Title of the project: - Hack2hack

Stage 1:

Introduction to the Open Web Application Security Project:

The Open Web Application Security Project (OWASP®) is a worldwide free and open community focused on improving the security of application software. Its mission is to make application security "visible", so that people and organizations can make informed decisions about application security risks.

The OWASP® Foundation works to improve the security of software through its community led open-source software projects, hundreds of chapters worldwide, tens of thousands of members, and by hosting local and global conferences. The OWASP is a nonprofit foundation that provides guidance on how to develop, purchase and maintain trustworthy and secure software applications. OWASP is noted for its popular Top 10 list of web application security vulnerabilities. It is globally recognized by developers as the first step towards more secure coding.

The OWASP Top 10 is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications. Companies should adopt this document and start the process of ensuring that their web applications minimize these risks. Using the OWASP Top 10 is perhaps the most effective first step towards changing the software development culture within your organization into one that produces more secure code.

List of teammates:

S.no.	Name	Collage	Contact
1.	Dr. Ashwin Raiyani	Nirma University	ashwin.rkcet@gmail.com
2.	Dr. Ashish Goswami	Adani University	ashish.goswami@adaniuni.ac.in

List of Vulnerability Table:

S.no	Vulnerability Name	CWE – No
1.	API-1 Broken object-level authorization	CWE-639: Authorization Bypass Through User-Controlled Key
2.	API-2 Broken authentication	CWE-204: Observable Response Discrepancy
3.	API-3 Broken object property level authorization	CWE-915: Improperly Controlled Modification of Dynamically-Determined Object Attributes
4.	API-4 Unrestricted resource consumption	CWE-799: Improper Control of Interaction Frequency
5.	API-5 Broken function level authorization	CWE-285: Improper Authorization
6.	API-6 Unrestricted access to sensitive business flows	CWE-223: Omission of Security-relevant Information
7.	API-7 Server-side request forgery (SSRF)	CWE-918 Server-Side Request Forgery (SSRF)
8.	API-8 Security misconfiguration	CWE-209 Generation of Error Message Containing Sensitive Information
9.	API-9 Improper inventory management	CWE-1059: Incomplete Documentation
10.	API-10 Unsafe consumption of APIs	CWE-319: Cleartext Transmission of Sensitive Information

Report:

1. **Vulnerability Name:** Broken object-level authorization

   CWE : CWE-639
   OWASP Category: API 1:2023 - Authorization Bypass Through User-Controlled Key
   Description: The system's authorization functionality does not prevent one user from gaining access to another user's data or record by modifying the key value identifying the data.
   Business Impact: Unauthorized access to other users' objects can result in data disclosure to unauthorized parties which may lead to data loss, or data manipulation. Under certain circumstances, unauthorized access to objects can also lead to full account takeover.

2. **Vulnerability Name:** Broken Authentication

   CWE: CWE-204
   OWASP Category: API 2:2023 - Observable Response Discrepancy
   Description: The product provides different responses to incoming requests in a way that reveals internal state information to an unauthorized actor outside of the intended control sphere.
   Business Impact: Attackers can gain complete control of other users' accounts in the system, read their personal data, and perform sensitive actions on their behalf. Systems are unlikely to be able to distinguish attackers' actions from legitimate user ones.

3. **Vulnerability Name:** Broken Object Property Level Authorization

   CWE: CWE-915
   OWASP Category: API 3:2023 - Observable Response Discrepancy
   Description: The product receives input from an upstream component that specifies multiple attributes, properties, or fields that are to be initialized or updated in an object, but it does not properly control which attributes can be modified.
   Business Impact: Unauthorized access to private/sensitive object properties may result in data disclosure, data loss, or data corruption. Under certain circumstances, unauthorized access to object properties can lead to privilege escalation or partial/full account takeover.

4. **Vulnerability Name:** Unrestricted Resource Consumption

   CWE: CWE-799

OWASP Category: API 4:2023 - Improper Control of Interaction Frequency
Description: The product does not properly limit the number or frequency of interactions that it has with an actor, such as the number of incoming requests.
Business Impact: Exploitation can lead to DoS due to resource starvation, but it can also lead to operational costs increase such as those related to the infrastructure due to higher CPU demand, increasing cloud storage needs, etc. For example, if an attacker writes a script that sends the first API call tens of thousands of times. The back-end follows and requests to send tens of thousands of text messages, leading the company to lose thousands of dollars in a matter of minutes.

5. **Vulnerability Name:** Broken Function Level Authorization

   CWE: CWE-285
   OWASP Category: API 5:2023 - Improper Authorization
   Description: The product does not perform or incorrectly performs an authorization check when an actor attempts to access a resource or perform an action.
   Business Impact: Such flaws allow attackers to access unauthorized functionality. Administrative functions are key targets for this type of attack and may lead to data disclosure, data loss, or data corruption. Ultimately, it may lead to service disruption.

6. **Vulnerability Name:** Unrestricted Access to Sensitive Business Flows

   CWE: CWE-223
   OWASP Category: API 6:2023 - Omission of Security-relevant Information
   Description: The product does not record or display information that would be important for identifying the source or nature of an attack, or determining if an action is safe.
   Business Impact: Exploitation might hurt the business in different ways, for example: rival companies may take benefit from known flows.

7. **Vulnerability Name:** Server-Side Request Forgery (SSRF)

   CWE: CWE-918
   OWASP Category: API 7:2023 - Server-Side Request Forgery (SSRF)
   Description: The web server receives a URL or similar request from an upstream component and retrieves the contents of this URL, but it does not sufficiently ensure that the request is being sent to the expected destination.

Business Impact: Exploitation might hurt the business in different ways, for example: prevent legitimate users from purchasing a product, or lead to inflation in the internal economy of a game.

8. **Vulnerability Name:** Security Misconfiguration

   CWE: CWE-209
   OWASP Category: API 8:2023 - Generation of Error Message Containing Sensitive Information
   Description: The product generates an error message that includes sensitive information about its environment, users, or associated data.
   Business Impact: Security misconfigurations not only expose sensitive user data, but also system details that can lead to full server compromise.

