Stage- 1

Title of the project: Vulnerability Assessment for the elective portal of our organization

Overview:-

The goal of the project "Vulnerability Assessment for the Elective Portal of Nirma University" is to find, assess, and reduce security threats related to the portal used by students to choose their elective courses. In order to safeguard sensitive user data, uphold the integrity of the academic process, and guarantee portal dependability, this vital system—which enables teachers and students to register for and administer elective courses—needs to be secured. Pre-assessment planning outlines the project's goals, scope, and essential resources. Information on the portal's architecture and current security measures is then gathered. In order to find potential vulnerabilities and threats like SQL injection, cross-site scripting (XSS), faulty authentication, and others, thorough vulnerability scanning is carried out utilizing automated tools and manual testing. Prioritizing remedial activities is made possible by the analysis of discovered vulnerabilities to determine their risk levels based on exploitability, impact, and likelihood of occurrence. Each vulnerability is addressed in detail, with suggestions for code repairs, configuration adjustments, security policy updates, secure coding guidelines, and frequent security audits all included.

The project aims to improve the security of the portal, lower the chance of a data breach, and encourage secure coding methods by ensuring compliance with cybersecurity standards such as the OWASP principles. Reporting and documentation gather information and highlight important concerns and suggested solutions into a thorough report with an executive summary for university stakeholders. In the end, this project aims to develop a more dependable and safe platform for Nirma University's elective course management, encouraging user trust and preserving the integrity and availability of the system.

List of teammates:

Sr. No.	Name	Collage	Contact
1	Dr Vijay Ukani	Institute of Technology, Nirma University	vijay.ukani@nirmauni.ac.in
2.	Dr Priyank Thakkar	Institute of Technology, Nirma University	priyank.thakkar@nirmauni.ac.in
3.	Dr Jai Prakash Verma	Institute of Technology, Nirma University	jaiprakash.verma@nirmauni.ac.in
4.	Dr Aashka Raval	School of Technology, Pandit Deendayal Energy University	aashkawork16@gmail.com

List of Vulnerability Table:

Sr. No.	Vulnerability Name	CWE No.
1	SQL Injection	CWE-89
2	Buffer Overflow	CWE-120
3	Cross-Site Scripting (XSS)	CWE-79
4	Command Injection	CWE-77
5	Insecure Deserialization	CWE-502
6	Path Traversal	CWE-22
7	XML External Entity (XXE)	CWE-611

8	Cross-Site Request Forgery (CSRF)	CWE-352
9	Broken Access Control	CWE-284
10	Sensitive Data Exposure	CWE-200
11	Hard-coded Passwords	CWE-798
12	Improper Authentication	CWE-287
13	Security Misconfiguration	CWE-933
14	Improper Input Validation	CWE-20
15	Using Components with Known Vulnerabilities	CWE-1104
16	Insecure Cryptographic Storage	CWE-311
17	Unrestricted File Upload	CWE-434
18	Improper Error Handling	CWE-388
19	Insufficient Logging & Monitoring	CWE-778
20	Directory Listing	CWE-548

REPORT:

Sr No	Vulnerability Name	CWE No	OWASP/SANS Category	Description	Business Impact
1	SQL Injection	CWE-89	OWASP Top 10 - Injection, SANS Top 25 - Porous Defenses	Allows attackers to manipulate a query by injecting arbitrary SQL code.	Can lead to unauthorized access, data breaches, or data loss. High risk to data confidentiality.
2	Buffer Overflow	CWE-120	SANS Top 25 - Risky Resource Management	Occurs when more data is written to a buffer than it can hold.	Can lead to system crashes and arbitrary code execution. Significant risk to system stability.
3	Cross-Site Scripting (XSS)	CWE-79	OWASP Top 10 - XSS, SANS Top 25 - Porous Defenses	Allows attackers to inject malicious scripts into web pages.	Can lead to data theft and session hijacking. High risk to user data confidentiality.
4	Command Injection	CWE-77	OWASP Top 10 - Injection, SANS Top 25 - Porous Defenses	Enables attackers to execute arbitrary commands on the host OS.	Can lead to full system compromise and unauthorized data access.

