Project Report – Stage 1

Testing of Website for Protection from SQL Injection Attacks

Team: Cyber Defender

12 July, 2024

The "Cyber Defender" project seeks to explore the complex realm of cybersecurity, emphasizing the detection, analysis, and mitigation of prevalent vulnerabilities. As cyber threats grow more advanced, the need for strong security protocols is more critical than ever. This project aims to educate and arm participants with the essential skills and knowledge to protect digital assets effectively.

Project Objectives

1. **Identify Common Vulnerabilities:**
    - The project will begin with a comprehensive analysis of prevalent vulnerabilities as listed in the OWASP Top 10. These include Broken Access Control, Cryptographic Failures, Injection, Insecure Design, SecurityMisconfiguration, and others.
2. **Analyze Impact and Mechanisms:**
    - Each identified vulnerability will be scrutinized to understand its mechanism, the potential impact on systems, and the ways it can be exploited by malicious actors. This analysis will include both technical and business perspectives, highlighting the significance of each vulnerability.
3. **Develop Mitigation Strategies:**
    - Participants will explore and develop effective strategies to mitigate these vulnerabilities. This will encompass both preventive measures and reactive solutions, ensuring a well-rounded approach to cyber security.
4. **Collaborative Learning:**
    - The project will foster a collaborative environment where participants from various institutions will work together. Sharing insights and strategies will enhance the collective understanding and lead to more robust security solutions.

List of Teammates:

#	Name	Collage	Contact
1	Hemang Chath	Darshan University	hemang.chath@darshan.ac.in
2	Saurin Parikh	Nirma University	saurin.parikh@nirmauni.ac.in
3	Vrajesh Chawra	Nirma University	vrajesh.chawra@nirmauni.ac.in
4	Sumedha Arora	Nirma University	sumedha.arora@nirmauni.ac.in

List of Vulnerabilities:

#	Vulnerability Name	CWE - No
1	**A01:2021** Broken Access Control	**CWE-1345:** Broken Access Control: Weaknesses in OWASP
2	**A02:2021** Cryptographic Failures	**CWE-259:** Use of Hard-coded Password
3	**A03:2021** SQL Injection	**CWE-20:** Improper Input Validation
4	**A04:2021** Insecure Design	**CWE-213:** Exposure of Sensitive Information Due to Incompatible Policies
5	**A05:2021** Security Misconfiguration	**CWE-756:** Missing Custom Error Page
6	**A06:2021** Vulnerable and Outdated Components	**CWE-1104:** Use of Unmaintained Third Party Components
7	**A07:2021** Identification and Authentication Failures	**CWE-287:** Improper Authentication
8	**A08:2021** Software and Data Integrity Failures	**CWE-830:** Inclusion of Web Functionality from an Untrusted Source
9	**A09:2021** Security Logging and Monitoring Failures	**CWE-778:** Insufficient Logging
10	**A10:2021** Server-Side Request Forgery	**CWE-918:** Server-Side Request Forgery (SSRF)

Report

Vulnerability Name	**A01:2021-SQL Injection**
CWE	CWE-20: SQL Injection: Improper Input Validation
OWASP/SANS Category	A01:2021-SQL Injection

Description

The product constructs all or part of an SQL command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended SQL command when it is sent to a downstream component.

Summary Table of Business Impact

Impact Area	Description
Financial Losses	Direct theft, legal fines, and incident response costs
Reputational Damage	Loss of customer trust, brand damage, and negative media coverage
Operational Disruption	Service downtime, data integrity issues, and operational challenges
Strategic Impact	Competitive disadvantage and regulatory compliance challenges
Legal Repercussions	Lawsuits, legal fees, and potential settlements
Long-term Costs	Increased security costs and impact on business relationships

Script

```
string userName = ctx.getAuthenticatedUserName();

string query = "SELECT * FROM items WHERE owner = '" + userName + "' AND
itemname = '" + ItemName.Text + "'";

sda = new SqlDataAdapter(query, conn);

DataTable dt = new DataTable();

sda.Fill(dt);
```

Project Report Stage 2

Nessus: Comprehensive Vulnerability Assessment

Team: Cyber Defender

12 July, 2024

Overview

What is Nessus?

Nessus is a powerful and widely-used vulnerability assessment tool developed by Tenable, Inc. It helps organizations identify, manage, and remediate security vulnerabilities within their IT environments. Designed for both small businesses and large enterprises, Nessus provides in-depth scanning capabilities to protect against potential threats and compliance issues.

Key Features

1. **Comprehensive Vulnerability Scanning**
    - **Deep Insight:** Nessus performs extensive vulnerability scans, detecting a wide range of security issues, including missing patches, misconfigurations, and potential exploit vulnerabilities.
    - **Regular Updates:** The tool's plugin-based architecture allows it to receive frequent updates, ensuring it identifies the latest vulnerabilities and emerging threats.
2. **User-Friendly Interface**
    - **Intuitive Dashboard:** Nessus features a user-friendly web-based interface that simplifies scan configuration, result analysis, and report generation.
    - **Customizable Scans:** Users can easily set up and schedule scans, choose specific targets, and customize scan policies to fit unique security needs.
3. **Detailed Reporting and Analysis**
    - **Comprehensive Reports:** Nessus provides detailed reports with clear descriptions of vulnerabilities, potential impacts, and remediation steps.
    - **Export Options:** Reports can be exported in various formats (PDF, CSV, HTML) for easy sharing and integration with other security tools.
4. **Advanced Detection Capabilities**
    - **Plugin Framework:** Nessus uses a plugin-based framework where each plugin is designed to detect specific vulnerabilities. This modular approach allows for scalable and versatile scanning.
    - **Network Discovery:** It offers network discovery features such as identifying open ports, services, and system configurations, which help in assessing security postures.
5. **Compliance and Auditing**
    - **Standards Compliance:** Nessus supports compliance checks for various standards and regulations like PCI-DSS, HIPAA, and ISO 27001, helping organizations meet regulatory requirements.

