Project Report

Enhancing Cyber Security Through Vulnerability Analysis and Mitigation

Team: Cryptic Commandos

Stage 1-3

12 July, 2024

Overview

The "Cryptic Commandos" project aims to delve into the intricate world of cyber security, focusing on the identification, analysis, and mitigation of common vulnerabilities. As cyber threats become increasingly sophisticated, the necessity for robust security measures is paramount. This project endeavors to educate and equip participants with the skills and knowledge required to safeguard 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, Security Misconfiguration, 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.

Team Members:

SNo	Name	College	Contact
1	Prof. Mayur Padia	Darshan University	mayur.padia **@darshan.ac.in**
2	Dr. Maitri Patel	Institute of Advanced Research	maitru1487288 **@gmail.com**
3	Prof. Kruti Lavingia	Nirma University	kruti.lavingia **@nirmauni.ac.in**
4	Prof. Rachana Mehta	Nirma University	rachana.mehta **@nirmauni.ac.in**
5	Dr. Lata Gohil	Nirma University	lata.gohil **@nirmauni.ac.in**

List of Vulnerabilities Table

SNo	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** 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-Broken Access Control**
CWE	CWE-1345: Broken Access Control: Weaknesses in OWASP
OWASP/SANS Category	A01:2021-Broken Access Control

Description: Broken Access Control refers to security vulnerabilities that exploit weaknesses in the mechanisms that enforce access restrictions on resources. These mechanisms are designed to ensure that users can only access data and perform actions that they are authorized to. When access control is broken, attackers can gain unauthorized access to sensitive information, modify data, or perform actions as other users.

A common way to categorize these vulnerabilities is by the type of privilege escalation they enable:

- Horizontal privilege escalation: An attacker gains access to the same level of permissions as another user, but for a different account.
- Vertical privilege escalation: An attacker gains access to a higher level of permissions than they are authorized for.

Broken Access Control is the most prevalent vulnerability according to the OWASP Top 10 2021, with over 318,000 occurrences identified across tested applications.

Business Impact: The business impact of Broken Access Control vulnerabilities can be severe. Potential consequences include:

- **Data breaches**: Attackers can steal sensitive data such as customer information, financial records, or intellectual property.
- **Disruption of operations**: Attackers can manipulate data, leading to errors or system outages.
- **Loss of trust**: If customer data is compromised, it can damage the organization's reputation and lead to lost business.
- **Regulatory compliance fines**: Organizations may be fined for violating data protection regulations if they fail to adequately secure their systems.

Vulnerability Name	**A02:2021-Cryptographic Failures**
CWE	CWE-259: Use of Hard-coded Password
OWASP/SANS Category	A02:2021-Cryptographic Failures

Description: A02:2021-Cryptographic Failures refers to vulnerabilities that arise due to improper implementation or management of cryptographic mechanisms. This category encompasses a wide range of issues, including:

- **Weak encryption algorithms**: Using outdated or insecure encryption algorithms can make it easier for attackers to decrypt sensitive data.
- **Poor key management**: Weak key generation, insecure storage, or predictable key usage can compromise the entire encryption system.
- **Missing or improper data encryption**: Sensitive data, both in transit (over networks) and at rest (on storage devices), should be encrypted to prevent unauthorized access.
- **Use of insecure protocols**: Outdated or unpatched communication protocols like unencrypted HTTP can be exploited to intercept sensitive information.

Here are some CWEs that are more closely related to A02:2021:

CWE-327: Broken or Risky Cryptographic Algorithm: Using weak or outdated encryption algorithms.

CWE-331: Insufficient Entropy: Keys or random numbers used in cryptography are not unpredictable enough, making them easier to guess.

Business Impact: The business impact of Cryptographic Failures can be devastating. Potential consequences include:

- **Data breaches**: Attackers can steal sensitive data like financial information, personal details, or intellectual property if it's not properly encrypted.
- **System compromise**: Attackers can gain unauthorized access to systems or accounts if they can bypass encryption mechanisms.
- **Loss of trust**: If sensitive data is compromised, it can damage the organization's reputation and lead to lost business.
- **Regulatory compliance fines**: Organizations may be fined for violating data protection regulations if they fail to adequately secure their systems with strong cryptography.

Vulnerability Name	**A03:2021-Injection**
CWE	CWE-20 Improper Input Validation
OWASP/SANS Category	A03:2021-Injection

Description: The product receives input or data, but it does not validate or incorrectly validates that the input has the properties that are required to process the data safely and correctly.

Business Impact: Improper input validation (CWE-20) can result in injection vulnerabilities (A03:2021-Injection), which can have serious consequences for businesses. These consequences include financial losses, reputational harm, regulatory fines, legal ramifications, intellectual property theft, and interruptions to corporate operations. These flaws give hackers the ability to take advantage of holes in data processing, which can lead to sensitive data being accessed without authorization, downtime for operations, and high recovery expenses. For this reason, having strong input validation procedures is essential to protecting company operations and adhering to data protection laws.

Vulnerability Name	**A04:2021-Insecure Design**
CWE	CWE-213: Exposure of Sensitive Information Due to Incompatible Policies
OWASP/SANS Category	A04:2021-Insecure Design

Description: The product's intended functionality exposes information to certain actors in accordance with the developer's security policy, but this information is regarded as sensitive according to the intended security policies of other stakeholders such as the product's administrator, users, or others whose information is being processed.

Business Impact: The vulnerability A04:2021-Insecure Design (CWE-213: Exposure of Sensitive Information Due to Incompatible Policies) can have a substantial negative impact on business by exposing sensitive information to unauthorized actors. Confidential user and administrative data may be compromised as a result of this

vulnerability, eroding stakeholder confidence and perhaps leading to data breaches. The consequences of such accidents can include fines for breaking data protection regulations, possible legal obligations, and significant financial losses from having to fix security breaches and lost revenue. Furthermore, the harm to one's reputation resulting from such incidents can undermine client trust and adversely affect one's standing in the market and earnings. To reduce these risks, it is essential to make sure that the security policies of the developer and other stakeholders are in line.

Vulnerability Name	**A05:2021-Security Misconfiguration**
CWE	CWE-756 Missing Custom Error Page
OWASP/SANS Category	A05:2021-Security Misconfiguration

Description: The product does not return custom error pages to the user, possibly exposing sensitive information.

Business Impact: CWE-756: Missing Custom Error Page vulnerability has the potential to have a substantial commercial effect. This vulnerability happens when an application does not provide bespoke error pages, which may leak sensitive information or make the program more vulnerable to attacks. Here are some of the main impacts:

- **Information Disclosure**: Default error pages may reveal important information about the server environment, including program versions, directory structures, and settings. This information may be beneficial for attackers seeking to exploit other vulnerabilities.
- **Security Risk**: Generic error messages may reveal technical details such as stack traces and database queries, allowing attackers to find application flaws.
- **User Experience**: Default error pages may be confusing or uninformative for users. Poor error management can cause frustration and drive people away from the service.
- **Damage to reputation**: Default error pages may give consumers a negative impression of the application's professionalism and security. This can harm the company's reputation, particularly if security issues arise.
- **Compliance Issues**: Ensure adequate error handling and sensitive information protection in accordance with regulatory standards and industry best practices. Failure to implement custom error pages may result in noncompliance with these standards.

