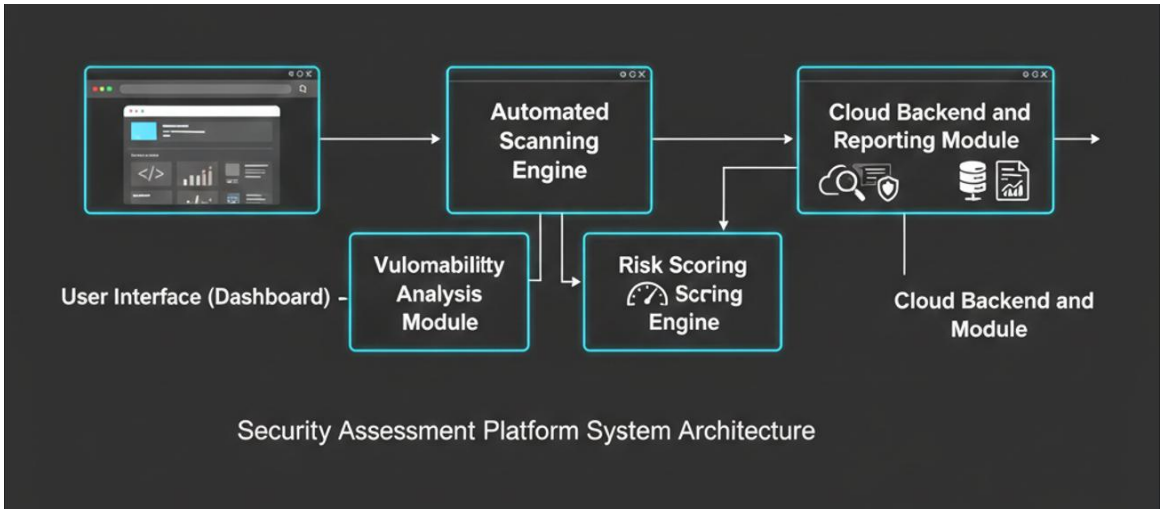


Fig -1 : System Architecture

- User Interface (Dashboard)
- Automated Scanning Engine
- Vulnerability Analysis Module
- Risk Scoring Engine
- Cloud Backend and Reporting Module

4.3 Automated Reconnaissance Module

This module includes URL analysis, port scanning, and endpoint discovery using automated security scripts run in a Kali Linux environment

4.4 Vulnerability Identification Module

The identified components are scanned for known vulnerability patterns such as SQL injection, XSS, CSRF, and insecure configuration.

4.5 Risk Scoring Engine

Each detected vulnerability is assigned a severity score using a weighted risk model.

Risk Scoring Formula

$$RiskScore = \alpha \times Impact + \beta \times Exploitability + \gamma \times Exposure$$

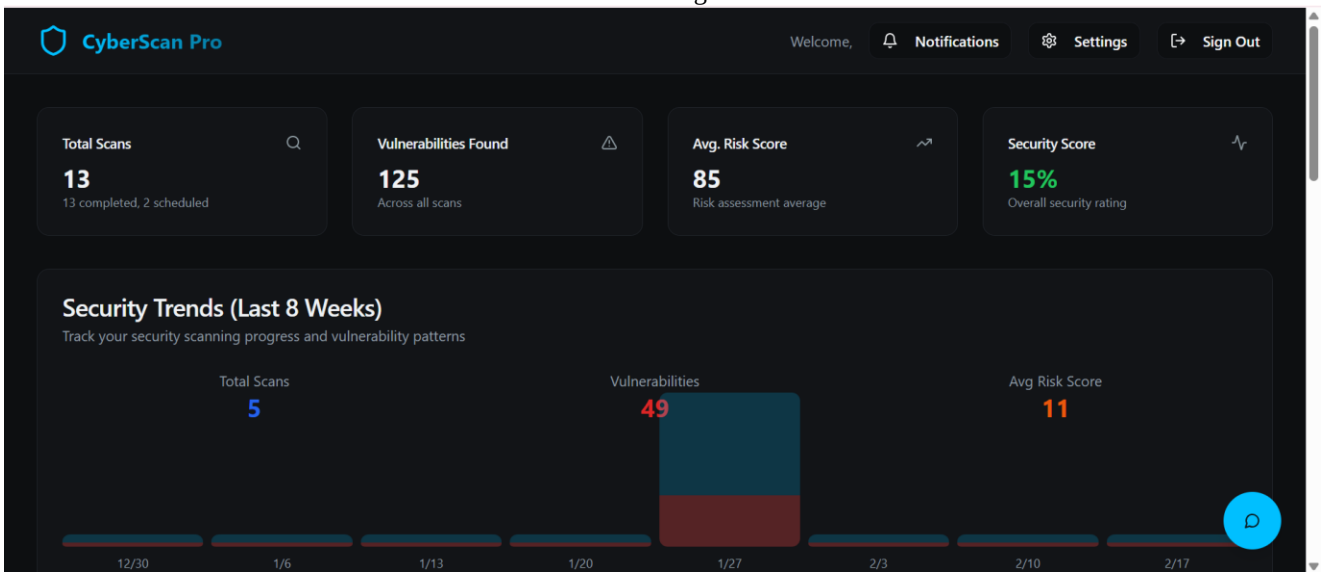
Where:

- $Impact$ represents potential damage
- $Exploitability$ indicates ease of exploitation
- $Exposure$ reflects system accessibility

α, β, γ are weighting coefficients

4.6 Cloud-Based Reporting and Analytics Module

Scan results are stored in the cloud backend and visualized through dashboards.