Benefits

1. **Enhanced Security Posture**
   - By identifying vulnerabilities and weaknesses, Nessus enables proactive measures to strengthen security defences and protect against cyber threats.
2. **Cost-Effective Solution**
   - Nessus provides a robust vulnerability assessment tool at a competitive price point, making it accessible for both small businesses and large enterprises.
3. **Efficient Vulnerability Management**
   - Regular scans and comprehensive reports help streamline the vulnerability management process, making it easier to prioritize and address issues.
4. **Improved Compliance**
   - Nessus helps organizations achieve and maintain compliance with security standards and regulations, reducing the risk of non-compliance penalties.

Use Cases

1. **Vulnerability Assessment**
   - Regular scanning for vulnerabilities in network devices, applications, and systems to identify potential risks.
2. **Penetration Testing**
   - Assists penetration testers in identifying vulnerabilities that could be exploited in simulated attacks.
3. **Security Audits**
   - Provides detailed information for security audits and helps organizations align with industry regulations and standards.
4. **Patch Management**
   - Helps in identifying missing patches and vulnerabilities that need to be addressed in the patch management process.

Conclusion

Nessus is a versatile and effective tool for vulnerability assessment, offering deep scanning capabilities, user-friendly features, and comprehensive reporting. Whether for regular vulnerability assessments, penetration testing, or compliance checks, Nessus is a valuable asset for maintaining a secure IT environment and managing security risks.

Target Website	http://www.jaduniv.edu.in
Target IP Address	136.232.79.162

List of Vulnerability

#	Vulnerability name	Severity	Plugins -ID
1	HTTP Server Type and Version	INFO	10107
2	ICMP Timestamp Request Remote Date Disclosure	Low	10114
3	Traceroute Information	INFO	10287
4	Nessus SYN scanner	INFO	11219
5	OS Identification	INFO	11936
6	Host Fully Qualified Domain Name (FQDN) Resolution	INFO	12053
7	Nessus Scan Information	INFO	19506
8	Service Detection	INFO	22964
9	HyperText Transfer Protocol (HTTP) Information	INFO	24260
10	HTTP Methods Allowed (per directory)	INFO	43111
11	Common Platform Enumeration (CPE)	INFO	45590
12	Apache HTTP Server Version	INFO	48204
13	Device Type	INFO	54615

Report

Vulnerability Name: - ICMP Timestamp Request Remote Date Disclosure

Severity: - LOW

Plugin: - 10114

Port: - 25,80,5353,5432

Description:

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.

Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Solution: - Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Business Impact: -

Impact Area	Details	Business Risks	Mitigation Strategies	Business Benefits
Security Risks	**Information Disclosure:** Exposes internal system date and time.	- Increased Attack Surface - Enhanced Reconnaissance Capabilities	- **Disable ICMP Timestamp Requests:** Block requests using firewall rules or network configurations. - **Patch Systems:** Apply updates to close vulnerabilities.	- **Reduced Risk of Exploits:** Prevents attackers from using timestamp information for further attacks. - **Improved Security Posture:** Strengthens defenses against potential threats.

Compliance & Regulatory	**Non-Compliance Risks:** May violate regulations such as PCI-DSS, HIPAA, or GDPR by disclosing internal system details.	- **Regulatory Penalties:** Risk of fines for non-compliance. - **Audit Failures:** Potential issues during security audits.	- **Ensure Compliance:** Follow security guidelines to meet regulatory requirements. - **Conduct Regular Audits:** Verify adherence to compliance standards.	- **Avoid Legal Penalties:** Helps in maintaining compliance with regulations. - **Audit Readiness:** Simplifies audit processes and demonstrates adherence to security practices.
Reputational Damage	**Perceived Security Weakness:** Vulnerability may suggest inadequate security practices.	- **Loss of Client Trust:** Negative perception affecting client relationships. - **Business Opportunities:** Potential loss of contracts or clients.	- **Enhance Security Practices:** Strengthen overall security measures. - **Communicate Proactively:** Address vulnerabilities transparently with stakeholders.	- **Strengthened Reputation:** Builds trust with clients and partners through effective security management. - **Improved Client Relations:** Demonstrates commitment to security and compliance.
Operational & Financial	**Operational Disruption:** Patching and remediation may require downtime or system adjustments.	- **Operational Downtime:** Potential service disruptions during remediation. - **Cost of Remediation:** Expenses for patching and configuration changes.	- **Plan Maintenance Windows:** Schedule updates during off-peak hours. - **Allocate Resources:** Budget for remediation efforts and operational changes.	- **Efficient Remediation:** Minimizes downtime and manages costs effectively. - **Enhanced Security:** Long-term protection from vulnerabilities.
General Recommendations	**Review and Assess:** Regular security assessments and updates are essential.	- **Overall Vulnerability Management:** Ensuring ongoing security measures are up-to-date.	- **Implement Best Practices:** Regularly review security policies and practices. - **Educate Staff:** Raise awareness about vulnerabilities and security best practices.	- **Ongoing Security Improvements:** Keeps security measures current and effective. - **Informed IT Staff:** Better preparedness for future security challenges.