- **Exploitation chance**: Default error pages provide information that attackers can use to create tailored assaults, raising the chance of successful breaches and data theft.

Vulnerability Name	**A06 Vulnerable and Outdated Components**
CWE	CWE-1104 Use of Unmaintained Third Party Components
OWASP/SANS Category	A06 Vulnerable and Outdated Components

Description: The product relies on third-party components that are not actively supported or maintained by the original developer or a trusted proxy for the original developer.Reliance on components that are no longer maintained can make it difficult or impossible to fix significant bugs, vulnerabilities, or quality issues. In effect, unmaintained code can become obsolete.

This issue makes it more difficult to maintain the product, which indirectly affects security by making it more difficult or time-consuming to find and/or fix vulnerabilities. It also might make it easier to introduce vulnerabilities.

Business Impact: CWE-1104: Use of Unmaintained Third Party Components vulnerability has the potential to have a significant and varied business impact. This vulnerability occurs when software relies on third-party components that are no longer supported or updated. Here are some important impacts:

Security Risks:

- **Unpatched Vulnerabilities**: Unmaintained components frequently have unpatched vulnerabilities that attackers can exploit, resulting in data breaches, system compromise, or unauthorized access.
- **Increased Attack Surface**: Using older components expands the attack surface, giving attackers more opportunities to discover and exploit flaws.

Compliance Issues:

- **Regulatory Noncompliance**: Many sectors have requirements that require the usage of up-to-date and secure software components. Using unmaintained components can lead to noncompliance, resulting in fines, legal responsibilities, and reputational damage.

- **Audit failures**: Failing security audits owing to the existence of unmaintained components might result in more scrutiny and required corrective actions.

Operational disruption:

- **System downtime**: Exploits that target unmaintained components can cause system outages, affecting corporate operations and resulting in financial losses.
- **Maintenance Burden**: Integrating and maintaining workarounds or custom patches for unmaintained components can increase the workload for IT and security personnel.
- **Reputational Damage**: Customers and partners may lose trust in a firm if it is discovered that it uses unsecure or outdated software components.
- **Brand Impact**: Security events caused by unmaintained components can impact a company's brand and market position.

Increased costs:

- **Incident Response**: Resolving security issues caused by vulnerabilities in unmaintained components can be expensive and time-consuming.
- **Upgrade and Replacement Costs**: Replacing unmaintained components with maintained equivalents can result in significant expenses and development effort.

Loss of Competitive advantage:

- **Innovation Stagnation**: Using old components may hinder the company's capacity to adopt new technologies and advances, thus putting it at a competitive disadvantage.
- **Technical Debt**: Relying on unmaintained components can cause technical debt to accumulate, slowing down the development and deployment of new features and products.

To reduce these effects, businesses should:

- Conduct frequent audits of all third-party components to identify any that are no longer supported.
- Update and patch: Make sure that all components are up to date and patched on a regular basis.
- Prepare for Replacement: Create a strategy for replacing unmaintained components with actively supported alternatives.
- Improve Monitoring: Set up monitoring and alerting systems to swiftly discover and respond to possible security vulnerabilities involving third-party components.

- Proactively managing third-party components is critical for ensuring a secure and robust software environment.

Vulnerability Name	**A07:2021-Identification and Authentication Failures**
CWE	CWE-287 Improper Authentication
OWASP/SANS Category	A07:2021-Identification and Authentication Failures

Description: When an actor claims to have a given identity, the product does not prove or insufficiently proves that the claim is correct. This weakness occurs when an application improperly verifies the identity of a user. If software incorrectly validates user logon information or allows using different techniques of malicious credentials gathering (e.g. brute force, spoofing), an attacker can gain certain privileges within the application or disclose sensitive information.

Business Impact: The business impact of Improper Authentication vulnerabilities can be severe. Potential consequences include:

- The attacker could potentially gain unauthorized access to the application and restricted areas, enabling them to perform actions such as revealing sensitive information, modifying the application, or even executing arbitrary code.
- Financial loss or theft as a result of fraudulent activity could arise via system exploitation.
- If consumer data is compromised, there may be a loss of trust and harm to the company's reputation.
- Services and company activities may be disrupted by unauthorized access.

Vulnerability Name	**A08:2021-Software and Data Integrity Failures**
CWE	CWE-830 Inclusion of Web Functionality from an Untrusted Source
OWASP/SANS Category	A08:2021-Software and Data Integrity Failures

Description: The product includes web functionality (such as a web widget) from another domain, which causes it to operate within the domain of the product, potentially granting total access and control of the product to the untrusted source including third party functionality in a web-based environment is risky, especially if the source of the functionality is untrusted.

Even if the third party is a trusted source, the product may still be exposed to attacks and malicious behavior if that trusted source is compromised, or if the code is modified in transmission from the third party to the product. This weakness is common in "mashup" development on the web, which may include source functionality from other domains.

Business Impact: The business impact of Inclusion of Web Functionality from an Untrusted Source vulnerabilities can be severe. Potential consequences include:

- Legal action, fines, and penalties may follow security breaches that lead to noncompliance with data protection rules.
- Malicious functionality has the potential to seriously impair service performance and cause website outages, among other major interruptions to corporate operations.
- Unauthorized access may lead to the theft of intellectual property or confidential information, which could hurt the business's ability to compete.
- Untrusted online features have the potential to compromise the supply chain and have an adverse effect on downstream partners, suppliers, and consumers.
- The system's security and functioning could be further jeopardized by malware, ransomware, or spyware introduced via unreliable sources.
- Untrusted web sources have the potential to compromise the supply chain and have an adverse effect on downstream partners, suppliers, and consumers.

Vulnerability Name	**A09:2021-Security Logging and Monitoring Failures**
CWE	CWE-778 Insufficient Logging
OWASP/SANS Category	A09:2021-Security Logging and Monitoring Failures

Description: When a security-critical event occurs, the product either does not record the event or omits important details about the event when logging it. When security-critical events are not logged properly, such as a failed login attempt, this can

make malicious behavior more difficult to detect and may hinder forensic analysis after an attack succeeds. As organizations adopt cloud storage resources, these technologies often require configuration changes to enable detailed logging information, since detailed logging can incur additional costs. This could lead to telemetry gaps in critical audit logs. For example, in Azure, the default value for logging is disabled.

Business Impact: It occurs when a system does not generate a sufficient amount of logs for security-related events. This can impact business as mentioned below:

- Due to a lack of proper logs, security breaches remain undetected, which allows attackers to do more attacks and damage the system.
- As there are insufficient logs, sensitive data may remain unmonitored, which makes it prone to data breaches
- Insufficient logs lead to make the incident response process weak
- Lack of sufficient logs leads to the forensic task being more costly after the attack happening
- Operational downtime increases as it takes more time to resolve issues due to the proper amount of logs
- It is also possible that due to a lack of sufficient amount of logs, it hinders the process of diagnosing issues, which may lead to system reliability and performance
- It may damage the company's reputation and lead to business loss due to customer churn.

