Ai-Driven Incident Response Platform

Assists Cybersecurity Teams in Automating Incident Triage and Response Tasks.

Team Members
Orra Raghavendra Reddy
Shaik Muhammed Faizaan Ali
Greeshma Reddy Basireddy
Farzeen Niaz

INTRODUCTION:

In an era where the digital landscape is constantly evolving, organizations face an ever-increasing threat from cyberattacks. The need for swift and effective incident response has become paramount to safeguard sensitive data, protect digital assets, and maintain the trust of stakeholders. In response to this growing challenge, we present a visionary project: the development of an AI-driven incident response platform that empowers cybersecurity teams with the tools to automate and enhance incident triage and response tasks.

Incident response has traditionally been a resource-intensive and time-critical process. The sheer volume and complexity of security incidents, ranging from malware outbreaks and data breaches to network intrusions, demand a more efficient approach. Enter the realm of Artificial Intelligence (AI) and machine learning, which promises to revolutionize the way cybersecurity teams detect, analyse, and respond to incidents. Our project aims to harness the power of AI to create a platform that not only accelerates incident triage but also augments decision-making capabilities, ultimately fortifying an organization's cyber defences.

This cutting-edge platform will serve as a force multiplier for cybersecurity teams, allowing them to focus their expertise on the most critical aspects of incident response while automating routine, time-consuming tasks. By leveraging AI-driven algorithms, machine learning models, and real-time data analysis, our system will provide early threat detection, context-rich incident categorization, and automated response recommendations. This will lead to reduced incident resolution times, minimized damage, and an overall improvement in an organization's security posture.

The project will draw upon a wide range of technologies, including natural language processing, anomaly detection, behavioural analytics, and threat intelligence integration. It will be designed with scalability, flexibility, and user-friendliness in mind, ensuring that it can adapt to the unique requirements of various organizations, regardless of size or industry.

The AI-driven incident response platform promises to be a game-changer in the world of cybersecurity. It represents a proactive stance in defending against the ever-evolving threat landscape, providing organizations with a reliable, intelligent, and efficient tool to mitigate risks and protect their digital assets. This project will not only shape the future of incident response but also play a pivotal role in strengthening the cybersecurity posture of businesses and institutions in an increasingly interconnected and vulnerable world.

"Having set the stage for our visionary initiative, it's time to explore the project's abstract, encapsulating the essence of our endeavour to create an intelligent incident response platform that will redefine how organizations combat cyber threats."

ABSTRACT:

Cybersecurity incidents pose an ever-increasing threat to organizations worldwide, necessitating swift and effective incident response. To address this critical challenge, this project focuses on the design and development of an AI-driven incident response platform that empowers cybersecurity teams to automate incident triage and response tasks.

In an era of growing data breaches and cyber threats, manual incident handling is no longer scalable. Leveraging the power of artificial intelligence and machine learning, our platform aims to revolutionize the incident response process. The platform integrates cutting-edge technologies to enable automatic incident detection, classification, and prioritization, thereby reducing response time and enhancing overall security posture.

In summary, this project endeavours to create an AI-driven incident response platform that not only reduces the workload on cybersecurity teams but also enhances the efficacy of incident response processes. By automating repetitive tasks, categorizing and prioritizing incidents, and providing valuable insights, the platform empowers organizations to defend against cyber threats more effectively in an increasingly complex threat landscape.

Amidst the escalating data breaches and evolving cyber threats, traditional incident response methods have become inadequate. It is essential to leverage the formidable capabilities of artificial intelligence and machine learning to not merely enhance but revolutionize the incident response process. Our platform stands at the forefront, integrating state-of-the-art technologies to facilitate automatic incident detection, classification, and prioritization, thus achieving a profound reduction in response time and a substantial enhancement in overall security posture. Key among the platform's capabilities is its prowess in transforming manual incident response into a dynamic, automated process. By harnessing the power of artificial intelligence and machine learning, the platform interprets and responds to incidents in real time. It empowers security teams to focus on strategic decisions, investigations, and critical tasks, while mundane and repetitive triage and response operations are efficiently managed by the system.

In an age where data breaches loom as a constant menace and cyber threats perpetually evolve, manual intervention is no longer a scalable solution. Our platform not only augments the capabilities of cybersecurity teams but also augments their speed and precision. This forward-looking technology integrates cutting-edge tools and processes to identify, classify, and prioritize incidents, thereby significantly reducing response time and elevating an organization's security posture to unprecedented levels.

In conclusion, the project's primary objective is to pioneer a new era of incident response, where AI-driven automation becomes the cornerstone of cybersecurity defence. By revolutionizing how organizations address incidents, we equip them with a formidable tool that adapts, learns, and outpaces the ever-evolving threat landscape.

VISION OF THE PROJECT:

1. Enhancing Cyber Resilience: The foremost vision is to significantly enhance an organization's resilience to cyber threats. By automating incident response, the project aims to reduce the impact of security incidents and, in some cases, prevent them altogether. This proactive approach to cybersecurity will lead to a future where organizations are better prepared, minimizing the disruption caused by cyberattacks.

2. Swift and Precise Incident Handling: The project envisions a world where cybersecurity incidents are handled with unrivalled speed and precision. Human analysts will be empowered with AI-driven tools that rapidly detect, classify, and prioritize incidents. This speed is critical in an era where minutes and seconds can make the difference between containment and a catastrophic data breach.

