AI-Enhanced Intrusion Detection System (IDS)

Securing Tomorrow's World Today: Empowering IDS with AI

Team ID
Team-591527

Team Members –
- Asim Shikhar
- R Gowtham
- Love Yadav

Team - 1.4

.

About Project

The objective of an AI-Enhanced Intrusion Detection System (IDS) project is to develop a sophisticated cybersecurity solution that makes use of machine learning and artificial intelligence techniques to more quickly and effectively identify and respond to network and system intrusions.

This project aims to enhance network and system security by harnessing the power of AI to detect and respond to intrusions with greater accuracy and speed, ultimately reducing the risk of cyber threats and data breaches.

.

Benefits of leveraging AI in IDS

Leveraging AI in IDS offers several benefits. Firstly, AI can efficiently analyze vast amounts of data, enabling quicker detection of anomalies and potential threats. Secondly, AI-powered IDS can adapt and learn from new attack patterns, improving their accuracy over time. Lastly, AI can automate the response to detected threats, reducing the burden on human operators and enabling faster mitigation of cybersecurity incidents.

vision And Abstract of project

•Monitoring and detection of the network will reduce downtime and future attacks.

•A comprehensive and organized analysis is conducted to verify the causes of the attack.

•Most household internet users lack the means to strengthen their internet connection or networking system.

•Unauthorized access into a home networking system may cause harm by stealing private and confidential information, and firewalls and anti-virus won't be sufficient against a determined attacker.

•The scope of the project is to develop an intrusion detection system that will improve the security of the home network.

•The objective of the project is to investigate the methods needed to detect any unauthorized access into a home networking system.

•The detection system will use an open-source system that is readily available but will be tuned for the usage of home users and based on the Windows operating system.

•The literature review component will discuss all the research that has been done prior to the pre-development and post-development of the project. All intrusion detection and prevention systems and their research will be further discussed in detail.

•The methodology section will discuss the usage of the Iteration Development Model as the methodology used in developing this project.

•The results and discussions section will discuss the preliminary findings, prototype development process and results, and testing results.

•All the justifications will be made clearly.

•The recommendations section will list and elaborate on all the related recommendations and some improvements that can be made for the future of this project.

•The conclusion section will conclude the overall project. The project phases will also be discussed in detail.

•The project will focus on developing a network intrusion detection system for Windows-based operating systems

Problem Statement

The problem addressed by this project is the unauthorized access into home networking systems, which poses a serious threat to the privacy and security of home users. Traditional security measures such as firewalls and antivirus software are often insufficient to protect against determined attackers. As a result, there is a pressing need for a dedicated intrusion detection system (IDS) tailored for Windows-based home networks. This IDS aims to detect and prevent unauthorized access, thereby reducing downtime and safeguarding private and confidential information for home users.

Problem Statement

The problem addressed by this project is the unauthorized access into home networking systems, which poses a serious threat to the privacy and security of home users. Traditional security measures such as firewalls and antivirus software are often insufficient to protect against determined attackers. As a result, there is a pressing need for a dedicated intrusion detection system (IDS) tailored for Windows-based home networks. This IDS aims to detect and prevent unauthorized access, thereby reducing downtime and safeguarding private and confidential information for home users.

Machine Learning algorithms for IDS

Machine Learning algorithms play a crucial role in enhancing IDS. They can analyze network traffic patterns and identify suspicious behaviors, allowing for more accurate detection of potential threats. Machine Learning models can also adapt and evolve, continuously learning from new data to improve their effectiveness in identifying and mitigating cybersecurity incidents.

User Research:

- **Security Analysts and Administrators:** Conduct interviews and surveys to understand their workflow, pain points, and the challenges they face in detecting and responding to security threats.
- **End-Users:** Understand their concerns regarding data security and privacy. Analyze their behaviors to identify potential security vulnerabilities.

Persona Development:

2. **Persona Develo**
   - Create detailed personas representing different user types within the organization. Include their goals, motivations, frustrations, and skills related to intrusion detection and response.

3. **Journey Mapping:**
   - Map out the typical workflow of security analysts and administrators, detailing each step from threat detection to resolution. Identify emotional highs and lows during this process.

Empathy Workshops:

- Conduct workshops with cross-functional teams involving developers, designers, and end-users. Encourage participants to share their experiences and insights related to intrusion incidents.

5. **Empathy Mapping:**
   - Create empathy maps for each persona. Identify what they Say, Think, Do, and Feel during various stages of dealing with security incidents. This helps in understanding their mindset and emotions better.

Iterative Design:

- Based on user feedback, iterate the design, focusing on enhancing usability and addressing user concerns. Continuous feedback loops are essential in refining the system empathetically.

8. **Training and Support:**
   - Provide comprehensive training to security analysts and administrators on using the AI-enhanced IDS effectively. Offer ongoing support channels, such as helpdesk and tutorials, to address their queries and challenges.

9. **Monitoring and Feedback:**
Continuously monitor the system's performance and gather feedback from users. Use this feedback to make necessary improvements and updates, ensuring the system aligns with users' evolving needs.

Implement machine learning algorithms to create a system that can learn and detect unusual patterns of network behaviour . This can help in identifying unauthorized access attempts.

Behavioural Analysis:
Create a system that not only detects known threats but also analyses user and device behaviour to identify anomalies. For example, if a device suddenly starts accessing a lot of sensitive information, it could triggeran alert.