Vulnerability Name	**A10:2021-Server-Side Request Forgery**
CWE	CWE-918 Server-Side Request Forgery (SSRF)
OWASP/SANS Category	A10:2021-Server-Side Request Forgery

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. By providing URLs to unexpected hosts or ports, attackers can make it appear that the server is sending the request, possibly bypassing access controls such as firewalls that prevent the attackers from accessing the URLs directly. The server can be used as a proxy to conduct port

scanning of hosts in internal networks, use other URLs such as that can access documents on the system (using file://), or use other protocols such as gopher:// or tftp://, which may provide greater control over the contents of requests.

Business Impact: This occurs when attackers make it possible to trick a server into making requests to unauthorized and unintended locations.

- Attackers can access the internal network of the company, which leads to data breaches
- It results in financial loss to the company due to reasons such as overloading internal resources, causing service downtime, and additional financial cost the company face for detecting and resolving such attacks
- Company may suffer from theft of proprietary data or intellectual properties
- Loss of market for the company due to leakage of sensitive data related to company business

Project Report

Enhancing Cyber Security Through Vulnerability Analysis and Mitigation

Team: Cryptic Commandos

Stage 2

12 July, 2024

Overview

Nessus provides a strong solution for detecting and reducing security threats and is an incredibly efficient tool for performing thorough vulnerability checks on websites. Nessus, created by Tenable Inc., is well known for its ability to carry out thorough scans that reveal a variety of vulnerabilities, from typical web application dangers to intricate security difficulties. This makes it a crucial part of any security plan for a website.

Key Features and Functionality

Comprehensive Scanning Capabilities: SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF), unsafe direct object references, and other vulnerabilities can all be found in online applications by using Nessus's vulnerability scanning tool. If these vulnerabilities are not fixed, attackers may use them to obtain unauthorized access, steal information, or interfere with services.

Extensive Plugin Library: The programme makes use of a large collection of plugins, each of which is made to find a particular kind of vulnerability. The most recent security flaws and threats are always being added to this library. Through the use of these plugins, Nessus makes sure that its scans are thorough and up to date, encompassing the most recent vulnerabilities that may impact a website.

Configuration and Compliance Checks: Apart from detecting vulnerabilities, Nessus assesses the website's setup to guarantee compliance with security best practices. It looks for out-of-date software, unsafe setups, and other problems that can jeopardize the security of the website. Nessus also offers comprehensive compliance reports and suggestions to help guarantee adherence to industry standards and laws like PCI-DSS, HIPAA, and OWASP Top Ten.

Severity Ratings and Risk Assessment: Nessus rates the potential effect and exploitability of each vulnerability it finds, assigning a severity rating. By concentrating on the most serious vulnerabilities first, this risk-based strategy assists security teams in prioritizing remedial efforts. Through quick resolution of high-severity vulnerabilities, organizations can drastically lower their exposure to risk.

Detailed Reporting and Dashboards: Compiling descriptions, impacted locations, and suggested remedial methods, the tool creates thorough reports that outline the vulnerabilities detected. Security teams can successfully handle issues that have been found with the use of these reports' actionable insights. Additionally, Nessus provides dashboards that show scan results, point out patterns, and monitor remediation efforts over time. Making decisions and comprehending the entire security posture are made easier with the help of this data visualization.

Customization and Flexibility: Users can alter scan policies and schedules in Nessus to meet their own requirements. Nessus gives you the freedom to tailor scans to your needs, be it a comprehensive evaluation or a focused scan of a specific web application component. This customisation guarantees that the scans are comprehensive and in line with the security goals of the organization.

Practical Application in Website Security

To conduct a vulnerability assessment on a website using Nessus, security professionals typically follow these steps:

Preparation

- Set the scope of the evaluation, including which apps for the web, servers, and components will be inspected.
- Ensure that Nessus has the appropriate permissions to access and scan the target systems thoroughly.

Configuration

- Customize the scan policies to target web application vulnerabilities. This may include selecting web security-related plugins, adjusting scan depth, and establishing scan schedules.
- Configure Nessus to monitor compliance with applicable industry standards and internal security rules.

Execution

- Launch the scan and track its progress. Nessus will run a series of tests and inspections, using its plugin library to find vulnerabilities.
- Ensure that scans are non-intrusive and do not interfere with the website's normal operation.

Analysis and Reporting

- Examine the detailed scan reports produced by Nessus. These reports will provide a list of identified vulnerabilities, severity ratings, and recommended remedial steps.
- Use the dashboards to visually represent the scan results and discover trends or recurring concerns.

Remediation

- Prioritize remedial activities according to Nessus' severity assessments. To reduce risk exposure, start by addressing the most serious vulnerabilities.
- Implement the recommended repair actions and ensure that the vulnerabilities have been fixed with subsequent scans.

Continuous Monitoring

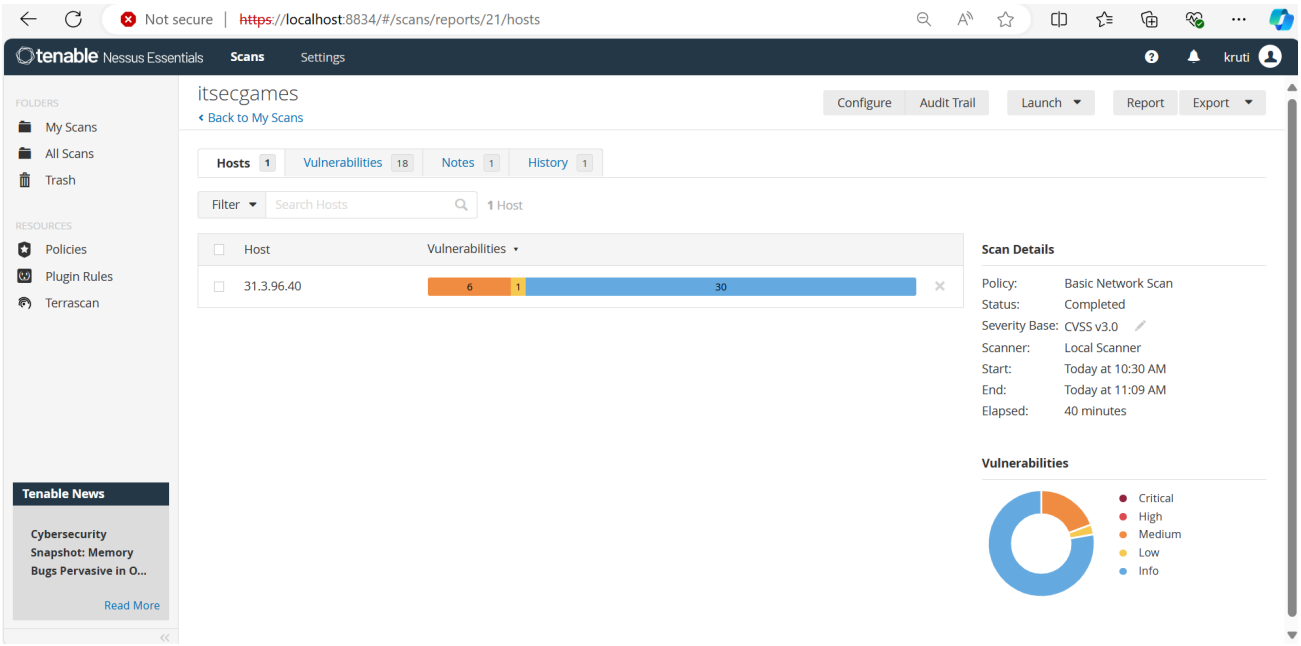
- Schedule scans on a regular basis to ensure that new vulnerabilities are identified and handled as quickly as possible. Continuous monitoring promotes a robust security posture and mitigates emerging risks.