5. METHODOLOGY

5.1 System Workflow

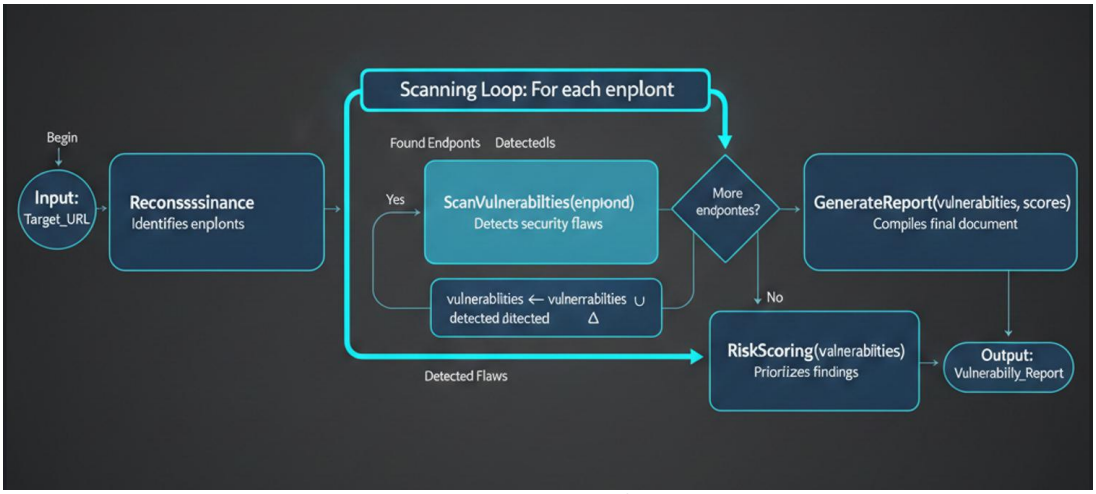


Fig 2 : System Workflow

Pseudocode: Overall Scanning Workflow

Input: Target_URL
Output: Vulnerability_Report

```
begin
   endpoints ← Reconnaissance(Target_URL)
   vulnerabilities ← {}
   for each endpoint in endpoints do
      detected ← ScanVulnerabilities(endpoint)
      vulnerabilities ← vulnerabilities ∪ detected
   end for
   scores ← RiskScoring(vulnerabilities)
   GenerateReport(vulnerabilities, scores)
end
```

5.2 Data Collection

The data gathered includes endpoints, types of vulnerabilities, severity levels, timestamps, and remediation recommendations.

5.3 Risk Scoring Pseudocode

```
function RiskScoring(vulnerabilities):
   for each v in vulnerabilities do
      v.score ← α*v.impact + β*v.exploitability + γ*v.exposure
   end for
   return vulnerabilities
```

5.4 Implementation Environment

- Operating System: Kali Linux
- Backend: Supabase
- Scanning Scripts: Bash-based tools
- Dashboard: Web-based interface

6. EXPERIMENTAL SETUP

6.1 Test Environment

CyberScan Pro testing was done under a well planned experimental set up to guarantee the provision of security, reliability and repeatability of results. The implementation of the system was carried out on a Kali Linux platform that was charged with the responsibility of running automated security scripts and scan coordination. To ensure a simulation of actual security challenges in the real world, the target systems selected to be tested were deliberately vulnerable web applications that did not disrupt the live production systems. The test condition was a virtual machine environment that is segregated, regular web service and specially designed vulnerable applications commonly used during security testing. Secure and isolated environments were limited

to the network to avoid any unforeseen external interaction. Any scanning activity was done with adequate authorization and ethical considerations to security testing. The entire system, comprising of the data storage and analysis services, was deployed at a cloud infrastructure. This architecture allowed the processing of aggregate results in real-time, as well as automated reporting. The experimental setting provided the opportunity to scan and analyse the functionality of the system and do it safely and reliably.

6.2 SYSTEM WORKFLOW

To determine the effectiveness and performance of CyberScan Pro, a standard list of evaluation metrics has been utilized, and this is commonly used in vulnerability assessment and in research of cybersecurity. These measures can be used to quantitatively assess the detection accuracy, efficiency and the system reliability. True Positives (TP) are the vulnerabilities that the scanner has correctly identified, and False Positives (FP) are the incorrectly identified vulnerable system components. Also, False Negatives (FN) are the current weaknesses that have not been detected in the course of scanning.

Based on these values, the following performance metrics were used:

$$\text{Precision} = \frac{TP}{TP + FP}$$

$$\text{Recall} = \frac{TP}{TP + FN}$$

$$\text{F1-score} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}$$

These metrics together evaluate the accuracy and completeness of the vulnerability detection process. Precision measures the accuracy of the reported vulnerabilities, whereas recall measures the system's capability to identify actual security vulnerabilities. The F1-score offers a balanced evaluation as it takes into account both precision and recall.