Project Report Stage 3

Review on Security Operation Centre

Team: Cyber Defender

12 July, 2024

SOC

A Security Operations Center (SOC) is a centralized unit within an organization that employs people, processes, and technology to continuously monitor and improve an organization's security posture while preventing, detecting, analyzing, and responding to cybersecurity incidents. The primary objective of a SOC is to detect, analyze, and respond to cybersecurity threats in real-time to mitigate potential damage.

Key Components of a SOC:

- **People**: The SOC team typically includes security analysts, incident responders, SOC managers, and sometimes forensic investigators. These professionals work around the clock to identify and respond to security incidents.
- **Processes**: A SOC operates based on predefined processes and procedures to ensure consistency and effectiveness. This includes incident response protocols, threat detection methods, and compliance with industry standards and regulations.
- **Technology**: The SOC relies on a range of tools and technologies to monitor and protect the organization's IT infrastructure. This includes Security Information and Event Management (SIEM) systems, intrusion detection systems (IDS), firewalls, antivirus software, and more. Advanced SOCs may also employ artificial intelligence and machine learning for threat detection.

Functions of a SOC:

- **Continuous Monitoring**: The SOC monitors network traffic, system activities, and logs 24/7 to detect suspicious activities and potential security breaches.
- **Incident Detection**: Using various detection tools, the SOC identifies potential security incidents. This involves correlating data from different sources to identify patterns indicative of threats.
- **Incident Response**: Upon detecting an incident, the SOC responds according to predefined incident response plans. This includes containment, eradication, and recovery actions to minimize the impact of the incident.
- **Threat Intelligence**: SOC analysts gather and analyze threat intelligence from various sources to stay informed about the latest threats and vulnerabilities. This helps in proactive defense measures.

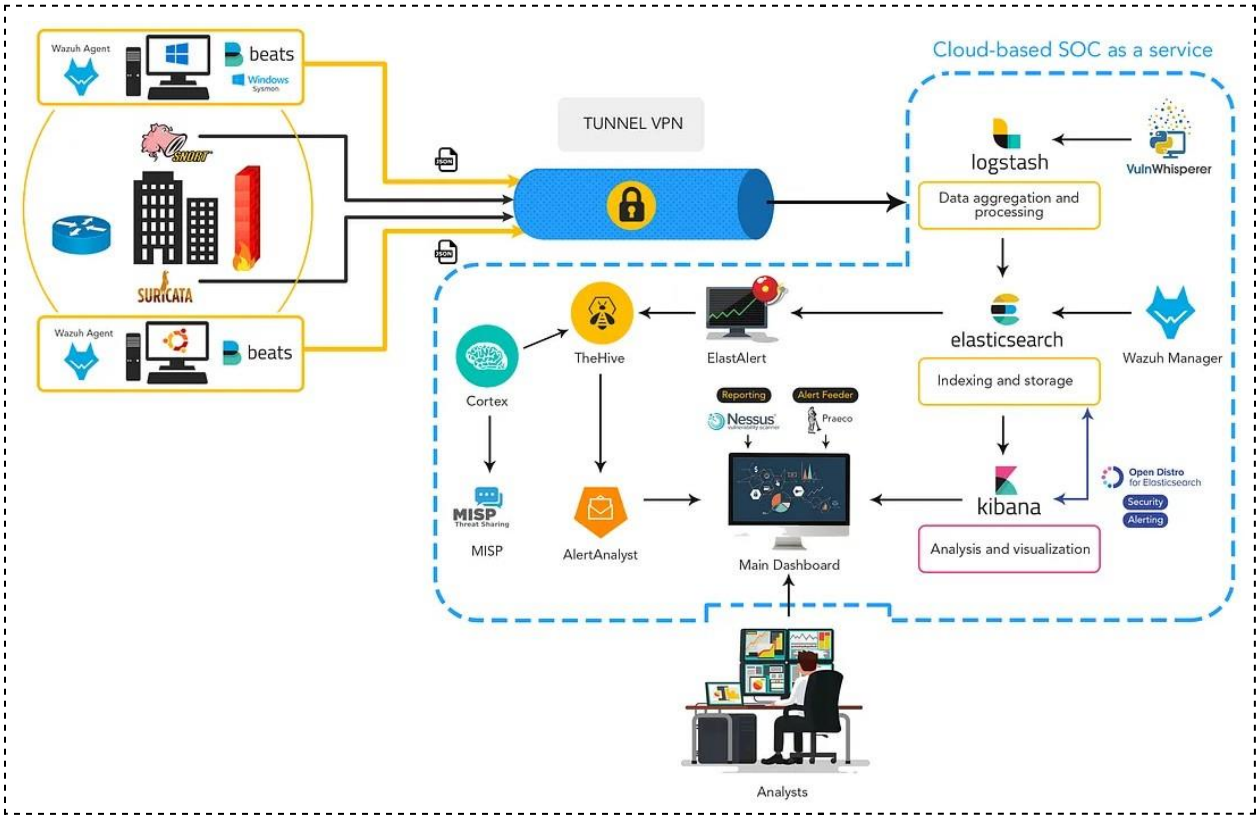
- **Forensic Analysis**: When an incident occurs, forensic analysis is conducted to understand the nature and extent of the breach. This helps in identifying the attackers, their methods, and any compromised data.
- **Reporting and Compliance**: The SOC generates reports on security incidents, threat trends, and overall security posture. This information is crucial for compliance with legal and regulatory requirements.

