AI FOR CYBER SECURITY WITH IBM QRADAR

PROJECT TITLE: AI BASED NETWORK ANOMALY DETECTION TOOL

TEAM 4.3
[Anomaly Detectors]

Team Members:
Jammalamadaka Manasa
Chikkam Venkat Satya Dhiraj
Avuthu Lasya
M. Om Nivas

INDEX

Content **Page No.**
Abstract ……………………………………………………… 3-4
List of vulnerabilities table ……………………………… 4
Report on the vulnerabilities obtained …………………. 5-10
Nessus ……………………………………………………… 11-12
List of vulnerabilities scanned through Nessus ……….. 12-13
Report on the vulnerabilities obtained ………………… 13-19
SOC, SIEM and IBM QRadar ………………………… 19-26
Conclusion ……………………………………………….. 26-30
Future Scope ……………………………………………... 30-32
Topics explored …………………………………………… 32
Tools explored ……………………………………………... 33

Abstract:

Network Anomaly Detection is a critical component of modern cybersecurity infrastructure. It involves the identification of abnormal patterns or behaviours within a network that may indicate security threats, performance issues, or operational problems. As networks grow in complexity and face ever evolving threats, the need for advanced Network Anomaly Detection tools becomes paramount. This abstract states the vision and key components of such a tool.

In the rapidly evolving landscape of network security, the detection of anomalies has become a critical component to safeguard against cyber threats. Traditional rule based methods fall short in addressing the complexity and sophistication of modern attacks. To combat this challenge, this paper presents a design thinking approach for developing a cutting edge Network Anomaly Detection tool using Artificial Intelligence (AI).

This innovative design thinking process involves a multi-dimensional framework that encompasses empathizing with end users, defining problem areas, ideation, prototyping, and testing. This iterative method not only identifies user pain points and requirements but also encourages creative solutions that align with their needs.

AI driven network anomaly detection promises to enhance security and reduce false positives by learning from historical data, analyzing patterns, and adapting to evolving threats. The tool combines supervised and unsupervised machine learning techniques, reinforced with deep neural networks to provide real time monitoring and analysis.

The design thinking process focuses on integrating AI into the network security workflow seamlessly, with user centric design principles to ensure usability and effectiveness. By leveraging this approach, the tool aims to bridge the gap between the sophistication of modern cyber threats and the agility of security solutions.

In addition, the paper addresses the ethical considerations surrounding AI in network security, emphasizing transparency and accountability to mitigate biases and privacy concerns. The development process also acknowledges the importance of human in theloop validation to ensure AI decisions align with the security objectives.

The network anomaly detection tool, driven by AI and shaped by design thinking, presents a holistic approach to enhancing network security. Through user centric design and the power of AI, this innovation aims to provide organizations with a more robust, adaptive, and effective solution for identifying and mitigating network anomalies in real time.

Vision:

Our vision is to develop a state of the art Network Anomaly Detection solution that empowers organizations to proactively safeguard their network infrastructure, data, and services. Our goal is to provide a comprehensive, intelligent, and user friendly platform that addresses the following key aspects:

1. Advanced Threat Detection: Our Network Anomaly Detection tool will employ cutting edge machine learning and artificial intelligence techniques to detect both known and emerging threats. It will continuously analyze network traffic and behavior to identify suspicious activities, zero day vulnerabilities, and insider threats.

2. Real time Monitoring: We aim to offer real time monitoring capabilities, allowing organizations to detect and respond to anomalies as they occur. This includes monitoring for sudden spikes in traffic, unusual user behavior, and deviations from established baselines.
3. Customization and Flexibility: Recognizing that every network environment is unique, our solution will be highly customizable. Users will have the flexibility to define their own detection rules, thresholds, and policies to align with their specific security and operational requirements.
4. Incident Investigation: In the event of an anomaly, our tool will provide comprehensive incident investigation capabilities. It will offer detailed forensics, packet capture analysis, and contextual information to help security teams quickly understand the nature and impact of the incident.
5. Alerting and Reporting: Timely alerts and informative reports are crucial for effective anomaly detection. Our platform will offer configurable alerting mechanisms and reporting features, enabling security professionals to take immediate action and meet compliance requirements.
6. Integration: We envision seamless integration with existing security and network infrastructure, including SIEM (Security Information and Event Management) systems, firewalls, and threat intelligence feeds. This will facilitate a holistic approach to cybersecurity.
7. User Friendly Interface: Usability is a top priority. Our tool will feature an intuitive and visually appealing interface, making it accessible to both security experts and network administrators.
8. Continuous Improvement: Our commitment to ongoing research and development means that our solution will evolve to counter emerging threats and challenges in the cybersecurity landscape.

List of Teammates:

S. No.	Name	College	Contact
1.	Jammalamadaka Manasa	VIT University	9178844649
2.	Chikkam Venkat Satya Dhiraj	VIT University	7093162749
3.	Avuthu Lasya	VIT University	7013905050
4.	M. Om Nivas	VIT University	9849872691

List of Vulnerabilities table:

S.No.	Vulnerability Name	CWE No.
1.	Information Exposure	200
2.	Relative Path Traversal	23
3.	Improper Input Validation	20
4.	Inadequate Encryption Strength	326
5.	Improper Encoding or Escaping of Output	116
6.	Failure to Sanitize Special Element	159
7.	Exposure of Backup File to an Unauthorised Control Sphere	530
8.	Cross Site Request Forgery (CSRF)	352
9.	Overly Permissive Cross domain Whitelist	942
10.	Configuration	16

REPORT

1. Vulnerability name : Information Exposure
CWE: 200
OWASP Category: A01:2021 Broken Access Control
Description: Information exposure is a security vulnerability that allows unauthorized access to sensitive information. Sensitive information can include things like personal data, financial data, health records, and trade secrets. Information exposure can occur in a variety of ways, including:

1. Misconfigured systems: Systems that are not properly configured can expose sensitive information to unauthorized users. For example, a web server that is configured to allow public access to its log files could expose sensitive information about the websites that are hosted on the server.
2. Software vulnerabilities: Software vulnerabilities can also allow attackers to expose sensitive information. For example, a vulnerability in a web application could allow an attacker to inject malicious code into the application, which could then be used to steal sensitive data from the application's database.
3. Human error: Human error can also lead to information exposure. For example, an employee may accidentally send an email containing sensitive information to the wrong person.

Business impact:
Information exposure can have a number of negative consequences, including:

1. Financial loss: Information exposure can lead to financial losses for individuals and organizations. For example, if an attacker steals credit card numbers, they can use them to make unauthorized purchases.
2. Identity theft: Information exposure can also lead to identity theft. For example, if an attacker steals someone's Social Security number, they can use it to open new credit accounts or file fraudulent tax returns.
3. Reputational damage: Information exposure can also damage an organization's reputation. For example, if a company exposes its customers' personal information, it could lose the trust of its customers.

2. Vulnerability Name: Relative Path Traversal
CWE : 23
OWASP Category: A01:2021 – Broken Access Control
Description : Relative Path Traversal is a vulnerability where an attacker manipulates file paths to gain unauthorised access to files or directories. By exploiting weaknesses in access controls, the attacker can traverse through the file system, potentially reaching files that should be restricted from their view. This can lead to unauthorised disclosure of sensitive information or even the execution of malicious code.

It is a security vulnerability that occurs when an application fails to properly validate and sanitize user input used to navigate the file system. Attackers can exploit this weakness by manipulating file paths to access files or directories outside the intended scope. This could lead to unauthorized access to sensitive data, disclosure of confidential information, or even remote code execution if not mitigated effectively.

Business Impact : The impact of Relative Path Traversal can be severe. It can result in unauthorised access to critical data, potentially exposing sensitive information, proprietary code, or confidential documents. This could lead to reputational damage, legal consequences, and financial losses for affected businesses.

It poses a significant threat to businesses as it can lead to data breaches, legal liabilities, and reputational damage. If exploited, attackers can gain unauthorized access to critical system files, customer data, or proprietary information, potentially causing financial losses and eroding customer trust. It's crucial for organizations to implement robust input validation and security controls to mitigate this risk.

3. Vulnerability Name: Improper Input Validation
CWE: 20
OWASP Category: A01:2021 – Broken Access Control
Description: Improper input validation occurs when an application does not adequately validate user inputs, allowing attackers to inject malicious code or data. This can lead to various types of attacks, including SQL injection, cross site scripting (XSS), and command injection, depending on the context. The consequences can be severe, as attackers may compromise the integrity, availability, or confidentiality of data, disrupt operations, or gain unauthorized access to the system.

Business Impact: Improper input validation can result in unauthorised data access, data manipulation, and even full compromise of the application or system. This can lead to data breaches, loss of user trust, and damage to an organisation's reputation. Security incidents resulting from this vulnerability may result in regulatory fines and legal consequences, further straining resources and credibility. To mitigate this risk, organizations must implement strong input validation mechanisms and maintain a proactive security posture to protect their assets and maintain customer trust.

4. Vulnerability name: Inadequate Encryption Strength
CWE: 326
OWASP Category: A02:2021 Cryptographic Failures
Description: Inadequate encryption strength is a critical cybersecurity vulnerability that arises when sensitive data is not sufficiently protected through encryption mechanisms. Encryption is the process of converting data into a secure, unreadable format, only accessible with the appropriate decryption key. Inadequate encryption strength refers to the utilization of weak, outdated, or easily breakable encryption algorithms, keys, or methods, making it easier for malicious actors to gain unauthorized access to confidential information.

Encryption is the process of converting data into a secure, unreadable format, only accessible with the appropriate decryption key. Inadequate encryption strength refers to the utilization of weak, outdated, or easily breakable encryption algorithms, keys, or methods, making it easier for malicious actors to gain unauthorized access to confidential information.

This vulnerability can manifest in several ways, such as using short or predictable encryption keys, relying on outdated encryption protocols, or implementing encryption incorrectly. When encryption strength is inadequate, it opens the door to data breaches, unauthorized access, and data theft, posing substantial risks to individuals, organizations, and their stakeholders.

Business Impact: The business impact of inadequate encryption strength is profound. Weak encryption can lead to unauthorised access to confidential information, such as customer data or trade secrets. This can result in financial losses, legal liabilities, and harm to the organisation's credibility. Inadequate encryption strength can have severe consequences for businesses. It exposes them to data breaches, regulatory non compliance, and reputational damage. If customer data, financial information, or intellectual property is compromised, it can result in financial losses, legal repercussions, and a loss of trust among customers and partners. To mitigate this risk, organizations must regularly update their encryption methods to ensure the security of their data and maintain compliance with data protection regulations.