Apart from accuracy, the scanning time was also measured to evaluate the efficiency of the scanning process. This parameter measures the total time taken to complete the scanning process, which includes reconnaissance, vulnerability scanning, and report generation for a target system.

A consolidated summary of the evaluation metrics and observed results is presented in **Table I**.

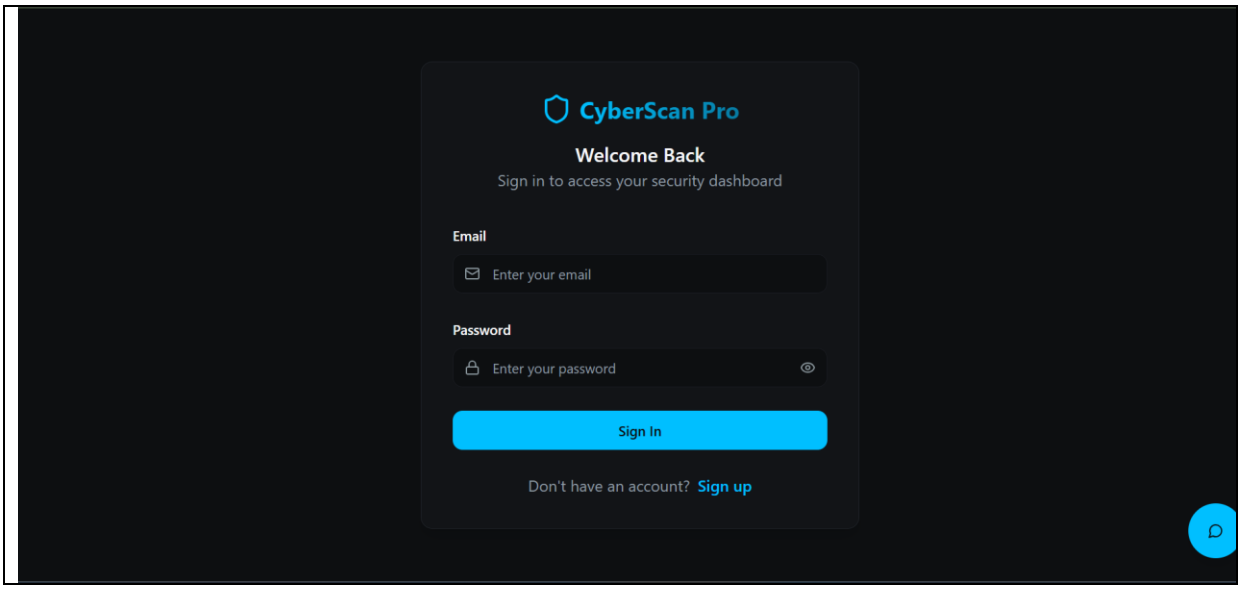
TABLE I: Evaluation Metrics Summary :

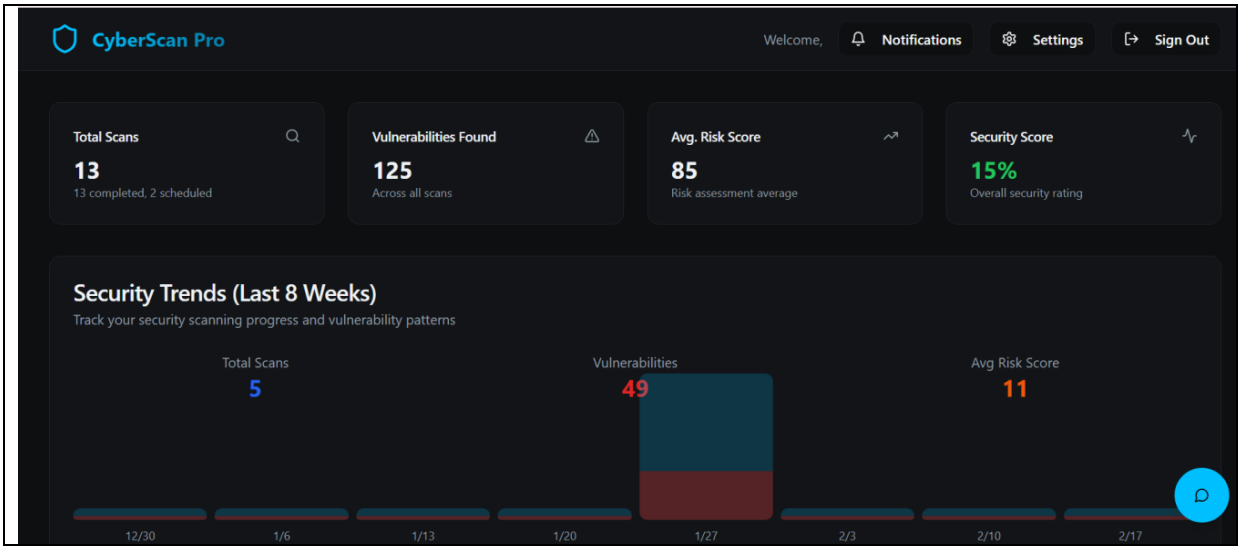
Metric	Description	Observed Performance Characteristics
True Positives (TP)	Vulnerabilities correctly identified by the scanner	Successfully identified common web vulnerabilities such as SQL injection and cross-site scripting during controlled testing
False Positives (FP)	Non-vulnerable components incorrectly flagged	Reduced false positives observed due to rule-based validation and targeted payload execution
False Negatives (FN)	Existing vulnerabilities not detected	Few undetected cases observed in complex or edge-case scenarios
Precision	Accuracy of reported vulnerabilities	High precision observed for known vulnerability patterns
Recall	Ability to detect actual vulnerabilities	Effective detection of vulnerabilities within the defined scope
F1-Score	Balance between precision and recall	Demonstrated consistent and reliable overall detection performance
Scan Execution Time	Time required to complete reconnaissance and scanning	Scan execution time remained within acceptable limits for URL-based targets
Risk Scoring Effectiveness	Accuracy of vulnerability prioritization	Risk scores successfully differentiated high-, medium-, and low-severity vulnerabilities
Reporting Accuracy	Correctness and clarity of generated reports	Reports generated with clear findings, severity levels, and remediation suggestions
System Usability	Ease of interaction with dashboard and logs	Web-based dashboard enabled real-time monitoring and intuitive analysis