Benefits of a SOC:

- **Enhanced Security Posture**: Continuous monitoring and rapid response to incidentssignificantly improve an organization's security posture.
- **Reduced Downtime and Damage**: Quick detection and response minimize thedamage and downtime caused by security incidents.
- **Regulatory Compliance**: A SOC helps ensure compliance with industry standards andregulations by maintaining proper security practices and documentation.
- **Improved Threat Detection**: With a dedicated team and advanced tools, a SOC candetect sophisticated threats that might be missed by standard security measures.

SOC Cycle

A Security Operations Center (SOC) architecture is a structured framework that combines people, processes, and technology to effectively monitor, detect, analyze, and respond to cybersecurity threats. The architecture of a SOC is designed to provide a comprehensive and cohesive approach to security management, ensuring that the organization's digitalassets are continuously protected.



SOC Architecture

- **Data Collection Layer**
  - Wazuh Agents and Beats: Installed on endpoints to collect security event data, such as logs and alerts, from various devices, including Windows systems (using Sysmon) and others.
  - Suricata and Snort: Network intrusion detection systems (NIDS) that monitor network traffic for suspicious activities and generate alerts.

- **Data Aggregation and Processing Layer**

- Tunnel VPN: Securely transports collected data to the cloud-based SOC for further processing.
- Logstash: Aggregates and processes data from various sources. It normalizes the data for consistency and forwards it to Elasticsearch for indexing.

- **Indexing and Storage Layer**
  - Elasticsearch: Serves as the central repository for storing and indexing security event data. It enables fast search and query capabilities.
  - Wazuh Manager: Manages and processes data collected by Wazuh agents, integrating it into Elasticsearch for analysis.

- **Analysis and Visualization Layer**
  - Kibana: Provides a graphical interface for visualizing and analyzing data stored in Elasticsearch. It allows analysts to create dashboards, perform searches, and generate reports.
  - ElastAlert: Monitors Elasticsearch data for predefined conditions and generates alerts when those conditions are met, facilitating timely responses.

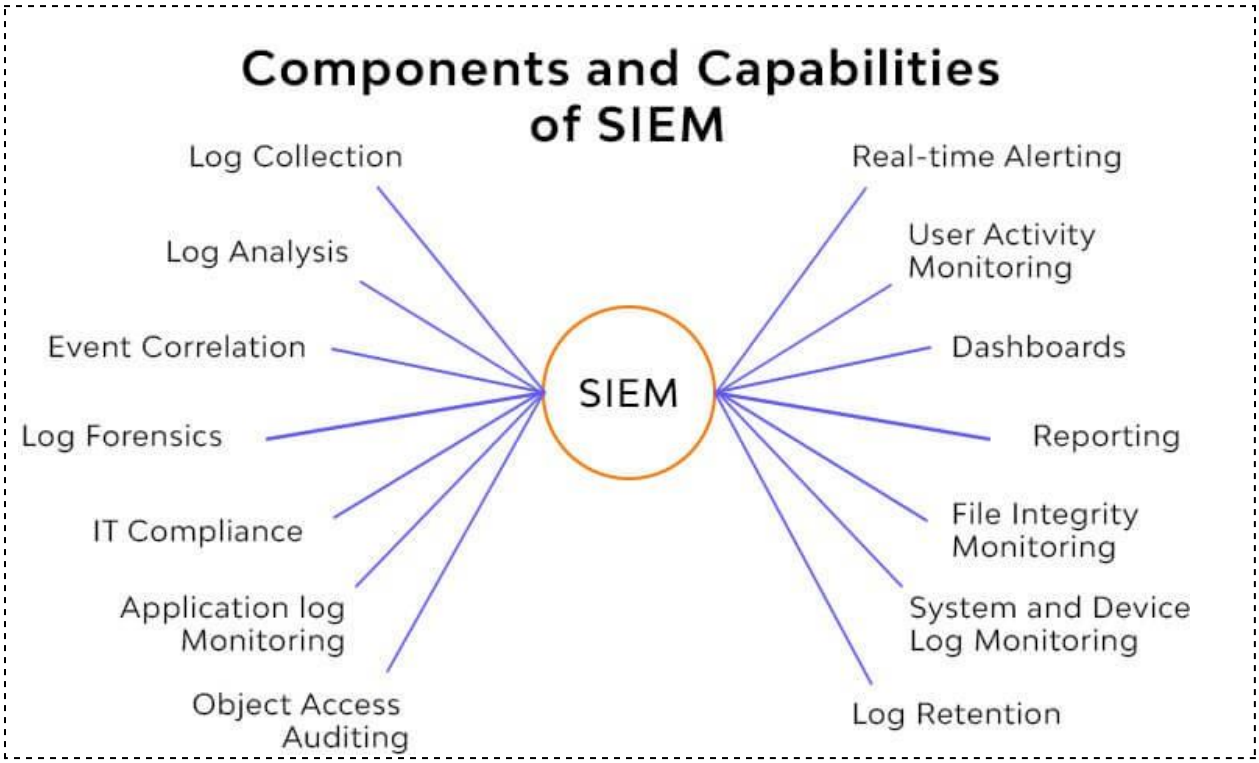
- **Threat Detection and Incident Response Layer**
  - TheHive: An incident response platform that integrates with ElastAlert for managing security incidents. It organizes and tracks incident response activities.
  - Cortex: Analyzes observables and indicators of compromise (IOCs) related to security incidents, aiding in the investigation and response processes.
  - MISP: A threat intelligence platform that facilitates sharing and enrichment of threat data. It helps SOC analysts stay informed about the latest threats.