9. **Vulnerability Name:** Improper Inventory Management

   CWE: CWE-1059
   OWASP Category: API 9:2023 - Insufficient Technical Documentation
   Description: The product does not contain sufficient technical or engineering documentation (whether on paper or in electronic form) that contains descriptions of all the relevant software/hardware elements of the product, such as its usage, structure, architectural components, interfaces, design, implementation, configuration, operation, etc.
   Business Impact: Attackers can gain access to sensitive data, or even take over the server. Sometimes different API versions/deployments are connected to the same database with real data. Threat agents may exploit deprecated endpoints available in old API versions to get access to administrative functions or exploit known vulnerabilities.

10. **Vulnerability Name:** Unsafe consumption of APIs

    CWE: CWE-319
    OWASP Category: API 10:2023 - Cleartext Transmission of Sensitive Information
    Description: The product does not contain sufficient technical or engineering documentation (whether on paper or in electronic form) that contains descriptions of all the relevant software/hardware elements of the product, such as its usage, structure, architectural components, interfaces, design, implementation, configuration, operation, etc.
    Business Impact: The impact varies according to what the target API does with pulled data. Successful exploitation may lead to sensitive information exposure to unauthorized actors, many kinds of injections, or denial of service.

Stage 2

Overview :-

Nessus, developed by Tenable Network Security, is a powerful and widely-used vulnerability assessment tool designed to help organizations identify and address security vulnerabilities in their networks, systems, and applications. Its comprehensive scanning capabilities cover a wide range of platforms, including operating systems, network devices, and web applications. Nessus offers customizable scans, allowing users to target specific systems or vulnerability types, and maintains an extensive, regularly updated vulnerability database. The tool can perform compliance checks against various standards, generate detailed reports with severity ratings and remediation advice, and integrate with other security tools. Nessus employs a plugin-based architecture for easy updates and can conduct both remote and local assessments, scaling from small networks to enterprise environments. It operates by discovering active systems, gathering configuration information, and identifying potential vulnerabilities. While Nessus is a valuable asset for maintaining a strong security posture, it should be part of a broader security strategy and requires skilled personnel for effective use and result interpretation. Regular updates are crucial to ensure Nessus can detect the latest vulnerabilities, making it an essential tool in the ongoing effort to protect against evolving cyber threats.

Nessus is a widely-used vulnerability assessment tool developed by Tenable Network Security. It's designed to help organizations identify and address security vulnerabilities in their networks, systems, and applications.
Key features of Nessus include:

1. Comprehensive scanning: Nessus can detect a wide range of vulnerabilities across various platforms, including operating systems, network devices, and web applications.
2. Customizable scans: Users can configure scans based on their specific needs, targeting particular systems or vulnerability types.
3. Regularly updated vulnerability database: Nessus maintains an extensive, constantly updated database of known vulnerabilities.
4. Compliance checks: It can assess systems against various compliance standards like PCI DSS, HIPAA, and others.
5. Reporting: Nessus generates detailed reports on discovered vulnerabilities, including severity ratings and remediation advice.
6. Integration capabilities: It can be integrated with other security tools and management systems for a more comprehensive security approach.

7. Credential-based scanning: Nessus can perform more thorough scans when provided with system credentials.
8. Plugin-based architecture: This allows for easy updates and additions to scanning capabilities.
9. Remote and local assessment: It can perform both network-based and local security checks.
10. Scalability: Nessus can scan small networks or scale up to enterprise-level environments.

Nessus operates by first discovering active systems on a network, then probing these systems to gather information about their configuration, installed software, and potential vulnerabilities. It uses this information to identify security weaknesses and misconfigurations that could be exploited by attackers.

The tool is valuable for regular security assessments, helping organizations maintain a strong security posture by identifying and prioritizing vulnerabilities for remediation. However, it's important to note that while Nessus is powerful, it should be part of a broader, comprehensive security strategy that includes other tools and practices.

Effective use of Nessus requires skilled personnel who can interpret results, prioritize findings, and implement appropriate remediation measures. It's also crucial to keep Nessus updated to ensure it can detect the latest vulnerabilities.

Target website — rku.ac.in

Target IP address:- 142.93.216.124

List of vulnerability —

S.no	Vulnerability name	Severity	plugins
1	Apache 2.4.x < 2.4.60 Multiple Vulnerabilities	High	201198
2	Apache 2.4.x < 2.4.61	High	201532
3	Apache HTTP Server Version	None	48204
4	Common Platform Enumeration (CPE)	None	45590
5	Device Type	None	54615
6	DNS Server Detection	None	11002
7	DNS Server hostname.bind Map Hostname Disclosure	None	35371
8	Host Fully Qualified Domain Name (FQDN) Resolution	None	12053
9	HTTP Methods Allowed (per directory)	None	43111
10	HTTP Server Type and Version	None	10107
11	Inconsistent Hostname and IP Address	None	46215
12	Nessus Scan Information	None	19506
13	Nessus SYN scanner	None	11219
14	Non-compliant Strict Transport Security (STS)	None	42823

15	Open Port Re-check	None	10919
16	OS Identification	None	11936
17	Patch Report	None	66334
18	Service Detection	None	22964
19	Strict Transport Security (STS) Detection	None	42822
20	TCP/IP Timestamps Supported	None	25220
21	Traceroute Information	None	10287

REPORT:-

Vulnerability Name	HTTP Server Type and Version
severity	None
Plugin	10107
Port	80, 443
Description	This plugin attempts to determine the type and the version of the remote web server.
Solution	n/a
Business Impact	Reduced Security: If attackers identify an older server version, they can search for known exploits specific to that version. For example: Imagine a company running an outdated Apache server. An attacker discovers this and exploits a known vulnerability (CVE-2021-41773) to gain unauthorized access. This could lead to data breaches, financial losses, and reputational damage2. Operational Disruption: Successful exploitation can disrupt services, causing downtime and affecting business continuity.