					High risk to system integrity.
5	Insecure Deserialization	CWE-502	OWASP Top 10 - Deserialization, SANS Top 25 - Porous Defenses	Untrusted data used to abuse application logic or execute arbitrary code.	Can lead to remote code execution and privilege escalation. High risk to application security.
6	Path Traversal	CWE-22	OWASP Top 10 - Injection, SANS Top 25 - Porous Defenses	Allows access to files and directories stored outside the web root folder.	Can lead to unauthorized file access and sensitive information leakage. Moderate to high risk.
7	XML External Entity (XXE)	CWE-611	OWASP Top 10 - XXE, SANS Top 25 - Risky Resource Management	Occurs when XML input contains a reference to an external entity.	Can lead to data exfiltration and denial of service. Moderate to high risk to system integrity.
8	Cross-Site Request Forgery (CSRF)	CWE-352	OWASP Top 10 - CSRF, SANS Top 25 - Insecure Interaction Between Components	Tricks a user into submitting a malicious request.	Can lead to unauthorized transactions and account compromise. Moderate risk to user data.

9	Broken Access Control	CWE-284	OWASP Top 10 - Broken Access Control, SANS Top 25 - Porous Defenses	Users can perform actions outside their intended permissions.	Can lead to unauthorized access to data and functionality. High risk to data confidentiality.
10	Sensitive Data Exposure	CWE-200	OWASP Top 10 - Sensitive Data Exposure, SANS Top 25 - Risky Resource Management	Sensitive data is not adequately protected.	Can lead to data breaches and legal implications. High risk to data confidentiality.
11	Hard-coded Passwords	CWE-798	SANS Top 25 - Porous Defenses	Involves embedding passwords directly into the source code.	Can lead to unauthorized access if passwords are discovered. High risk to system security.
12	Improper Authentication	CWE-287	OWASP Top 10 - Broken Authentication, SANS Top 25 - Porous Defenses	Application fails to correctly verify user identity.	Can lead to unauthorized access and privilege escalation. High risk to system integrity.
13	Security Misconfiguration	CWE-933	OWASP Top 10 - Security Misconfiguration, SANS Top 25 - Risky	Occurs due to default settings or incomplete configurations.	Can lead to unauthorized access and exposure of sensitive data.

			Resource Management		High risk to system integrity.
14	Insecure Cryptographic Storage	CWE-311	OWASP Top 10 - Sensitive Data Exposure, SANS Top 25 - Risky Resource Management	Sensitive data is inadequately encrypted or stored insecurely.	Can lead to data breaches and loss of confidentiality. High risk to sensitive information.
15	Improper Input Validation	CWE-20	OWASP Top 10 - Injection, SANS Top 25 - Risky Resource Management	Application fails to validate input properly, leading to various attacks.	Can lead to unauthorized actions and data corruption. Moderate to high risk to data integrity.
16	Unrestricted File Upload	CWE-434	OWASP Top 10 - Security Misconfiguration, SANS Top 25 - Risky Resource Management	Allows uploading of files without proper restrictions.	Can lead to code execution and server compromise. High risk to system integrity.
17	Directory Listing	CWE-548	SANS Top 25 - Insufficient Security Measures	Exposes a directory structure that can reveal sensitive files.	Can lead to unauthorized information disclosure. Moderate risk to data confidentiality.

18	Hard-coded Passwords	CWE-798	SANS Top 25 - Porous Defenses	Embedding passwords directly into code.	Can lead to unauthorized access. High risk to system security.
19	Improper Error Handling	CWE-388	SANS Top 25 - Insufficient Security Measures	Application does not handle errors securely, revealing sensitive info.	Can lead to information disclosure and exploitation opportunities. Moderate risk to system security.
20	Insufficient Logging & Monitoring	CWE-778	OWASP Top 10 - Insufficient Logging & Monitoring, SANS Top 25 - Insufficient Security Measures	Lack of adequate logging and monitoring of security events.	Can hinder detection and response to incidents, increasing risk exposure. High risk to incident response.

