Stage 1

Title of the project :-
Understanding of session management vulnerability in Web Application

—

Overview :-

Session management involves maintaining stateful interactions in a stateless HTTP environment. When a user logs into a web application, the server creates a session, assigns a unique session identifier (session ID), and tracks the user's activity during that session. This session ID is typically stored in a cookie on the client-side and sent with each request to the server. session management vulnerabilities can lead to significant security risks, including unauthorized access, session hijacking, and data breaches.

Common Attacks on Session Management:

Session Hijacking:

- **Description: An attacker steals a valid session ID to impersonate a user.**
- **Mitigation: Use secure cookies, HTTPS, and regenerate session IDs frequently.**

Session Fixation:

- **Description: An attacker forces a user to use a known session ID, which the attacker can then hijack.**
- **Mitigation: Regenerate session IDs after login and significant actions.**

Cross-Site Request Forgery (CSRF):

- **Description: An attacker tricks a user into performing actions on a web application where they are authenticated.**
- **Mitigation: Use the SameSite cookie attribute, implement anti-CSRF tokens, and validate the origin of requests.**

List of teammates–

S.no	Name	Collage	contact	Email-ID
1	Vipul Chudasama	Institute of Technology, Nirma University	9737962626	vipul.chudasama@nirmauni.ac.in
2	Umesh Bodkhe	Institute of Technology, Nirma University	8888123279	umesh.bodkhe@nirmauni.ac.in
3		Institute of	9099921763	ajaypatel@nirm

	Ajaykumar Patel	Technology, Nirma University		auni.ac.in
4	Devendra Vashi	Institute of Technology, Nirma University	9426774300	devendra.vashi@nirmauni.ac.in

List of Vulnerability Table –

CWE Number	Vulnerability Name
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-311	Missing Encryption of Sensitive Data
CWE-384	Session Fixation
CWE-502	Deserialization of Untrusted Data
CWE-613	Insufficient Session Expiration
CWE-614	Sensitive Cookie in HTTPS Session Without 'Secure' Attribute
CWE-915	Improperly Controlled Modification of Dynamically-Determined Object Attributes
CWE-1021	Improper Restriction of Rendered UI Layers or Frames
CWE-285	Improper Authorization

REPORT:-

Vulnerability Name:- Exposure of Sensitive Information to an Unauthorized Actor

CWE : - CWE-200

OWASP/SANS Category:-Sensitive Data Exposure

Description:- When session information, such as session IDs, is exposed to unauthorized users.

Business Impact::-Data breaches, loss of customer trust, legal and regulatory consequences

CWE Number	Description	OWASP Category	Business Impact

CWE-200	Exposure of Sensitive Information to an Unauthorized Actor	Sensitive Data Exposure	Data breaches, loss of customer trust, legal and regulatory consequences
CWE-311	Missing Encryption of Sensitive Data	Sensitive Data Exposure	Data breaches, financial losses, compliance violations
CWE-384	Session Fixation	Broken Authentication and Session Management	Account hijacking, unauthorized access to user data, reputation damage
CWE-502	Deserialization of Untrusted Data	Security Misconfiguration	Remote code execution, application compromise, significant financial loss

CWE-613	Insufficient Session Expiration	Broken Authentication and Session Management	Unauthorized access, session hijacking, prolonged exposure to attacks
CWE-614	Sensitive Cookie in HTTPS Session Without 'Secure' Attribute	Sensitive Data Exposure	Session hijacking, data breaches, financial and reputational damage
CWE-915	Improperly Controlled Modification of Dynamically-Determined Object Attributes	Insecure Design	Unauthorized data manipulation, business logic vulnerabilities, financial loss
CWE-1021	Improper Restriction of	Cross-Site Scripting (XSS)	Clickjacking attacks, unauthorized actions, reduced user trust

	Rendered UI Layers or Frames		
CWE-285	Improper Authorization	Broken Access Control	Unauthorized access to sensitive functions, data breaches, compliance issues

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

'><script>alert('you are hacked ')</script>
<></>

Stage 2

Overview of Nessus:-

- One popular vulnerability detection tool in the world of security testing and cyber security is Nessus.
- Tenable created the Nessus platform, which checks for security flaws in hardware, software, operating systems, cloud services, and other network resources. It is a remote security scanning tool that looks for security holes in a computer and sounds an alert if it finds any that could allow malevolent hackers to access any computer that is connected to any network.
- In order to determine whether any of these assaults could be used to compromise or damage a particular machine, it performs over 1200 checks on it.
- It is an excellent tool to assist in maintaining the domains free of the simple weaknesses that hackers and viruses frequently try to exploit if you are an administrator in charge of any computer or a group of computers linked to the internet.