Vulnerability Name	Traceroute Information
Severity	None
Plugin	10287
Port	0
Description	Makes a traceroute to the remote host.
Solution	n/a
Business Impact	

Vulnerability Name	Open Port Re-check
Severity	None
Plugin	10919
Port	0
Description	One of several ports that were previously open are now closed or unresponsive. There are several possible reasons for this : - The scan may have caused a service to freeze or stop running. - An administrator may have stopped a particular service during the scanning process. This might be an availability problem related to the following : - A network outage has been experienced during the scan, and the remote network cannot be reached anymore by the scanner. - This scanner may has been blacklisted by the system administrator or by an automatic intrusion detection / prevention system that detected the scan. - The remote host is now down, either because a user turned it off during the scan or because a select denial of service was effective. In any case, the audit of the remote host might be incomplete and may need to be done again.
Solution	Steps to resolve this issue include : - Increase checks_read_timeout and/or reduce max_checks. - Disable any IPS during the Nessus scan
Business Impact	Reconnaissance: Attackers can use Traceroute to map your network topology. By analysing the hops between routers, they gain insights into your organization's architecture. Vulnerability Identification: Traceroute exposes potential weak points. For instance: Imagine a financial institution. An attacker traces the route to their online banking server. If they find an unexpected intermediary server (say, an outdated firewall), they might exploit it. Risk to Confidentiality: Traceroute reveals IP addresses. If sensitive servers are exposed, attackers can target them directly. Operational Disruption: Malicious Traceroute requests can overload network devices, causing service disruptions.

Vulnerability Name	DNS Server Detection
Severity	None

Plugin	11002
Port	53
Description	The remote service is a Domain Name System (DNS) server, which provides a mapping between hostnames and IP addresses.
Solution	Disable this service if it is not needed or restrict access to internal hosts only if the service is available externally.
Business Impact	Exposed DNS servers can be a goldmine for attackers. They might hijack your web traffic, redirect customers to fake sites, or launch denial-of-service attacks. This can lead to data breaches, financial losses, and damaged reputation. Imagine your clients unable to reach you or, worse, being sent to malicious copycats. Protecting your DNS is crucial for maintaining trust and business continuity.

Vulnerability Name	Nessus SYN scanner
Severity	None
Plugin	11219
Port	53,80,443
Description	This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.
Solution	Protect your target with an IP filter.
Business Impact	The Nessus SYN scanner vulnerability is like leaving your front door unlocked. It allows attackers to map out your network's weak spots without you noticing. This can lead to data breaches, system downtime, and loss of customer trust. For your business, that could mean financial losses, damaged reputation, and potential legal issues. It's crucial to patch this vulnerability to protect your digital assets and maintain business continuity.

Vulnerability Name	OS Identification
Severity	None
Plugin	11936
Port	0
Description	Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.
Solution	n/a

Business Impact	company's systems as an open book, easily read by potential attackers. They can spot weaknesses, tailor attacks, and exploit specific flaws in your operating systems. This puts your sensitive data, operations, and reputation at risk. It's like leaving your house keys under the doormat – convenient for you, but also for intruders. Addressing this vulnerability is crucial to protect your business assets and maintain customer trust.

Vulnerability Name	Host Fully Qualified Domain Name (FQDN) Resolution
Severity	None
Plugin	12053
Port	0
Description	Nessus was able to resolve the fully qualified domain name (FQDN) of the remote host.
Solution	n/a
Business Impact	This issue can significantly affect your organization's network security and operations. Attackers exploiting this vulnerability may redirect users to malicious sites, compromising sensitive data and damaging your reputation. It could lead to financial losses, operational disruptions, and regulatory non-compliance. Addressing this vulnerability promptly is crucial to maintain customer trust, protect your brand, and ensure business continuity. I recommend immediate action to mitigate this risk.

Vulnerability Name	Nessus Scan Information
Severity	None
Plugin	19506
Port	0
Description	This plugin displays, for each tested host, information about the scan itself : - The version of the plugin set. - The type of scanner (Nessus or Nessus Home). - The version of the Nessus Engine. - The port scanner(s) used. - The port range scanned. - The ping round trip time - Whether credentialed or third-party patch management checks are possible. - Whether the display of superseded patches is enabled - The date of the scan. - The duration of the scan.

	- The number of hosts scanned in parallel. - The number of checks done in parallel.
Solution	n/a
Business Impact	These scans uncover potential weaknesses in your systems that cybercriminals could exploit. Left unaddressed, these vulnerabilities may lead to data breaches, financial losses, operational disruptions, and reputational damage. By prioritizing and patching these issues promptly, you're not just improving security – you're safeguarding your business continuity, customer trust, and bottom line. Remember, in today's digital landscape, robust cybersecurity is a competitive advantage and a crucial aspect of risk management.

Vulnerability Name	Service Detection
Severity	None
Plugin	22964
Port	80,443
Description	Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.
Solution	n/a
Business Impact	This flaw can expose your network services, giving attackers a roadmap to potential weak points. It's like leaving your company's blueprint visible to thieves. This vulnerability could lead to targeted attacks, data breaches, or service disruptions, damaging your reputation and bottom line. Addressing it is crucial to protect your assets, maintain customer trust, and avoid costly downtime. Think of it as reinforcing your digital fortress to keep your business safe and running smoothly.

Vulnerability Name	TCP/IP Timestamps Supported
Severity	None
Plugin	25220
Port	0
Description	The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.
Solution	n/a
Business Impact	It potentially allows attackers to fingerprint your systems, making targeted attacks easier. This could lead to data breaches, service disruptions, or unauthorized access. The impact may include financial losses, reputational damage, and regulatory fines. While not critical,

	addressing this vulnerability is a smart step in strengthening your overall security posture and reducing risk to your business operations.