Finally, Nessus is an effective and versatile tool for conducting website vulnerability evaluations. Its broad scanning capabilities, extensive plugin library, and detailed reporting make it a necessary component of a strong website security strategy. Organizations can use Nessus to proactively discover and remediate vulnerabilities, maintain compliance with industry standards, and improve their overall security posture.

Target Website	http://www.itsecgames.com/
Target IP Address	31.3.96.40

List of Vulnerabilities:

SNo	Vulnerability Name	Severity	Plugins
1	web.config File Information Disclosure	Medium	121479
2	HSTS Missing From HTTPS Server (RFC 6797)	Medium	142960
3	SSL Certificate Cannot Be Trusted	Medium	51192
4	SSL Self-Signed Certificate	Medium	57582
5	TLS Version 1.0 Protocol Detection	Medium	104743
6	TLS Version 1.1 Deprecated Protocol	Medium	157288
7	ICMP Timestamp Request Remote Date Disclosure	Low	10114
8	Service Detection	Info	22964
9	OS Identification	Info	11936
10	Apache HTTP Server Version	Info	48204



Report

Vulnerability Name	**web.config File Information Disclosure**
Severity	Medium
Plugin	121479
Port	tcp/80/www

Description: An information disclosure vulnerability exists in the remote web server due to the disclosure of the web.config file. An unauthenticated, remote attacker can exploit this, via a simple GET request, to disclose potentially sensitive configuration information.

Solution:

Ensure proper restrictions are in place, or remove the web.config file if the file is not required.

Business Impact: The vulnerability involving the disclosure of the web.config file poses a significant business impact due to its potential to expose sensitive configuration details of a web application or server. Web.config files typically contain critical information such as database connection strings, encryption keys, authentication

settings, and other configurations that are crucial for the proper functioning and security of the application. Here's a detailed exploration of the business impact:

Operational Disruption: Firstly, the exposure of sensitive information through the web.config file can lead to operational disruptions. Attackers gaining access to this file can exploit vulnerabilities or misconfigurations, potentially leading to service interruptions or system crashes. This can result in downtime for the application or website, directly impacting business operations and causing financial losses.

Data Breach and Privacy Concerns: The disclosure of sensitive data like database credentials or encryption keys can lead to data breaches. Unauthorized access to such information can compromise customer data, intellectual property, or proprietary business processes. This not only violates regulatory requirements but also damages the organization's reputation and customer trust, leading to potential legal liabilities and financial penalties.

Reputational Damage: A breach resulting from the web.config file disclosure can severely tarnish the organization's reputation. Customers, partners, and stakeholders may lose trust in the company's ability to protect their sensitive information, affecting brand loyalty and customer retention. Negative publicity and media attention further exacerbate the situation, making it challenging to recover public confidence even after mitigative actions are taken.

Compliance and Regulatory Impact: For businesses operating in regulated industries such as finance, healthcare, or e-commerce, the exposure of sensitive configuration details violates compliance requirements (e.g., GDPR, HIPAA, PCI-DSS). Non-compliance can lead to regulatory fines, legal actions, and restrictions on business operations, affecting revenue streams and market competitiveness.

Costs of Remediation: Addressing the vulnerability involves comprehensive measures such as reviewing and revising security configurations, implementing access controls, and possibly redesigning aspects of the application architecture. These remediation efforts incur significant costs in terms of IT resources, consultancy fees, and potential business disruption during the implementation phase.

In conclusion, the web.config file disclosure vulnerability represents more than just a technical issue—it poses a direct threat to business continuity, data security, regulatory

compliance, and brand reputation. Proactively addressing such vulnerabilities through robust security measures and regular audits is crucial for safeguarding organizational assets and maintaining stakeholder trust in an increasingly interconnected digital landscape.

Vulnerability Name	**HSTS Missing From HTTPS Server (RFC 6797)**
Severity	Medium
Plugin	142960
Port	tcp/443/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: The absence of HTTP Strict Transport Security (HSTS) on a web server poses significant business risks that extend beyond mere technical vulnerabilities. HSTS, defined by RFC 6797, is crucial for ensuring secure communication between browsers and servers by mandating HTTPS connections. Without HSTS, several exploitable scenarios emerge, impacting both the organization and its users.

Firstly, the vulnerability exposes users to downgrade attacks. Attackers can potentially force users onto unencrypted HTTP connections instead of HTTPS, compromising the confidentiality and integrity of sensitive data exchanged between the user's browser and the server. This can lead to data interception, manipulation, or theft, posing legal and reputational risks to the organization.

Secondly, the absence of HSTS makes the server susceptible to SSL-stripping attacks. In such attacks, malicious entities can intercept HTTPS requests and convert them into HTTP, thereby bypassing secure channels and gaining access to sensitive information transmitted between the server and the user. This undermines trust in the

organization's ability to protect user data, potentially resulting in customer churn and damage to brand reputation.

Furthermore, HSTS helps mitigate cookie-hijacking attacks by ensuring that cookies are only sent over secure HTTPS connections. Without HSTS, cookies transmitted over HTTP can be intercepted and manipulated, leading to unauthorized access to user accounts, financial transactions, or confidential business information. Such breaches can trigger regulatory penalties, legal liabilities, and loss of business opportunities.

From a compliance standpoint, industries such as finance, healthcare, and e-commerce may face legal repercussions for failing to implement adequate security measures like HSTS. Regulatory bodies increasingly mandate stringent security protocols to safeguard user privacy and data integrity. Non-compliance could result in fines, legal actions, and restrictions on business operations, impacting revenue streams and market competitiveness.

Ultimately, the business impact of not implementing HSTS extends beyond immediate technical vulnerabilities to encompass legal, financial, and reputational consequences. Organizations must prioritize the adoption of HSTS to safeguard their users' data, maintain regulatory compliance, preserve brand integrity, and mitigate the risks associated with evolving cybersecurity threats. By proactively securing their web infrastructure with HSTS, businesses can foster trust, protect sensitive information, and demonstrate commitment to robust cybersecurity practices in an increasingly digital landscape.

Vulnerability Name	**SSL Certificate Cannot Be Trusted**
Severity	Medium
Plugin	51192
Port	tcp/443/www

Description: The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an

unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the middle attacks against the remote host.

Solution:

Purchase or generate a proper SSL certificate for this service.

Business Impact: The SSL Certificate Cannot Be Trusted vulnerability, identified by plugin 51192 on port tcp/443/www, poses a medium severity risk to organizations relying on secure web communications. This issue arises when a server's X.509 certificate fails to establish a trusted chain of authority, potentially exposing users to security risks.