In today's data driven world, safeguarding sensitive information through robust encryption is a fundamental component of cybersecurity, and neglecting it can have far reaching and costly consequences. Organizations must continually assess and enhance their encryption practices to mitigate this vulnerability and protect their valuable data assets from the ever present threat of cyberattacks.

5. Vulnerability name: Improper Encoding or Escaping of Output
CWE: 116
OWASP Category: A03:2021 Injection
Description: Improper encoding or escaping of output is a vulnerability where an application fails to properly sanitize and escape user generated data before displaying it in a web page or other output. This can lead to cross site scripting (XSS) attacks, enabling attackers to inject malicious code that can steal user data or manipulate website content.

Business Impact: XSS attacks can lead to unauthorised access, data theft, and the injection of malicious scripts on a website. This can damage an organisation's reputation, result in data breaches, and compromise the security of its users. This vulnerability can have significant business impacts.

XSS attacks can damage a company's reputation, as attackers can deface websites, steal sensitive customer information, or spread malware through the compromised application. Moreover, it can result in legal consequences and regulatory fines, especially if personal data is exposed. Implementing proper input validation and output encoding is crucial for protecting sensitive data and maintaining the trust of users.

6. Vulnerability name: Failure to Sanitize Special Element
CWE: 159
OWASP Category: A03:2021 Injection
Description: This vulnerability arises when user input is not adequately sanitised, allowing malicious elements (e.g., scripts, tags) to be included in web content. This is a common vector for Cross Site Scripting (XSS) attacks. Failure to sanitize special elements refers to a security flaw where user provided data is not properly sanitized, allowing malicious users to inject harmful code or script elements into web applications.

Business Impact: XSS attacks through this vulnerability can lead to compromised user accounts, data manipulation, and potential theft of sensitive information, causing reputational damage and regulatory penalties. Failing to sanitize special elements can lead to data breaches, unauthorized access, and application compromise.

The impact on a business can be substantial, including reputational damage, legal liabilities, and financial losses. Such vulnerabilities can result in the theft of sensitive customer data, loss of customer trust, and potential regulatory fines. To mitigate this risk, organizations should implement robust input validation and data sanitization processes in their applications.

7. Vulnerability Name: Exposure of Backup File to an Unauthorised Control Sphere
CWE: 530
OWASP Category: A03:2021 – Injection
Description: This vulnerability occurs when backup files, which may contain sensitive data, are accessible to unauthorised entities or control spheres. Backup files often have less security measures in place compared to the live production data. If not properly protected, they can be exploited by attackers to gain access to sensitive information.

Exposure of backup files to an unauthorized control sphere occurs when sensitive backup data is accessible to individuals or entities without proper authorization. This vulnerability can result from poor access controls and security measures, potentially leading to data leaks or unauthorized system recovery.

Business Impact: Exposure of backup files can lead to data breaches, data leakage, and unauthorised access to critical information. This can result in reputation damage, legal consequences, and financial losses for organisations. Files are usually backed up in an organisation when they are important. Therefore, they should be securely stored and should be confidential.

Exposing backup files to unauthorized parties can be disastrous for businesses. It can lead to data breaches, intellectual property theft, and unauthorized system access. This can result in severe financial losses, legal repercussions, and harm to a company's reputation. To mitigate this risk, organizations should implement stringent access controls and encryption for backup files, ensuring that only authorized personnel can access and manage these critical assets.

8. Vulnerability name: Cross Site Request Forgery (CSRF)
CWE: 352
OWASP Category: A05:2021 – Security Misconfiguration
Description:
Cross Site Request Forgery (CSRF) is a web security vulnerability that allows an attacker to induce an authenticated user to perform an unwanted action on a website. CSRF attacks are often carried out by tricking the victim into clicking on a malicious link or opening a specially crafted web page.

CSRF attacks exploit the fact that web browsers automatically send authentication cookies with every request. When a user is authenticated on a website, their browser stores an authentication cookie on their computer. This cookie is used to identify the user to the website on subsequent requests.

An attacker can exploit this behaviour by constructing a malicious request that is designed to be executed by the victim's browser. The request will typically contain the victim's authentication cookie, so the website will believe that the request is coming from the victim. If the request is successful, the attacker can cause the victim to perform any action that they are authorised to perform on the website. For example, the attacker could transfer money from the victim's bank account, change their password, or post a message on a social media account.

Business impact:
Cross Site Request Forgery (CSRF) can have a significant business impact, leading to unauthorized actions on behalf of authenticated users. This can result in data breaches,

financial losses, unauthorized data modifications, damage to reputation, and legal liabilities, affecting customer trust and overall business operations. Affected users may blame the business for their losses, and it can lead to legal issues and regulatory fines. Implementing proper security measures, such as anti CSRF tokens, is essential to protect against these attacks and maintain a secure web application environment.

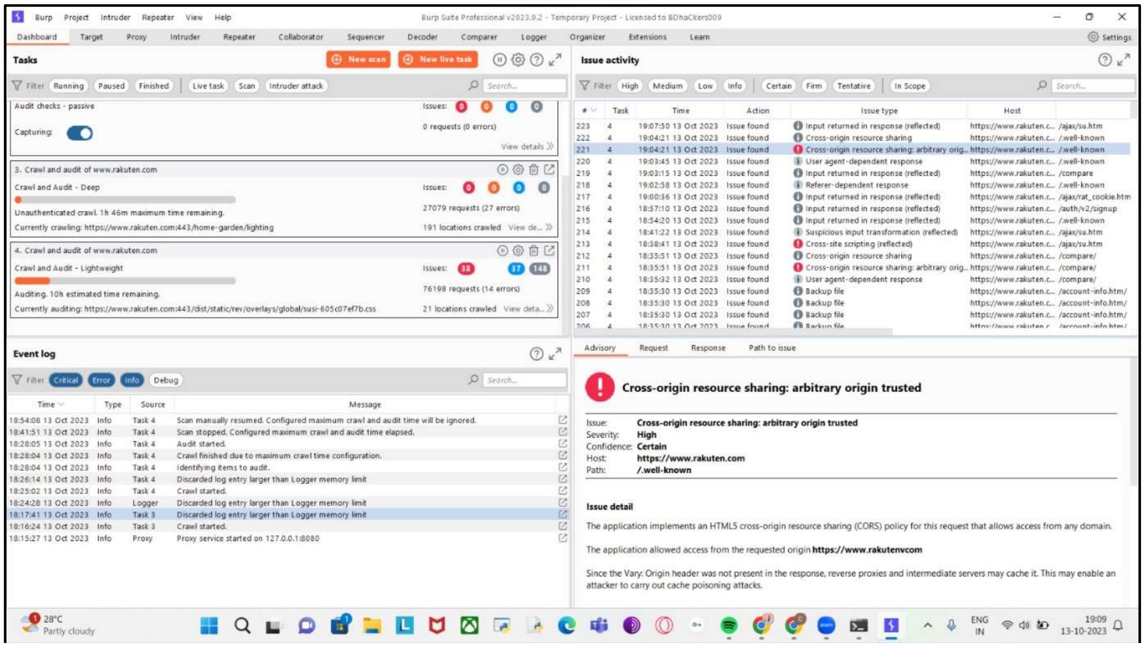
9. Vulnerability name: Overly Permissive Cross Domain Whitelist
CWE: 942
OWASP Category: A05: 2021 Security Misconfiguration
Description: This vulnerability occurs when a web application permits overly broad cross origin requests in its cross-domain whitelist, potentially allowing unauthorised parties to access sensitive data. An overly permissive cross domain whitelist is a configuration error that allows web applications to make requests to domains that should be restricted. This can enable cross site request forgery (CSRF) attacks and unauthorized data access.

Business Impact: Allowing unrestricted cross domain requests can enable data exposure, cross site request forgery (CSRF), potential data breaches and other security breaches. This can lead to unauthorised data access, reputational damage, and legal consequences. This can damage the business's reputation, erode trust, and result in legal consequences. Properly configuring cross domain whitelists and maintaining strict security policies is essential to prevent these issues.

10. Vulnerability Name: Configuration
CWE : 16
OWASP Category: A06:2021 – Vulnerable and Outdated Components
Description : This vulnerability arises from inadequately managed configurations, which may include default settings, access controls, or sensitive information inadvertently exposed. Attackers exploit these misconfigurations to gain unauthorised access, escalate privileges, or retrieve sensitive data. Configuration vulnerabilities encompass a broad range of security issues related to incorrect or insecure configurations in systems, software, and network settings. These vulnerabilities can result in unauthorized access, data exposure, and system compromises.

Business Impact : The business impact of a configuration vulnerability can be severe. It may lead to data breaches, financial losses, reputational damage, and legal consequences. Additionally, downtime and disruption of services can occur as a result of exploiting misconfigurations, potentially causing significant harm to an organisation's operations and reputation.

Configuration vulnerabilities can have a severe impact on businesses leading to service disruptions. Attackers can exploit these weaknesses to gain unauthorized access to systems, manipulate settings, and steal sensitive information. Regular security assessments and audits are crucial to identifying and remedying configuration vulnerabilities to protect the business and its assets.


Burp Project Intruder Repeater View Help
Burp Suite Professional v2023.9.2 - Temporary Project - Licensed to BDhaCkers009
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Tasks
New scan
New live task
Filter Running Paused Finished Live task Scan Intruder attack
Search...
Issue activity
Filter High Medium Low Info Certain Firm Tentative In Scope
Search...
Event log
Filter Critical Error Info Debug
Search...
Advisory Request Response Path to issue
28°C
Partly cloudy
ENG
IN
19:09
13-10-2023

Audit checks - passive
Issues: 0 0 0 0
Capturing:
0 requests (0 errors)
View details »

3. Crawl and audit of www.rakuten.com
Crawl and Audit - Deep
Issues: 0 0 0 0
Unauthenticated crawl. 1h 46m maximum time remaining.
27079 requests (27 errors)
Currently crawling: https://www.rakuten.com:443/home-garden/lighting
191 locations crawled View de... »

4. Crawl and audit of www.rakuten.com
Crawl and Audit - Lightweight
Issues: 38 37 148
Auditing. 10h estimated time remaining.
76198 requests (14 errors)
Currently auditing: https://www.rakuten.com:443/dist/static/rev/overlays/global/susi-605c07ef7b.css
21 locations crawled View deta... »