—--------------------- this is stage 1 where we understand web application testing —--- we take help from OWASP top 10 understand them :-----------------------------

Stage 2

Overview :-

- **What you understood about nessus**

Nessus is a powerful and popular vulnerability assessment tool made to assist cybersecurity experts in locating, evaluating, and controlling security threats in IT environments. Nessus, created by Tenable, is mostly used to scan networks, systems, and apps for security holes that could be exploited by hackers. Nessus's goal is to improve an organization's security posture by spotting any vulnerabilities early on and fixing them to prevent attacks.

Nessus's broad support for a variety of operating systems, hardware, and apps makes it extremely adaptable for various IT infrastructures, which is one of its main advantages. The program promises to be able to identify the most recent security dangers thanks to its often updated database of vulnerabilities. Nessus creates thorough reports with insightful details and remediation recommendations that are actionable, assisting organizations in efficiently prioritizing and addressing security issues. Even people with little technical knowledge may easily and efficiently complete the scanning process because to its automated features and user-friendly interface. Nessus can also be incorporated into more comprehensive security procedures and frameworks, which improves an organization's overall security approach.

Nessus is not without limitations, though. Although it works well for locating vulnerabilities that are already known, it might not be as good at finding advanced persistent threats (APTs) or zero-day vulnerabilities, which call for more complex detection methods. Nessus also needs to be updated and maintained on a regular basis to ensure that it continues to function effectively, which might be resource-intensive for certain enterprises. Additionally, the tool depends on precise setups and network access, both of which might be difficult in environments that are extremely complicated or divided.

Network scanning, vulnerability detection, compliance audits, and configuration assessment are just a few of the many functions that Nessus provides. Its extensive plugin library expands its capabilities and allows it to perform customized checks based on various requirements and circumstances. Nessus offers thorough vulnerability evaluations that identify problems including out-of-date software, weak passwords, open ports, and incorrect setups. It also has functions for planning recurring evaluations, automating scans, and interacting with other security platforms and technologies.

In conclusion, Nessus is a crucial tool for proactive cybersecurity management since it provides a thorough and approachable way to find and fix security flaws. Although it has several drawbacks, its benefits and functionality make it an invaluable tool for businesses looking to safeguard their IT infrastructure against any attacks.

Target website: https://nuweb.nirmauni.ac.in/OE

Target ip address: 202.131.110.6

List of vulnerability:

Sr. No.	Vulnerability Name	Severity	OWASP ZAP
1	SQL Injection - MySQL	High	40019
2	CSRF TOKENS	Medium	3501
3	HTTP and HTTPS insecure transition in FORM (POST METHOD)	Medium	1901
4	Missing Anti Clickjacking Header	Medium	1721
5	Vulnerable JS Library	Medium	11

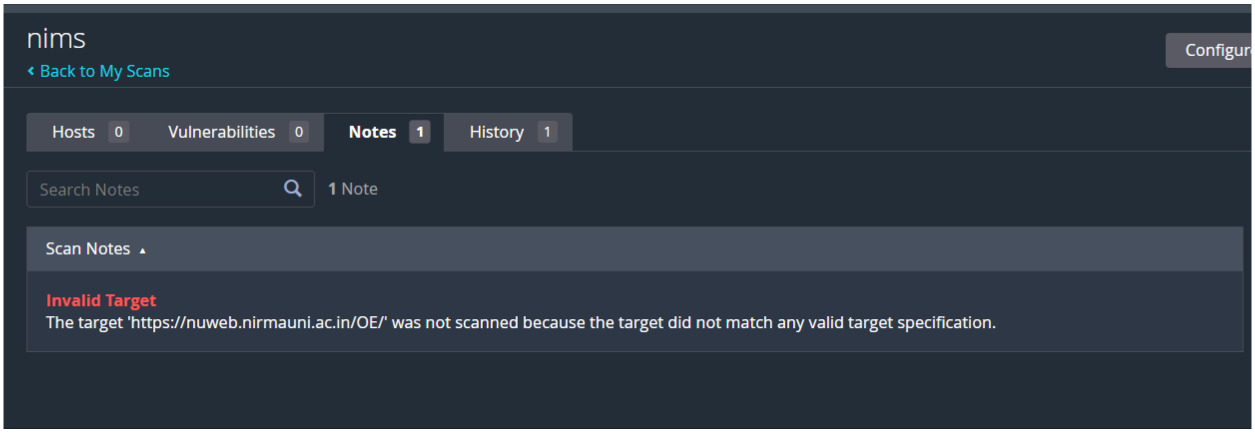
6	**Cookie without SameSite Attribute**	**Medium**	**3**
7	**Hidden File Found**	**Medium**	**4**
8	**Application Error Disclosure**	**Medium**	**90022**
9	**Cookie without SameSite Attribute**	**Medium**	**1275**
10	**Cross Domain Script Disclosure**	**Medium**	**10095**