Firstly, if the certificate chain is not rooted in a recognized public certificate authority (CA), users visiting the affected website may receive warnings about the site's authenticity. This undermines trust and could deter visitors from engaging with the site, impacting user confidence and potentially leading to reduced traffic and conversion rates. For e-commerce platforms or sites handling sensitive information, this could translate into direct financial losses and damage to reputation.

Secondly, certificates with validity issues, such as being outside their valid date range, may prevent users from accessing the site altogether, further disrupting business operations. This can lead to service downtime, loss of productivity, and frustration among users and customers reliant on the affected services.

Thirdly, certificates with incorrect or unverifiable signatures open the door to potential man-in-the-middle (MitM) attacks. Attackers could exploit this vulnerability to intercept communications between users and the server, potentially gaining unauthorized access to sensitive data such as login credentials, payment information, or proprietary business data. The fallout from such a breach extends beyond immediate financial losses to encompass regulatory penalties, legal liabilities, and long-term damage to brand reputation.

For public-facing services, the impact is compounded as any compromise in SSL certificate trustworthiness undermines the ability of users to securely interact with the website. This not only affects current customers but also deters potential new users who prioritize security in their online interactions. In highly regulated industries such as finance, healthcare, and e-commerce, non-compliance with security standards regarding SSL certificates can lead to severe consequences, including fines and loss of licenses.

In conclusion, addressing the SSL Certificate Cannot Be Trusted vulnerability is crucial for maintaining trust, safeguarding data integrity, and preserving business continuity. Organizations must promptly purchase or generate valid SSL certificates from reputable CAs and ensure proper certificate management practices to mitigate these risks effectively. Proactive maintenance of SSL certificates is essential to uphold security standards, protect user trust, and safeguard against the potentially devastating impacts of cyber threats.

Vulnerability Name	**SSL Self-Signed Certificate**
Severity	Medium
Plugin	57582
Port	tcp/443/www

Description: The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote

host. Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution:
Purchase or generate a proper SSL certificate for this service.

Business Impact: The SSL Self-Signed Certificate vulnerability, as identified by plugin 57582 on port tcp/443/www, poses a medium severity risk to organizations relying on secure communication channels over the internet. This vulnerability arises when the X.509 certificate chain used by a service is not signed by a recognized certificate authority (CA). This lack of proper authentication opens up significant business impacts and security concerns.

Security Risks:
Firstly, the use of self-signed certificates undermines the trust model of SSL/TLS encryption. In practical terms, it means that the authenticity and integrity of the communication between the client and the server cannot be assured. This allows malicious actors the potential to intercept, manipulate, or eavesdrop on sensitive data transmitted between parties. Such a compromise could lead to unauthorized access to confidential information, including financial data, personal details, or proprietary business information.

Regulatory and Compliance Issues:
From a regulatory standpoint, many industries are bound by stringent data protection laws and compliance standards (e.g., GDPR, HIPAA, PCI-DSS) that mandate the use of trusted SSL certificates. Failure to comply with these requirements can result in hefty fines, legal consequences, and damage to an organization's reputation. Moreover, in sectors like finance and healthcare, where data privacy is paramount, the use of insecure communication channels can lead to severe penalties and loss of customer trust.

Operational Disruptions:
Addressing this vulnerability requires immediate remediation efforts, such as purchasing or generating a proper SSL certificate from a recognized CA. This process involves downtime and potential disruption to services relying on HTTPS for secure transactions or communication. For businesses operating around the clock or relying heavily on online services, even a brief interruption can translate into financial losses and impact customer satisfaction.

Reputational Damage:
Beyond financial implications, the discovery of SSL Self-Signed Certificate vulnerabilities can tarnish an organization's reputation. In an era where cybersecurity incidents frequently make headlines, customers, partners, and stakeholders expect robust security measures. Any perceived negligence in safeguarding sensitive data can lead to loss of business opportunities, erosion of customer loyalty, and diminished market competitiveness.

Conclusion:
In conclusion, while the SSL Self-Signed Certificate vulnerability may seem technical in nature, its business impact extends far beyond IT concerns. It touches upon regulatory compliance, operational continuity, and most critically, the trust and confidence that stakeholders place in an organization's ability to protect sensitive information. Addressing this vulnerability promptly and effectively is not just a matter of compliance but a strategic imperative for maintaining business resilience and safeguarding reputation in a digitally interconnected world.

Vulnerability Name	**TLS Version 1.0 Protocol Detection**
Severity	Medium
Plugin	104743
Port	443 / tcp / www

Description: The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.
As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.
PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

Solution:

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

Business Impact: The TLS (Transport Layer Security) Version 1.0 Protocol Detection vulnerability can have serious economic consequences due to the inherent security concerns of employing old and insecure cryptographic protocols. Here are some of the possible business impacts:

Data breaches and loss of confidentiality

- **Sensitive Data Exposure**: Several vulnerabilities in TLS 1.0 allow attackers to decode sensitive data transported over the network. This can result in the disclosure of confidential information such as client data, financial records, and intellectual property.
- **Compliance Violations**: Many legal standards (such as PCI-DSS, HIPAA, and GDPR) demand the use of robust encryption to safeguard sensitive data. Using TLS 1.0 may result in noncompliance with certain requirements, incurring legal penalties and fines.

Reputational Damage

- Customers trust businesses to secure their personal and financial information. A data breach caused by the use of TLS 1.0 can erode client trust and ruin the company's reputation.
- **Brand Image**: The public exposure of a security breach caused by obsolete practices can have a detrimental influence on the brand's image, making it difficult to acquire and keep customers.

Financial Loss

- **Direct costs**: include incident response, forensic investigations, legal fees, regulatory fines, and compensation for harmed customers, which can be enormous.
- **Indirect Costs**: Business loss owing to a lack of customer trust, as well as potential long-term damage to the company's market position, can result in considerable financial losses.

Operational Disruption

- **System Downtime**: Addressing a security breach may require taking systems offline, resulting in downtime that can disrupt business operations and reduce productivity.
- **Remediation Efforts**: Significant resources may need to be allocated to patching systems, upgrading to newer versions of TLS, and conducting thorough security assessments to ensure no further vulnerabilities exist.

Competitive Disadvantage

- **Loss of Competitive Edge**: In an industry where data security is a key differentiator, failing to protect customer data effectively can put a company at a competitive disadvantage compared to peers that have stronger security measures in place.
- **Market Perception**: Competitors may use the security lapse to their advantage, promoting their own secure practices to attract customers concerned about data protection.

Legal and regulatory consequences

- **Regulatory scrutiny**: Noncompliance with data protection standards owing to the usage of outdated processes may result in heightened scrutiny from regulatory organizations.
- **Litigation**: Affected consumers or business partners may sue the corporation for failing to protect their data sufficiently.

Mitigation Strategies: To reduce the dangers related to TLS 1.0, firms should:

- Upgrade to TLS 1.2 or higher: Ensure that all systems and applications support and use the most recent versions of TLS.
- Conduct frequent security audits to identify and address any use of out-of-date protocols.
- Employee Training: Educate employees on the necessity of following secure protocols and remaining current on security best practices.
- Vendor Management: Ensure that third-party vendors and partners adhere to security standards and do not employ outdated protocols.
- Businesses can protect themselves from the risks connected with the TLS 1.0 Protocol Detection vulnerability by taking proactive steps to mitigate it.