#	Task	Time	Action	Issue type	Host	
223	4	19:07:50 13 Oct 2023	Issue found	Input returned in response (reflected)	https://www.rakuten.c...	/ajax/su.htm
222	4	19:04:21 13 Oct 2023	Issue found	Cross-origin resource sharing	https://www.rakuten.c...	/.well-known
221	4	19:04:21 13 Oct 2023	Issue found	Cross-origin resource sharing: arbitrary orig...	https://www.rakuten.c...	/.well-known
220	4	19:03:45 13 Oct 2023	Issue found	User agent-dependent response	https://www.rakuten.c...	/.well-known
219	4	19:03:15 13 Oct 2023	Issue found	Input returned in response (reflected)	https://www.rakuten.c...	/compare
218	4	19:02:58 13 Oct 2023	Issue found	Referer-dependent response	https://www.rakuten.c...	/.well-known
217	4	19:00:36 13 Oct 2023	Issue found	Input returned in response (reflected)	https://www.rakuten.c...	/ajax/rat_cookie.htm
216	4	18:57:10 13 Oct 2023	Issue found	Input returned in response (reflected)	https://www.rakuten.c...	/auth/v2/signup
215	4	18:54:20 13 Oct 2023	Issue found	Input returned in response (reflected)	https://www.rakuten.c...	/.well-known
214	4	18:41:22 13 Oct 2023	Issue found	Suspicious input transformation (reflected)	https://www.rakuten.c...	/ajax/su.htm
213	4	18:38:41 13 Oct 2023	Issue found	Cross-site scripting (reflected)	https://www.rakuten.c...	/ajax/su.htm
212	4	18:35:51 13 Oct 2023	Issue found	Cross-origin resource sharing	https://www.rakuten.c...	/compare/
211	4	18:35:51 13 Oct 2023	Issue found	Cross-origin resource sharing: arbitrary orig...	https://www.rakuten.c...	/compare/
210	4	18:35:32 13 Oct 2023	Issue found	User agent-dependent response	https://www.rakuten.c...	/compare/
209	4	18:35:30 13 Oct 2023	Issue found	Backup file	https://www.rakuten.c...	/account-info.htm/
208	4	18:35:30 13 Oct 2023	Issue found	Backup file	https://www.rakuten.c...	/account-info.htm/
207	4	18:35:30 13 Oct 2023	Issue found	Backup file	https://www.rakuten.c...	/account-info.htm/
206	4	18:35:30 13 Oct 2023	Issue found	Backup file	https://www.rakuten.c	/account-info.htm/

Time	Type	Source	Message
18:54:08 13 Oct 2023	Info	Task 4	Scan manually resumed. Configured maximum crawl and audit time will be ignored.
18:41:51 13 Oct 2023	Info	Task 4	Scan stopped. Configured maximum crawl and audit time elapsed.
18:28:05 13 Oct 2023	Info	Task 4	Audit started.
18:28:04 13 Oct 2023	Info	Task 4	Crawl finished due to maximum crawl time configuration.
18:28:04 13 Oct 2023	Info	Task 4	Identifying items to audit.
18:26:14 13 Oct 2023	Info	Task 4	Discarded log entry larger than Logger memory limit
18:25:02 13 Oct 2023	Info	Task 4	Crawl started.
18:24:28 13 Oct 2023	Info	Logger	Discarded log entry larger than Logger memory limit
18:17:41 13 Oct 2023	Info	Task 3	Discarded log entry larger than Logger memory limit
18:16:24 13 Oct 2023	Info	Task 3	Crawl started.
18:15:27 13 Oct 2023	Info	Proxy	Proxy service started on 127.0.0.1:8080

Cross-origin resource sharing: arbitrary origin trusted

Issue:	**Cross-origin resource sharing: arbitrary origin trusted**
Severity:	**High**
Confidence:	**Certain**
Host:	**https://www.rakuten.com**
Path:	**/.well-known**

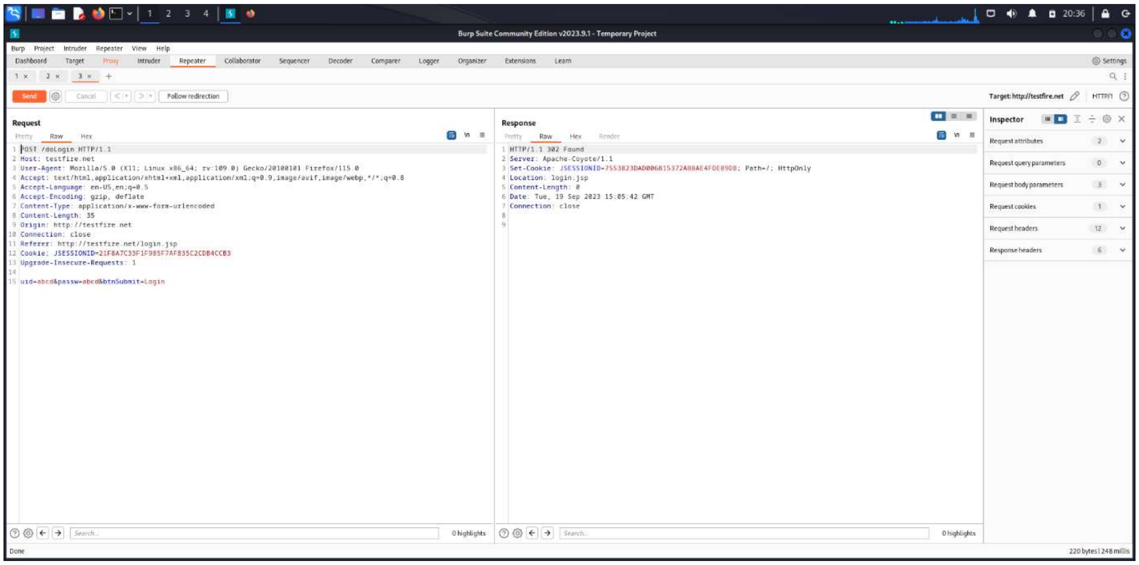
Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://www.rakutenvcom**

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Fig.1 Scanning for vulnerabilities in Burp Suite


1 2 3 4
20:36
Burp Suite Community Edition v2023.9.1 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
1 × 2 × 3 × +
Send
Cancel
Follow redirection
Target: http://testfire.net
HTTP/1
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
0 highlights
Search...
Done
220 bytes | 248 millis

Request

```
POST /doLogin HTTP/1.1
Host: testfire.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 35
Origin: http://testfire.net
Connection: close
Referer: http://testfire.net/login.jsp
Cookie: JSESSIONID=21F8A7C33F1F985F7AFB35C2CDB4CCB3
Upgrade-Insecure-Requests: 1

uid=abcd&passw=abcd&btnSubmit=Login
```

Response

```
HTTP/1.1 302 Found
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=7553823DAD006815372AB8AE4F0E89D8; Path=/; HttpOnly
Location: login.jsp
Content-Length: 0
Date: Tue, 19 Sep 2023 15:05:42 GMT
Connection: close


```

Inspector	
Request attributes	2
Request query parameters	0
Request body parameters	3
Request cookies	1
Request headers	12
Response headers	6

Fig.2 Performing attacks through Burp Suite

Nessus:

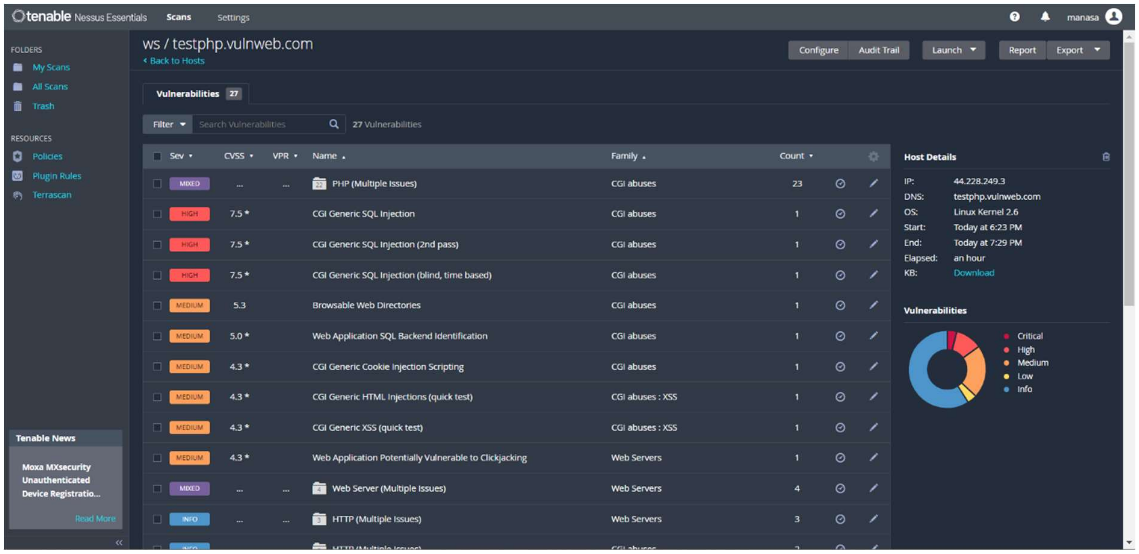
Tenable Nessus, also known as Nessus, is a widely used and well-known network vulnerability scanner and security assessment tool. It is designed to help organizations identify and assess vulnerabilities in their computer systems, networks, and infrastructure to enhance their overall cybersecurity posture. It employs an extensive database of security plugins to identify vulnerabilities, misconfigurations, and weaknesses, and provides detailed reports with risk prioritization and remediation recommendations.

Nessus is known for its flexibility, allowing users to customize scans and target specific areas of concern, as well as its support for compliance auditing against various industry standards. Its integration capabilities and regularly updated database make it an invaluable tool for proactive vulnerability management and aiding in the mitigation of security risks.

These are some of the features of Nessus tool:

1. Vulnerability Scanning: Nessus performs automated vulnerability scanning to identify weaknesses, misconfigurations, and security issues in network devices, servers, applications, and other components of an IT environment.
2. Extensive Plugin Database: Nessus uses a vast database of security plugins that cover a wide range of vulnerabilities, including software flaws, weak configurations, and known exploits. These plugins are regularly updated to keep pace with emerging threats.
3. Customizable Scans: Users can customize scans to target specific systems, IP ranges, or types of vulnerabilities. This flexibility allows organizations to tailor their scans to meet their unique security needs.
4. Prioritization and Risk Assessment: Nessus assigns severity levels and risk scores to identified vulnerabilities, helping organizations prioritize their remediation efforts based on the potential impact and severity of each vulnerability.
5. Compliance Checks: Nessus includes checks for compliance with various industry standards and regulatory requirements, such as CIS (Center for Internet Security) benchmarks, PCI DSS (Payment Card Industry Data Security Standard), and NIST (National Institute of Standards and Technology) guidelines.
6. Reporting: Nessus generates detailed reports that provide comprehensive information about identified vulnerabilities, their descriptions, remediation recommendations, and historical data. These reports can be customized to suit the needs of both technical and non technical stakeholders.
7. Integration: Nessus can be integrated with other security tools and platforms to automate the vulnerability management process and facilitate the tracking and remediation of vulnerabilities.
8. Scanning Flexibility: Nessus supports a range of scanning methods, including authenticated scans (using valid credentials to access systems) and non-authenticated scans. Authenticated scans can provide more in-depth insights into the system's security configuration.
9. Agent Based Scanning: Nessus also offers agent based scanning, which allows organizations to deploy lightweight agents on systems for more granular and real time vulnerability assessments.
10. Commercial and Open-Source Versions: Nessus is available in both commercial and open source (community) versions. The commercial version, known as Tenable Nessus, offers additional features and support, while the open source version, called Nessus Essentials, provides basic vulnerability scanning capabilities.