REPORT:-

ATTACHING OWASP ZAP rapport & SS of Nessus Not accepting the URL

Report:
https://drive.google.com/file/d/10mxbUoPfpdgAi_ZX_2JmnZFaZ4dZyx0b/view?usp=drive_link

SS:



Invalid Target
The target 'https://nuweb.nirmauni.ac.in/OE/' was not scanned because the target did not match any valid target specification.

Stage 3

Report

Title: Leveraging Machine Learning for Threat Detection in SIEM Systems

Below are side headings we need to write at least a paragraph for each what we understood from each topic:

Security Operations Center (SOC):

An organization's centralized entity in charge of tracking, identifying, and handling cybersecurity issues is called a Security Operations Center (SOC). It integrates technology, people, and procedures to guarantee ongoing security monitoring and defense against possible attacks. The Security Operations Center (SOC) functions continuously, employing cutting-edge instruments like Security Information and Event Management (SIEM) systems to evaluate security data, detect weaknesses, and react to occurrences instantaneously. An organization's entire security posture and resilience against evolving cyber threats are maintained in large part by the SOC, which facilitates coordination amongst cybersecurity analysts, threat hunters, and incident responders.

SOC Cycle:

A continuous loop of procedures intended to provide reliable cybersecurity makes up the SOC cycle. Security analysts start by monitoring the network traffic, logs, and alerts produced by different security tools. Detection then entails finding possible threats or anomalies that might point to a security incident. The SOC begins an investigation as soon as a threat is identified, examining the incident's circumstances and level of intensity while compiling data to comprehend its consequences. Following containment and remediation of the threat, the SOC team responds to minimize damage and resume regular operations. Finally, the cycle concludes with post-incident analysis, which involves reviewing the incident response to identify lessons learned and improve future security measures, ensuring the SOC remains adaptive and resilient against emerging threats. This cyclical approach fosters continuous improvement.

SIEM:

A key component of contemporary cybersecurity strategies is Security Information and Event Management (SIEM), which gives businesses real-time visibility into their security posture. SIEM systems enable the detection of anomalies and possible threats by aggregating and analyzing log data from a variety of sources, including servers, network devices, and applications. Security teams can detect potentially malicious activity by identifying patterns through the use of SIEM tools, which enable advanced threat detection and incident response by relating events across multiple systems. SIEM solutions also help organizations stay compliant with regulations while improving their overall security framework by providing insightful data for forensic investigations and compliance reporting. SIEM's powerful analytics and ongoing monitoring enable Security Operations Centers (SOCs) to proactively manage and reduce cybersecurity threats.

SIEM Cycle:

The SIEM cycle is an ongoing procedure created to improve an organization's data management and analysis capabilities and security posture. Data collection is the first step, during which log and event data are obtained from multiple sources, including servers, firewalls, and applications. Normalization comes next, standardizing the data format to make analysis simpler. The SIEM system examines the gathered data to find patterns and relationships that might point to possible security risks in the event correlation phase, which comes next. Alerting produces notifications when threats are identified so that security teams can look into them more. After that, incident response entails acting in accordance with the conclusions, potentially containing or eliminating the threat. Finally, the cycle concludes with reporting and analysis, where insights are generated to refine security strategies and improve overall incident response processes. This cyclical approach ensures that organizations remain vigilant and adaptive to evolving cyber threats.