- **Main Dashboard and Analyst Interaction Layer**
  - AlertAnalyst: A tool used for managing and analyzing security alerts, integrating with TheHive and other platforms.
  - Main Dashboard: A central interface where analysts monitor alerts, incidents, and overall security posture. It integrates data from various tools, including Nessus for vulnerability scanning and Praeco for alert management.
  - Analysts: Security professionals who monitor the main dashboard, analyze alerts,

respond to incidents, and perform threat hunting and forensic analysis.

- **Additional Integrations**
  - VulnWhisperer: Integrates with vulnerability scanning tools to aggregate and process vulnerability data, feeding it into Logstash for further processing

SIEM



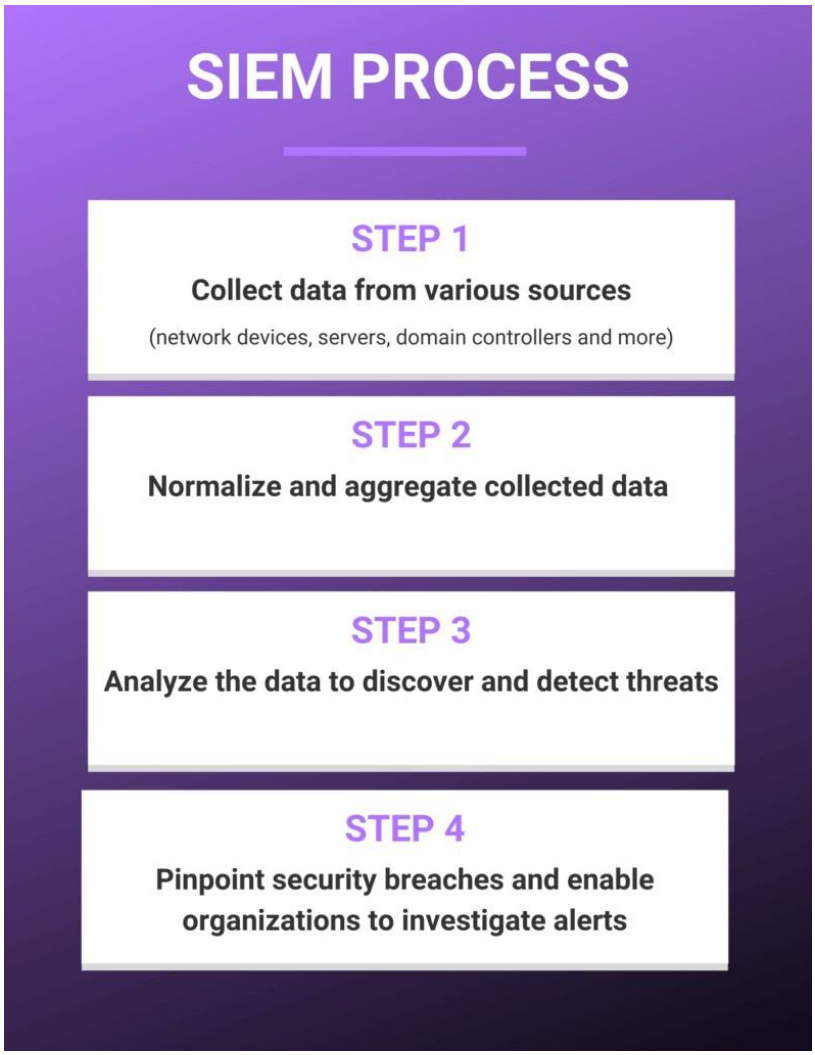
SIEM Architecture

Security Information and Event Management (SIEM) is a comprehensive system that enables real-time analysis of security alarms generated by applications and network devices. It combines two critical components: Security Information Management (SIM), which involves the collection, processing, and reporting of log data, and Security Event Management (SEM), which focuses on real-time monitoring, event correlation, and incident response. SIEM systems enable enterprises to detect and respond to possible security threats by aggregating and analyzing data from several sources throughout theIT infrastructure, allowing for more effective incident response and compliance reporting. SIEM assists in recognizing patterns indicative of cyber threats and ensuring timely risk mitigation by offering a comprehensive view of an organization's security posture.

SIEM Cycle

Security information and event management, or SIEM, is a security solution that aids organizations to recognize and address potential security threats and vulnerabilities before they hamper business operations.

A SIEM solution works by collecting data from various sources such as computers, network devices, servers, and more. The data is then normalized and aggregated. Next, security professionals analyze the data to discover and detect threats. As a result, businesses are able to pinpoint security breaches and enable organizations to investigate alerts. A generalized life cycle of SIEM is shown in image below:



SIEM Process

- **Data Collection**: In order to do more analysis, data must first be gathered. SIEM gathers information from various sources, such as host systems, antivirus software, network protocols, etc. Agents that support data collection connected to event logs from corporate systems are frequently used to gather data. It also includes data storing. The information must be kept for future research after it has been gathered. RDBMS storage is used by conventional SIEM systems. Distributed, horizontally scalable architecture and storage configurations are becoming the norm for modernSIEM for data storage.
- **Data Enrichment**: Information gains value through data enrichment. Data enrichment involves storing data along with its true identity, geolocation, and threat intelligence, which may further help with threat investigations.
- **Log management**: In order to facilitate future evaluations, data must be saved in a variety of forms. Over time, SIEM solutions typically store data in two formats: Tiered simply indicates that data that has been gathered under several categories is kept in various storage locations. These are newly gathered data. For improved performance, this data is kept on a storage medium that offers the highest throughput rates. Archived: Since there is a lower likelihood of using this kind of data, it is kept in archived places.
- **Correlations and Analytics**: SIEM solutions employ a variety of strategies to extract more insightful information from the data. Conventional SIEM employed signature-based alerts and looked for data abnormalities to drive relationships between different data sets. To focus on the dangers, modern SIEM employs machine learning and sophisticated analytical algorithms. User and Entity Behavior Analytics is another technique similar to this one used by contemporary SIEM solutions (UEBA).
- **Threat Investigation and Elimination**: A Security, Orchestration, Automation, and Response method solution is typically what a SIEM platform relies on for threat investigation and its eventual removal. It offers an automated method for handling security risks. This solution assists analysts by providing them with the records that were previously gathered for threats. It helps them determine if the danger was genuine or not, how it was removed, and what procedures were performed.
- **Compliance and Reporting**: Compliance reports in real time will be available from an effective SIEM system. SIEM solutions require that the data they collect meet compliance requirements. The compliance criteria are also verified for the data that SIEM collects. Because of its automated reports generation and compliance verifying standards, it is the most sought out security solution.

MISP

MISP (Malware Information Sharing Platform & Threat Sharing) is an open-source threat intelligence platform designed to improve the sharing of structured threat information. It enables our community of trustworthy people to share and trade threat intelligence, indicators of compromise (IoCs) concerning targeted malware and assaults, financial fraud, or any other intelligence. A distributed paradigm called MISP sharing allows for the exchange of technical and non-technical knowledge in closed, semi-private, or open groups. By sharing this information, targeted assaults should be detected more quickly,increasing the detection ratio and lowering the amount of false positives.

Important Characteristics of MISP are:

- **Collecting and Ingesting Threat Data**: Gather threat information from several sourcesboth automatically and manually.
- **Data Normalization and Structuring**: Use custom objects and taxonomies to standardize and organize data.
- **Analyze and enrich**: establish connections between data, show linkages, and provide context.
- **Threat Intelligence Sharing**: Coordinate with partners, oversee distribution levels,and manage sharing groups.
- **Collaboration and Communication**: Facilitate conversations, workflow management,alerts, and notifications.
- **Search and Retrieval**: Use stored query choices to conduct comprehensive and sophisticated searches.
- **Integration and Export**: Integrate with SIEM and API systems, and export data in avariety of formats.
- **Dashboards and Reporting**: Produce personalized reports and design dashboards tosee important metrics.
- **Security and Compliance**: To secure data, use audit trails, encryption, and role-based access control.
- **Maintenance and Support**: Receive regular updates, access community support, anduse comprehensive documentation.

Your college network information

There are five blocks (Block – A, B, C, D, E) and each block has 200 systems.

How you think you deploy SOC in your college

The key steps for deploying the Security Operations Center (SOC) in the organization are as follows.

- Thorough assessment of the present setup for cyber security
- Defining the goal and objectives of the SOC deployment
- Prepare a budget for SOC setup and maintenance, including hardware, software and human resources
- Forming and training the SOC team
- Infrastructure and technology setup, which includes hardware and software
- Integration of security tools and collecting data in the form of logs from critical data sources such as networks, servers, firewalls, etc.
- Define and implement standard operating procedures (SOPs) for various SOC activities and implement incident categorisation and prioritization mechanisms.
- Configure the SIEM to generate real-time alerts, including procedures for minimizing false positive alerts and emphasis on critical alerts.
- Prepare a formal incident response plan to respond to security incidents, along withthe roles and responsibilities for handling the incident.
- Train the SOC team to use security tools effectively and handle incidents according to best practices. Also, keep the team updated on the latest practices in the cyber security domain.
- Improve and refine the SOC's processes and procedures by simulating cyber attacks and responses to these attacks, which also enhances the SOC team's response capabilities.
- Monitor the SOC's performance and effectiveness
- Collaboration between the SOC team and IT and business teams for better executionof security policy and procedures
- Reporting and discussing with executive management to explain the current trends, and needs for the organization and thus gaining support for new initiatives for SOC
- Regular assessments, training, and updates are instrumental in keeping SOC effectivein addressing the organization's evolving security challenges.

Threat intelligence

Data that is collected, processed and analyzed to understand the goals, objectives and attack patterns of a threat actor is called threat intelligence. Security awareness helps us become more proactive in combating threats because we can make security decisions faster and smarter.

Source: https://flashpoint.io/blog/threat-intelligence-lifecycle/

Threat intelligence is critical because it helps security teams make better decisions by shedding light on the unknown. Enables cybersecurity stakeholders by exposing adversarial motives and their strategies, methods, and procedures (TTP). It helps security experts understand the decision-making process of threat actors. Enables business stakeholders, including boards, CISOs, CIOs, and CTOs, to make more informed decisions faster, more efficiently and with less risk. Each member of the security team benefits from threat intelligence in a different way, from top to bottom, including: CSIRT, Intel Analyst, SOC, Sec/IT Analyst, and Executive Management.

Incident Response

The term "incident response" refers to an organization's handling of a data breach or cyber-attack, including initiatives to manage the consequences of the attack or data breach (also known as an "event"). The ultimate goal is to deal with the situation effectively to minimize collateral damage, such as damage to brand reputation, and to minimize the amount of damage, recovery and costs. At a minimum, organizations should have a well-defined incident strategy. This plan should describe the company's definitionof an event and the precise actions to be taken in the event of an event. It is also a good idea to identify the groups, staff or managers who are responsible for overseeing the event as a whole.