Nessus is a valuable tool for organizations seeking to proactively identify and address security vulnerabilities in their infrastructure, reducing the risk of cyberattacks and data breaches. It is widely used by IT professionals, network administrators, and cybersecurity experts to help maintain a strong security posture.



ws / testphp.vulnweb.com

‹ Back to Hosts

27 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
MIXED	...	...	PHP (Multiple Issues)	CGI abuses	23
HIGH	7.5 *		CGI Generic SQL Injection	CGI abuses	1
HIGH	7.5 *		CGI Generic SQL Injection (2nd pass)	CGI abuses	1
HIGH	7.5 *		CGI Generic SQL Injection (blind, time based)	CGI abuses	1
MEDIUM	5.3		Browsable Web Directories	CGI abuses	1
MEDIUM	5.0 *		Web Application SQL Backend Identification	CGI abuses	1
MEDIUM	4.3 *		CGI Generic Cookie Injection Scripting	CGI abuses	1
MEDIUM	4.3 *		CGI Generic HTML Injections (quick test)	CGI abuses : XSS	1
MEDIUM	4.3 *		CGI Generic XSS (quick test)	CGI abuses : XSS	1
MEDIUM	4.3 *		Web Application Potentially Vulnerable to Clickjacking	Web Servers	1
MIXED	...	...	Web Server (Multiple Issues)	Web Servers	4
INFO	...	...	HTTP (Multiple Issues)	Web Servers	3
INFO			HTTP (Multiple Issues)	CGI abuses	

Host Details

IP:	44.228.249.3
DNS:	testphp.vulnweb.com
OS:	Linux Kernel 2.6
Start:	Today at 6:23 PM
End:	Today at 7:29 PM
Elapsed:	an hour
KB:	Download

Vulnerabilities

Fig. 3 Scanning for vulnerabilities in Nessus Tool

Target website: http://testphp.vulnweb.com
Target ip address: 44.228.249.3

List of vulnerabilities:

S. No.	Vulnerability name	Severity	Plugins
1.	PHP Unsupported Version Detection	Critical - 10.0	tcp/80/www
2.	CGI Generic SQL Injection	High - 7.5	tcp/80/www
3.	CGI Generic SQL Injection (2nd pass)	High - 7.5	tcp/80/www
4.	CGI Generic SQL Injection (blind, time based)	High - 7.5	tcp/80/www
5.	PHP 5 < 5.2.7 Multiple Vulnerabilities	High - 6.7	tcp/80/www
6.	PHP 5.x < 5.2 Multiple Vulnerabilities	High - 6.7	tcp/80/www

7.	PHP 5.x < 5.2.2 Multiple vulnerabilities	High - 6.6	tcp/80/www
8.	PHP < 5.2.1 Multiple Vulnerabilities	High - 6.7	tcp/80/www
9.	PHP < 5.2.11 Multiple Vulnerabilities	High - 6.7	tcp/80/www
10.	PHP < 5.2.3 Multiple Vulnerabilities	High - 7.3	tcp/80/www

REPORT

1.**Vulnerability Name**: PHP Unsupported Version Detection
Severity: 10.0 Critical
Plugin: tcp/80/www
Port: TCP-80
Description: According to its version, the installation of PHP on the remote host is no longer supported. Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security **vuln**erabilities.
Solution: Upgrade to a version of PHP that is currently supported.
Business Impact: Running an unsupported version of PHP can have a significant impact on your business, including:

- Increased security risk: Unsupported versions of PHP are known to contain security vulnerabilities that can be exploited by attackers to gain access to your systems and data. This can lead to data breaches, financial losses, and reputational damage.
- Compliance issues: Many industries and regulations require organizations to use supported versions of software. Failing to do so could result in fines, penalties, or even legal action.
- Performance and stability problems: Unsupported versions of PHP may not be compatible with the latest versions of web frameworks, libraries, and other software. This can lead to performance and stability problems, which can impact your website or application's availability and reliability.
- Reduced developer productivity: Developers working on unsupported versions of PHP may have to spend more time debugging and fixing problems. This can reduce their productivity and increase the cost of developing and maintaining your website or application.

2.**Vulnerability Name**: CGI Generic SQL Injection
Severity: 7.5 high
Plugin: tcp/80/www
Port: TCP-80
Description: By providing specially crafted parameters to CGIs, Nessus was able to get an error from the underlying database. This error suggests that the CGI is affected by a SQL injection vulnerability. An attacker may exploit this flaw to bypass authentication, read

confidential data, modify the remote database, or even take control of the remote operating system.
Solution: Modify the relevant CGIs so that they properly escape arguments.
Business Impact: CGI Generic SQL Injection is a vulnerability that can allow an attacker to execute arbitrary SQL queries on a web application's database. This can have a significant business impact, including:

- Data theft: An attacker can use SQL injection to steal sensitive data from the database, such as customer information, financial data, and intellectual property.
- Data corruption: An attacker can use SQL injection to corrupt or delete data in the database. This can disrupt business operations and lead to financial losses.
- Denial of service: An attacker can use SQL injection to launch a denial-of-service attack against the web application. This can make the application unavailable to legitimate users and cause significant business disruption.
- System compromise: In some cases, an attacker can use SQL injection to gain control of the underlying operating system. This can allow the attacker to install malware, steal files, or launch further attacks.

The business impact of CGI Generic SQL Injection will vary depending on the specific application and the data that is stored in the database. However, in all cases, it is a serious vulnerability that can have significant financial and reputational consequences.

3.**Vulnerability Name**:- CGI Generic SQL Injection (2nd pass)
Severity: 7.5 High
Plugin: tcp/80/www
Port: TCP-80
Description: By providing specially crafted parameters to CGIs, Nessus was able to get an error from the underlying database. This error suggests that the CGI is affected by a SQL injection vulnerability. An attacker may exploit this flaw to bypass authentication, read confidential data, modify the remote database, or even take control of the remote operating system.
Solution: Modify the relevant CGIs so that they properly escape arguments
Business Impact:
The business impact of a CGI Generic SQL Injection (2nd pass) vulnerability can be severe. An attacker can exploit this vulnerability to:

- Bypass authentication and gain unauthorized access to sensitive data or systems. This includes customer information, financial data, and intellectual property.
- Read, modify, or delete data in the database. This could include damaging or destroying critical data, or stealing confidential information.
- Execute arbitrary code on the server. This could give the attacker complete control over the server, allowing them to launch attacks against other systems or steal data.

4.**Vulnerability Name**:-CGI Generic SQL Injection (blind, time based)
Severity: 7.5 High
Plugin: tcp/80/www
Port: TCP-80
Description: By sending specially crafted parameters to one or more CGI scripts hosted on the remote web server, Nessus was able to get a slower response, which suggests that it may have been able to modify the behavior of the application and directly access the underlying database. An attacker may be able to exploit this issue to bypass authentication, read confidential data, modify the remote database, or even take control of the remote operating system. Note that this script is experimental and may be prone to false positives.

Solution: Modify the affected CGI scripts so that they properly escape arguments
Business Impact:
A CGI Generic SQL Injection (blind, time based) vulnerability can have a significant business impact on an organization. An attacker could exploit this vulnerability to:

- Bypass authentication and gain unauthorized access to sensitive data. This could include customer information, financial data, or intellectual property.
- Read or modify data in the database. This could allow the attacker to steal confidential information, corrupt data, or even delete data entirely.
- Disrupt or disable the web application. This could deny service to legitimate users and cause significant financial losses to the organization.
- Execute arbitrary code on the web server. This could allow the attacker to take control of the server and launch further attacks against the organization or its customers.

5.**Vulnerability Name**:-PHP 5 < 5.2.7 Multiple Vulnerabilities
Severity: 6.7 High
Plugin: tcp/80/www
Port: TCP-80
Description: According to its banner, the version of PHP installed on the remote host is prior to 5.2.7. It is, therefore, affected by multiple vulnerabilities : - There is a buffer overflow flaw in the bundled PCRE library that allows a denial of service attack. (CVE-2008-2371) - Multiple directory traversal vulnerabilities exist in functions such as 'posix_access', 'chdir', and 'ftok' that allow a remote attacker to bypass 'safe_mode' restrictions. (CVE-2008-2665 and CVE-2008-2666). - A buffer overflow flaw in 'php_imap.c' may be triggered when processing long message headers due to the use of obsolete API calls. This can be exploited to cause a denial of service or to execute arbitrary code. (CVE-2008-2829) - A buffer overflow in the 'imageloadfont' function in 'ext/gd/gd.c' can be triggered when a specially crafted font is given. This can be exploited to cause a denial of service or to execute arbitrary code. (CVE-2008-3658) - A buffer overflow flaw exists in PHP's internal function 'memnstr' which can be exploited by an attacker using the delimiter argument to the 'explode' function. This can be used to cause a denial of service or to execute arbitrary code. (CVE-2008-3659) - When PHP is used as a FastCGI module, an attacker by requesting a file whose file name extension is preceded by multiple dots can cause a denial of service. (CVE-2008-3660) - A heap-based buffer overflow flaw in the mbstring extension can be triggered via a specially crafted string containing an HTML entity that is not handled during Unicode conversion. This can be exploited to execute arbitrary code.(CVE-2008-5557) - Improper initialization of global variables 'page_uid' and 'page_gid' when PHP is used as an Apache module allows the bypassing of security restriction due to SAPI 'php_getuid' function overloading. (CVE-2008-5624) - PHP does not enforce the correct restrictions when 'safe_mode' is enabled through a 'php_admin_flag' setting in 'httpd.conf'. This allows an attacker, by placing a specially crafted 'php_value' entry in '.htaccess', to able to write to arbitrary files. (CVE-2008-5625) - The 'ZipArchive::extractTo' function in the ZipArchive extension fails to filter directory traversal sequences from file names. An attacker can exploit this to write to arbitrary files. (CVE-2008-5658) - Under limited circumstances, an attacker can cause a file truncation to occur when calling the 'dba_replace' function with an invalid argument. (CVE-2008-7068) - A buffer overflow error exists in the function 'date_from_ISO8601' function within file 'xmlrpc.c' because user-supplied input is improperly validated. This can be exploited by a remote attacker to cause a denial of service or to execute arbitrary code. (CVE-2014-8626)
Solution: Upgrade to PHP version 5.2.8 or later. Note that version 5.2.7 has been removed from distribution because of a regression in that version that results in the 'magic_quotes_gpc' setting remaining off even if it was set to on.