Real-time Notifications: Design a system that provides real- time notifications to users when it detects potential threats. These notifications could be in the form of mobile app alerts or emails.

User-Friendly Dashboard: Build a user-friendly dashboard for the intrusion detection system, allowing users to monitor their network's security easily. They should be able to see network activityand potential threats in acomprehensible manner.

Automatic Quarantine: Implement a feature that, when a threat is detected, automatically quarantines the affected device, preventing it from accessing the network until the user confirms its legitimacy.

Regular Software Updates: Ensure the intrusion detection software is regularly updated to stay ahead of evolving threats. Provide users with automated updates to keep their network security current.

Network Traffic Encryption: Promote the use of encrypted connections (e.g., VPNs) to add an extra layer of security to the network.Integrate this with the intrusion detection system

Collaboration with ISPs: Partner with Internet Service Providers (ISPs) to offer intrusion detection as part of their service package to residential customers.

Cloud-Based IDS: Consider implementing a cloud- based intrusion detection system that can provide enhanced security features and scalability.

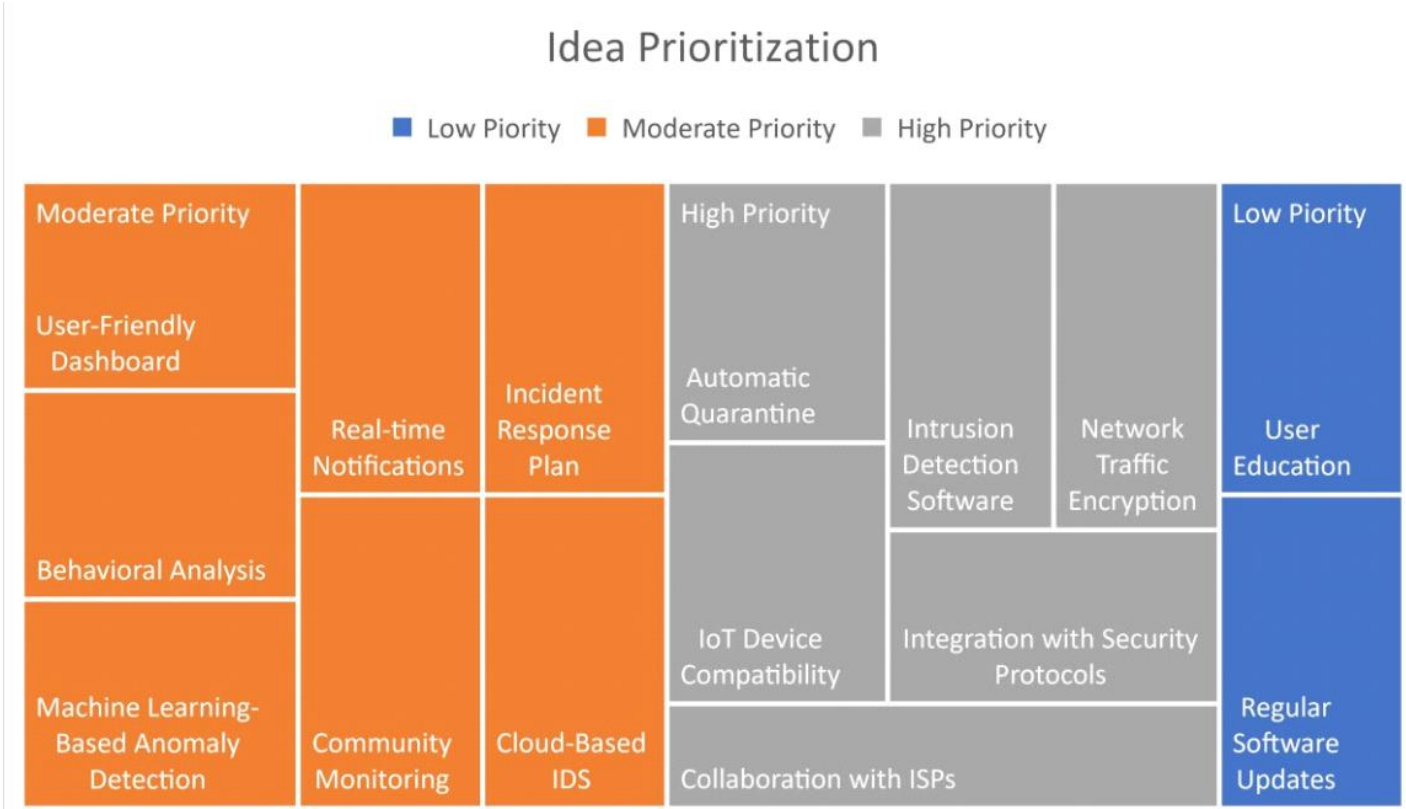
Community Monitoring: Create a community-based approach where users can share information about potential threats and collectively enhance networksecurity.

IoT Device Compatibility: Ensure that the intrusion detection system is compatible with the increasing number of IoT devices in home networks.