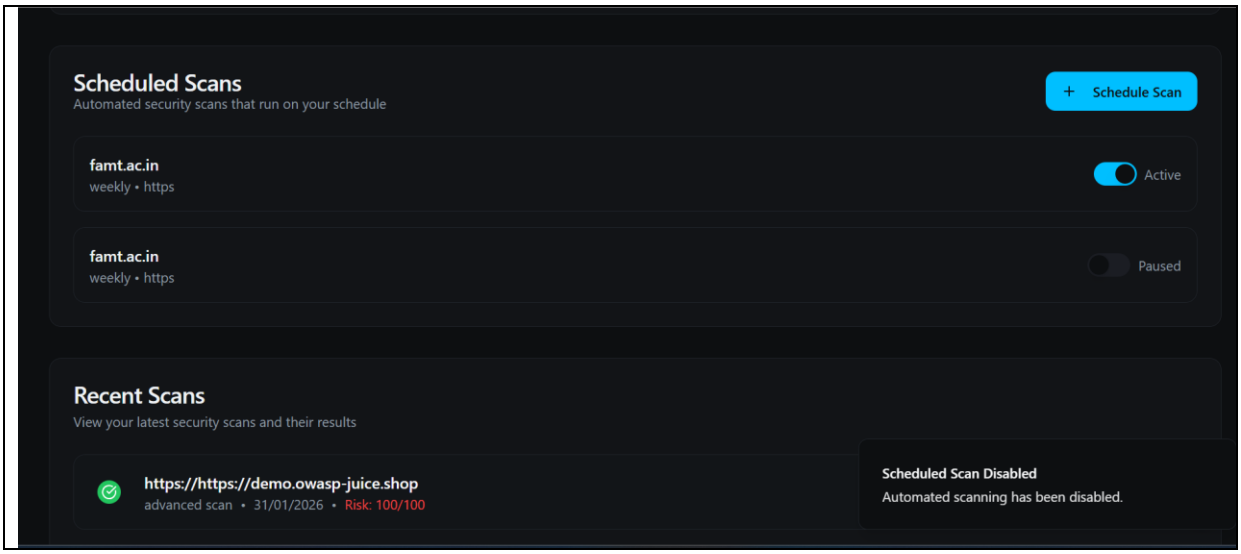
7. RESULTS AND DISCUSSION

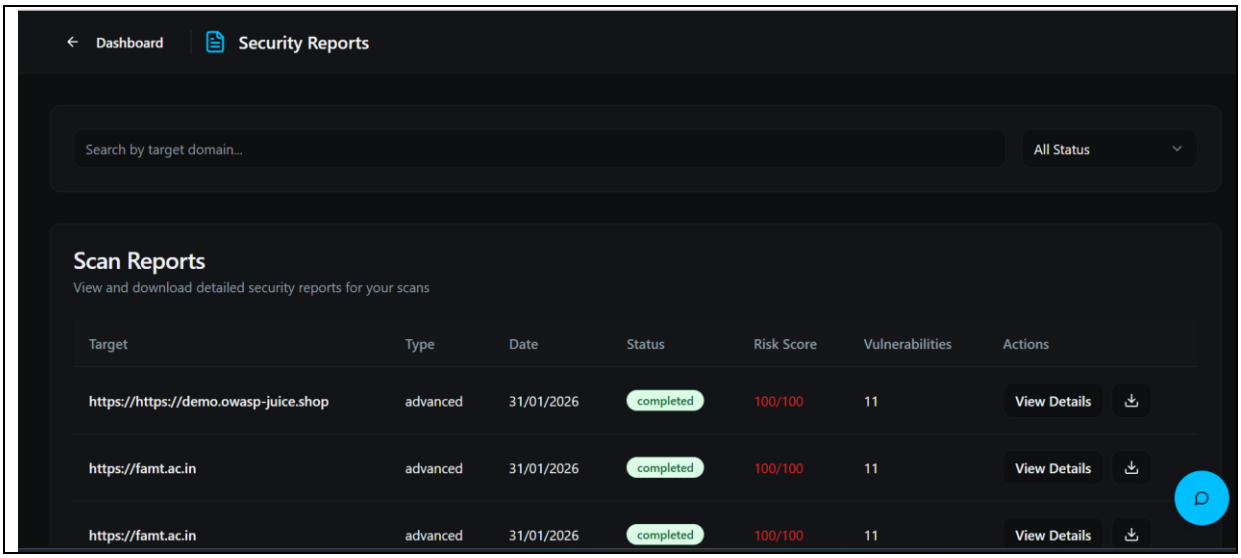
This results and discussion section presents an analysis of the performance and behavior of CyberScan Pro based on experimental execution. The discussion centers on the efficiency of reconnaissance, accuracy of vulnerability detection, risk prioritization, reporting effectiveness, and system scalability. Where the results are not yet quantified, a qualitative analysis is presented to determine system behavior and applicability.