- Software developers, IT administrators, system and security administrators, and security specialists are among the users of this product.
- For vulnerability management and security assessments, a wide variety of businesses and experts from many industries use Nessus.

Target website: testfire.net

Target IP address: 65.61.137.117

OS: Dell EMC VMX, Microsoft Windows Embedded Standard 7

List of vulnerability: —

s.no	Vulnerability name	Severity	plugins
1	HSTS Missing From HTTPS Server (RFC 6797)	Medium	ID:142960 Version:1.12 Type: remote Family: Web Servers
2	SSL Certificate Cannot Be Trusted	Medium	ID:51192 Version:1.19 Type: remote Family: General

3	SSL Certificate Expiry	Medium	ID:15901 Version:1.50 Type: remote Family: General
4	TLS Version 1.0 Protocol Detection	Medium	ID:104743 Version:1.10 Type: remote Family: Service detection
5	TLS Version 1.1 Deprecated Protocol	Medium	ID:157288 Version:1.4 Type: remote Family: Service detection
6	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Low	ID:83875 Version:1.40 Type: remote Family: Misc.
7	ICMP Timestamp Request Remote Date Disclosure	Low	ID:10114 Version:1.53 Type: remote Family: General
8	SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)	Info	ID:95631 Version:1.15 Type: remote Family: General
9	SSL/TLS Recommended Cipher Suites	Info	ID:156899 Version:1.4 Type: remote Family: General

10	Service Detection	Info	ID:22964 Version:1.194 Type: remote Family: Service detection
11	Apache Tomcat Detection	Info	ID:39446 Version:1.29 Type: remote Family: Web Servers
12	Nessus SYN scanner	Info	ID:11219 Version:1.60 Type: remote Family: Port scanners
13	Additional DNS Hostnames	Info	ID:46180 Version:1.18 Type: remote Family: General
14	Common Platform Enumeration (CPE)	Info	ID:45590 Version:1.157 Type: combined Family: General
15	Device Type	Info	ID:54615 Version:1.2 Type: combined Family: General
16	Nessus Scan Information	Info	ID:19506 Version:1.122 Type: summary

			Family: Settings
17	OS Identification	Info	ID:11936 Version:2.67 Type: combined Family: General
18	TCP/IP Timestamps Supported	Info	ID:25220 Version:1.22 Type: remote Family: General
19	Traceroute Information	Info	ID:10287 Version:1.71 Type: remote Family: General

REPORT

Vulnerability Name:- HSTS Missing From HTTPS Server (RFC 6797)

Severity: - Medium

Plugin:- 142960

Port:- 443 / tcp / www

Description:- The remote web server is not enforcing HSTS, as defined by RFC 6797. HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

Solution:- Configure the remote web server to use HSTS.

Business Impact:- According to RFC 6797, the remote web server is not enforcing HSTS. The server can set up HSTS, an optional response header, to tell the browser to only communicate over HTTPS. The absence of HSTS makes it possible for SSL-stripping man-in-the-middle assaults, downgrade attacks, and weakened defences against cookie-hijacking.

Stage 3

Report

Tittle :- Automating Incident Response in SOC using SIEM Systems

—--

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

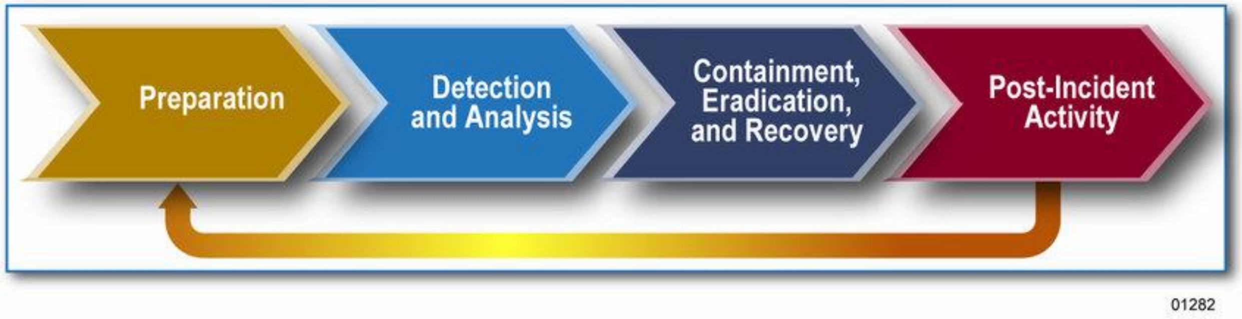
SOC

- **A Security Operations Center (SOC) offers numerous benefits to an organization by providing a centralized approach to monitoring, detecting, and responding to security threats.**