Vulnerability Name	DNS Server hostname.bind Map Hostname Disclosure
Severity	None
Plugin	35371
Port	53
Description	It is possible to learn the remote host name by querying the remote DNS server for 'hostname.bind' in the CHAOS domain.
Solution	It may be possible to disable this feature. Consult the vendor's documentation for more information.
Business Impact	This vulnerability can expose your organization's network structure, potentially giving attackers valuable intel for further exploits. It's like accidentally leaving your building's blueprints visible to passersby. This information could help bad actors identify weak points, plan targeted attacks, or impersonate legitimate servers. The impact may include data breaches, service disruptions, or damage to your company's reputation. Addressing this issue is crucial to maintain a strong security posture and protect your business assets.

Vulnerability Name	Strict Transport Security (STS) Detection
Severity	None
Plugin	42822
Port	443
Description	The remote web server implements Strict Transport Security (STS). The goal of STS is to make sure that a user does not accidentally downgrade the security of his or her browser. All unencrypted HTTP connections are redirected to HTTPS. The browser is expected to treat all cookies as 'secure' and to close the connection in the event of potentially insecure situations.
Solution	n/a
Business Impact	As a cyber security consultant, I'd like to highlight the business impact of Strict Transport Security (STS) Detection vulnerability. This issue can leave your website open to man-in-the-middle attacks, potentially compromising sensitive data. Without proper STS implementation, attackers could intercept and manipulate traffic, leading to data breaches, financial losses, and reputational damage. Customers may lose trust in your online services, affecting your bottom line. Implementing STS is crucial for maintaining a secure connection and protecting your business assets in today's digital landscape.

Vulnerability Name	Non-compliant Strict Transport Security (STS)
Severity	None
Plugin	42823
Port	443
Description	The remote web server implements Strict Transport Security. However, it does not respect all the requirements of the STS draft standard.
Solution	n/a
Business Impact	This vulnerability leaves your website open to downgrade attacks, potentially exposing sensitive data. Customers may lose trust if their information is compromised, leading to reputational damage and financial losses. Additionally, non-compliance with STS could result in regulatory fines and legal issues. Fixing this vulnerability is crucial to protect your data, maintain customer confidence, and ensure smooth business operations in our increasingly digital world.

Vulnerability Name	Common Platform Enumeration (CPE)
Severity	None
Plugin	45590
Port	0
Description	By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host. Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.
Solution	n/a
Business Impact	Think of CPE as a universal language for IT products and systems. When vulnerabilities are found in these, it's like discovering weak spots in your company's armor. This can lead to data breaches, system downtime, or even theft of sensitive information. For businesses, this means potential financial losses, damage to reputation, and legal headaches. Staying on top of CPE vulnerabilities is crucial for protecting your digital assets and maintaining customer trust.

Vulnerability Name	HTTP Methods Allowed (per directory)
Severity	None
Plugin	43111
Port	80

Description	By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory. The following HTTP methods are considered insecure: PUT, DELETE, CONNECT, TRACE, HEAD Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request. As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes' in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501. Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.
Solution	n/a
Business Impact	It's like leaving multiple doors unlocked in your business. Attackers can exploit these open methods to manipulate your web server, potentially leading to unauthorized data access or system compromise. This could result in data breaches, reputational damage, and financial losses. Properly restricting HTTP methods to only those necessary for each directory is crucial. It's a simple yet effective way to reduce your attack surface and protect your business assets.

Vulnerability Name	Inconsistent Hostname and IP Address
Severity	None
Plugin	46215
Port	0
Description	The name of this machine either does not resolve or resolves to a different IP address. This may come from a badly configured reverse DNS or from a host file in use on the Nessus scanning host. As a result, URLs in plugin output may not be directly usable in a web browser and some web tests may be incomplete.
Solution	Fix the reverse DNS or host file.
Business Impact	This issue can be a real headache for your company. It opens the door for attackers to redirect your traffic, potentially exposing sensitive data or allowing malware infections. Your reputation could take a hit if

	customers can't trust your online presence. Plus, it might interfere with your network management, causing confusion and wasted time for your IT team. Addressing this vulnerability is crucial to maintain your business integrity and operational efficiency.

Vulnerability Name	Apache HTTP Server Version
Severity	None
Plugin	48204
Port	80,443
Description	The remote host is running the Apache HTTP Server, an open-source web server. It was possible to read the version number from the banner.
Solution	n/a
Business Impact	This issue could lead to unauthorized access and data breaches, potentially exposing sensitive customer information. It may result in significant downtime, lost revenue, and reputational damage. Compliance violations could trigger hefty fines. The cost of incident response and system upgrades could strain your budget. Overall, this vulnerability poses a serious threat to your business operations and customer trust if left unaddressed.

Vulnerability Name	Patch Report
Severity	None
Plugin	66334
Port	0
Description	The remote host is missing one or more security patches. This plugin lists the newest version of each patch to install to make sure the remote host is up-to-date. Note: Because the 'Show missing patches that have been superseded' setting in your scan policy depends on this plugin, it will always run and cannot be disabled.
Solution	Install the patches listed below.
Business Impact	This issue can seriously disrupt your business operations by exposing sensitive data and potentially leading to unauthorized system access. It may result in financial losses, damage to your reputation, and legal consequences. Swift action is crucial to protect your assets and maintain customer trust. By addressing this vulnerability promptly, you'll safeguard your business continuity and demonstrate your

	commitment to security. Let's work together to implement necessary patches and strengthen your overall cyber Défense strategy.

Vulnerability Name	Device Type
Severity	None
Plugin	54615
Port	0
Description	Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).
Solution	n/a
Business Impact	This vulnerability can be a real headache for businesses. It allows attackers to mess with your network devices, potentially causing chaos in your operations. Imagine your routers or firewalls suddenly going haywire - that's the kind of disruption we're talking about. It could lead to network outages, data breaches, or even unauthorized access to sensitive information. The financial hit from downtime and recovery efforts can be significant, not to mention the potential damage to your reputation. It's crucial to address this vulnerability promptly to protect your business interests.