Business Impact:

The business impact of the PHP 5 < 5.2.7 Multiple Vulnerabilities is high. These vulnerabilities could allow an attacker to execute arbitrary code on the affected server, steal sensitive data, or disrupt operations. This could have a significant impact on businesses of all sizes, including:

- Financial losses: Attackers could steal customer data, such as credit card numbers and Social Security numbers, which could lead to financial losses for businesses.
- Reputational damage: A data breach or other security incident could damage a company's reputation and make it difficult to attract and retain customers.
- Regulatory compliance fines: Businesses that are subject to industry regulations, such as PCI DSS or HIPAA, could face fines for failing to protect customer data.
- Disruption to operations: If an attacker gains control of a company's website or servers, they could disrupt operations and prevent customers from accessing products or services.

6.**Vulnerability Name**:-PHP 5.x < 5.2 Multiple Vulnerabilities
Severity: 6.7 High
Plugin: tcp/80/www
Port: TCP-80
Description: According to its banner, the version of PHP 5.x installed on the remote host is older than 5.2. Such versions may be affected by several buffer overflows. To exploit these issues, an attacker would need the ability to upload an arbitrary PHP script on the remote server or to manipulate several variables processed by some PHP functions such as 'htmlentities().'
Solution: Upgrade to PHP version 5.2.0 or later.
Business Impact:

The business impact of the PHP 5.x < 5.2 multiple vulnerabilities is high. These vulnerabilities can be exploited to allow an attacker to remotely execute code on the affected server, which could give them complete control over the server and its resources. Attackers could then use the server to steal sensitive data, launch attacks against other systems, or even install ransomware.

7.**Vulnerability Name**:-- PHP 5.x < 5.2.2 Multiple vulnerabilities
Severity: 6.6 High
Plugin: tcp/80/www
Port: TCP-80
Description: According to its banner, the version of PHP 5.x installed on the remote host is older than 5.2.2. It is, therefore, affected by multiple vulnerabilities: - A heap-based buffer overflow vulnerability was found in PHP's gd extension. A script that could be forced to process WBMP images from an untrusted source could result in arbitrary code execution. (CVE-2007-1001) - A vulnerability in the way the mbstring extension setglobal variables was discovered where a script using the mb_parse_str() function to set global variables could be forced to to enable the register_globals configuration option, possibly resulting in global variable injection. (CVE-2007-1583) - A context-dependent attacker could read portions of heap memory by executing certain scripts with a serialized data input string beginning with 'S:', which did not properly track the number of input bytes being processed. (CVE-2007-1649) - A vulnerability in how PHP's mail() function processed email messages, truncating potentially important information after the first ASCIIZ (\0) byte. (CVE-2007-1717) - A vulnerability in how PHP's mail() function processed header data was discovered. If a script

sent mail using a subject header containing a string from an untrusted source, a remote attacker could send bulk email to unintended recipients (CVE-2007-1718).
Solution: Upgrade to PHP version 5.2.2 or later.
Business Impact:
The business impact of running PHP 5.x < 5.2.2 is high. This version of PHP contains multiple vulnerabilities that can be exploited by attackers to gain unauthorized access to your systems and data, or to launch denial-of-service attacks.
Here are some specific examples of the business impact of these vulnerabilities:

- Remote code execution: An attacker could exploit a vulnerability in PHP 5.x < 5.2.2 to execute arbitrary code on your server. This could allow them to steal data, install malware, or even take complete control of your system.
- SQL injection: An attacker could exploit a vulnerability in PHP 5.x < 5.2.2 to inject malicious SQL code into your database. This could allow them to dump your database contents, modify data, or even delete it entirely.
- Cross-site scripting (XSS): An attacker could exploit a vulnerability in PHP 5.x < 5.2.2 to inject malicious JavaScript code into your web pages. This could allow them to steal cookies, session tokens, and other sensitive information from your users.
- Denial-of-service (DoS) attacks: An attacker could exploit a vulnerability in PHP 5.x < 5.2.2 to launch a DoS attack against your server. This could overwhelm your server with traffic and prevent it from serving legitimate users.

8.**Vulnerability Name**:- PHP < 5.2.1 Multiple Vulnerabilities
Severity: 6.7 High
Plugin: tcp/80/www
Port: TCP-80
Description: According to its banner, the version of PHP installed on the remote host is older than 5.2.1. Such versions may be affected by several issues, including buffer overflows, format string vulnerabilities, arbitrary code execution, 'safe_mode' and 'open_basedir' bypasses, and clobbering of super-globals.
Solution: Upgrade to PHP version 5.2.1 or later.
Business Impact:
The business impact of running PHP 5.x < 5.2.2 is high. This version of PHP contains multiple vulnerabilities that can be exploited by attackers to gain unauthorized access to your systems and data, or to launch denial-of-service attacks.
Here are some specific examples of the business impact of these vulnerabilities:

- Remote code execution: An attacker could exploit a vulnerability in PHP 5.x < 5.2.2 to execute arbitrary code on your server. This could allow them to steal data, install malware, or even take complete control of your system.
- SQL injection: An attacker could exploit a vulnerability in PHP 5.x < 5.2.2 to inject malicious SQL code into your database. This could allow them to dump your database contents, modify data, or even delete it entirely.
- Cross-site scripting (XSS): An attacker could exploit a vulnerability in PHP 5.x < 5.2.2 to inject malicious JavaScript code into your web pages. This could allow them to steal cookies, session tokens, and other sensitive information from your users.
- Denial-of-service (DoS) attacks: An attacker could exploit a vulnerability in PHP 5.x < 5.2.2 to launch a DoS attack against your server. This could overwhelm your server with traffic and prevent it from serving legitimate users.

9.**Vulnerability Name**:- PHP < 5.2.11 Multiple Vulnerabilities
Severity: 6.7 High
Plugin: tcp/80/www
Port: TCP-80
Description: According to its banner, the version of PHP installed on the remote host is older than 5.2.11. Such versions may be affected by several security issues : - An unspecified error occurs in certificate validation inside 'php_openssl_apply_verification_policy'. - An unspecified input validation vulnerability affects the color index in 'imagecolortransparent()'. - An unspecified input validation vulnerability affects exif processing. - Calling 'popen()' with an invalid mode can cause a crash under Windows. (Bug #44683) - An integer overflow in 'xml_utf8_decode()' can make it easier to bypass cross-site scripting and SQL injection protection mechanisms using a specially crafted string with a long UTF-8 encoding. (Bug #49687) - 'proc_open()' can bypass 'safe_mode_protected_env_vars'. (Bug #49026)
Solution: Upgrade to PHP version 5.2.11 or later.
Business Impact:
The business impact of PHP < 5.2.11 multiple vulnerabilities can be severe, depending on the specific vulnerabilities that are exploited. Some of the potential business impacts include:

- Data breaches: Remote code execution (RCE) and SQL injection vulnerabilities can be exploited to steal sensitive data from customer databases, such as credit card numbers, Social Security numbers, and other personally identifiable information (PII).
- Website downtime: Denial-of-service (DoS) vulnerabilities can be exploited to make websites unavailable to visitors, which can disrupt business operations and lead to lost revenue.
- Loss of customer trust: If a company's website is hacked or customer data is breached, it can damage the company's reputation and lead to the loss of customers.
- Regulatory compliance violations: In some industries, such as healthcare and finance, companies are required to comply with strict data security regulations. If a company is found to be using outdated and vulnerable software, it could be fined or face other penalties.

10.**Vulnerability Name**:- PHP < 5.2.3 Multiple Vulnerabilities
Severity: 7.3 High
Plugin: tcp/80/www
Port: TCP-80
Description: According to its banner, the version of PHP installed on the remote host is older than 5.2.3. It is, therefore, affected by multiple vulnerabilities: - A buffer overflow in the sqlite_decode_function() in the bundled sqlite library could allow contextdependent attackers to execute arbitrary code. (CVE-2007-1887) - A CRLF injection vulnerability in the FILTER_VALIDATE_EMAIL filter could allow an attacker to inject arbitrary email headers via a special email address. This only affects Mandriva Linux 2007.1. (CVE-2007-1900) - An infinite-loop flaw was discovered in the PHP gd extension. A script that could be forced to process PNG images from an untrusted source could allow a remote attacker to cause a denial of service. (CVE-2007-2756) - An integer overflow flaw was found in the chunk_split() function that ould possibly execute arbitrary code as the apache user if a remote attacker was able to pass arbitrary data to the third argument of chunk_split() (CVE-2007-2872). - An open_basedir and safe_mode restriction bypass which could allow context-dependent attackers to determine the existence of arbitrary files. (CVE-2007-3007)
Solution: Upgrade to PHP version 5.2.3 or later.

Business Impact:
The business impact of running a PHP version that is affected by multiple vulnerabilities can be severe. Depending on the specific vulnerabilities that are present, attackers could be able to:

- Execute arbitrary code on the server, giving them complete control over the system and its data.
- Inject malicious scripts into web pages, which could then be executed by visitors to the website, compromising their security.
- Gain access to sensitive data, such as customer passwords or financial information.
- Disrupt or disable the website or web application.

All of these scenarios can have a significant negative impact on a business, leading to financial losses, reputational damage, and regulatory compliance issues.

SOC, SIEM and IBM QRadar

SOC

A security operations center (SOC) – sometimes called an information security operations center, or ISOC – is an in-house or outsourced team of IT security professionals that monitors an organization’s entire IT infrastructure, 24/7, to detect cybersecurity events in real time and address them as quickly and as effectively as possible.

An SOC also selects, operates, and maintains the organization’s cybersecurity technologies, and continually analyzes threat data to find ways to improve the organization's security posture.

The chief benefit of operating or outsourcing an SOC is that it unifies and coordinates an organization’s security tools, practices, and response to security incidents. This usually results in improved preventative measures and security policies, faster threat detection, and faster, more effective and more cost-effective response to security threats. An SOC can also improve customer confidence, and simplify and strengthen an organization's compliance with industry, national and global privacy regulations.

SOC cycle

The SOC (Security Operations Center) cycle is a structured approach to managing cybersecurity within an organization. It encompasses various stages to ensure effective threat detection, response, and mitigation.

Firstly, the cycle begins with "Detection and Monitoring." This involves constant surveillance of an organization's digital environment, including networks, systems, and applications. Advanced tools and technologies are employed to identify anomalous activities, potential vulnerabilities, or signs of a security breach. This proactive monitoring helps in early threat identification, reducing the likelihood of a successful cyber-attack.