MISP:

MISP (Malware Information Sharing Platform & Threat Sharing) is an open-source software solution designed to facilitate the sharing, storing, and correlation of structured threat information. Organizations, security teams, and threat intelligence analysts utilize it extensively to increase their defensive capabilities and gain a better understanding of cyber threats. Indicators of compromise (IOCs), malware, vulnerabilities, and other cyber threat intelligence (CTI) can be collaboratively exchanged via MISP, which helps users identify, stop, and respond to cyberattacks more skillfully. Because of its features—which include automated data ingestion, extensive correlation capabilities, and compatibility with a wide range of security products and standards—it is an essential part of contemporary cybersecurity tactics.

Our Organization network information:

There are several buildings/departments in our organization. All buildings are interconnected by fiber optic cables to central switch which in turn is connected to Internet through a router and firewall. All incoming and outgoing traffic is routed through the firewall. Logically the network is divided into several VLANs for different sections of the network.

How do you think you deploy SOC in your organization:

Since the network has centralized controller we can have a centralized SOC with physical setup being done on a designated workstation. The SOC will deployed for threat detection and incidence response. An appropriate SIEM platform will be chosen for log collection, correlation, and analysis. An IDS/IPS will be implemented to monitor network traffic for suspicious activities. Network perimeter security is already ensured with firewalls and web proxies.

Threat intelligence:

Threat intelligence, often referred to as cyber threat intelligence (CTI), is the process of gathering, analyzing, and disseminating information about potential or current threats to an organization's information systems and networks. This intelligence is crucial for understanding the tactics, techniques, and procedures (TTPs) used by adversaries, helping organizations to anticipate, prevent, and respond to cyber attacks. CTI includes data on threat actors, their motivations, capabilities, and indicators of compromise (IOCs) such as malicious IP addresses, domain names, and file hashes. By leveraging threat intelligence, organizations can enhance their cybersecurity posture, make informed decisions, and implement proactive measures to mitigate risks and protect their assets.

Incident response:

An organized method for dealing with and overseeing the fallout from a cyberattack or security breach is called incident response, or IR. Its main objective is to effectively handle the crisis in order to minimize expenses and damages to a business, limit damage, and shorten the recovery period. Preparation, detection and analysis, containment, eradication, recovery, and post-incident actions are usually included in the process. Organizations set up guidelines, practices, and resources for efficient incident handling throughout preparedness. Identification and comprehension of the incident's extent and effects are necessary for both detection and analysis. Eradication is the process of eliminating the threat from the environment, whereas containment tries to separate impacted systems in order to stop additional harm. Restoring regular operations and services is the main goal of recovery.

Qradar & understanding about tool:

QRadar is a robust Security Information and Event Management (SIEM) solution by IBM. It is designed to help organizations detect, prioritize, and respond to security threats. Its capable of

Log Management, Threat Detection, Incident Response, Compliance Management and Network Traffic Analysis. Overall, IBM QRadar is a versatile SIEM solution that provides organizations with the tools and insights needed to protect their assets, detect and respond to threats, and maintain compliance with industry regulations.

Conclusion:

We recognize our role in the organization's security posture, understanding that cybersecurity is not solely the responsibility of IT departments but a collective effort of each individual. Key lessons learned from the training program include identifying and mitigating common threats, implementing best practices for secure password management, recognizing phishing attempts, and responding to security incidents effectively. Also, we understood the usage of modern security tools and platforms available for the detection and mitigation of cyber threats. We believe this training should instill a culture of security awareness, urging continuous learning and adaptation to new threats.

Stage 1: What you understand from Web application testing?