Benefits of a Security Operations Center (SOC)

1. **Continuous Monitoring:**
   - ○ **24/7 Surveillance: Provides around-the-clock monitoring of network traffic, systems, and data to detect potential threats in real-time.**
   - ○ **Early Detection: Identifies and addresses security incidents promptly, minimizing potential damage.**
2. **Improved Incident Response:**
   - ○ **Rapid Response: Ensures quick and coordinated response to security incidents, reducing the impact and recovery time.**
   - ○ **Standardized Procedures: Implements consistent and repeatable processes for handling incidents, improving efficiency and effectiveness.**
3. **Enhanced Threat Intelligence:**
   - ○ **Proactive Threat Hunting: Actively seeks out potential threats before they can cause harm.**
   - ○ **Data-Driven Insights: Utilizes threat intelligence to understand and anticipate potential security challenges.**
4. **Comprehensive Security Coverage:**
   - ○ **Vulnerability Management: Regularly identifies and mitigates vulnerabilities in systems and networks.**
   - ○ **Compliance and Reporting: Ensures adherence to regulatory requirements and generates reports for audits and compliance checks.**
5. **Cost Efficiency:**
   - ○ **Resource Optimization: Centralizes security efforts, reducing the need for multiple disparate security solutions.**
   - ○ **Reduced Impact of Breaches: Minimizes financial losses and reputational damage by preventing or quickly mitigating security incidents.**

SOC - cycle



-
- Source: https://www.researchgate.net/figure/1-Incident-Response-Life-Cycle_fig2_330026402

1. Preparation

This initial phase involves setting up the necessary infrastructure, processes, and teams to establish the SOC.

- **Define Objectives: Establish the goals and scope of the SOC, aligning with the organization's security strategy.**
- **Build the Team: Recruit and train security analysts, incident responders, and threat hunters.**
- **Implement Technology: Deploy and configure essential tools like SIEM, IDS/IPS, EDR, and threat intelligence platforms.**
- **Develop Processes: Create standard operating procedures (SOPs), incident response plans, and communication protocols.**
- **Compliance and Policies: Ensure adherence to regulatory requirements and organizational security policies.**

2. Detection

The detection phase focuses on identifying potential security incidents through continuous monitoring and analysis of security data.

- **Continuous Monitoring: Use SIEM, IDS/IPS, and other tools to monitor network traffic, system logs, and endpoint activities.**
- **Threat Intelligence: Integrate threat intelligence feeds to stay updated on emerging threats and vulnerabilities.**
- **Data Analysis: Analyze collected data to identify patterns, anomalies, and potential indicators of compromise (IOCs).**
- **Alert Generation: Configure rules and use machine learning to generate alerts for suspicious activities.**

Containment ,Eradication and Recovery

In this phase, the SOC team takes action to contain, eradicate, and recover from the security incident.

- **Containment: Implement measures to isolate affected systems and prevent the spread of the threat.**
- **Eradication: Remove the threat from the affected systems and eliminate the root cause.**
- **Recovery: Restore systems to normal operation, ensuring no remnants of the threat remain.**
- **Post-Incident Review: Conduct a thorough analysis to understand the incident's root cause and improve future response.**

Post incident Recovery

- **Post-Mortem Analysis: Document findings from incident responses to identify gaps and areas for improvement.**
- **Process Refinement: Update SOPs, incident response plans, and detection rules based on insights gained.**
- **Training and Development: Provide ongoing training to SOC personnel to keep them updated on the latest threats and response techniques.**