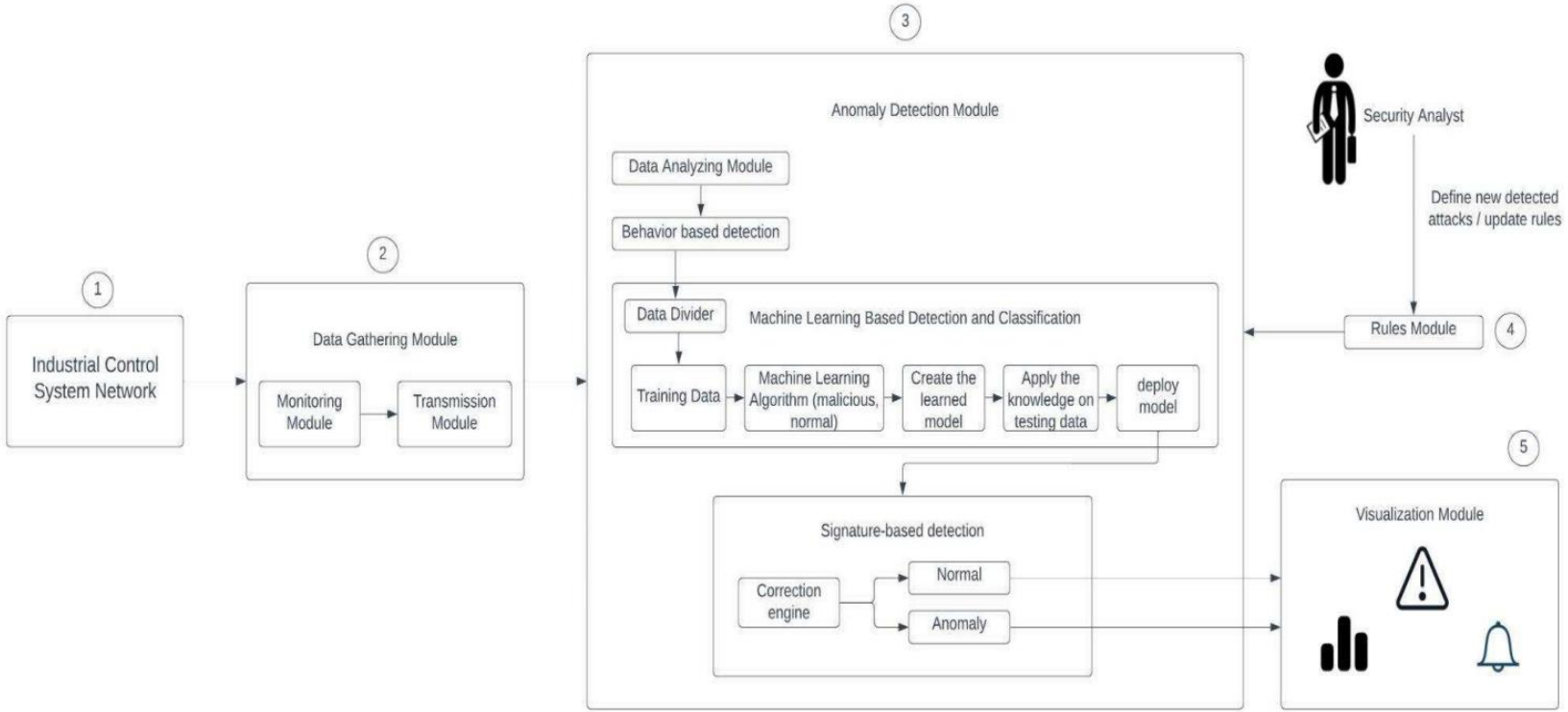
Incident Response Plan: Develop a clear incident response plan for users, guiding them on what to do if a breach is detected, including contacting support and reporting the incident to authorities if necessary.

Integration with Security Protocols: Ensure the intrusion detection system integrates seamlessly with existing security protocols and standards to enhance overall network security

Idea Prioritization



Solution Architecture



S.No.	Parameter	Description
1.	Problem Statement (Problem to be solved)	Unauthorized access to networks poses a significant security risk, as firewalls and traditional security measures may not be sufficient to protect against determined attackers.
2.	Idea / Solution description	The solution we have developed is a sophisticated AI-enhanced Intrusion Detection System (AI-IDS), which is intended to more accurately and efficiently identify security threats early on. It offers a complete solution to network security by fusing artificial intelligence, machine learning, and real-time monitoring.
3.	Novelty / Uniqueness	The project's distinctiveness stems from its concentration on tackling a particular and frequently disregarded facet of network security: home network security. Its user-centric design, platform-specific tailoring, iterative development, and transparent testing distinguish it as a unique addition to the intrusion detection systems sector.
4.	Social Impact / Customer Satisfaction	By improving digital security, decreasing downtime, safeguarding privacy, empowering people, promoting digital literacy, saving money, encouraging community collaboration, assuring health and safety, and aiding in the development of critical cybersecurity skills, the project's development of an NIDS for Windows-based home networks can have a significant positive social impact. In the end, it creates a digital environment that is safer and more secure for people as well as communities.
5.	Business Model (Revenue Model)	In addition to improving cybersecurity for individual users, the creation of a network intrusion detection system (NIDS) for Windows-based home networks has the potential to yield major business benefits. These benefits include increased market share, increased revenue, decreased incident rates, customer confidence, and the encouragement of cybersecurity awareness and education. Companies taking part in this initiative have the chance to improve their financial line and users'