Vulnerability Name	Apache 2.4.x < 2.4.60 Multiple Vulnerabilities
Severity	High
Plugin	201198
Port	80, 443
Description	The version of Apache httpd installed on the remote host is prior to 2.4.60. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.60 advisory. - Serving WebSocket protocol upgrades over a HTTP/2 connection could result in a Null Pointer dereference, leading to a crash of the server process, degrading performance. (CVE-2024-36387) - SSRF in Apache HTTP Server on Windows allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests or content Users are recommended to upgrade to version 2.4.60 which fixes this issue. Note: Existing configurations that access UNC paths will have to configure new directive UNCList to allow access during request processing. (CVE-2024-38472)

	- Encoding problem in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows request URLs with incorrect encoding to be sent to backend services, potentially bypassing authentication via crafted requests. Users are recommended to upgrade to version 2.4.60, which fixes this issue. (CVE-2024-38473) - Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts in directories permitted by the configuration but not directly reachable by any URL or source disclosure of scripts meant to only to be executed as CGI. Users are recommended to upgrade to version 2.4.60, which fixes this issue. Some RewriteRules that capture and substitute unsafely will now fail unless rewrite flag UnsafeAllow3F is specified. (CVE-2024-38474) - Improper escaping of output in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows an attacker to map URLs to filesystem locations that are permitted to be served by the server but are not intentionally/directly reachable by any URL, resulting in code execution or source code disclosure. Substitutions in server context that use a backreferences or variables as the first segment of the substitution are affected. Some unsafe RewiteRules will be broken by this change and the rewrite flag UnsafePrefixStat can be used to opt back in once ensuring the substitution is appropriately constrained. (CVE-2024-38475) - Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution via backend applications whose response headers are malicious or exploitable. Users are recommended to upgrade to version 2.4.60, which fixes this issue. (CVE-2024-38476) - null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request. Users are recommended to upgrade to version 2.4.60, which fixes this issue. (CVE-2024-38477) - Potential SSRF in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows an attacker to cause unsafe RewriteRules to unexpectedly setup URL's to be handled by mod_proxy. Users are recommended to upgrade to version 2.4.60, which fixes this issue. (CVE-2024-39573)

	Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.
Solution	Upgrade to Apache version 2.4.60 or later.
Business Impact	These flaws could allow attackers to disrupt your web services, potentially leading to downtime and lost revenue. Customer data might be at risk, damaging trust and reputation. Compliance issues may arise, resulting in fines. Addressing these vulnerabilities promptly is crucial to maintain business continuity, protect sensitive information, and preserve your company's standing. Upgrading to a patched version is strongly recommended to mitigate these risks.

Vulnerability Name	Apache 2.4.x < 2.4.61
Severity	High
Plugin	201532
Port	80,443
Description	The version of Apache httpd installed on the remote host is prior to 2.4.61. It is, therefore, affected by a vulnerability as referenced in the 2.4.61 advisory. - Apache HTTP Server: source code disclosure with handlers configured via AddType: A regression in the core of Apache HTTP Server 2.4.60 ignores some use of the legacy content-type based configuration of handlers. AddType and similar configuration, under some circumstances where files are requested indirectly, result in source code disclosure of local content. For example, PHP scripts may be served instead of interpreted. Users are recommended to upgrade to version 2.4.61, which fixes this issue. (CVE-2024-39884) Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.
Solution	Upgrade to Apache version 2.4.61 or later.
Business Impact	This flaw could allow attackers to bypass security restrictions and potentially execute malicious code. The impact may include data breaches, system compromises, and reputational damage. Businesses relying on affected Apache versions could face operational disruptions and financial losses. Prompt patching is crucial to mitigate these risks. However, the update process might temporarily affect web services, requiring careful planning to minimize downtime and ensure business continuity

Stage 3:

What is SOC?

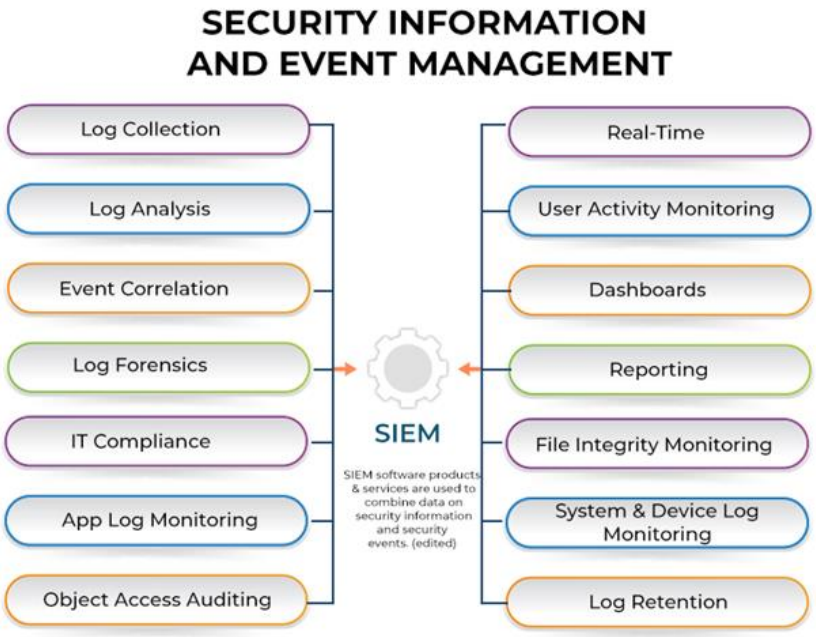
- A Security Operation Center (SOC) is a team of expert individuals who dedicate themselves to high-quality IT security operations.
- A SOC seeks to prevent cybersecurity threats, detects and responds to any incident on the computers, servers and networks it oversees. SOC has a unique ability to monitor all systems on an ongoing basis, as employees work in shifts, rotating and logging activity around the clock.
- As opposed to a traditional IT department, a SOC staff includes highly experienced cybersecurity analysts and trained engineers. These individuals use various computer programs and specialized security processes to point weaknesses in the company's virtual infrastructure and prevent these vulnerabilities from leading to theft.