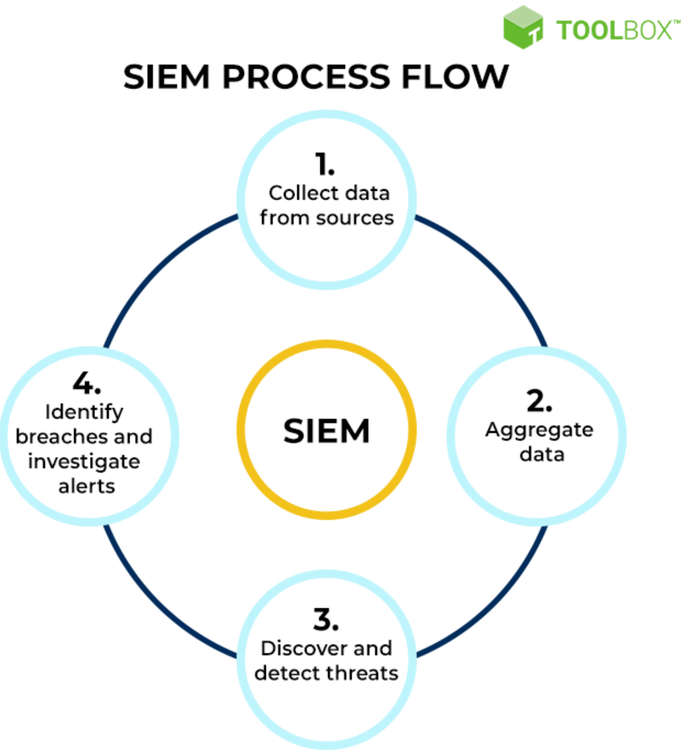
Siem

- A security system called security information and event management, or SIEM, assists companies in identifying and resolving any security threats and vulnerabilities before they have an opportunity to interfere with day-to-day operations.
- By producing real-time compliance reports for PCI-DSS, GDPR, HIPAA, SOX, and other compliance requirements, SIEM systems help lessen the load of security management and identify possible infractions early on, allowing for prompt correction. Numerous SIEM solutions include pre-configured, out-of-the-box add-ons that can produce automatic reports that are made to comply with regulatory standards.
- The benefits of SIEM are Real-time threat recognition, AI-driven automation, Improved organizational efficiency, Detecting advanced and unknown threats, Conducting forensic investigations, Assessing and reporting on compliance and Monitoring users and applications.

Siem Cycle

- All SIEM solutions, at their most basic, carry out some degree of data consolidation, aggregation, and sorting operations in order to detect threats and fulfill data compliance mandates. While the capabilities of certain solutions differ, the majority provide the same core set of functions:
    - ***Log management:*** Real-time data collection, correlation, and analysis are done on event logs originating from users, endpoints, apps, data sources, cloud workloads, networks, and security hardware and software, like firewalls and antivirus programs.

- ○ ***Event correlation and analytics:***An integral component of every SIEM system is event correlation. Event correlation offers valuable insights to promptly identify and mitigate potential threats to enterprise security through the use of advanced analytics to comprehend complex data patterns.
- ○ ***Incident monitoring and security alerts:*** Security teams use SIEM to compile their analysis into a single, central dashboard from which they can monitor activity, prioritize warnings, spot dangers, and start responding or fixing issues.
- ○ ***Compliance management and reporting:*** By producing real-time compliance reports for PCI-DSS, GDPR, HIPAA, SOX, and other compliance requirements, SIEM systems help lessen the load of security management and identify possible infractions early on, allowing for prompt correction.


TOOLBOX™
SIEM PROCESS FLOW
1. Collect data from sources
2. Aggregate data
3. Discover and detect threats
4. Identify breaches and investigate alerts
SIEM

[Source: https://www.spiceworks.com/it-security/vulnerability-management/articles/what-is-siem/]

MISP

- The MISP (Malware Information Sharing Platform & Threat Sharing) framework is a vital tool in cybersecurity, facilitating the collaborative sharing of threat intelligence among organizations. By enabling the exchange of data on malware, vulnerabilities, and indicators of compromise (IOCs), MISP enhances the ability of cybersecurity teams to detect, analyze, and respond to threats more effectively. Its open-source nature allows for customization and integration with existing security tools, promoting a more unified and proactive defense strategy against cyberattacks. Through community-driven contributions, MISP continuously evolves, adapting to emerging threats and helping organizations stay ahead in the ever-changing landscape of cybersecurity.

- **Your college network information:**
- **I**nstitution: Institute of Technology, Nirma University.
- Location: Ahmedabad, India
- Size: 5,000 students, 500 faculty members
- IT Infrastructure: Centralized data center, multiple satellite campuses, online learning platforms, and extensive research networks
- **How you think you deploy soc in your college:**
- **Challenge:**

Green Valley University faced escalating cyber threats, including phishing attacks, ransomware, and data breaches. With sensitive research data, student records, and financial information at risk, the university recognized the need to establish a Security Operations Center (SOC) to enhance its cybersecurity posture.