Technical Architecture

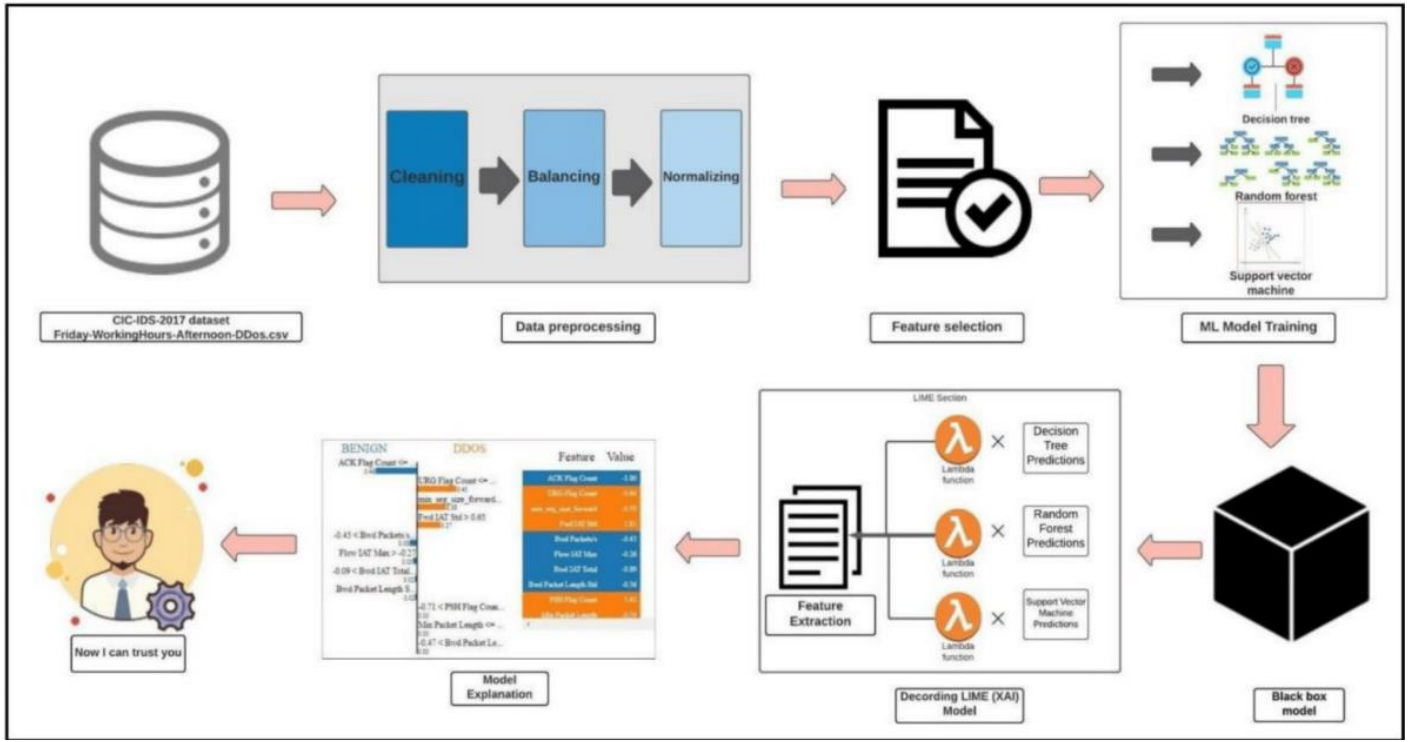


Table-1 : Components & Technologies:

S.No	Component	Description	Technology
1.	User Interface	How user interacts with application e.g. Web UI, Mobile App, Chatbot etc.	HTML, CSS, JavaScript / Angular Js / React Js etc.
2.	Application Logic-1	The application logic is the back-end of the system that performs the actual intrusion detection. It can be implemented in a variety of programming languages, such as Java, Python, and C++.	Java / Python
3.	Database	The database stores the data that is used to train and operate the machine learning model, as well as the results of the intrusion detection process.	MySQL, PostgreSQL, NoSQL, etc..
4	Cloud Database	To store and manage data in the cloud	Amazon RDS, Google Cloud SQL, Azure SQL Database
5.	File Storage	Amazon S3, Google Cloud Storage, Azure Blob Storage	To store large files such as machine learning models and training data
6.	Machine Learning Model	TensorFlow, PyTorch, scikit-learn	The machine learning model used to detect intrusions
7.	External API-1	Threat intelligence API, such as IBM Watson Threat Intelligence Platform, Cisco AMP Threat Grid, or Palo Alto Networks Cortex XDR	To provide the system with information about known threats
8.	External API-2	Identity and access management API, such as IBM Security Identity and Access Manager, Okta, or Microsoft Azure Active Directory	To provide the system with information about users and devices
9.	Infrastructure	On-premises servers, cloud computing platform such as Amazon Web Services (AWS), Google Cloud Platform (GCP), or Microsoft Azure	The platform on which the system is deployed

Table-2: Application Characteristics:

S.No	Characteristic	Description
1	Open-Source Frameworks	TensorFlow, PyTorch, scikit-learn
2	Security Implementations	IAM Controls, OWASP
3	Scalable Architecture	3-tier architecture
4	Availability	Load balancers, distributed servers
5	Performance	Cache, CDN