How SOC cycle works?

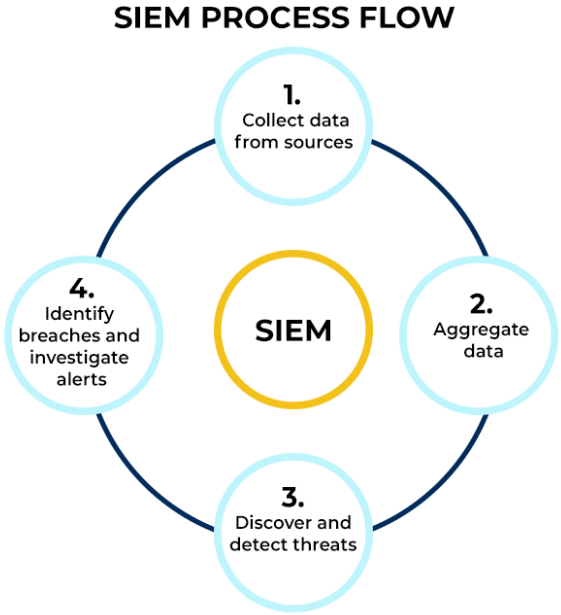
SOCs were created to facilitate collaboration among security personnel, with a primary focus on security monitoring and alerting, including the collection and analysis of data to identify suspicious activity and improve the organization's security.
A SOC can streamline the security incident handling process as well as help analysts triage and resolve security incidents more efficiently and effectively. In today's digital world, a SOC can be located in-house, in the cloud (a virtual SOC), staffed internally, outsourced (e.g., to an MSSP or MDR) or a mix of these.
SOCs can provide continuous protection with uninterrupted monitoring and visibility into critical assets across the attack surface. They can provide a fast and effective response, decreasing the time elapsed between when the compromise first occurred and the mean time to detection.

What Is Security Information and Event Management (SIEM)?

Security information and event management (SIEM) is a security solution that helps improve security awareness and identify security threats and risks. It collects information from various security devices, monitors and analyzes this information, and then presents the results in a manner that is relevant to the enterprise using it.



How Security Information and Event Management (SIEM) Cycle works ?



Data Collection:

- SIEM collects data from various sources within your organization. Imagine it as a cosmic net capturing signals from servers, applications, security devices, and systems.
- These signals include logs (like audit logs, firewall logs, and system logs) and events (such as login attempts, file modifications, or suspicious network traffic).

Data Aggregation:

- SIEM sorts and aggregates this data into meaningful categories. It's like organizing a chaotic library—putting all the mystery novels together, the cookbooks in their section, and the sci-fi books on their shelf.
- Aggregated data provides a comprehensive view of what's happening across your IT environment.

Data Analysis:

- SIEM doesn't just hoard data; it's an analytical wizard. It examines patterns, trends, and deviations.
- Behavioral rules (defined by your IT teams) come into play. SIEM compares the data against these rules to identify potential threats.
- For example, if a user suddenly accesses sensitive files at 3 AM, SIEM raises an eyebrow (or an alert).

Threat Detection and Alerting:

- SIEM's superpower is real-time threat detection. It spots anomalies faster than a caffeinated squirrel.
- When it detects something fishier than a sushi bar, it alerts your security team. "Hey, boss, we've got a breach attempt!"

Automated Responses (Optional):

- SIEM can also take action. Imagine it as a cyber butler: "Sir, someone's trying to break in. Shall I lock the virtual doors?"
- Automated responses might include quarantining a compromised device, blocking suspicious IPs, or sending stern emails to misbehaving users.

What is MISP?

MISP, formerly known as the Malware Information Sharing Platform, has now donned a new cape—it's the Open Source Threat Sharing Platform.

MISP is like a digital hub where cybersecurity superheroes gather to exchange vital information about threats, malware, and vulnerabilities. Imagine it as a secure vault where organizations can store, share, and receive structured intelligence related to cyber incidents.

Your college network information

Network Information Summary

- **Wi-Fi Security Protocols**: Nirma University uses WPA2, 802.1X, and firewalls to secure their campus-wide Wi-Fi network.
- **Privacy and Data Protection**: The university has a comprehensive Privacy Policy and employs encryption (WPA2), MAC ID filtering, and static IP addressing to protect students' data.
- **Network Monitoring**: The university uses CCTV surveillance to monitor activities on the campus, including academic areas, classrooms, libraries, and common spaces.
- **Access Control**: Only pre-approved devices are allowed to access the Wi-Fi network through MAC ID filtering.
- **Encryption**: Data transmitted over the Wi-Fi network is encrypted to prevent unauthorized access and eavesdropping.
- This summary highlights the key aspects of Nirma University's network security and privacy measures, ensuring a secure and private digital environment for its students and faculty.

How you think you deploy soc in your college

Deploying a SOC at Nirma University

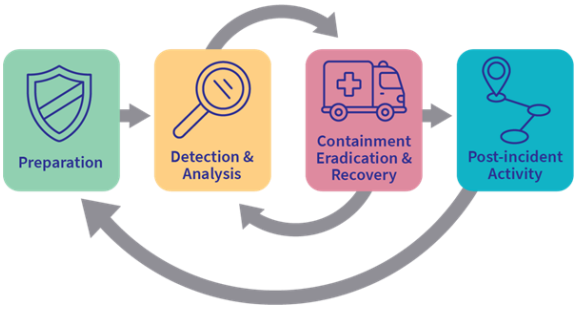
- Design and Planning: Define the university's security requirements, design the SOC infrastructure, and determine the necessary hardware, software, and personnel.
- Infrastructure and Technology: Install and configure the SIEM systems, network monitoring tools, and other security technologies to enable real-time monitoring and analysis.
- Personnel and Training: Recruit and train a team of security analysts, incident responders, and other personnel to operate the SOC 24/7.
- Monitoring and Detection: Establish detection rules and utilize various monitoring tools to collect and analyze data from multiple sources.
- Incident Response: Develop incident handling procedures and communication channels to ensure timely and effective response to security incidents.
- Maintenance and Improvement: Continuously monitor, maintain, and improve the SOC through regular audits and assessments.
- Integration with Existing Systems: Integrate the SOC with the university's CCTV surveillance, hostel, and campus security systems.
- Regulatory Compliance: Ensure the SOC complies with national, international, and university-specific security policies and regulations.