Objectives

1. Centralized Threat Monitoring: Establish a unified platform for real-time monitoring and response to security incidents.
2. Enhanced Incident Response: Develop a robust incident response plan to mitigate the impact of security breaches.
3. Improved Threat Intelligence: Leverage threat intelligence to anticipate and defend against potential cyberattacks.
4. Compliance: Ensure compliance with regulatory requirements such as FERPA (Family Educational Rights and Privacy Act) and GDPR (General Data Protection Regulation).

Implementation

Phase 1: Planning and Assessment

- Risk Assessment: Conducted a comprehensive risk assessment to identify vulnerabilities and critical assets.
- Stakeholder Engagement: Involved key stakeholders, including IT, administration, and faculty, to gather requirements and ensure alignment with the university's strategic goals.
- SOC Design: Designed the SOC infrastructure, including hardware, software, and staffing requirements.

Phase 2: Infrastructure Setup

- Technology Deployment: Implemented security information and event management (SIEM) systems, intrusion detection/prevention systems (IDS/IPS), and endpoint detection and response (EDR) tools.
- Network Segmentation: Segmented the network to isolate sensitive data and reduce the attack surface.
- Threat Intelligence Integration: Integrated MISP (Malware Information Sharing Platform) for threat intelligence sharing and analysis.

Phase 3: Staff Training and Development

- SOC Team Formation: Hired and trained a dedicated SOC team, including analysts, incident responders, and threat hunters.
- Continuous Education: Established ongoing training programs to keep the SOC team updated on the latest threats and technologies.

Phase 4: Operations and Continuous Improvement

- 24/7 Monitoring: Implemented round-the-clock monitoring to detect and respond to incidents in real-time.
- Incident Response Plan: Developed and tested an incident response plan, including regular tabletop exercises and simulations.
- Performance Metrics: Established key performance indicators (KPIs) to measure the effectiveness of the SOC and identify areas for improvement.

Results

- Reduced Incident Response Time: The SOC significantly reduced the time to detect and respond to security incidents, minimizing potential damage.
- Improved Security Posture: Regular monitoring and proactive threat hunting led to a more secure IT environment.
- Enhanced Compliance: The university achieved compliance with FERPA and GDPR, ensuring the protection of student and research data.
- Community Engagement: The SOC fostered a culture of cybersecurity awareness across the campus, engaging students and faculty in best practices.

Threat intelligence

Monitoring your environment for nefarious activity assumes that you know what those nefarious folks are doing, what “it” looks like, and how to find this activity across your critical infrastructure in the cloud and on-premises. The “bread crumbs” that these adversaries leave are usually of the same sort: IP addresses, host and domain names, email addresses, filenames, and file hashes.

With this amount of information, you can’t actually get that far. As a SOC analyst conducting an in-depth investigation, you need to be able to attribute these bread crumbs to specific adversaries, understand their methods, know their tools, recognize their infrastructure, and then build countermeasures for preventing attacks from them.

Some may refer to these “bread crumbs” or indicators (IOCs = indicators of compromise) as threat intelligence. This is far from the truth. On their own, without any context, they

exist only as artifacts or clues. They can be used to begin an investigation but they rely on context, attribution, and action to become the high-quality threat intelligence that is essential for building a SOC.

Incident response

Among the most critical strategies for incident response among SOC analysts is the establishment of a proficient team. This team should consist of adept professionals possessing expertise in various domains such as threat intelligence, malware analysis, forensics, and incident detection.

Qradar & understanding about tool

QRadar is a comprehensive security intelligence platform that enables organizations to gain real-time visibility into their IT infrastructures, detect and respond to threats efficiently, and ensure Compliance with regulatory requirements. It collects and analyzes log data, network flows, and security events from various sources within an organization's network, allowing security teams to identify and prioritize potential security incidents.