Product Backlog, Sprint Schedule, and Estimation (4 Marks

Sprint	Functional Requirement (Epic)	User Story Number	User Story/Task	Story Points	Priority
Sprint 1	Core IDS Functionality	USN-1	As a user, I want to be able to deploy and configure the AI-Enhanced IDS on my network.	5	High
Sprint 1	Core IDS Functionality	USN-2	As a user, I want to be able to monitor the AI-Enhanced IDS for suspicious activity.	5	High
Sprint 1	Core IDS Functionality	USN-3	As a user, I want to be able to receive alerts from the AI-Enhanced IDS when suspicious activity is detected.	5	High
Sprint 2	AI-Enhanced Functionality	USN-4	As a user, I want the AI-Enhanced IDS to be able to learn and adapt to new threats over time.	5	Hig
Sprint 2	AI-Enhanced Functionality	USN-5	As a user, I want the AI-Enhanced IDS to be able to detect and block attacks that traditional IDS systems	5	High

Project Tracker, Velocity & Burndown Chart: (4 Marks)

Sprint	Total Story Points	Sprint Start Date	Duration	Sprint End Date (Planned)	Story Points Completed (as on Planned End Date)
Sprint 1	20	24 Oct 2022	6 Days	29 Oct 2022	20
Sprint 2	20	31 Oct 2022	6 Days	07 Nov 2022	20
Sprint 3	20	14 Nov 2022	6 Days	19 Nov 2022	20
Sprint 4	20	21 Nov 2022	6 Days	26 Nov 2022	20
Sprint 5	20	28 Nov 2022	6 Days	03 Dec 2022	20
Sprint 6	20	05 Dec 2022	6 Days	10 Dec 2022	20

Velocity: 20

Stage 1

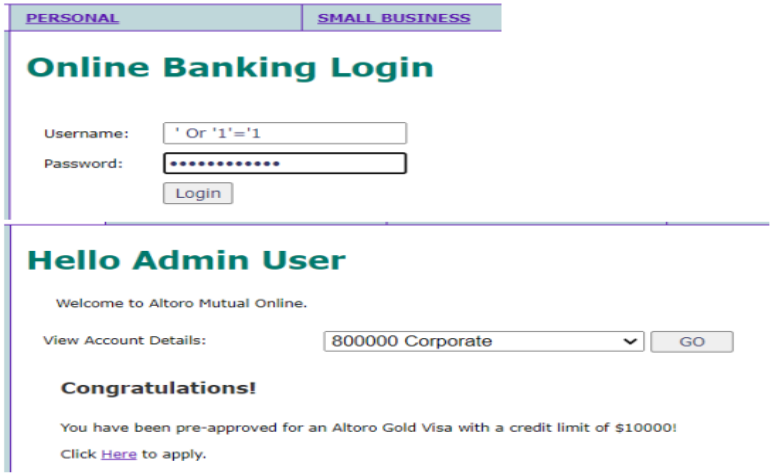
- this is stage 1 where we understand web application testing Altoro Mutual (testfire.net) we take help from OWASP top 10 understand them :

List of Vulnerability Table

SNO	Vulnerability Name	CWE - No
1	SQL injection	:CWE – 89
2	Cross site scripting (XSS)	CWE-79
3	Insecure Direct Object Reference	CWE-639
4	Information Disclosure or Sensitive Data Exposure	CWE-200
5	Broken Authentication	: CWE-287

Steps to Reproduce:

1) I was able to easily get through the login page of demo.testfire.net, accessible at http://testfire.net/login.jsp by using the payload ' Or '1'='1



Vulnerability Name: Cross site scripting (XSS)

CWE: CWE-79

OWASP Category: A4: Cross-Site Scripting (XSS)

Description: Cross-site scripting (XSS) is a type of web security vulnerability that allows an attacker to inject malicious code into web pages viewed by other users. This code can then be executed when the victim views the page, potentially giving the attacker access to the victim's account, cookies, or other sensitive information.

Business Impact: Attackers can masquerade as authorized users via session cookies, allowing them to perform any action allowed by the user account. XSS can also impact a business's reputation. An attacker can deface a corporate website by altering its content, thereby damaging the company's image or spreading misinformation.

Vulnerability Path: http://testfire.net/

Vulnerability Parameter: http://testfire.net/index.jsp

Vulnerability Name: SQL injection

CWE: CWE – 89

OWASP Category: A03:2021 – Injection

Description: SQL injection is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. This can be done by injecting malicious SQL code into the application's input fields. If the application does not properly validate the input, the attacker's code will be executed by the database, potentially giving the attacker access to sensitive data or allowing them to modify or delete data.

Business Impact: SQL injection attacks allow attackers to spoof identity, tamper with existing data, cause repudiation issues such as voiding transactions or changing balances, allow the complete disclosure of all data on the system, destroy the data or make it otherwise unavailable, and become administrators of the database server.

Vulnerability Path: http://testfire.net/login.jsp

Vulnerability Parameter: http://testfire.net/bank/main.jsp

Steps to Reproduse:

1) here you can retrive the cookie information using payload <script>alert(document.cookie)</script>

2) Enter "<script>alert(1)</script>" in the search box returns with the output programmed by us. This shows the search box is vulnerable to Reflected XSS.

Vulnerability Name: Insecure Direct Object Reference

CWE: CWE-639

OWASP Category: A1: Broken Access Control

Description: Insecure Direct Object Reference (IDOR) is a type of access control vulnerability that occurs when an application allows users to access objects directly without performing proper authorization checks. This can allow attackers to bypass authorization and access resources that they should not have access to, such as other users' data, sensitive files, or system functionality.