What is Threat intelligence?

Threat intelligence helps security teams be more proactive, enabling them to take effective, data-driven actions to prevent cyberattacks before they occur. It can also help an organization detect and respond to attacks in progress faster.

Security analysts create threat intelligence by gathering raw threat information and security-related information from multiple sources, then correlating and analyzing the data to uncover trends, patterns and relationships that provide an in-depth understanding of the actual or potential threats.

What is Incident response?



- Incident response refers to the strategic process companies, particularly IT and development teams, execute to swiftly address unplanned events or service interruptions. It aims to restore operational functionality and mitigate potential damages caused by cyber threats or breaches.

- Cyber-attacks or data breaches pose severe risks to businesses affecting customers, brand value, intellectual property, and resources. Incident response seeks to mitigate this harm and facilitate rapid recovery.

What is Qradar & understanding about tool

What Is IBM QRadar?:
QRadar is like a digital sentinel—a network security management platform designed to keep your castle (or rather, your network) safe.

It combines several superpowers:

Flow-Based Network Knowledge: Imagine QRadar as a traffic cop at a busy intersection. It analyzes network flows—data moving between devices—to spot anomalies and potential threats.
Security Event Correlation: QRadar connects the dots. It looks at security events—login attempts, firewall alerts, etc.—and figures out if they're part of a larger plot (like a cybercrime saga).
Asset-Based Vulnerability Assessment: QRadar scans your digital assets (servers, applications, endpoints) for vulnerabilities. It's like a health checkup for your network.

Why Does QRadar Matter?:
Real-Time Threat Detection: QRadar doesn't wait for smoke signals. It spots threats as they happen—whether it's a suspicious login, a worm wriggling through your servers, or an unauthorized file transfer.
Incident Prioritization: QRadar doesn't panic over every leaf rustling. It focuses on high-priority incidents. Think of it as a security butler whispering, "Sir, the dragon is at the gate!"
Full Visibility: QRadar shines a spotlight on your network, applications, and user activity. It's like having night vision goggles for your digital world.
How Does QRadar Work?:

Data Collection: QRadar gathers logs, flows, vulnerabilities, user activity, and asset data. It's the ultimate data hoarder (but in a good way).
Correlation Engine: QRadar's brain—the correlation engine—analyzes this data. It looks for patterns, outliers, and signs of trouble.
Anomaly Detection: If QRadar spots a user suddenly downloading the entire company database at 3 AM, it raises an eyebrow (or an alert).
Incident Response: When a threat knocks, QRadar doesn't just ring the doorbell; it kicks into action. It can quarantine devices, block malicious IPs, and send you urgent messages.
Use Cases:
Threat Hunting: QRadar helps you track down cyber beasts hiding in the forest of data.

Compliance: It ensures you're following the kingdom's rules (regulations) and keeps the auditors happy.
Incident Investigation: When the castle walls are breached, QRadar provides clues for your cyber detectives.

Conclusion :-

- **Stage 1 :- what you understand from Web application testing .**
  Web application testing is a critical process in software development and cybersecurity that focuses on evaluating the functionality, performance, and security of web-based applications. This comprehensive approach involves examining various aspects of a web application to ensure it meets specified requirements, performs efficiently, and resists potential security threats.

  The process typically includes testing the application's user interface, server-side logic, database interactions, and overall system integration. Testers use a combination of manual techniques and automated tools to simulate real-world usage scenarios and uncover potential issues. Key areas of focus often include functionality testing (ensuring all features work as intended), usability testing (evaluating user experience), compatibility testing (checking performance across different browsers and devices), performance testing (assessing speed and responsiveness under various loads), and security testing (identifying vulnerabilities that could be exploited by attackers).

  Security testing is particularly crucial in web application testing. It involves techniques like penetration testing, vulnerability scanning, and code reviews to identify potential security flaws such as cross-site scripting (XSS), SQL injection, or insecure authentication mechanisms. The goal is to uncover and address these vulnerabilities before they can be exploited by malicious actors.

  Web application testing is an ongoing process, as applications often undergo updates and face evolving security threats. It plays a vital role in maintaining the quality, reliability, and security of web applications in an increasingly interconnected digital landscape.
- **Stage 2 :- what you understand from the nessus report .**
  A Nessus report is a comprehensive document generated after a vulnerability scan, providing detailed insights into the security posture of the scanned systems or networks. These reports are crucial for understanding potential vulnerabilities and prioritizing remediation efforts.

Typically, a Nessus report includes an executive summary, detailing the overall risk level and key findings. It then breaks down discovered vulnerabilities by severity (critical, high, medium, low), providing specific details for each, including affected systems, vulnerability descriptions, potential impacts, and recommended fixes.

The report often includes technical details like affected ports, services, and specific vulnerability identifiers (e.g., CVE numbers). It may also provide compliance information related to various security standards.

Importantly, Nessus reports offer actionable intelligence, helping security teams prioritize their efforts by focusing on the most critical vulnerabilities first. They serve as a valuable tool for ongoing security management, allowing organizations to track their progress in addressing vulnerabilities over time and maintain a robust security posture.

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

SOC (Security Operations Center), SIEM (Security Information and Event Management), and QRadar Dashboard are all integral components of modern cybersecurity infrastructure, working together to provide comprehensive threat detection and response capabilities.

A SOC is the central unit that oversees an organization's security operations, continuously monitoring and analyzing the security posture of an organization's systems and networks. It's staffed by security analysts who use various tools and processes to detect, investigate, and respond to cyber threats in real-time.

