**Title of the project :-**

### Intelligent Threat Detection And Response: AI Integration In Cybersecurity Frameworks

**Overview :-**

A Security Operations Center (SOC) serves as a centralized unit within an organization with the key role of monitoring, detecting, and responding to security incidents. It acts as the primary hub for addressing security-related issues and is staffed by a team of professionals, including security analysts, incident responders, and other personnel dedicated to safeguarding the organization's assets and data. In addition to incident response, SOCs often oversee the management of various security technologies like firewalls, intrusion detection systems, and Security Information and Event Management (SIEM) systems. They are also involved in the development and implementation of security policies and procedures.

* Top of Form

**List of teammates–**

|  |  |  |  |
| --- | --- | --- | --- |
| **S.no** | **name** | **college** | **contact** |
| **1** | **S.Padmavathy** | **Sona college of technology** | **9043755225** |
|  |  |  |  |

**List of Vulnerability Table ➖**

|  |  |  |
| --- | --- | --- |
| **S.no** | **Vulnerability Name** | **CWE - No** |
| **1** | **SQL Injection** | **CWE-89** |
| **2** | **Cross-Site Scripting (XSS)** | **CWE-79** |
| **3** | **Cross-Site Request Forgery (CSRF)** | **CWE-352** |
| **4** | **Buffer Overflow** | **CWE-120** |
| **5** | **Insecure Direct Object References (IDOR)** | **CWE-639** |
| **6** | **Security Misconfiguration** | **CWE-732** |
| **7** | **Unvalidated Redirects and Forwards** | **CWE-601** |
| **8** | **Authentication Bypass** | **CWE-592** |
| **9** | **XML External Entity (XXE)** | **CWE-611** |
| **10** | **Remote Code Execution (RCE)** | **CWE-94** |

**REPORT:-**

Vulnerability Name: Buffer Overflow

**CWE: CWE-119**

OWASP Category: A1: Injection

Description:

Overview: Buffer Overflow is a condition where a program writes more data to a block of memory, or buffer, than it was allocated for.

Technical Details: Attackers can exploit this vulnerability by injecting more data than a program can handle, leading to overwriting adjacent memory and potentially executing arbitrary code.

Business Impact:

Risk: High

Consequences: Successful exploitation can lead to unauthorized access, execution of arbitrary code, or even a system crash. This can result in loss of data, service disruption, and potential legal and financial ramifications for the affected organization.

CWE-79: Improper Neutralization of Input During Web Page Generation

Vulnerability Name: Improper Neutralization of Input During Web Page Generation

**CWE: CWE-79**

OWASP Category: A1: Injection

Description:

Overview: This vulnerability occurs when user input is not properly neutralized during the generation of web pages, leading to potential injection attacks.

Technical Details: Attackers can inject malicious input, leading to various security issues, including but not limited to cross-site scripting (XSS) vulnerabilities.

Business Impact:

Risk: High

Consequences: Successful exploitation can lead to unauthorized access, data manipulation, or the execution of malicious scripts.

CWE-89: Improper Neutralization of Special Elements used in an SQL Command

Vulnerability Name: Improper Neutralization of Special Elements used in an SQL Command

**CWE: CWE-89**

OWASP Category: A1: Injection

Description:

Overview: This vulnerability involves the improper neutralization of special elements in SQL commands, leading to potential SQL injection attacks.

Technical Details: Attackers can manipulate SQL queries to execute unauthorized actions on a database.

Business Impact:

Risk: High

Consequences: Unauthorized access to or manipulation of the database, potential data breaches.

CWE-20: Improper Input Validation

Vulnerability Name: Improper Input Validation

**CWE: CWE-20**

OWASP Category: A1: Injection

Description:

Overview: Improper input validation occurs when an application does not properly validate or sanitize user input, leading to various injection vulnerabilities.

Technical Details: Attackers can exploit this weakness to inject malicious code or conduct other injection attacks.

Business Impact:

Risk: High

Consequences: Unauthorized access, data manipulation, or compromise of the application's security.