Business Impact: Insecure Direct Object Reference (IDOR) vulnerabilities can have a significant business impact on organizations of all sizes. By exploiting an IDOR vulnerability, an attacker could gain access to sensitive data, such as financial information, personal information, or trade secrets. They could also modify or delete data, or even take control of the application itself.

This could have a number of negative consequences for businesses, including:

- Financial losses
- Damage to reputation
- Legal and regulatory fines
- Lost productivity
- Increased IT costs

Vulnerability Path: http://testfire.net/

Vulnerability Parameter: http://testfire.net/bank/transaction.jsp

Steps to Reproduse:

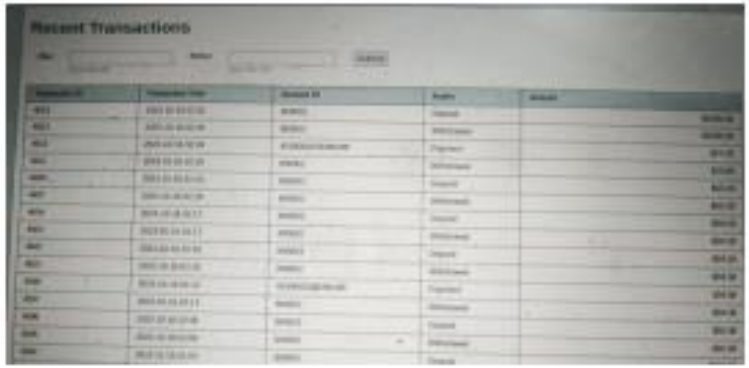
1) Enter the credentials to the sign in page.

- inside the sign in page transfer money from savings account.
- To checking account.
- open Burp suite and change browser proxy setting

- change receiver account. Number in intercept

- transfer money

- check Recent transaction



Vulnerability Name: Information Disclosure or Sensitive Data Exposure

CWE: CWE-200

OWASP Category: A3:2017-Sensitive Data Exposure

Description: Sensitive Data Exposure occurs when an organization unknowingly exposes sensitive data or when a security incident leads to the accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of, or access to sensitive data.

Business Impact: Risks of sensitive data exposure include identity theft, financial fraud, reputation damage, regulatory penalties, and loss of trust among customers or clients.

Vulnerability Path: http://testfire.net/

Vulnerability Parameter: http://testfire.net/index.jsp?content=inside_jobs.htm

Steps to Reproduse:

1) The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.

   - Screenshot of the rendered page containing this vulnerability.

Vulnerability Name: Broken Authentication

CWE: CWE-287

OWASP Category: A2:2017- Broken Authentication

Description: When attackers are able to compromise passwords, keys or session tokens, user account information, and other details to assume user identities. Due to poor design and implementation of identity and access controls, the prevalence of broken authentication is widespread.

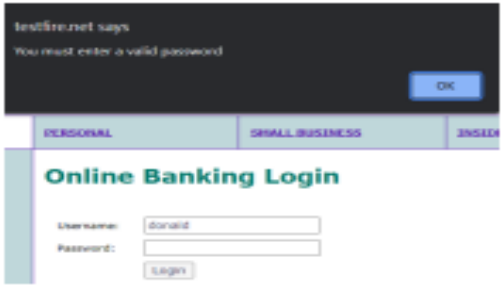
Business Impact: Attackers can also manipulate or delete user data, impersonate legitimate users, perform fraudulent transactions, or even escalate their privileges within the application.

Vulnerability Path: http://testfire.net/

Vulnerability Parameter: http://testfire.net/index.jsp?content=inside_jobs.htm

Steps to Reproduse:

1) give Username without password. We can see that it uses client-side JS validation



Enter your name into the username and a single tick into the password

What you understood about nessus

Nessus is a vulnerability scanner that identifies and reports on security weaknesses in computer systems. It is one of the most widely used vulnerability scanners in the world, and is trusted by tens of thousands of organizations around the globe.

Nessus works by scanning a network or system for known vulnerabilities. It does this by comparing the configuration of the system to a database of known vulnerabilities. If Nessus finds a match, it will report the vulnerability to the user.

Nessus can be used to scan a wide variety of systems, including Windows, Linux, Unix, and MacOS. It can also be used to scan network devices, such as routers and switches.

Nessus is a powerful tool that can help organizations identify and remediate security vulnerabilities.

However, it is important to note that Nessus is not a silver bullet. It cannot find all vulnerabilities, and it is important to use Nessus in conjunction with other security tools.

Target website

- www.dream11.com

Target ip address:-

34.197.28.159

Vulnerabilities Total: 8

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	6.5	-	142960	HSTS Missing From HTTPS Server (RFC 6797)
INFO	N/A	-	84502	HSTS Missing From HTTPS Server
INFO	N/A	-	43111	HTTP Methods Allowed (per directory)
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	10386	Web Server No 404 Error Code Check

* indicates the v3.0 score was not available; the v2.0 score is shown

Vulnerabilities

142960 - HSTS Missing From HTTPS Server (RFC 6797)

Synopsis

The remote web server is not enforcing HSTS, as defined by RFC 6797.

Description

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

See Also

https://tools.ietf.org/html/rfc6797

Solution

Configure the remote web server to use HSTS.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS v2.0 Base Score

5.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N)

Plugin Information

Published: 2020/11/17, Modified: 2023/06/08

Plugin Output

tcp/443/www

```
The remote HTTPS server does not send the HTTP
"Strict-Transport-Security" header.
```

84502 - HSTS Missing From HTTPS Server

Synopsis

The remote web server is not enforcing HSTS.