SIEM is a key technology used within SOCs. It collects and aggregates log data generated throughout the organization's technology infrastructure, from network devices and applications to identity systems and data access. SIEM tools provide real-time analysis of security alerts generated by applications and network hardware.

QRadar, developed by IBM, is a specific SIEM solution. Its dashboard offers a centralized view of an organization's security posture, presenting complex security data in a visually accessible format. The QRadar dashboard typically displays key security metrics, threat intelligence, and real-time alerts. It allows security analysts to quickly identify potential threats, track ongoing investigations, and manage incident response activities.

These systems work together to provide a holistic view of an organization's security landscape, enabling rapid threat detection, efficient incident response, and continuous

improvement of security measures. They're essential for maintaining a robust cybersecurity posture in the face of evolving threats.

Future Scope :-

- **Stage 1 :- future scope of web application testing**
  The future scope of web application testing is evolving rapidly, driven by technological advancements and changing threat landscapes. Here are key areas of development:

  AI and Machine Learning integration will enhance automated testing, improving detection of complex vulnerabilities and reducing false positives. This will allow for more efficient, accurate, and predictive testing processes.

  With the rise of IoT and mobile applications, testing will expand to cover a wider range of devices and platforms, requiring more sophisticated cross-platform testing methodologies.

  As applications become more complex and interconnected, there will be an increased focus on API security testing and microservices architecture testing.

  Continuous testing in DevOps pipelines will become standard, with more emphasis on shift-left testing practices to catch vulnerabilities earlier in the development cycle.

  The growing adoption of cloud-native applications will necessitate specialized testing for cloud environments, focusing on issues like data privacy, multi-tenancy, and scalability.

  As privacy regulations evolve, there will be a greater emphasis on testing for compliance with data protection laws like GDPR and CCPA.

  Emerging technologies like blockchain and quantum computing will introduce new security challenges, requiring novel testing approaches.

  This evolving landscape will demand more sophisticated tools and highly skilled professionals who can adapt to these changing requirements.
  Stage 2 :- future scope of testing process you understood .
  The future of testing processes is poised for significant evolution, driven by technological advancements and changing software development paradigms. Here's a concise overview of the key trends: Automation will become more prevalent, with AI and machine learning

enhancing test creation, execution, and result analysis. This will lead to more efficient, accurate, and comprehensive testing. Continuous testing will be further integrated into DevOps and CI/CD pipelines, enabling faster feedback and more frequent releases. Shift-left testing will become standard, catching issues earlier in development.

Testing will expand to cover a wider range of platforms and technologies, including IoT devices, cloud-native applications, and emerging technologies like blockchain and quantum computing. There will be increased focus on non-functional testing aspects such as security, performance, and user experience, reflecting growing concerns in these areas. Test data management and synthetic data generation will become more sophisticated to address privacy concerns and regulatory compliance. Crowd-sourced and AI-assisted testing may supplement traditional QA teams, providing diverse perspectives and scalability. As systems become more complex, there will be a growing emphasis on end-to-end testing and integration testing across interconnected services and APIs. These trends point towards a future where testing processes are more automated, integrated, and comprehensive, requiring testers to continually update their skills and adapt to new technologies and methodologies.

- **Stage 3 :- future scope of SOC / SEIM**

The future scope of SOC (Security Operations Center) and SIEM (Security Information and Event Management) is poised for significant evolution:

AI and Machine Learning integration will enhance threat detection and response capabilities, enabling more accurate prediction and automated remediation of security incidents. This will help handle the increasing volume and complexity of threats. Cloud-native SOC and SIEM solutions will become more prevalent, offering scalability and flexibility to accommodate diverse and distributed IT environments. This will include better integration with cloud services and containerized applications. There will be increased focus on User and Entity Behavior Analytics (UEBA) to detect insider threats and sophisticated attacks that bypass traditional security measures.

SOCs will adopt more proactive approaches, emphasizing threat hunting and continuous security posture improvement rather than just reactive incident response. Integration of Threat Intelligence will become more sophisticated, providing real-time, contextualized insights to inform decision-making and response strategies.

Automation and orchestration will play a larger role in SOC operations, streamlining routine tasks and allowing analysts to focus on complex issues. Extended Detection and Response (XDR) capabilities will be integrated, providing a more holistic view of threats across multiple security layers. As privacy regulations evolve, SOC and SIEM solutions will incorporate more robust data privacy and compliance features.

These advancements aim to address the growing sophistication of cyber threats and the increasing complexity of IT environments, making SOC and SIEM more effective and efficient in protecting organizations.

Topics explored :-

key areas typically covered in cybersecurity workshop:

1. Vulnerability Assessment and Management
2. Web Application Security Testing
3. Network Security and Penetration Testing
4. Security Information and Event Management (SIEM)
5. Incident Response and Forensics
7. Mobile Application Security
8. API Security
10. Threat Intelligence and Threat Hunting
11. Compliance and Regulatory Requirements
12. Identity and Access Management
13. Encryption and Cryptography
14. Malware Analysis
15. Social Engineering and Phishing
16. Wireless Network Security
17. IoT Security
18. Artificial Intelligence and Machine Learning in Cybersecurity
20. Risk Assessment and Management

These topics cover a broad spectrum of cybersecurity domains, reflecting the multifaceted nature of modern information security. They encompass both offensive and defensive security practices, as well as emerging technologies and methodologies in the field.

Tools explored:-

Vulnerability Scanners:
- Nessus: Comprehensive vulnerability assessment tool

Web Application Security:
- OWASP ZAP: Open-source web app scanner
- Burp Suite: Popular web vulnerability scanner and proxy

Network Security:
- Nmap: Network discovery and security auditing

SIEM Tools:
- Splunk: Data analysis and visualization platform

Penetration Testing:
- Metasploit: Exploitation framework
- Kali Linux: Penetration testing OS with various tools