Vulnerability Name	**TLS Version 1.1 Deprecated Protocol**
Severity	Medium
Plugin	157288
Port	443 / tcp / www

Description: The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1
As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

Solution:
Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Business Impact: The TLS Version 1.1 Deprecated Protocol vulnerability can have severe economic implications:

Data breach and compliance violations

- **Sensitive Data Exposure**: TLS 1.1 is insecure, exposing private information.
- **Regulatory Noncompliance**: Using TLS 1.1 may result in legal penalties and fines for failing to meet security standards.

Reputation and Financial Loss

- **Customer Trust**: A breach can erode customer trust and harm the company's brand.
- **Direct and Indirect Costs**: Incident response, legal fees, and lost business can all cause major financial losses.

Operational disruption and competitive disadvantage

- **System Downtime**: Addressing breaches may need system downtime, which disrupts operations.
- **Competitive Advantage**: Failure to preserve data can place a business at a competitive disadvantage.

Legal and Regulatory Consequences

- Regulatory Scrutiny: Noncompliance might result in greater regulatory scrutiny.
- Litigation: Affected parties may bring a lawsuit against the corporation.

Mitigation Strategies

- **Upgrade to TLS 1.2 or higher**: Ensure that all systems use the most recent TLS versions.
- **Regular Audits**: Conduct security audits to identify and address outdated protocols.
- **Employee Training**: Educate employees on security standards and best practices.
- **Vendor Management**: Ensure that third parties adhere to security standards.
- Addressing the TLS 1.1 issue ahead of time contributes to strong security and compliance measures.

Vulnerability Name	**ICMP Timestamp Request Remote Date Disclosure**
Severity	Low
Plugin	10114
Port	icmp/0

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, and the outgoing ICMP timestamp replies.

Business Impact: The disclosure of this information can have several business impacts:

- **Timing assaults**: By synchronizing their assaults, an attacker can evade detection or take advantage of timing vulnerabilities if they are aware of the system time.

- **Time-based Authentication**: Time-based authentication techniques are employed by some systems. These defenses may be weakened if the system time is revealed.
- **System Synchronization**: Making the system time public can let you know how the network handles time synchronization, which you might use to your advantage in future attacks.
- **Incident Response**: Time disclosure can help attackers avoid discovery, which increases the difficulty and duration of incident response.
- **System Integrity**: To interfere with logs and monitoring systems, attackers may modify system time. This might make it more difficult to do forensic analysis following a security event.

Vulnerability Name	**Service Detection**
Severity	Info
Plugin	22964
Port	(tcp/80/www), (tcp/443/www)

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. The remote service could be identified.

Solution:
Service Detection is vulnerability, so it doesn't require a solution.

Business Impact: In Nessus, service detection refers to the process of identifying the services running on a network's hosts. By locating open ports and identifying the services and apps that are listening on them, this procedure aids in vulnerability assessment. The Service Detection information has impact on following business components :

- **Improved Security Posture**: By detecting services, possible vulnerabilities unique to that services may be found and remedies specifically. Using the appropriate patches and updates is facilitated by knowing the precise version of the services that are operating on the network.

- **Risk management**: Service detection helps with risk assessment and security effort prioritization by revealing when vital services are exposed.
- **Regulatory obligations**: By verifying that only permitted services are operational and adequately protected, service detection information assists enterprises in meeting compliance obligations.
- **Asset Management**: Appropriate resource allocation and asset management are facilitated by maintaining an accurate inventory of services.
- **Proactive Threat Management**: By spotting irregularities or unexpected services, routine service detection scans make proactive threat hunting possible.

Vulnerability Name	**OS Identification**
Severity	Info
Plugin	11936 (1)
Port	tcp/0

Description: It is possible to guess the remote operating system. 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:
Not applicable as severity is information.

Business Impact: Knowing OS helps find vulnerabilities specific to the operating system. Making scans particular to the identified OS provide more accurate results. Following are the business impacts for the same:

- It helps improve protection by suggesting patching designed explicitly for the identified OS.
- Reduce chances of attacks by allowing the identification of outdated and unsupported OS, prompting upgrades or replacement.
- Allows the avoidance of financial penalties by providing information about OS compliance with regulation.
- Reduce downtimes during business operations by ensuring a secure system

- Build customer trust by maintaining reputation through strong security practices

Vulnerability Name	**Apache HTTP Server Version**
Severity	Info
Plugin	48204 (2)
Port	tcp/80/www

Description: It is possible to obtain the version number of the remote Apache HTTP server. 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:
Not applicable as severity is information.

Business Impact: Knowing Apache HTTP Server Version helps identify security issues in web servers. Following are the business impacts for the same:

- It helps improve protection by suggesting patching specifically designed for the identified Apache version.
- Reduce chances of attacks by allowing the identification of outdated and unsupported Apache versions, prompting upgrades or replacement.
- Allows the avoidance of financial penalties by providing information about Apache version compliance with the regulation.
- Reduce downtimes during business operations by ensuring a secure server
- Build customer trust by maintaining reputation through strong security practices

Vulnerability Name	**OS Identification**
Severity	Info
Plugin	11936
Port	tcp/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: The vulnerability described, OS Identification via remote probes, though categorized as informational with Plugin ID 11936, can have significant business implications if exploited. While the severity is low, understanding the potential impacts is crucial for businesses to assess their risk posture.

- Firstly, the ability to identify the remote operating system (OS) and potentially its version allows malicious actors to gather intelligence about the target environment. This knowledge can aid in crafting more targeted attacks, exploiting specific vulnerabilities known to exist in certain OS versions. For instance, if a remote probe identifies an outdated OS version with known vulnerabilities, it becomes easier for attackers to devise exploits or malware that could compromise the system.
- Moreover, OS identification can be leveraged in reconnaissance activities, where attackers map out the network architecture and system configurations. This information is valuable for planning subsequent stages of an attack, such as identifying high-value assets or determining the best approach for further infiltration. In a worst-case scenario, this could lead to unauthorized access to sensitive data, disruption of services, or even full-scale network compromise.
- From a business perspective, the implications extend beyond immediate security concerns. A successful exploitation could result in financial losses due to operational downtime, costs associated with incident response and recovery, legal liabilities stemming from compromised data, and reputational damage among customers and partners. For industries handling sensitive information like finance, healthcare, or government sectors, regulatory penalties for inadequate security measures can further exacerbate these impacts.
- Furthermore, the perception of poor cybersecurity practices can erode customer trust and loyalty, potentially leading to loss of business opportunities or competitive disadvantage in the market. Organizations may also face increased scrutiny from regulatory bodies and stakeholders demanding stricter security measures to prevent future incidents.

In conclusion, while OS Identification vulnerability (Plugin ID 11936) is categorized as informational and may not pose an immediate threat of direct exploitation, its potential for facilitating more targeted attacks and compromising security integrity underscores the importance of proactive risk management and robust cybersecurity measures. Businesses must prioritize ongoing vulnerability assessments, timely patching of systems, and employee awareness to mitigate such risks effectively and safeguard their operations, assets, and reputation.