Incident response is usually handled by the organization's Computer Incident Response Team (CIRT), aka Incident Response Team. CIRT teams often consist of IT and security personnel, and representatives from PR, HR, and legal departments. According to Gartner, a team that "responds to security breaches, viruses and other potentially catastrophic events in companies facing significant security risks." In addition to technical experts who can deal with specific risks, there should be professionals who can advise business leaders on proper communication after such events.

Qradar & Understanding about Tool

IBM QRadar is a premier Security Information and Event Management (SIEM) solution that provides real-time visibility into an organization's security posture. QRadar combines several data sources to provide complete security monitoring, threat detection, and incident response capabilities. It is well-known for its advanced analytics, which aid in detecting possible security issues by connecting events and data from various sources throughout the IT infrastructure. IBM QRadar captures and aggregates log data from numerous sources, including as firewalls, routers, servers, and applications.

This unified log management system provides quick access to previous data forcompliance and forensic investigation.

- Threat information: QRadar uses threat information feeds to improve its detection and response to known threats. It is constantly updating its database with information on new vulnerabilities, malware signatures, and attack methods.
- Behavioral Analytics: The technology employs machine learning and behavioral analytics to detect unusual activity that could suggest a security concern. It creates a baseline of normal behavior and detects departures from it.
- Correlation Engine: QRadar's correlation engine examines data from many sources to detect trends that indicate potential security problems. This feature aids in decreasingfalse positives and identifying significant threats.
- QRadar offers capabilities for incident response, including alerting, investigation, and reporting. It enables security teams to prioritize and respond to issues according to their severity and impact.
- Dashboards and Reporting: The platform includes customisable dashboards and reports that provide an overview of the organization's security state. These visualizations aid in monitoring critical indicators and disseminating security information to stakeholder

Understanding QRadar as a Tool

QRadar takes data from a variety of sources, including syslog, APIs, and log files. Accurate and thorough monitoring requires proper data source configuration.

- **Normalization**: Following data collection, QRadar normalizes the data to ensure that it is consistent in format. This procedure entails parsing and categorizing log data for effective analysis.
    - QRadar uses correlation criteria to identify probable security problems. These rules might be predefined or changed to meet the organization's specific security requirements.
- **Offenses**: When QRadar detects a potential threat, it issues an offense. Offenses are notifications that collect linked occurrences and provide context to aid security teams in their investigation and response.
    - QRadar may work with vulnerability management systems to correlate vulnerabilities with detected threats, giving the organization a more complete picture of its risk landscape.
    - QRadar can be installed on-premises, in the cloud, or in a hybrid environment, giving enterprises with varying infrastructure needs greater flexibility.

Conclusion: IBM QRadar is a robust SIEM solution with comprehensive capabilities for threat detection, incident response, and security monitoring. Understanding QRadar's major features and functionalities enables enterprises to improve their security posture, respond to incidents more effectively, and maintain regulatory compliance.

Conclusion

Stage 1: What you understand from Web application testing.

Web application testing is a comprehensive process aimed at ensuring the functionality, performance, security, and usability of web-based applications. The goal is to identify and resolve issues before the application is deployed to end-users.

Here's a detailed understanding of what web application testing involves:

1. **Functionality Testing**
   - *Objective*: To ensure that the web application operates according to the specified requirements.
   - *Activities*: Verifying links, forms, databases, cookies, and business workflows to ensure they work as expected. Testing for input validation, session management,and error handling.

2. **Usability Testing**
   - *Objective*: To evaluate the user-friendliness of the web application.
   - *Activities*: Assessing navigation, interface design, and overall user experience. Ensuring that the application is intuitive and easy to use.

3. **Interface Testing**
   - *Objective*: To ensure that the interfaces between different components or systems work seamlessly.
   - *Activities*: Testing the interaction between the web server and application server, and between the application server and database server. Checking if error messages are correctly displayed.

4. **Compatibility Testing**
   - *Objective*: To ensure that the web application performs well across different browsers, devices, and operating systems.
   - *Activities*: Testing the application on various web browsers (Chrome, Firefox, Safari, Edge) and devices (desktop, tablet, mobile) to ensure consistent behavior.

5. **Performance Testing**
   - *Objective*: To assess the application's performance under different conditions.
   - *Activities*: Conducting load testing to see how the application behaves under normal and peak loads. Stress testing to determine the application's breaking point. Measuring response times and throughput rates.

6. **Security Testing**
   - *Objective*: To identify and mitigate security vulnerabilities.
   - *Activities*: Checking for vulnerabilities such as SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF), and other common security threats. Ensuring secure data transmission and user authentication.

7. **Database Testing**
   - *Objective*: To ensure the integrity and reliability of the database.
   - *Activities*: Validating data storage, retrieval, updates, and deletion. Ensuring data consistency and integrity through various transactions.

8. **Regression Testing**
   - *Objective*: To verify that new code changes do not adversely affect the existing functionality.
   - *Activities*: Re-running previously executed tests to ensure that the application still performs as expected after updates or enhancements.

9. **Automation Testing**
   - *Objective*: To increase testing efficiency and coverage.
   - *Activities*: Using automated testing tools and frameworks to execute repetitive tests, such as regression tests, quickly and accurately.

In summary, web application testing is a multi-faceted process that covers all aspects ofthe application to ensure it is robust, reliable, and secure. It involves a combination ofmanual and automated testing techniques to identify and fix issues, thereby ensuring ahigh-quality user experience.