Once a potential threat is detected, the SOC moves into the "Analysis and Investigation" phase. Here, skilled cybersecurity professionals thoroughly examine the identified indicators of compromise (IoCs) or suspicious behavior. They assess the severity, scope, and potential impact of the threat. This stage involves deep dives into logs, network traffic, and system behavior to gain a comprehensive understanding of the incident. It is crucial for determining the appropriate response measures and understanding the threat's nature.

SIEM

Security information and event management, SIEM for short, is a solution that helps organizations detect, analyze, and respond to security threats before they harm business operations.

SIEM, pronounced “sim,” combines both security information management (SIM) and security event management (SEM) into one security management system. SIEM technology collects event log data from a range of sources, identifies activity that deviates from the norm with real-time analysis, and takes appropriate action.

In short, SIEM gives organizations visibility into activity within their network so they can respond swiftly to potential cyberattacks and meet compliance requirements. In the past decade, SIEM technology has evolved to make threat detection and incident response smarter and faster with artificial intelligence.

SIEM Cycle

The SIEM (Security Information and Event Management) cycle is a critical process in cybersecurity that involves collecting, correlating, and analyzing security data from various sources within an organization's IT infrastructure.

Firstly, the cycle commences with "Data Collection and Aggregation." This phase involves gathering security-related data from diverse sources like firewalls, intrusion detection systems, servers, and applications. This data is then centralized in a SIEM platform, which acts as a centralized nerve center for security events. The platform normalizes and structures this data, making it easier to analyze and identify potential security incidents.

Next comes "Event Correlation and Analysis." In this phase, the SIEM system uses predefined rules and algorithms to correlate and analyze the collected data. It looks for patterns, anomalies, and potential threats that might be indicative of a security incident. Security analysts play a crucial role in this stage, fine-tuning the rules and investigating any alerts generated by the system. They also contextualize the information, assessing the potential impact and determining the appropriate response. This phase is pivotal in identifying and prioritizing security incidents for further investigation and action.

MISP

MISP (Malware Information Sharing Platform)is an open-source threat intelligence platform that enables organizations to share and collaborate on information about malware, vulnerabilities, and other cybersecurity threats. It is a community-driven project that is used by organizations of all sizes, including government agencies, businesses, and non-profit organizations.

MISP provides a number of features that make it a valuable tool for cybersecurity teams, including:

- Structured data model: MISP uses a structured data model to represent threat intelligence information. This makes it easy to share and correlate information across different organizations and systems.
- Flexible sharing policies: MISP provides flexible sharing policies that allow organizations to control who has access to their data and how it can be used.

- Powerful search and filtering capabilities: MISP's powerful search and filtering capabilities make it easy to find the information you need quickly and easily.
- Integration with other security tools: MISP can be integrated with other security tools, such as SIEMs and intrusion detection systems, to automate the sharing and consumption of threat intelligence information.

MISP can be used for a variety of cybersecurity purposes, including:

- Incident response: MISP can be used to share information about ongoing incidents with other organizations, which can help to accelerate the response and recovery process.
- Threat hunting: MISP can be used to search for and correlate threat intelligence information to identify new and emerging threats.
- Security awareness: MISP can be used to share threat intelligence information with employees to help them raise awareness of the latest threats and how to protect themselves.

Overall, MISP is a valuable tool for cybersecurity teams of all sizes. It can help organizations to improve their security posture by enabling them to share and collaborate on threat intelligence information more effectively.

MISP architecture: MISP is a web-based application that is typically hosted on a server within an organization's network. Users can access MISP through a web browser using their organization's credentials.

MISP data model: MISP uses a structured data model to represent threat intelligence information. This data model is based on the Common Vocabulary for Information Exchange (CVE) and the OpenIOC format.

MISP features: MISP provides a number of features that make it a valuable tool for cybersecurity teams, including:

Collaboration: MISP allows organizations to share threat intelligence information with each other in a secure and controlled manner.
Analysis: MISP provides tools for analyzing threat intelligence information, such as correlation and enrichment.
Automation: MISP can be integrated with other security tools, such as SIEMs and intrusion detection systems, to automate the sharing and consumption of threat intelligence information.

MISP community: MISP is an open-source project with a large and active community. The community provides support to MISP users through a variety of channels, including mailing lists, IRC chat, and forums.

MISP deployments: MISP is used by a wide range of organizations, including government agencies, businesses, and non-profit organizations. Some notable examples include:

- The United States Department of Homeland Security
- The United Kingdom National Cyber Security Centre

- The Australian Cyber Security Centre
- The NATO Cooperative Cyber Defence Centre of Excellence
- The Financial Services Information Sharing and Analysis Center (FS-ISAC)

College Network Information:

Most of the colleges and universities use CAN (Campus Area Network) is a computer network that connects multiple buildings within a college or university campus. CANs typically provide Internet access to students, faculty, and staff, as well as allow for the sharing of files and resources across the campus.

CANs are typically larger and more complex than local area networks (LANs), which are typically limited to a single building or office. However, CANs are smaller than metropolitan area networks (MANs) and wide area networks (WANs), which connect networks across large geographic areas.

CANs are typically owned and operated by the college or university itself. This allows the institution to have complete control over the network and its security.

Components of a college network

A college network typically consists of the following components:

- Core network: The core network is the backbone of the CAN and connects the different buildings and networks on campus. It typically consists of high-speed switches and routers.
- Distribution network: The distribution network connects the core network to the access networks in each building. It typically consists of switches and routers that are less powerful than the core network devices.
- Access network: The access network provides connectivity to end users in each building. It typically consists of switches and wireless access points.
- Internet access: College networks typically provide Internet access to students, faculty, and staff. This is done through a connection to an Internet service provider (ISP).

Security of college networks

College networks are a prime target for cyberattacks. This is because they contain a wealth of sensitive data, such as student records, research data, and financial information.

Colleges and universities take a number of steps to secure their networks, including:

- Firewalls: Firewalls are used to block unauthorized access to the network.
- Intrusion detection systems (IDS): IDS are used to detect and respond to malicious activity on the network.
- Encryption: Encryption is used to protect sensitive data from unauthorized access.
- User education: Users are educated about cybersecurity best practices, such as how to create strong passwords and avoid phishing scams.

Benefits of college networks:
College networks provide a number of benefits to students, faculty, and staff, including:

- Internet access: College networks provide students, faculty, and staff with access to the Internet, which is essential for academic research and collaboration.
- Resource sharing: College networks allow students, faculty, and staff to share files and resources across the campus. This can save time and money.
- Communication: College networks facilitate communication between students, faculty, and staff. This can be done through email, instant messaging, and other online tools.
- Security: College networks are typically secure and provide protection from cyberattacks. This helps to protect the sensitive data that is stored on the network.

Overall, college networks play an important role in the academic and administrative life of colleges and universities. They provide students, faculty, and staff with the tools and resources they need to succeed.

How do you think you deploy soc in your college?

To deploy a SOC in a college, the following steps are recommended:

1. Establish a SOC team. The SOC team should be composed of experienced cybersecurity professionals who have the skills and knowledge to monitor and protect the college network.
2. Select and implement the appropriate security tools. The SOC team will need to select and implement a variety of security tools, such as firewalls, intrusion detection systems, and SIEMs.
3. Develop a SOC playbook. The SOC playbook should outline the steps that the SOC team will take to respond to different types of security incidents.
4. Train the SOC team. The SOC team should be trained on the security tools that they will be using and on the SOC playbook.
5. Communicate with stakeholders. The SOC team should communicate with key stakeholders on campus, such as the IT department, the administration, and the student body, about the SOC and its mission.

Here is a more detailed look at each step:

1. Establish a SOC team

The SOC team should be composed of experienced cybersecurity professionals who have the skills and knowledge to monitor and protect the college network. The team should be responsible for the following tasks:

- Monitoring the college network for suspicious activity
- Investigating security incidents
- Responding to security incidents
- Proactively improving the college's security posture

2. Select and implement the appropriate security tools

The SOC team will need to select and implement a variety of security tools to monitor and protect the college network. Some of the essential tools include:

- Firewalls: Firewalls block unauthorized access to the college network.
- Intrusion detection systems (IDS): IDS detect malicious activity on the network.
- Security information and event management (SIEM): SIEMs aggregate and correlate security events from across the network.

In addition to these essential tools, the SOC team may also want to consider implementing other security tools, such as threat intelligence feeds, vulnerability scanners, and security orchestration, automation, and response (SOAR) tools.

3. Develop a SOC playbook

The SOC playbook should outline the steps that the SOC team will take to respond to different types of security incidents. The playbook should include the following information:

- Incident response procedures
- Communication protocols
- Escalation procedures

The SOC playbook should be reviewed and updated on a regular basis to reflect changes in the college's security environment.

4. Train the SOC team

The SOC team should be trained on the security tools that they will be using and on the SOC playbook. The training should cover the following topics:

- Security fundamentals
- Security tools and technologies
- SOC procedures
- Incident response
- Communicate with stakeholders

The SOC team should communicate with key stakeholders on campus, such as the IT department, the administration, and the student body, about the SOC and its mission. The SOC team should provide regular updates on the college's security posture and should communicate any security incidents that occur.

By following these steps, a college can deploy a SOC that will help to protect its network and its students, faculty, and staff from cyberattacks.

Threat intelligence

Threat intelligence is detailed, actionable threat information for preventing and fighting cyberthreats targeting an organization. It is data containing detailed knowledge about the cybersecurity threats targeting an organization. Threat intelligence helps security teams be more proactive, enabling them to take effective, data-driven actions to prevent cyber-attacks before they occur. It can also help an organization better detect and respond to attacks in progress .

Threat intelligence involves gathering, analysing, and using information about current and potential cybersecurity threats. It helps organizations understand the types of threats they might face, the tactics, techniques, and procedures used by threat actors, and the vulnerabilities they might exploit.

Threat intelligence is crucial for proactive cybersecurity. It helps organizations assess their risks, make informed decisions, and improve their security posture.

Incident response

Incident response refers to an organization's processes and technologies for detecting and responding to cyberthreats, security breaches or cyberattacks. The goal of incident response is to prevent cyberattacks before they happen, and to minimize the cost and business disruption resulting from any cyberattacks that occur. Ideally, an organization defines incident response processes and technologies in a formal incident response plan (IRP) that specifies exactly how different types of cyberattacks should be identified, contained, and resolved .