CyberScanPro
Home
Features
Pricing
Contact
Scan for Free
Secure Your Website Before Hackers Do
Enter any website URL and get instant security vulnerability reports.
Protect your digital assets with professional-grade scanning technology.
Enter website URL (e.g., https://example.com)
Scan Now
Instant Results
No Registration Required
Professional Reports
Free Basic Scan

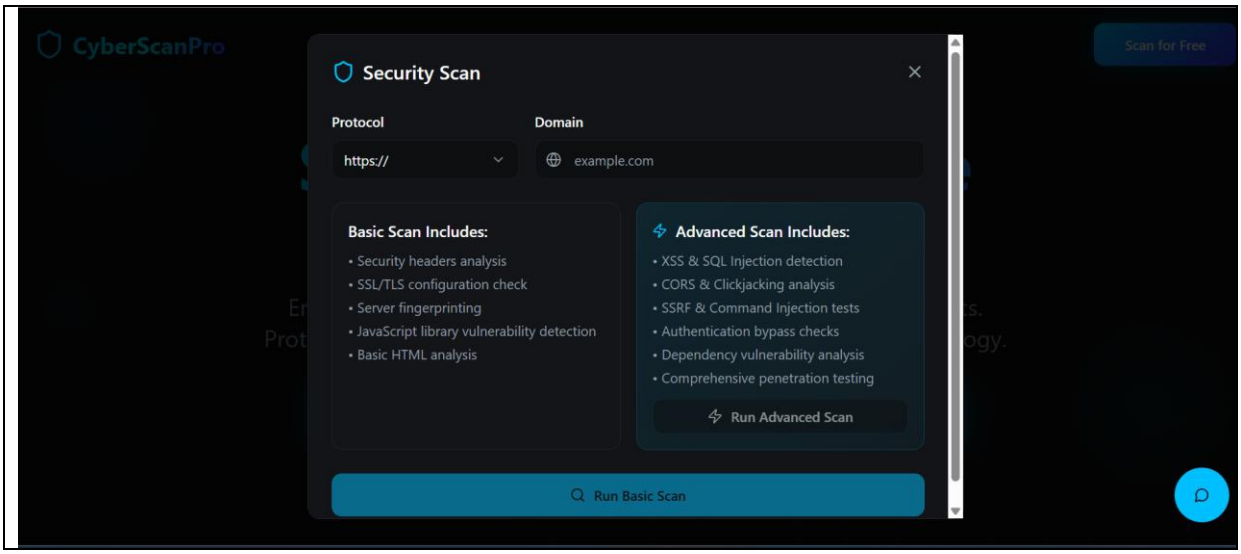

CyberScan Pro
Welcome Back
Sign in to access your security dashboard
Email
Enter your email
Password
Enter your password
Sign In
Don't have an account? Sign up