Stage 2: What you understand from the Nessus report.

The Nessus report provides valuable insights into the security posture of the scanned system. Key findings include:

1. SSL/TLS vulnerabilities: Deprecated protocols (TLS 1.0, 1.1) and discouraged cipher suites are in use. HSTS is missing.
2. Certificate issues: The SSL certificate is self-signed and untrusted.
3. Web server configuration: Running Apache with Drupal 7.69. The web.config file is accessible, potentially exposing sensitive information.
4. System information: Linux Kernel 2.6, with web services on ports 80 and 443.
5. Network configuration: ICMP and TCP timestamp responses enabled.

The report categorizes findings by severity, provides detailed descriptions of each vulnerability, and offers specific remediation advice. While no critical vulnerabilities were found, several medium-risk issues were identified, primarily related to SSL/TLS configuration and web server setup.

This report serves as a roadmap for improving the system's security, highlighting areas that require attention such as updating SSL/TLS configurations, implementing HSTS, using a trusted SSL certificate, and restricting access to sensitive files. It demonstrates the value of vulnerability scanning in identifying potential security weaknesses and guiding remediation efforts.

Stage 3: What you understand from SOC / SEIM / QradarDashboard.

Security Operations Center (SOC) Dashboard

- Provides a high-level overview of an organization's security posture
- Displays real-time alerts, incidents, and threat intelligence
- Often includes key performance indicators (KPIs) for security operations
- May show trends in security events over time
- Typically, customizable to focus on specific areas of concern

Security Information and Event Management (SIEM) Dashboard

- Aggregates and correlates data from various security tools and systems
- Presents a unified view of security events across the organization
- Often includes visualizations of log data, network traffic, and user activities
- Highlights potential security incidents and anomalies
- Provides drill-down capabilities for detailed investigation

QRadar Dashboard (a specific SIEM solution):

- Offers a customizable interface for security monitoring and analysis
- Displays real-time threat detection and incident response information
- Includes pre-built dashboards for common use cases (e.g., compliance, threat hunting)
- Allows creation of custom dashboards tailored to specific needs
- Provides visual representations of data like charts, graphs, and tables
- Offers features like offense management, asset profiling, and risk assessment

Key components often found in these dashboards:

- Incident/event timelines
- Threat maps showing geographic origins of attacks
- Top offenders and targets
- Risk scores for systems or users
- Compliance status indicators
- Workflow management for security analysts
- Integration with threat intelligence feeds

These dashboards aim to provide security teams with a centralized, easily digestible view of their organization's security landscape, enabling quick identification of threats and efficient response to incidents.

Future Scope

Stage 1: Future Scope of Web Application Testing

The future of web application testing will likely focus on increased automation and AI integration, earlier security integration in development (shift-left), expanded IoT and mobile testing, and adaptation to emerging technologies like blockchain and quantum computing. There will be greater emphasis on API and microservices testing, cloud-native applications, and privacy compliance. Advanced threat simulations, performance testing under extreme conditions, and accessibility considerations will also gain prominence. Overall, testing methodologies will evolve to become more comprehensive, efficient, and integrated throughout the development lifecycle to address the growing complexity of web applications and emerging security challenges.

Stage 2: Future Scope of Testing Process you Understood

The future of software testing will be characterized by increased automation, integration with emerging technologies, and a holistic approach to quality assurance. Key developments will include:

- AI-driven automation in test generation, execution, and analysis
- Continuous testing integrated seamlessly with CI/CD pipelines
- Expanded focus on security, performance, and user experience testing
- Adaptation to new paradigms like IoT, edge computing, and quantum systems
- Shift-left and shift-right testing approaches for comprehensive quality coverage
- Low-code/no-code testing tools to empower non-technical testers
- Advanced analytics for test prioritization and defect prediction
- Cloud-based solutions for scalable performance and load testing

Testing professionals will need to continuously update their skills, balancing technical expertise with adaptability and collaboration. As software ecosystems become more complex, the testing process will evolve to ensure quality, security, and performance across diverse platforms and technologies. This evolution will position testing as a critical driver of innovation and reliability in the rapidly changing software landsca

Stage 3: Future Scope of SOC / SEIM

The future of SOC and SIEM will be characterized by advanced technologies, increased automation, and a more holistic approach to cybersecurity. Key developments will include:

- AI and machine learning integration for enhanced threat detection and automated response
- Cloud-native solutions offering scalability and multi-cloud security management
- Extended Detection and Response (XDR) for unified security incident handling across multiple layers
- Expanded monitoring capabilities for IoT and Operational Technology (OT)environments
- Real-time threat intelligence integration and automated threat hunting
- Advanced User and Entity Behavior Analytics (UEBA) for anomaly detection
- Increased adoption of Security Orchestration, Automation, and Response (SOAR) tools
- Integration with zero trust security models for continuous authentication and authorization
- Enhanced compliance and privacy-focused features to meet evolving regulations
- Growth in Managed Detection and Response (MDR) services for 24/7 threat monitoring

These advancements will enable organizations to more effectively combat sophisticated cyber threats, manage the growing complexity of IT environments, and protect expanding digital assets. SOC and SIEM systems will evolve to become more intelligent,automated, and proactive, playing a crucial role in maintaining robust cybersecurity postures in an increasingly challenging threat landscape.

Topics Explored	Tools Explored
Cyber Ethical Hacking, OSINT Framework, Hacking Web Applications, SOC & SIEM & Qradar, Threat intelligence integration	nslookup, nmap, nessus, metasploit, Qradar