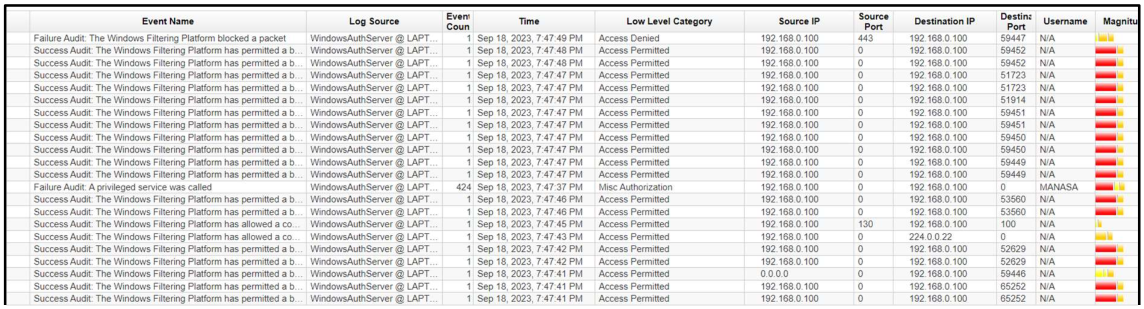
The key steps in incident response include preparation, identification, containment, eradication, recovery, and lessons learned. It's a cyclical process designed to minimize damage and reduce recovery time and costs. Effective incident response can help organizations limit the impact of a breach and prevent it from happening again.

Qradar & understanding about tool

QRadar is a network security management platform that provides situational awareness and compliance support. QRadar uses a combination of flow-based network knowledge, security event correlation, and asset-based vulnerability assessment. It collects log data from an enterprise, its network devices, host assets and os (Operation System), applications, vulnerabilities, and user activities and behaviours. QRadar administrators can browse and download apps from the IBM Security App Exchange to address specific security requirements .

QRadar collects and analyzes data from a wide range of sources, including network traffic, logs, and events, to identify security threats and anomalies. Key features of QRadar include real-time event correlation, log management, user behavior analytics, and vulnerability assessment.

QRadar is often used by organizations to centralize their security information, detect and respond to security incidents, and improve compliance with security regulations.



Event Name	Log Source	Event Coun	Time	Low Level Category	Source IP	Source Port	Destination IP	Destina Port	Username	Magnitu
Failure Audit: The Windows Filtering Platform blocked a packet	WindowsAuthServer @ LAPT...	1	Sep 18, 2023, 7:47:49 PM	Access Denied	192.168.0.100	443	192.168.0.100	59447	N/A	
Success Audit: The Windows Filtering Platform has permitted a b...	WindowsAuthServer @ LAPT...	1	Sep 18, 2023, 7:47:48 PM	Access Permitted	192.168.0.100	0	192.168.0.100	59452	N/A	
Success Audit: The Windows Filtering Platform has permitted a b...	WindowsAuthServer @ LAPT...	1	Sep 18, 2023, 7:47:48 PM	Access Permitted	192.168.0.100	0	192.168.0.100	59452	N/A	
Success Audit: The Windows Filtering Platform has permitted a b...	WindowsAuthServer @ LAPT...	1	Sep 18, 2023, 7:47:47 PM	Access Permitted	192.168.0.100	0	192.168.0.100	51723	N/A	
Success Audit: The Windows Filtering Platform has permitted a b...	WindowsAuthServer @ LAPT...	1	Sep 18, 2023, 7:47:47 PM	Access Permitted	192.168.0.100	0	192.168.0.100	51723	N/A	
Success Audit: The Windows Filtering Platform has permitted a b...	WindowsAuthServer @ LAPT...	1	Sep 18, 2023, 7:47:47 PM	Access Permitted	192.168.0.100	0	192.168.0.100	51914	N/A	
Success Audit: The Windows Filtering Platform has permitted a b...	WindowsAuthServer @ LAPT...	1	Sep 18, 2023, 7:47:47 PM	Access Permitted	192.168.0.100	0	192.168.0.100	59451	N/A	
Success Audit: The Windows Filtering Platform has permitted a b...	WindowsAuthServer @ LAPT...	1	Sep 18, 2023, 7:47:47 PM	Access Permitted	192.168.0.100	0	192.168.0.100	59451	N/A	
Success Audit: The Windows Filtering Platform has permitted a b...	WindowsAuthServer @ LAPT...	1	Sep 18, 2023, 7:47:47 PM	Access Permitted	192.168.0.100	0	192.168.0.100	59450	N/A	
Success Audit: The Windows Filtering Platform has permitted a b...	WindowsAuthServer @ LAPT...	1	Sep 18, 2023, 7:47:47 PM	Access Permitted	192.168.0.100	0	192.168.0.100	59450	N/A	
Success Audit: The Windows Filtering Platform has permitted a b...	WindowsAuthServer @ LAPT...	1	Sep 18, 2023, 7:47:47 PM	Access Permitted	192.168.0.100	0	192.168.0.100	59449	N/A	
Success Audit: The Windows Filtering Platform has permitted a b...	WindowsAuthServer @ LAPT...	1	Sep 18, 2023, 7:47:47 PM	Access Permitted	192.168.0.100	0	192.168.0.100	59449	N/A	
Failure Audit: A privileged service was called	WindowsAuthServer @ LAPT...	424	Sep 18, 2023, 7:47:37 PM	Misc Authorization	192.168.0.100	0	192.168.0.100	0	MANASA	
Success Audit: The Windows Filtering Platform has permitted a b...	WindowsAuthServer @ LAPT...	1	Sep 18, 2023, 7:47:46 PM	Access Permitted	192.168.0.100	0	192.168.0.100	53560	N/A	
Success Audit: The Windows Filtering Platform has permitted a b...	WindowsAuthServer @ LAPT...	1	Sep 18, 2023, 7:47:46 PM	Access Permitted	192.168.0.100	0	192.168.0.100	53560	N/A	
Success Audit: The Windows Filtering Platform has allowed a co...	WindowsAuthServer @ LAPT...	1	Sep 18, 2023, 7:47:45 PM	Access Permitted	192.168.0.100	130	192.168.0.100	100	N/A	
Success Audit: The Windows Filtering Platform has allowed a co...	WindowsAuthServer @ LAPT...	1	Sep 18, 2023, 7:47:43 PM	Access Permitted	192.168.0.100	0	224.0.0.22	0	N/A	
Success Audit: The Windows Filtering Platform has permitted a b...	WindowsAuthServer @ LAPT...	1	Sep 18, 2023, 7:47:42 PM	Access Permitted	192.168.0.100	0	192.168.0.100	52629	N/A	
Success Audit: The Windows Filtering Platform has permitted a b...	WindowsAuthServer @ LAPT...	1	Sep 18, 2023, 7:47:42 PM	Access Permitted	192.168.0.100	0	192.168.0.100	52629	N/A	
Success Audit: The Windows Filtering Platform has permitted a b...	WindowsAuthServer @ LAPT...	1	Sep 18, 2023, 7:47:41 PM	Access Permitted	0.0.0.0	0	192.168.0.100	59446	N/A	
Success Audit: The Windows Filtering Platform has permitted a b...	WindowsAuthServer @ LAPT...	1	Sep 18, 2023, 7:47:41 PM	Access Permitted	192.168.0.100	0	192.168.0.100	65252	N/A	
Success Audit: The Windows Filtering Platform has permitted a b...	WindowsAuthServer @ LAPT...	1	Sep 18, 2023, 7:47:41 PM	Access Permitted	192.168.0.100	0	192.168.0.100	65252	N/A	

Fig.4 QRadar Logs

Conclusion :

Stage 1 : What you understand from Web application testing?

Web application testing is a thorough evaluation of a web-based software application, focusing on functionality, security, and performance.

The assessment of functionality covers various aspects, from basic navigation to complex tasks like database interactions, ensuring a bug-free user experience. Compatibility with different browsers and devices is also checked for seamless user interaction.

Security is a key concern, with testers actively seeking vulnerabilities like SQL injection and cross-site scripting. By simulating potential attacks, weaknesses are identified, and recommendations for fortification are provided. This ensures the protection of sensitive data and resilience against cyber threats. Overall, web application testing is crucial for a secure, reliable, and user-friendly online experience.

Stage 2 : What you understand from the Nessus report?

A Nessus report refers to a report generated by Nessus, which is a popular vulnerability scanning tool used for identifying and assessing security vulnerabilities in computer systems and networks. Nessus is often employed by cybersecurity professionals, network administrators, and penetration testers to conduct security assessments and ensure the security of their systems.

A Nessus report typically includes information like vulnerability findings, risk management, historical data, recommendations etc. The report lists all identified vulnerabilities, including their severity level, a brief description, and the affected systems or devices as a part of vulnerability findings. Nessus assigns a risk score or severity level to each vulnerability, helping users prioritize their remediation efforts as a part of risk assessment. Common severity levels include Critical, High, Medium, and Low.

In recommendations, for each vulnerability, Nessus provides recommendations and remediation steps to help system administrators or security professionals mitigate or resolve the identified issues. The report often includes detailed technical information about each vulnerability, such as its CVE (Common Vulnerabilities and Exposures) identifier, affected software versions, and any additional relevant details.

Nessus can also check systems against specific security compliance standards (e.g., CIS benchmarks, NIST guidelines), and the report may include compliance-related findings and recommendations. Some Nessus reports include an executive summary section designed for non-technical stakeholders, providing an overview of the security posture and key findings in a more easily digestible format. Nessus can be used to track changes in a network's vulnerability over time, and some reports may include historical data to show how vulnerabilities have evolved.

Stage-3: What do you understand from SOC/ SIEM/ QRadar Dashboard?

SOC:

A Security Operations Center (SOC) is a centralized team of cybersecurity professionals responsible for monitoring, detecting, investigating, and responding to cybersecurity threats. SOCs typically operate 24/7/365 to ensure that organizations are protected from a wide range of cyberattacks, including malware infections, data breaches, and denial-of-service attacks.

SOC functions:

SOCs perform a variety of functions, including:

- Security monitoring: SOCs use a variety of security tools and technologies to monitor organization networks and systems for suspicious activity. This activity may include unusual network traffic, unauthorized access attempts, and malicious code infections.
- Threat detection: SOCs use security monitoring data and threat intelligence feeds to detect cybersecurity threats. This may involve identifying known malware signatures, identifying new and emerging threats, and correlating events from different sources to identify patterns of malicious activity.
- Incident investigation: SOCs investigate cybersecurity incidents to determine the root cause, assess the impact, and recommend remediation steps. This may involve gathering evidence, analyzing logs, and interviewing stakeholders.
- Incident response: SOCs respond to cybersecurity incidents to contain the threat, mitigate the damage, and recover from the incident. This may involve deploying security countermeasures, restoring affected systems, and communicating with stakeholders.