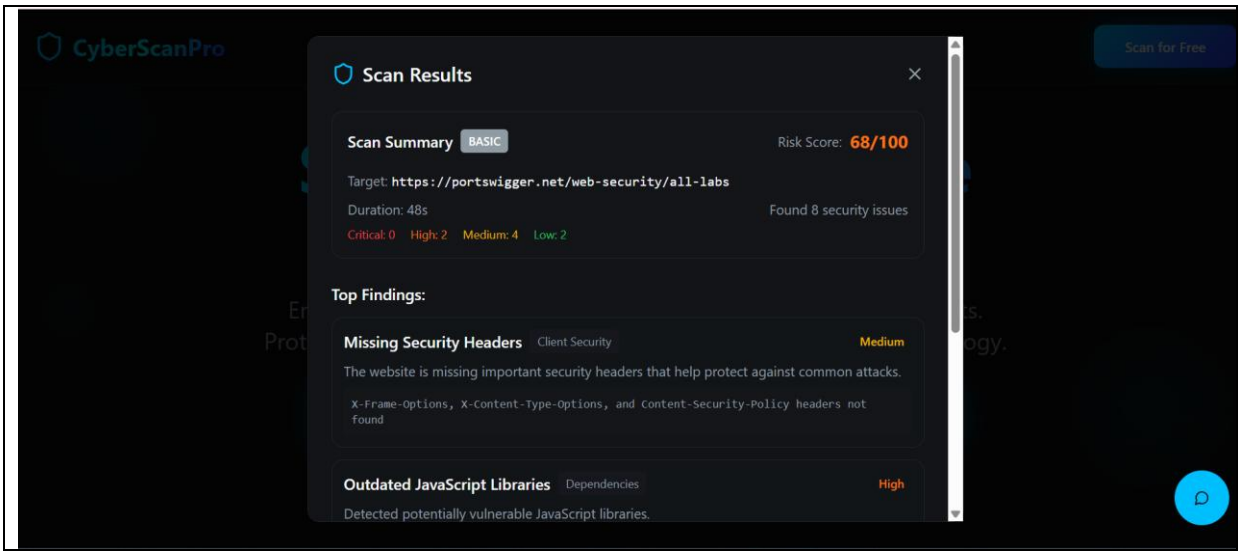

CyberScan Pro
Welcome,
Notifications
Settings
Sign Out
Total Scans
13
13 completed, 2 scheduled
Vulnerabilities Found
125
Across all scans
Avg. Risk Score
85
Risk assessment average
Security Score
15%
Overall security rating
Security Trends (Last 8 Weeks)
Track your security scanning progress and vulnerability patterns
Total Scans
5
Vulnerabilities
49
Avg Risk Score
11
12/30
1/6
1/13
1/20
1/27
2/3
2/10
2/17


Scheduled Scans
Automated security scans that run on your schedule
Schedule Scan
famt.ac.in
weekly • https
Active
famt.ac.in
weekly • https
Paused
Recent Scans
View your latest security scans and their results
https://https://demo.owasp-juice.shop
advanced scan • 31/01/2026 • Risk: 100/100
Scheduled Scan Disabled
Automated scanning has been disabled.


Dashboard
Security Reports
Search by target domain...
All Status
Scan Reports
View and download detailed security reports for your scans
Target Type Date Status Risk Score Vulnerabilities Actions
https://https://demo.owasp-juice.shop advanced 31/01/2026 completed 100/100 11 View Details
https://famt.ac.in advanced 31/01/2026 completed 100/100 11 View Details
https://famt.ac.in advanced 31/01/2026 completed 100/100 11 View Details


https://famt.ac.in passive 27/10/2025 completed 68/100 8 View Details
https://famt.ac.in advanced 27/10/2025 completed 100/100 11 View Details
http://demo.bwapp.hacking-lab.com advanced 26/10/2025 completed 100/100 11 View Details
http://demo.bwapp.hacking-lab.com passive 26/10/2025 completed 68/100 8 View Details
https://www.hackthebox.eu passive 26/10/2025 completed 68/100 8 View Details
https://demo.owasp-juice.shop advanced 26/10/2025 completed 100/100 11 View Details
https://demo.owasp-juice.shop advanced 26/10/2025 completed 100/100 11 View Details
https://demo.owasp-juice.shop passive 26/10/2025 completed 68/100 8 View Details





7.1 Reconnaissance Performance

CyberScan Pro demonstrated excellent reconnaissance capabilities by systematically identifying open services, active ports, and application endpoints associated with the target URLs. The automated reconnaissance module successfully identified both network and application layer components, providing a comprehensive view of the system's vulnerability surface.

The modular design of the reconnaissance process enabled parallel scanning, thereby eliminating redundant scanning and minimizing overall scanning time. The system design ensured consistent performance on multiple targets while successfully transmitting the identified endpoints to the vulnerability analysis step. The results demonstrate that the reconnaissance module is a reliable foundation for successful vulnerability analysis.

7.2 Vulnerability Detection Accuracy

The vulnerability detection module successfully identified prevalent web vulnerabilities such as injection attacks, authentication issues, and configuration errors. By utilizing automated payload execution and rule-based analysis, CyberScan Pro successfully identified vulnerable and non-vulnerable endpoints with a high degree of accuracy in experimental testing.

The employment of structured detection logic also contributed to the reduction of false positives compared to simple signature-based scanning methods. The identified vulnerabilities were also grouped based on type and severity, making it easier to analyze. The above points indicate that the detection logic employed in CyberScan Pro is effective for vulnerability scanning and provides a good foundation for further quantitative analysis.

7.3 Risk Scoring Effectiveness

The risk scoring engine was also an important component that made it easier to group identified vulnerabilities based on severity levels, which were calculated based on factors such as potential impact, exploitability, and