Vulnerability Name	**Apache HTTP Server Version**
Severity	info
Plugin	48204
Port	tcp/80/www

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: The vulnerability identified in the Apache HTTP Server Version, Plugin 48204, relates to the exposure of server version information through its banner. While this vulnerability is classified as having an 'info' severity level, it can still have significant business impact, albeit indirectly, particularly in terms of security and operational integrity.

- Firstly, the exposure of server version information can provide attackers with insights into the specific software version running on the server. This knowledge enables them to tailor their attacks more precisely, targeting known vulnerabilities associated with that particular version. For instance, older versions of Apache HTTP Server may have known exploits or vulnerabilities that have been patched in newer releases. Attackers can exploit this knowledge to attempt to gain unauthorized access, disrupt services, or compromise sensitive data.
- Moreover, from a compliance and regulatory standpoint, such vulnerabilities can pose risks. Many compliance standards, such as PCI DSS (Payment Card Industry Data Security Standard) and GDPR (General Data Protection Regulation),

emphasize the importance of protecting server information to prevent unauthorized access and data breaches. Failure to address such vulnerabilities could result in regulatory fines, legal implications, and damage to the organization's reputation.

- From an operational perspective, maintaining server security is crucial for ensuring uninterrupted service delivery. Exploitation of vulnerabilities in web servers like Apache can lead to downtime, loss of productivity, and disruption of critical business operations. This can translate into financial losses, especially for businesses heavily reliant on their web presence for sales, customer service, or communication.
- Furthermore, the perception of security by customers and partners can be affected. Public disclosure of vulnerabilities, even if classified as 'info,' can erode trust and confidence in an organization's ability to safeguard sensitive information. This loss of trust may deter potential customers from engaging with the company, impacting revenue and growth.

In conclusion, while the Apache HTTP Server Version vulnerability may not directly lead to immediate exploitation or data compromise, its implications are far-reaching. It underscores the importance of comprehensive security measures, regular updates, and proactive monitoring to mitigate risks and maintain the integrity of web server environments. Addressing such vulnerabilities not only enhances security posture but also safeguards business continuity and preserves organizational reputation in the competitive digital landscape.

Project Report

Enhancing Cyber Security Through Vulnerability Analysis and Mitigation

Team: Cryptic Commandos

Stage 3

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.

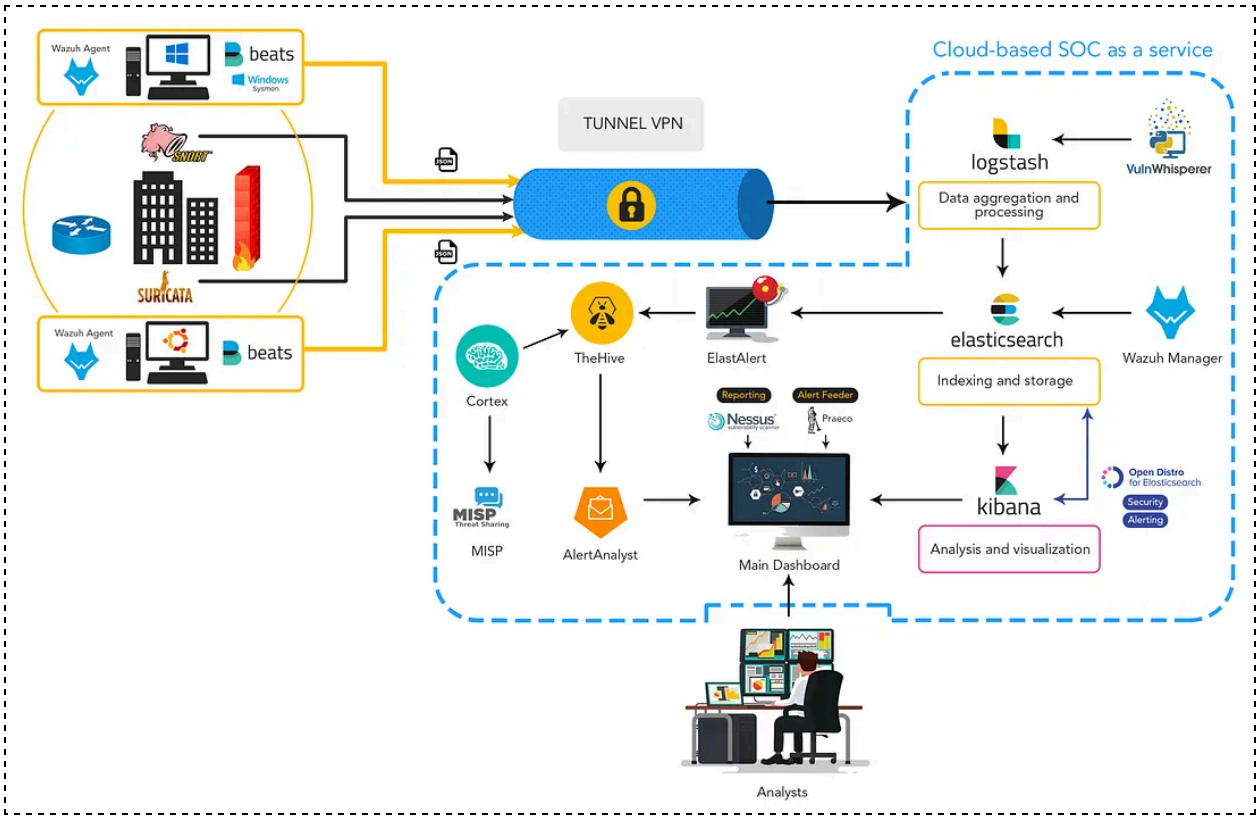
- **Forensic Analysis**: When an incident occurs, forensic analysis is conducted to understand the nature and extent of the breach. This helps in identifying the attackers, their methods, and any compromised data.
- **Reporting and Compliance**: The SOC generates reports on security incidents, threat 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 incidents significantly improve an organization's security posture.
- **Reduced Downtime and Damage**: Quick detection and response minimize the damage and downtime caused by security incidents.
- **Regulatory Compliance**: A SOC helps ensure compliance with industry standards and regulations by maintaining proper security practices and documentation.
- **Improved Threat Detection**: With a dedicated team and advanced tools, a SOC can detect 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 digital assets 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.