SOC benefits

SOCs provide a number of benefits to organizations, including:

- Improved security posture: SOCs help organizations to improve their security posture by proactively monitoring for threats and responding to incidents quickly and effectively.
- Reduced risk of data breaches: SOCs can help organizations to reduce the risk of data breaches by detecting and responding to threats before they can compromise sensitive data.
- Compliance with regulations: Many regulations require organizations to have a SOC in place. SOCs can help organizations to comply with these regulations and avoid penalties.

SOC deployment

SOCs can be deployed in a variety of ways. Some organizations choose to build and operate their own SOCs, while others choose to outsource SOC services to a managed security service provider (MSSP).

SOC best practices:

There are a number of best practices that organizations can follow when deploying and operating a SOC, including:

- Establish a clear mission and scope: The SOC's mission and scope should be clearly defined and aligned with the organization's overall security strategy.
- Select the right security tools and technologies: The SOC should be equipped with the right security tools and technologies to monitor and protect the organization's network and systems.
- Train and hire qualified staff: The SOC team should be composed of qualified cybersecurity professionals who have the skills and knowledge to monitor, detect, investigate, and respond to cybersecurity threats.
- Develop and implement a SOC playbook: The SOC should develop and implement a playbook that outlines the steps that the team will take to respond to different types of security incidents.
- Test and improve the SOC: The SOC should be regularly tested and improved to ensure that it is effective in detecting and responding to cybersecurity threats.

Conclusion:
SOCs play an important role in protecting organizations from cybersecurity threats. By following the best practices outlined above, organizations can deploy and operate effective SOCs that can help to reduce the risk of data breaches and improve their overall security posture.

SIEM:

SIEM stands for Security Information and Event Management. It is a security solution that collects, analyzes, and correlates security events from across an organization's IT infrastructure. SIEMs can be used to detect, investigate, and respond to security incidents, as well as to improve an organization's overall security posture.

SIEMs typically collect data from a variety of sources, including:

- Network devices (such as firewalls and routers)
- Security devices (such as intrusion detection systems and intrusion prevention systems)
- Servers
- Applications
- End user devices

Once the data is collected, SIEMs use a variety of techniques to analyze and correlate it. This can include:

- Pattern matching: SIEMs can look for patterns in security events that may indicate a malicious attack.
- Anomaly detection: SIEMs can identify anomalous activity that may be indicative of a security incident.

- Correlation: SIEMs can correlate security events from different sources to identify relationships that may not be obvious from looking at the events individually.

Once SIEMs have identified potential security incidents, they can be used to investigate and respond to them. This can include:

- SIEMs can provide analysts with context for the security events that have been identified.
- SIEMs can help analysts to prioritize their investigations.
- SIEMs can automate some of the tasks involved in responding to security incidents, such as blocking malicious IP addresses and quarantining infected systems.

SIEMs can also be used to improve an organization's overall security posture. This can be done by:

- Identifying security gaps
- Measuring the effectiveness of security controls
- Proactively detecting and responding to emerging threats

SIEMs are an essential tool for any organization that wants to protect its IT infrastructure from cyberattacks. By collecting, analyzing, and correlating security events from across the organization, SIEMs can help to detect, investigate, and respond to security incidents more effectively.

Here are some specific examples of how SIEMs can be used in a college environment:

- SIEMs can be used to detect unauthorized access to student records or financial data.
- SIEMs can be used to detect malware infections on college servers or student devices.
- SIEMs can be used to detect phishing attacks directed at college students or faculty.
- SIEMs can be used to monitor for suspicious activity on the college network, such as brute force attacks or denial-of-service attacks.

By using SIEMs to monitor and protect its network, a college can help to ensure the confidentiality, integrity, and availability of its data and systems.

Qradar Dashboard

A QRadar dashboard is a visual representation of security data that is collected and analyzed by the QRadar SIEM platform. QRadar dashboards can be used to monitor the security posture of an organization's network and systems, to investigate security incidents, and to generate reports on security trends.

QRadar dashboards typically contain a variety of widgets, such as charts, graphs, and tables. Each widget displays a different type of security data, such as the number of security events that have occurred, the top sources of security events, and the most common types of security events.

QRadar dashboards are customizable, so organizations can create dashboards that are tailored to their specific needs. For example, an organization may create a dashboard to monitor the security of its web servers, or it may create a dashboard to monitor the security of its network endpoints.

QRadar dashboards can be used for a variety of purposes, including:

- Security monitoring: QRadar dashboards can be used to monitor the security posture of an organization's network and systems in real time. This allows organizations to quickly identify and respond to security incidents.
- Incident investigation: QRadar dashboards can be used to investigate security incidents by providing insights into the root cause of the incident and the impact of the incident.
- Security reporting: QRadar dashboards can be used to generate reports on security trends and incidents. This information can be used to improve the organization's security posture over time.

Here are some examples of specific QRadar dashboards that an organization might use:

- Overview dashboard: This dashboard provides a high-level overview of the organization's security posture. It typically includes widgets that display the number of security events that have occurred, the top sources of security events, and the most common types of security events.
- Endpoint security dashboard: This dashboard provides a detailed view of the security of the organization's network endpoints. It typically includes widgets that display the status of endpoint security software, the number of security events that have occurred on each endpoint, and the most common types of security events on each endpoint.
- Web security dashboard: This dashboard provides a detailed view of the security of the organization's web servers. It typically includes widgets that display the number of web attacks that have occurred, the top sources of web attacks, and the most common types of web attacks.
- Incident response dashboard: This dashboard provides a single view of all open security incidents. It typically includes widgets that display the status of each incident, the severity of each incident, and the assigned investigator for each incident.

QRadar dashboards are a valuable tool for organizations of all sizes. They can help organizations to improve their security posture by providing insights into their security data and by helping them to quickly and effectively respond to security incidents.

Future Scope :

Stage 1 : Future scope of web application testing

The future scope of web application testing is poised for significant growth and evolution, driven by the continuous advancement of technology and the increasing reliance on web-based solutions across industries.

Firstly, with the proliferation of complex web applications and the adoption of emerging technologies like AI, IoT, and blockchain, the demand for specialized testing approaches is expected to rise. This will necessitate the development of more sophisticated testing tools and methodologies to ensure the robustness, security, and performance of these advanced applications.

Secondly, as cybersecurity threats continue to escalate, web application testing will play an even more critical role in safeguarding digital assets. With the expanding attack surface, including cloud-based services and interconnected systems, there will be a heightened need for comprehensive security testing. This will lead to the integration of advanced security testing techniques, such as threat modelling and vulnerability assessments, to fortify web applications against evolving cyber threats. Additionally, compliance with stringent data protection regulations will further drive the demand for rigorous testing practices. Overall, the future of web application testing is poised to be dynamic and pivotal in ensuring the reliability and security of the digital landscape.

Stage 2 : Future scope of testing process you understood
The future scope of testing process holds significant promise. This integration combines the strengths of traditional vulnerability scanning with the advanced capabilities of artificial intelligence. First and foremost, it offers an enhanced approach to threat detection. Nessus, with its vast plugin library, can systematically identify known vulnerabilities and weaknesses within a network. When complemented by AI-driven anomaly detection, it becomes capable of spotting unusual patterns or behaviors that might go unnoticed through conventional vulnerability scans. This comprehensive approach empowers organizations to proactively safeguard their networks by detecting both known issues and emerging threats.

Moreover, the integration of Nessus and AI brings about a crucial reduction in false positives. Traditional network security scanning often generates numerous false alarms, which can be resource-intensive to investigate and rectify. AI algorithms can be employed to discern genuine threats from benign anomalies, streamlining the security analysis process. This, in turn, allows security teams to concentrate their efforts on addressing actual risks and thus optimizes resource allocation while bolstering the network's overall security posture.

A critical facet of this integration is the shift from a reactive to a proactive security approach. By using Nessus to identify vulnerabilities and AI for anomaly detection, organizations can act proactively. They can pre-emptively pinpoint potential threats before they can be exploited, a fundamental requirement in today's dynamic threat landscape where zero-day vulnerabilities and sophisticated attacks are prevalent.

Lastly, this combination facilitates continuous improvement in network security. AI algorithms, learning from historical data, refine the anomaly detection process and enhance accuracy over time. The network becomes increasingly adept at identifying real threats and adapting to new attack vectors. This self-improving capability ensures that organizations remain resilient against emerging threats, making it a forward-looking approach to network security that is adaptable and future-ready. In essence, the integration of Nessus with AI-driven anomaly detection presents a powerful and comprehensive solution for addressing the ever-evolving challenges of network security in an era dominated by artificial intelligence.

Stage 3 : Future scope of SOC / SEIM
The future of Security Operations Centers (SOCs) and Security Information and Event Management (SIEM) systems is incredibly promising, reflecting the evolving landscape of cybersecurity threats and technological advancements.

Firstly, SOCs are poised to become even more sophisticated and proactive in threat detection and response. As cyber threats become more advanced and persistent, SOCs will increasingly leverage artificial intelligence and machine learning algorithms to analyze vast amounts of data in real-time. This predictive approach will enable SOCs to identify and mitigate potential threats before they can cause significant damage. Additionally, SOCs will likely integrate with threat intelligence platforms and collaborate more closely with other security teams to stay ahead of emerging threats.

Secondly, SIEM systems are anticipated to become more intelligent and context-aware. They will evolve to not only detect security incidents but also provide richer insights into the nature and impact of these incidents. SIEM platforms will likely incorporate advanced analytics and behavioral analysis to differentiate between genuine threats and false alarms. Moreover, the integration of automation and orchestration capabilities will enhance the efficiency of incident response, allowing security teams to react swiftly to mitigate risks.

Overall, the future of SOCs and SIEM systems promises a more robust, agile, and intelligent approach to cybersecurity, crucial in safeguarding organizations against increasingly sophisticated threats.

Topics explored :

1. Web Application Testing
2. Nessus
3. SOC
4. SIEM
5. QRadar
6. Anomaly Detection
7. Deep Learning
8. Machine Learning
9. Intrusion Detection
10. Network Security
11. Predictive Analytics
12. Behavioral Analysis
13. Pattern Recognition
14. Data Mining
15. Threat Detection
16. Packet Analysis
17. Network Traffic Analysis
18. Feature Engineering
19. Alert Prioritization
20. DNS Traffic Analysis
21. User Behavior Profiling
22. Network Forensics
23. Signature-based Detection
24. Heuristic Analysis

Tools explored :

1. Burpsuite
2. SQL Map
3. Nessus
4. Kali Linux
5. Wireshark
6. Python
7. TensorFlow
8. Scikit-learn
9. Keras
10. Pandas
11. Numpy
12. Matplotlib
13. GitHub
14. Jupyter Notebook
15. Jira
16. Mural

----------------------------------THE END --