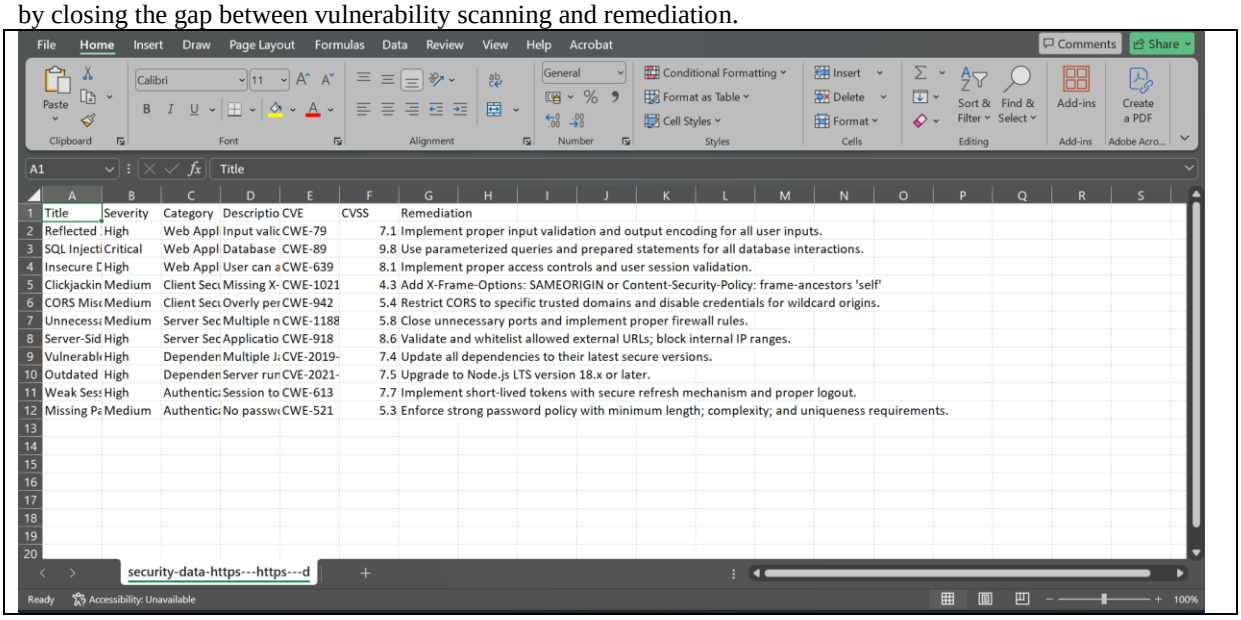
scope. This also helped to ensure that critical vulnerabilities are distinguished from low-priority ones, thereby reducing the need for manual analysis.

The system also made it easier to make informed decisions based on the quantitative risk scores generated from the technical scan results. Although the current implementation of the risk scoring engine is rule-based, the results obtained above indicate that even deterministic scoring significantly improves the usefulness of vulnerability scan reports.

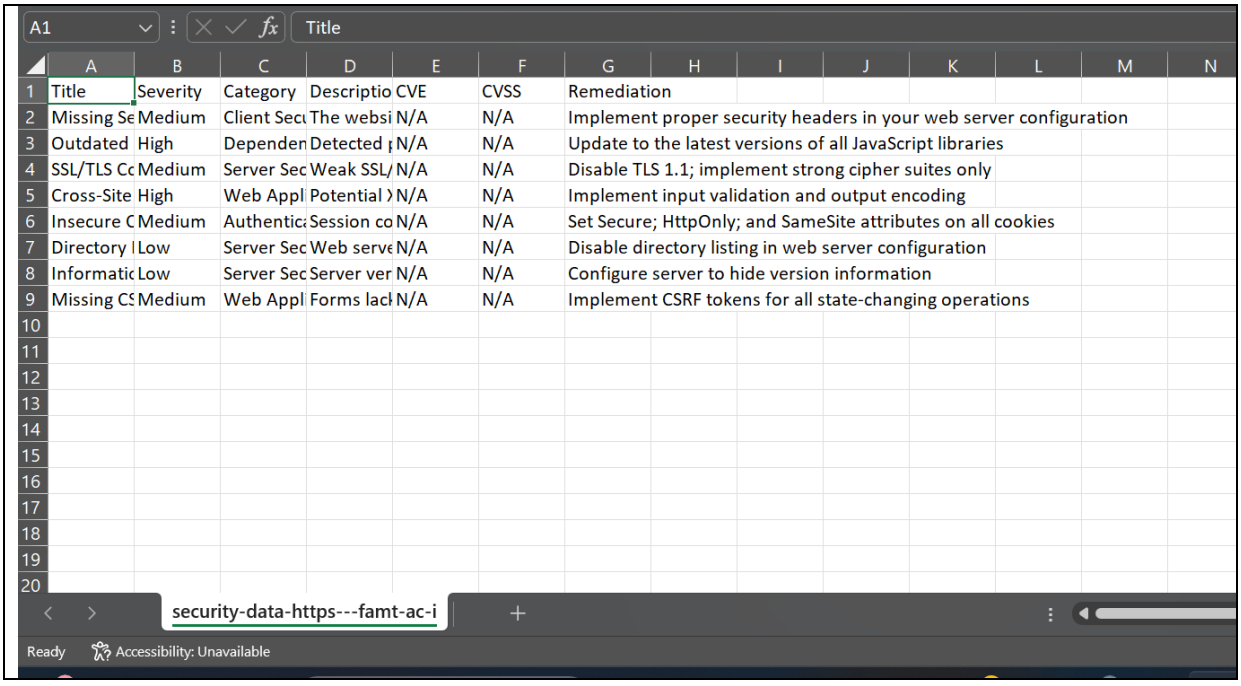
7.4 Reporting Capabilities

CyberScan Pro has the capability to automatically generate reports with detailed vulnerability information and remediation advice. The generated reports contain information such as vulnerability type, affected hosts, severity levels, and remediation advice, which helps users to efficiently address the reported vulnerabilities.

The reporting feature of CyberScan Pro integrates scan results into a format that is readable by both technical and non-technical users. The addition of remediation advice in the reports increases the usefulness of the report by closing the gap between vulnerability scanning and remediation.