Web application testing focuses on identifying and mitigating vulnerabilities that could be exploited by attackers. The key aspects include:

1. Vulnerability Scanning: This involves using automated tools to scan the web application for known vulnerabilities such as SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF), and other common security flaws. These tools help identify potential weak points that could be exploited.
2. Penetration Testing: Also known as ethical hacking, penetration testing involves simulating attacks on the web application to identify security weaknesses. Security experts attempt to exploit vulnerabilities to understand their impact and determine how they can be fixed.
3. Authentication Testing: This ensures that the authentication mechanisms of the web application are robust. It involves testing the login process, password policies, multi-factor authentication (MFA), and other controls to prevent unauthorized access.
4. Authorization Testing: This verifies that users have appropriate access levels and cannot perform actions or access data beyond their permissions. It involves testing role-based access controls (RBAC) and ensuring proper segregation of duties.
5. Input Validation: This ensures that all user inputs are properly validated and sanitized to prevent injection attacks. It involves testing input fields, forms, and other data entry points to ensure they are protected against malicious input.
6. Data Protection: This involves testing how the web application handles sensitive data, such as personal information and payment details. It ensures that data is encrypted both in transit and at rest, and that proper data handling and storage practices are followed.

7. Security Configuration: This involves reviewing and testing the security configurations of the web application, web server, and database. It ensures that default settings are changed, unnecessary services are disabled, and best practices are followed for security settings.

Stage 2: What you understand from the nessus report?

A Nessus report is a detailed document generated by the Nessus vulnerability scanner, which provides insights into the security posture of a network or system. The report includes various sections and information that help security professionals identify, assess, and prioritize vulnerabilities.

Stage 3: What you understand from SOC / SEIM / Qradar Dashboard?

Following are some of our understanding from SOC/SIEM/QRadar:

1. SOC Fundamentals: SOC plays the role as the central hub for monitoring, detecting, and responding to cybersecurity incidents. It highlights the importance of a well-coordinated team that utilizes various tools and processes to maintain an organization's security posture.
2. SIEM Capabilities: SIEM systems, such as QRadar performs the critical function in aggregating and analyzing log data from multiple sources. They are essential for identifying and correlating security events to detect potential threats, providing a comprehensive view of the security landscape.
3. QRadar Dashboard Proficiency: QRadar dashboard has interface, provision for data visualizations, and features for threat detection and incident response. Important components include real-time monitoring, alerts, and detailed reports on security incidents and network activity. QRadar also generates compliance reports and maintains adherence to regulatory requirements.

Future Scope:

Stage 1: Future scope of web application testing

The future scope of web application testing is expected to evolve significantly due to advancements in technology, changes in user expectations, and emerging security threats. AI and Machine Learning will be key in enhancing automation testing by predicting potential issues, optimizing test cases, and improving test coverage.

Stage 2: Future scope of the testing process you understood.

The web application security testing process involves identifying and addressing potential security vulnerabilities to ensure that the application is secure against various threats. The future of web application security testing is expected to be shaped by advancements in technology, evolving security threats, and the increasing complexity of web applications.

Stage 3: Future scope of SOC/SEIM

Future Scope of SOC and SIEM is expansive and promising, driven by evolving and ever-growing cyber threats.

Advanced Threat Detection: As cyber threats become more sophisticated, SOCs and SIEMs will increasingly rely on artificial intelligence (AI) and machine learning (ML) to detect advanced persistent threats (APTs) and zero-day vulnerabilities. These technologies will enable more accurate anomaly detection and predictive analytics.

Integration with Threat Intelligence: Future SOCs and SIEMs will integrate more seamlessly with threat intelligence platforms, providing real-time updates on emerging threats and enabling quicker, more informed responses. This will involve automated ingestion of threat feeds and enhanced correlation capabilities.

Cloud Security: With the increasing adoption of cloud services, SOCs and SIEMs will need to evolve to monitor and secure cloud environments effectively. This includes managing hybrid and multi-cloud infrastructures and ensuring compliance with various cloud security standards.

IoT Security: As the Internet of Things (IoT) become more integrated into business operations, SOCs and SIEMs will need to extend their monitoring and protection to these devices, which often have unique security challenges.

Topics explored :

Cyber Security as a whole, types of hackers, vulnerabilities and its types, Threat intelligence, SOC/SIEM

Tools explored:

Nmap, Nessus, Nikto, MetaSploit, Wireshark, BurpSuite, QRadar

—--------THE END —---------------