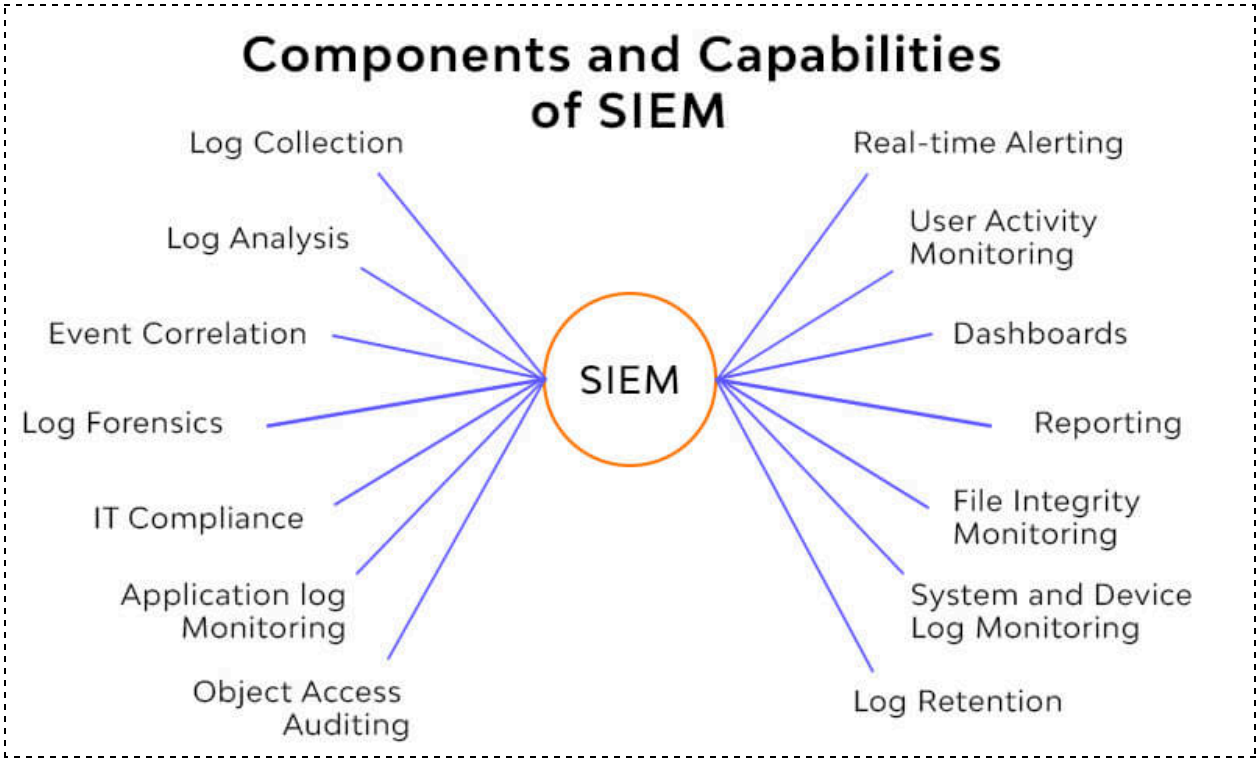
- **Threat Detection and Incident Response Layer**
  - TheHive: An incident response platform that integrates with ElastAlert for managing security incidents. It organizes and tracks incident response activities.
  - Cortex: Analyzes observables and indicators of compromise (IOCs) related to security 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.

- Open Distro for Elasticsearch: Provides security alerting and additional functionalities to enhance the SOC's capabilities.

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 the IT 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 modern SIEM 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. This helps SIEM investigate any risks within the enterprise and go farther.
- **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. Through this connection, SIEM may produce more effective outcomes.
- **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 sources both 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 a variety of formats.
- **Dashboards and Reporting**: Produce personalized reports and design dashboards to see 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, and use 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 with the 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 execution of 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 effective in 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 definition of 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.

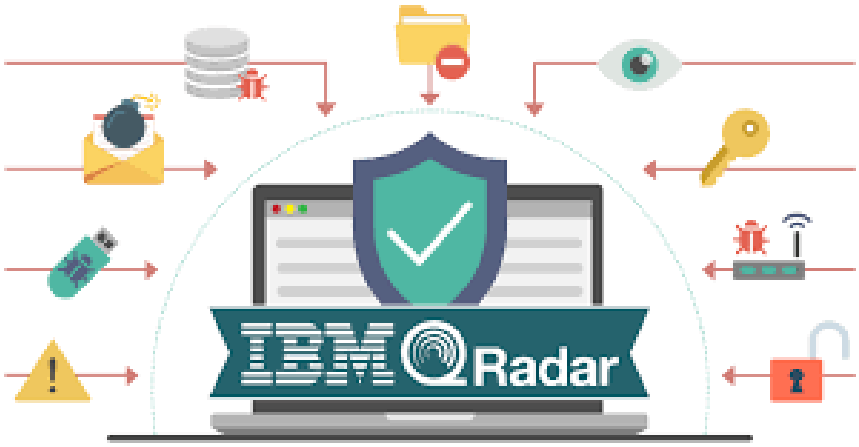
Qradar & Understanding about Tool

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 for compliance 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 decreasing false 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 stakeholders.

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 of the application to ensure it is robust, reliable, and secure. It involves a combination of manual and automated testing techniques to identify and fix issues, thereby ensuring a high-quality user experience.

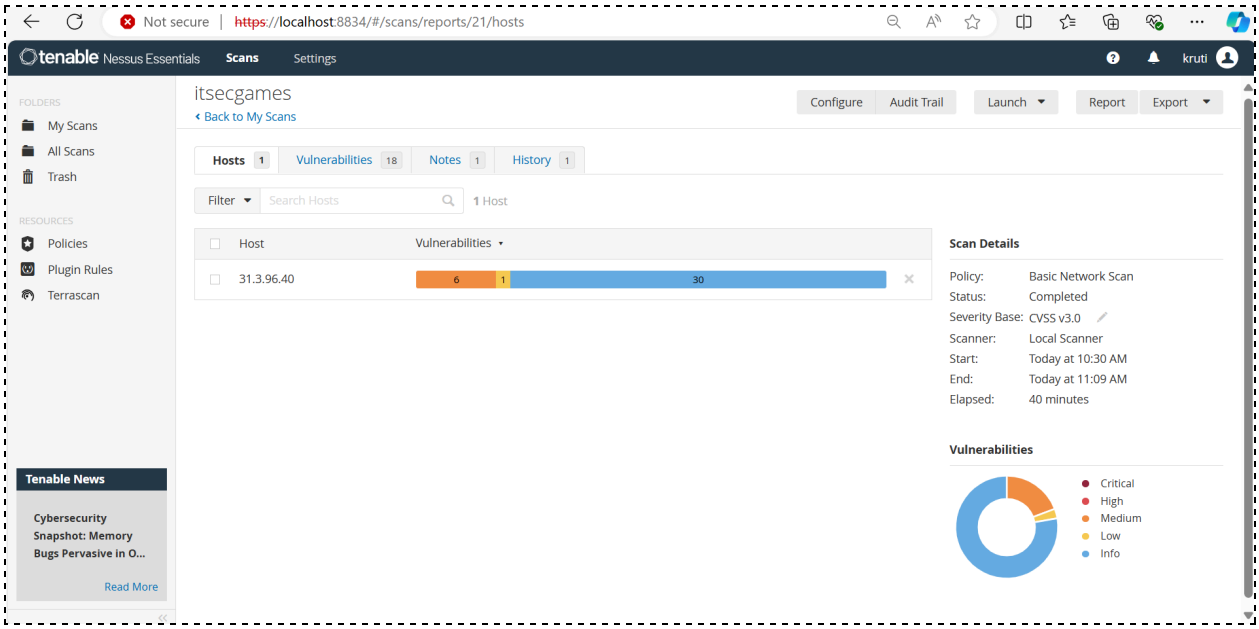
Stage 2: What you understand from the Nessus report.

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 / Qradar Dashboard.

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 landscape.

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