CWE-200: Information Exposure

Vulnerability Name: Information Exposure

**CWE: CWE-200**

OWASP Category: A3: Sensitive Data Exposure

Description:

Overview: Information exposure vulnerabilities involve the unintentional disclosure of sensitive information, potentially leading to unauthorized access or data breaches.

Technical Details: Attackers may exploit this weakness to gain access to sensitive information.

Business Impact:

Risk: High

Consequences: Unauthorized access to sensitive information, potential legal and financial repercussions.

CWE-352: Cross-Site Request Forgery (CSRF)

Vulnerability Name: Cross-Site Request Forgery (CSRF)

**CWE: CWE-352**

OWASP Category: A8: Cross-Site Request Forgery (CSRF)

Description:

Overview: CSRF occurs when an attacker tricks a user's browser into performing actions on a website without their knowledge or consent.

Technical Details: Attackers may exploit this vulnerability to perform actions on behalf of authenticated users without their consent.

Business Impact:

Risk: Medium to High

Consequences: Unauthorized actions performed on behalf of users, potential data manipulation.

CWE-285: Improper Authorization

Vulnerability Name: Improper Authorization

**CWE: CWE-285**

OWASP Category: A5: Broken Access Control

Description:

Overview: Improper authorization vulnerabilities occur when an application does not properly enforce access controls, allowing unauthorized users to perform actions they shouldn't.

Technical Details: Attackers may exploit this weakness to gain unauthorized access to resources.

Business Impact:

Risk: High

Consequences: Unauthorized access, data breaches, compromised system integrity.

CWE-22: Improper Limitation of a Pathname to a Restricted Directory

Vulnerability Name: Improper Limitation of a Pathname to a Restricted Directory

**CWE: CWE-22**

OWASP Category: A5: Broken Access Control

Description:

Overview: This vulnerability involves improper restrictions on the locations or directories that a user can access, potentially leading to unauthorized access to sensitive files.

Technical Details: Attackers may exploit this weakness to access files or directories they shouldn't be able to access.

Business Impact:

Risk: High

Consequences: Unauthorized access to sensitive files, potential data breaches.

CWE-78: Improper Neutralization of Special Elements used in an OS Command

Vulnerability Name: Improper Neutralization of Special Elements used in an OS Command

**CWE: CWE-78**

OWASP Category: A1: Injection

Description:

Overview: Similar to SQL injection, this vulnerability involves improper neutralization of special elements in OS commands, leading to potential command injection attacks.

Technical Details: Attackers may exploit this weakness to execute arbitrary commands on the underlying operating system.

Business Impact:

Risk: High

Consequences: Unauthorized execution of commands, potential compromise of the host system.

CWE-287: Improper Authentication

Vulnerability Name: Improper Authentication

**CWE: CWE-287**

OWASP Category: A2: Broken Authentication

Description:

Overview: Improper authentication vulnerabilities occur when an application does not properly verify the identity of users, potentially leading to unauthorized access.

Technical Details: Attackers may exploit this weakness to gain access to user accounts without proper credentials.

Business Impact:

Risk: High

Consequences: Unauthorized access to user accounts, potential data breaches.

CWE-434: Unrestricted Upload of File with Dangerous Type

Vulnerability Name: Unrestricted Upload of File with Dangerous Type

**CWE: CWE-434**

OWASP Category: A4: XML External Entity (XXE)

Description:

Overview: This vulnerability involves allowing users to upload files with dangerous types, which can lead to various security issues, including the execution of malicious code.

Technical Details: Attackers may exploit this weakness to upload malicious files that can compromise the security of the application or the server.

Business Impact:

Risk: High

Consequences: Execution of malicious code, potential compromise of the application or server.

CWE-311: Missing Encryption of Sensitive Data

Vulnerability Name: Missing Encryption of Sensitive Data

**CWE: CWE-311**

OWASP Category: A3: Sensitive Data Exposure

Description:

Overview: This vulnerability occurs when sensitive data is not properly encrypted, leading to potential exposure and unauthorized access.

Technical Details: Attackers may exploit this weakness to intercept and gain access to sensitive information.

Business Impact:

Risk: High

Consequences: Unauthorized access to sensitive information, potential data breaches.