QRadar's relevance in the cybersecurity industry stems from its ability to provide organizations with a holistic view of their security posture, enabling them to proactively detect and respond to threats. To maximize the benefits of QRadar, organizations should adhere to certain best practices:

1. **Data Source Coverage: Ensure that all critical log sources and network devices are integrated with QRadar to provide comprehensive visibility into the IT environment.**
2. **Rule and Alert Tuning: Regularly review and fine-tune the platform's rules and alerts to minimize false positives and focus on actionable security events.**
3. **Threat Intelligence Integration: Leverage external threat intelligence feeds to enhance QRadar's Threat detection capabilities and stay updated on the latest threat landscape.**
4. **Automation and Orchestration: Integrate QRadar with other security tools and automate response actions to improve incident response times and reduce manual effort.**
5. **Continuous Monitoring and Reporting: Regularly monitor the platform's performance, review security events, and generate reports to identify potential gaps, optimize resources, and demonstrate compliance.**

Conclusion :-

- **Stage 1 :- what you understand from Web application testing .:** Web application testing involves evaluating and validating web applications to ensure they function correctly, securely, and efficiently across various browsers and devices. This process includes multiple testing types, such as functional testing to verify that the application performs its intended tasks, performance testing to assess its responsiveness and stability under load, security testing to identify vulnerabilities, and usability testing to ensure a positive user experience. Automated testing tools and frameworks are often employed to streamline repetitive tasks and enhance accuracy. Ultimately, web application testing aims to deliver a reliable, secure, and user-friendly application that meets user expectations and business requirements.

- **Stage 2 :- what you understand from the nessus report .**

  To gain insight into the security posture and vulnerabilities of your organization, you can check the results of the scan. The way you display the results from your scan can be customized using color-coded indicators and adjustable viewing choices. For each vulnerability, we can check its detailed attributes like Vulnerability Name, Severity, Plugin, Port, Description and Solution.

- **Stage 3 :- what you understand from SOC / SEIM / Qradar Dashboard .**

  A tool that assists businesses in identifying, evaluating, and mitigating security risks before they impair day-to-day operations is called security information and event management, or SIEM for short. Security event management (SEM) and security information management (SIM) are combined into one security management system, or SIEM, as it is pronounced. Event log data is gathered from many sources by SIEM technology, which then uses real-time analysis to spot unusual activity and takes the necessary action. Organizations may meet compliance standards and respond quickly to suspected assaults by using SIEM, which provides them with visibility into network activities.

Future Scope :-

- **Stage 1 :- future scope of web application testing:** The future of web application testing will be marked by increased automation and AI integration, enabling more efficient and accurate testing processes. The shift-left and shift-right testing approaches will embed testing earlier in the development cycle and extend it to post-deployment, enhancing overall quality. Cloud-based testing will offer scalable, cost-effective solutions, while heightened focus on security and performance testing will ensure robust defenses and optimal functionality. Cross-browser and cross-device testing will be crucial for compatibility across diverse environments, and continuous testing within DevOps will promote agile development. User experience and accessibility testing will also gain importance, ensuring applications are user-friendly and inclusive.
- **Stage 2 :- future scope of testing process you understood . :** The future scope of web application testing will see significant advancements through increased automation and the integration of AI and machine learning, leading to more efficient and accurate testing processes. Emphasis on shift-left and shift-right testing will ensure earlier and continuous testing, enhancing quality throughout the development lifecycle. Cloud-based testing will offer scalable and cost-effective solutions, while a heightened focus on security and performance testing will address the growing threats and demands for optimal functionality. Cross-browser and cross-device compatibility testing will remain essential, and continuous testing within DevOps pipelines will support agile development. Additionally, user experience and accessibility testing will become increasingly important to ensure applications are user-friendly and inclusive for all users.

- **Stage 3 :- future scope of SOC / SEIM**
    - Future security operation center (SOC) scope expansion is expected to be contingent upon technological advancements and a more complex threat scenario. Future SOC priority areas could include cloud and multi-cloud security, advanced threat detection and response, automation and orchestration, Internet of Things (IoT) security, and regulatory compliance.
    - As cognitive skills advance the system's ability to make decisions, artificial intelligence (AI) will play a bigger role in SIEM in the future. Additionally, as the number of endpoints rises, it will enable systems to expand and adapt. A SIEM solution has to ingest more data as a result of the Internet of Things, cloud computing, mobile devices, and other technologies. With AI, a system that can accommodate a wider variety of data types and a more intricate comprehension of the dynamic threat landscape may be possible.

Topics explored :- SOC, Threat intelligence integration, AI with Cyber Security, Project report creation & management, SEIM, Qradar
Tools explored :- NMAP, NESSUS, NIKTO, NSLOOKUP, SHODAN, Qradar, OWASP - Top 10 , Burp Suite

—--------THE END —-----------