Description

The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

See Also

https://tools.ietf.org/html/rfc6797

Solution

Configure the remote web server to use HSTS.

Risk Factor

None

Plugin Information

Published: 2015/07/02, Modified: 2021/05/19

Plugin Output

tcp/443/www

```
The remote HTTPS server does not send the HTTP
"Strict-Transport-Security" header.
```

43111 - HTTP Methods Allowed (per directory)

Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

The following HTTP methods are considered insecure:

PUT, DELETE, CONNECT, TRACE, HEAD

Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could acce GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowe unauthorized blind submission of any privileged GET request.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'

in the scan policy - various known HTTP methods on each directory and considers them as unsupported i it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

See Also

http://www.nessus.org/u?d9c03a9a

http://www.nessus.org/u?b019cbdb

https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006)

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/12/10, Modified: 2022/04/11

Plugin Output

tcp/80/www

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/80/www

```
The remote web server type is :

awselb/2.0
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2019/11/22

Plugin Output

tcp/80/www

```
Response Code : HTTP/1.1 301 Moved Permanently

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Server: awselb/2.0
  Date: Thu, 19 Oct 2023 11:06:51 GMT
  Content-Type: text/html
  Content-Length: 134
  Connection: keep-alive
  Location: https://www.ec2-34-197-28-159.compute-1.amazonaws.com:443/

Response Body :

<html>
<head><title>301 Moved Permanently</title></head>
<body>
<center><h1>301 Moved Permanently</h1></center>
</body>
</html>
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2023/09/25

Plugin Output

tcp/80/www

```
Port 80/tcp was found to be open
```

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2023/07/31

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.6.1
Nessus build : 20021
Plugin feed version : 202310190641
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : debian10-x86-64
Scan type : Normal
Scan name : my scan
```

10386 - Web Server No 404 Error Code Check

Synopsis

The remote web server does not return 404 error codes.

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.

Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/04/28, Modified: 2022/06/17

Plugin Output

tcp/80/www

```
CGI scanning will be disabled for this host because the host responds
to requests for non-existent URLs with HTTP code 301
rather than 404. The requested URL was :