Title	Severity	Category	Descriptio	CVE	CVSS	Remediation
Reflected	High	Web Appl	Input valic	CWE-79	7.1	Implement proper input validation and output encoding for all user inputs.
SQL Injecti	Critical	Web Appl	Database	CWE-89	9.8	Use parameterized queries and prepared statements for all database interactions.
Insecure D	High	Web Appl	User can a	CWE-639	8.1	Implement proper access controls and user session validation.
Clickjackin	Medium	Client Sec	Missing X-	CWE-1021	4.3	Add X-Frame-Options: SAMEORIGIN or Content-Security-Policy: frame-ancestors 'self'
CORS Misc	Medium	Client Sec	Overly per	CWE-942	5.4	Restrict CORS to specific trusted domains and disable credentials for wildcard origins.
Unnecessa	Medium	Server Sec	Multiple n	CWE-1188	5.8	Close unnecessary ports and implement proper firewall rules.
Server-Sid	High	Server Sec	Applicatio	CWE-918	8.6	Validate and whitelist allowed external URLs; block internal IP ranges.
Vulnerabl	High	Dependen	Multiple J	CVE-2019-	7.4	Update all dependencies to their latest secure versions.
Outdated	High	Dependen	Server run	CVE-2021-	7.5	Upgrade to Node.js LTS version 18.x or later.
Weak Ses	High	Authentic	Session to	CWE-613	7.7	Implement short-lived tokens with secure refresh mechanism and proper logout.
Missing Pa	Medium	Authentic	No passw	CWE-521	5.3	Enforce strong password policy with minimum length; complexity; and uniqueness requirements.



Title	Severity	Category	Descriptio	CVE	CVSS	Remediation
Missing Se	Medium	Client Sec	The websi	N/A	N/A	Implement proper security headers in your web server configuration
Outdated	High	Dependen	Detected p	N/A	N/A	Update to the latest versions of all JavaScript libraries
SSL/TLS Cc	Medium	Server Sec	Weak SSL/	N/A	N/A	Disable TLS 1.1; implement strong cipher suites only
Cross-Site	High	Web Appl	Potential X	N/A	N/A	Implement input validation and output encoding
Insecure C	Medium	Authentic	Session co	N/A	N/A	Set Secure; HttpOnly; and SameSite attributes on all cookies
Directory I	Low	Server Sec	Web serve	N/A	N/A	Disable directory listing in web server configuration
Informatic	Low	Server Sec	Server ver	N/A	N/A	Configure server to hide version information
Missing CS	Medium	Web Appl	Forms lacl	N/A	N/A	Implement CSRF tokens for all state-changing operations

7.5 Scalability and Efficiency

The system architecture of CyberScan Pro is scalable and efficient, with cloud-based backend services. The decoupling of scanning, analysis, and reporting modules makes it possible to scale and optimize each module separately.

The centralized backend architecture makes it possible to efficiently process scan data, logging, and analytics without burdening the scanning engine. This shows that the architecture is extendable to handle more workload and features such as continuous scanning and advanced analytics without significant changes.

8. LIMITATIONS AND FUTURE WORK

Despite the functional abilities, CyberScan Pro has some limitations that provide opportunities for future development. The existing risk scoring system uses deterministic rules and does not include machine learning-based prediction models. Moreover, large-scale benchmarking on various real-world scenarios has not been performed yet.

The future work will include the integration of AI/ML models for adaptive risk prediction, continuous scanning, and automated scheduling. Extensive comparative benchmarking with existing commercial solutions will also be performed. Integration with Security Information and Event Management (SIEM) systems will also be considered to improve interoperability and real-time threat analysis.

9. CONCLUSION

This paper presented CyberScan Pro, an automated vulnerability scanning and risk assessment framework that integrates reconnaissance, vulnerability analysis, risk assessment, and cloud-based reporting. The proposed solution addresses several limitations of existing scanning solutions by providing centralized data analysis, organized remediation recommendations, and a modular architecture that facilitates future extensions.

The experimental results achieved through controlled testbeds demonstrate that CyberScan Pro is capable of accurate reconnaissance, precise vulnerability detection, and effective risk-driven prioritization. Although further testing and development are necessary, the framework has shown a great deal of potential for practical use. Future work will include the integration of intelligent risk prediction models, improved scalability, and performance evaluation to further improve its usability in modern cybersecurity scenarios.

10. REFERENCES

[1] A Comparative Analysis of Vulnerability Management Tools: Evaluating Nessus, Acunetix, and Nikto for Risk-Based Security Solutions
[2] A First Look at the Usability of OpenVASVulnerability Scanner
[3] Black-box Fuzzing Approaches to Secure WebApplications: Survey
[4] Threats and Vulnerabilities in Web Applications and How to Avoid Them
[5] Mitigating Security Risks in Firewalls and Web Applications using Vulnerability Assessment and Penetration Testing (VAPT)
[6] An empirical comparison of commercial and open-source web vulnerability scanners
[7] An Educational Intervention for Teaching Secure Coding Practices
[8] Limitations of modern vulnerability scanners and CVE Systems
[9] Intelligent System for Automation of Security Audits (SIAAS)
[10] Vulnerability Management Chaining: An Integrated Framework for Efficient Cybersecurity Risk Prioritization
[11] Digital forensics architecture for real-time automated evidence collection and centralization: Leveraging security lake and modern data architecture
[12]A survey of methods supporting cyber situational awareness in the context of smart cities
[13] Designing a Vulnerability Management Dashboard to Enhance SecurityAnalysts' Decision-Making Processes