CWE-352: Cross-Site Scripting (XSS)

Vulnerability Name: Cross-Site Scripting (XSS)

**CWE: CWE-352**

OWASP Category: A7: Cross-Site Scripting (XSS)

Description:

Overview: XSS vulnerabilities allow attackers to inject malicious scripts into web pages viewed by other users, potentially leading to the theft of sensitive information.

Technical Details: Attackers may exploit this weakness to execute scripts in the context of a user's browser.

Business Impact:

Risk: Medium to High

Consequences: Compromised user accounts, defaced websites, theft of sensitive information.

CWE-601: URL Redirection to Untrusted Site ('Open Redirect')

Vulnerability Name: URL Redirection to Untrusted Site ('Open Redirect')

**CWE: CWE-601**

OWASP Category: A10: Unvalidated Redirects and Forwards

Description:

Overview: This vulnerability occurs when an application redirects users to a different site without proper validation, which can be abused for phishing attacks.

Technical Details: Attackers may exploit this weakness to trick users into visiting malicious sites.

Business Impact:

Risk: Medium

Consequences: Phishing attacks, potential compromise of user credentials.

CWE-732: Insecure Permission Assignment for Critical Resource

Vulnerability Name: Insecure Permission Assignment for Critical Resource

**CWE: CWE-732**

OWASP Category: A5: Broken Access Control

Description:

Overview: Insecure permission assignment vulnerabilities involve assigning improper permissions to critical resources, potentially leading to unauthorized access.

Technical Details: Attackers may exploit this weakness to gain unauthorized access to critical resources.

Business Impact:

Risk: High

Consequences: Unauthorized access to critical resources, potential data breaches.

CWE-862: Missing Authorization

Vulnerability Name: Missing Authorization

**CWE: CWE-862**

OWASP Category: A5: Broken Access Control

Description:

Overview: Missing authorization vulnerabilities occur when an application incorrectly determines whether a user should have access to a specific resource.

Technical Details: Attackers may exploit this weakness to gain unauthorized access to resources.

Business Impact:

Risk: High

Consequences: Unauthorized access, potential data breaches.

CWE-94: Improper Control of Generation of Code ('Code Injection')

Vulnerability Name: Improper Control of Generation of Code ('Code Injection')

**CWE: CWE-94**

OWASP Category: A1: Injection

Description:

Overview: Improper control of code generation can lead to code injection attacks, allowing attackers to execute arbitrary code on a system.

Technical Details: Attackers may exploit this weakness to inject and execute malicious code on the target system.

Business Impact:

Risk: High

Consequences: Unauthorized code execution, potential compromise of the target system.

CWE-798: Use of Hard-coded Credentials

Vulnerability Name: Use of Hard-coded Credentials

**CWE: CWE-798**

OWASP Category: A2: Broken Authentication

Description:

Overview: This vulnerability involves using hard-coded or embedded credentials in the code, making it easier for attackers to gain unauthorized access.

Technical Details: Attackers may exploit this weakness to access systems or services using the hard-coded credentials.

Business Impact:

Risk: High

Consequences: Unauthorized access, potential compromise of systems or accounts.

CWE-863: Incorrect Authorization

Vulnerability Name: Incorrect Authorization

**CWE: CWE-863**

OWASP Category: A5: Broken Access Control

Description:

Overview: Incorrect authorization vulnerabilities occur when an application incorrectly determines whether a user should have access to a specific resource.

Technical Details: Attackers may exploit this weakness to gain unauthorized access to resources.

Business Impact:

Risk: High

Consequences: Unauthorized access, potential data breaches.

CWE-476: NULL Pointer Dereference

Vulnerability Name: NULL Pointer Dereference

**CWE: CWE-476**

OWASP Category: A6: Security Misconfiguration

Description:

Overview: This vulnerability occurs when a program dereferences a null or undefined pointer, potentially leading to crashes or other unintended behavior.

Technical Details: Attackers may exploit this weakness to cause system crashes or execute arbitrary code.

Business Impact:

Risk: High

Consequences: System crashes, potential unauthorized code execution.