    http://ec2-34-197-28-159.compute-1.amazonaws.com/0ObQFHJpHhAX.html
```

Stage 3

Soc/Siem and Siem Response to Security Incidents

Introduction

Security Operations Centers (SOCs) and Security Information and Event Management (SIEM) systems are essential tools for organizations seeking to protect their networks and data from cyber attacks. By collecting, analyzing, and correlating data from a variety of sources, SOCs and SIEMs can help organizations identify, investigate, and respond to security incidents.

Soc

The ability of SoC/Siem to collect, analyze and correlate data from various sources is essential for effective security incident response. SoC/Siem can help to identify and prioritize security incidents, as well as provide context for investigations. By understanding the ability of SoC/Siem to detect and respond to security incidents, organizations can better protect their assets from cyber threats.

SOC - cycle

The SOC - cycle is a continuous process that helps to ensure that organizations are prepared to respond to security incidents. The cycle consists of four phases: detection, investigation, containment, and recovery. By following the SOC - cycle, organizations can effectively identify, investigate, and respond to security incidents.

Siem

Siem is a type of security information and event management (SIEM) system that collects, analyzes, and correlates data from various sources. Siem can help to identify and prioritize security incidents, as well as provide context for investigations. By understanding the ability of Siem to detect and respond to security incidents, organizations can better protect their assets from cyber threats.

Siem Cycle

The Siem Cycle is a continuous process that helps to ensure that organizations are prepared to respond to security incidents. The cycle consists of four phases: detection, investigation, containment, and recovery. By following the Siem Cycle, organizations can effectively identify, investigate, and respond to security incidents.

MISP

MISP is a threat intelligence platform that helps to collect, analyze, and share threat intelligence data. MISP can help to identify and prioritize security incidents, as well as provide context for investigations. By understanding the ability of MISP to detect and respond to security incidents, organizations can better protect their assets from cyber threats.

How you think you deploy soc in your college?

1. Assess the need for a SOC. The first step is to assess the need for a SOC. This can be done by considering the following factors:

- The size of the college
- The budget
- The level of security expertise
- The types of security threats that the college faces
- The college's compliance requirements

2. Define the scope of the SOC. Once the need for a SOC has been assessed, the next step is to define the scope of the SOC. This will involve defining the goals of the SOC, the types of security incidents that it will be responsible for, and the level of security coverage that is needed.

3. Determine the staffing needs of the SOC. The next step is to determine the staffing needs of the SOC. This will involve determining the number of security analysts that will be needed, the skills and experience that they should have, and the budget that is available for staffing.

4. Select the right technology. There are a variety of SOC technologies available, such as SIEM systems, security analytics tools, and threat intelligence platforms. The right technology for a college will depend on its specific needs and budget.

5. Integrate the SOC with other security systems. The SOC should be integrated with other security systems, such as firewalls, intrusion detection systems, and endpoint security solutions. This will ensure that the SOC has a comprehensive view of the college's network and security posture.

6. Develop a training program for SOC staff. SOC staff should be trained on how to use the SOC technology and how to respond to security incidents. This will ensure that they are able to effectively operate the SOC and protect the college's network.

7. Establish a reporting process. The SOC should have a process for reporting security incidents to management and other stakeholders. This will ensure that everyone is aware of the security risks that the college faces and that the SOC is taking appropriate action to address them.

8. Continuously monitor and improve the SOC. The SOC should be continuously monitored and improved to ensure that it is effective in protecting the college's network. This will involve reviewing security incidents, identifying areas for improvement, and making changes to the SOC as needed.

Deploying a SOC can be a complex and time-consuming process, but it is an important step in protecting a college's network and data. By following the steps outlined above, colleges can ensure that they are deploying a SOC that is right for their needs and that will effectively protect their network from cyber attacks.

Threat intelligence

Threat intelligence is the knowledge and information about cyber threats, their actors, their tools and techniques, and their motivations. Threat intelligence is used to proactively identify and mitigate cyber threats. It is an essential component of an effective cybersecurity strategy.

There are three main types of threat intelligence:

•**Technical threat intelligenc**e: This type of threat intelligence focuses on the technical aspects of cyber threats, such as the vulnerabilities that are exploited, the malware that is used, and the tactics and techniques that are employed.

•**Operational threat intelligence**: This type of threat intelligence focuses on the operational aspects of cyber threats, such as the threat actors who are behind them, their targets, and their motives.

•**Strategic threat intelligence**: This type of threat intelligence focuses on the strategic aspects of cyber threats, such as the trends that are emerging, the potential impact of cyber threats, and the best way to mitigate them.

Incident response

incident response is the process of identifying, containing, eradicating, and recovering from a security incident. It is a critical component of cybersecurity, and it is essential for any organization that wants to protect its data and assets.

The incident response process typically consists of the following steps:

1.Identification: The first step is to identify that a security incident has occurred. This can be done by monitoring logs, observing network traffic, or receiving alerts from security systems.

2.Containment: Once an incident has been identified, the next step is to contain it. This involves taking steps to prevent the incident from spreading or causing further damage. For example, this might involve isolating infected systems, disabling users' accounts, or blocking malicious traffic.

3.Eradication: Once an incident has been contained, the next step is to eradicate it. This involves removing the malware or other threat that caused the incident. This might involve patching vulnerabilities, deleting infected files, or restoring from backups.

4.Recovery: The final step in the incident response process is recovery. This involves restoring systems and data to their normal state. This might involve reinstalling software, restoring data from backups, or restoring configurations.

Qradar & understanding about tool

QRadar is a Security Information and Event Management (SIEM) system developed by IBM. It is a software platform that collects, analyzes, and correlates security data from a variety of sources, such as logs, network traffic, and endpoint security solutions. QRadar is used to identify, prioritize, and respond to security incidents.

QRadar has a number of features that make it a powerful tool for security analysts, including:

- **Data collection**: QRadar can collect data from a variety of sources, including logs, network traffic, and endpoint security solutions. This data is then stored in a central repository, where it can be analyzed and correlated.
- **Data analysis:** QRadar can analyze data to identify patterns and anomalies. This can help security analysts to identify potential security incidents.

•**Data correlation**: QRadar can correlate data from multiple sources to provide a holistic view of a security incident. This can help security analysts to understand the root cause of an incident and determine the extent of the damage.

•**Threat intelligence:** QRadar can integrate with threat intelligence feeds to provide security analysts with up-to-date information about known threats. This information can help security analysts to prioritize their work and focus on the most critical threats.

•**Incident response:** QRadar can help security analysts to respond to security incidents by providing a number of tools, such as incident workflows and playbooks. These tools can help security analysts to automate tasks and quickly contain and eradicate threats.

QRadar is a valuable tool for security analysts, and it can help to improve an organization's security posture. By using QRadar, organizations can identify, prioritize, and respond to security incidents more effectively.

what you understand from SOC / SEIM / Qradar Dashboard .

A SOC (Security Operations Center) is a centralized facility that collects, analyzes, and responds to security data from a variety of sources. A SIEM (Security Information and Event Management) system is a software platform that helps to manage and analyze security data. A QRadar dashboard is a graphical user interface (GUI) that provides a centralized view of security data from a QRadar SIEM system.

future scope of SOC / SEIM

The future of Security Operations Centers (SOCs) and Security Information and Event Management (SIEM) systems is bright. As cyber threats continue to evolve and become more sophisticated, SOCs and SIEMs will play an increasingly critical role in protecting organizations from cyber attacks.

Conclusion

In conclusion, leveraging artificial intelligence for an enhanced Intrusion Detection System (IDS) has the potential to revolutionize cybersecurity. By utilizing machine learning algorithms for anomaly detection, integrating AI with other security technologies, and developing AI-powered IDS that can adapt and self-learn, organizations can significantly improve their threat detection capabilities. It is recommended that organizations stay updated on the latest AI trends in IDS and invest in the necessary resources to implement and optimize AI-based IDS solutions.

Future scope

As the field of AI continues to evolve, there are several future trends to watch out for in AI-based IDS. These include the use of machine learning algorithms for anomaly detection, the integration of AI with other security technologies such as threat intelligence feeds, and the development of AI-powered IDS that can adapt and self-learn to detect new and emerging threats. By staying informed about these trends, organizations can proactively enhance their intrusion detection capabilities and stay ahead of cyber threats.