3. Augmented Human Expertise: The project's vision is not to replace human expertise but to augment it. The AI-driven platform will empower cybersecurity teams to focus on strategic decision-making, threat analysis, and complex investigations, allowing them to harness their skills where they matter most, while the routine and repetitive tasks are efficiently managed by the AI system.

4. Continuous Learning and Adaptation: The project envisions a system that continually learns from each incident and response, becoming smarter and more effective over time. It adapts to new attack vectors and evolving threat landscapes, ensuring that it remains at the forefront of cybersecurity defense.

5. Global Collaboration and Knowledge Sharing: The project seeks to promote a collaborative approach to cybersecurity incident response. It envisions a future where organizations share knowledge, best practices, and threat intelligence through the platform, creating a collective defence against cyber threats.

6. Simplified Compliance and Reporting: The project aims to streamline the process of compliance and reporting by automating data collection and incident documentation. This vision ensures that organizations can meet regulatory requirements effortlessly and focus on proactive security measures.

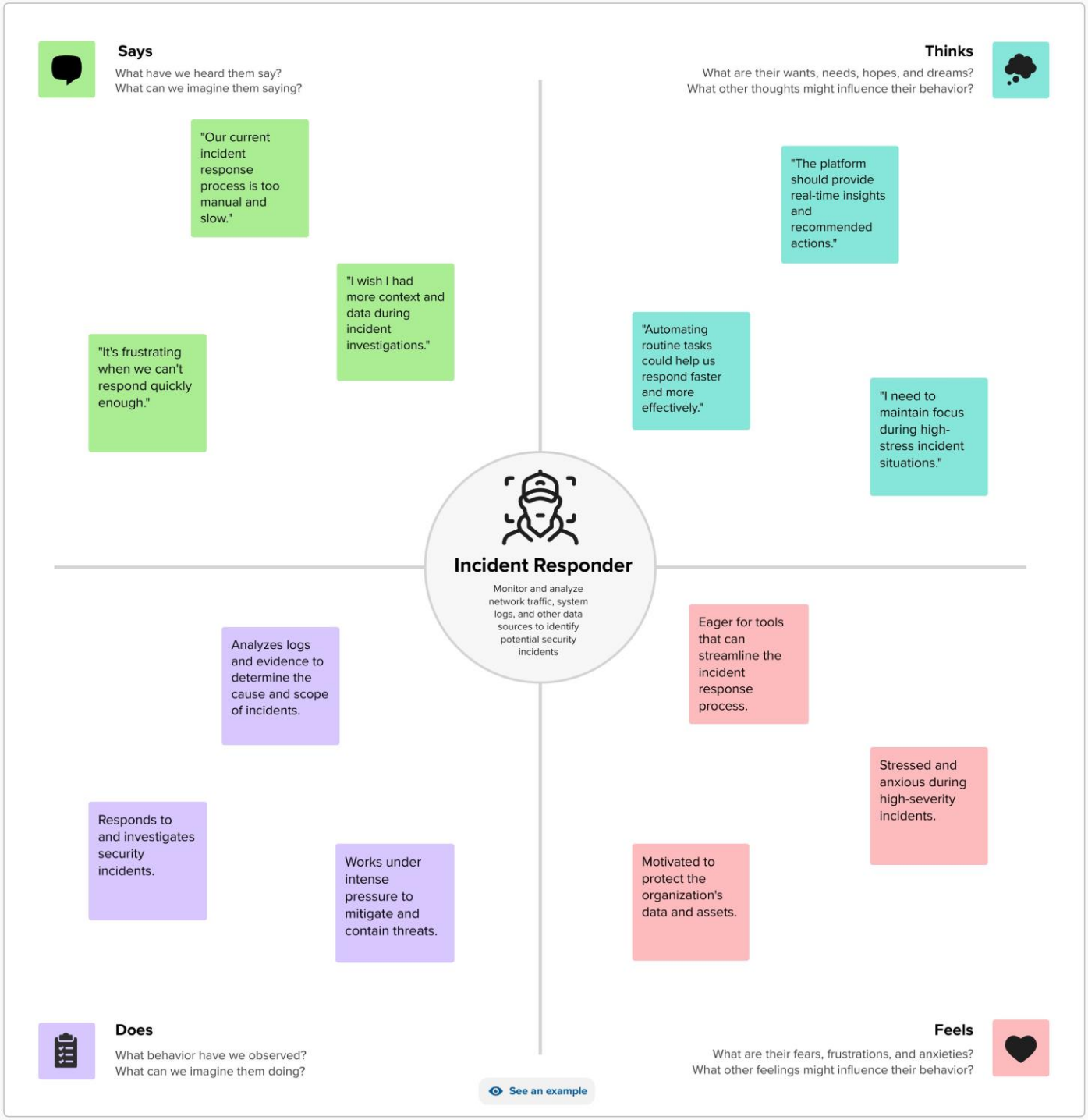
7. Cost Efficiency and Scalability: The vision includes making AI-driven incident response accessible to organizations of all sizes. The platform will be designed to scale as per the organization's needs and offer cost-effective solutions that democratize advanced incident response capabilities.

8. Global Security Posture Improvement: Ultimately, the project envisions a world where organizations across industries and geographies significantly improve their security postures. This collective improvement will lead to a safer digital environment for individuals, businesses, and society.

In summary, the project's vision is to create a future where AI augments human expertise, where incident response is swift and precise, and where organizations, regardless of size, can effectively defend against the ever-growing cyber threat landscape. This vision embodies a commitment to proactive cybersecurity, resilience, and the continued evolution of defence against emerging threats.

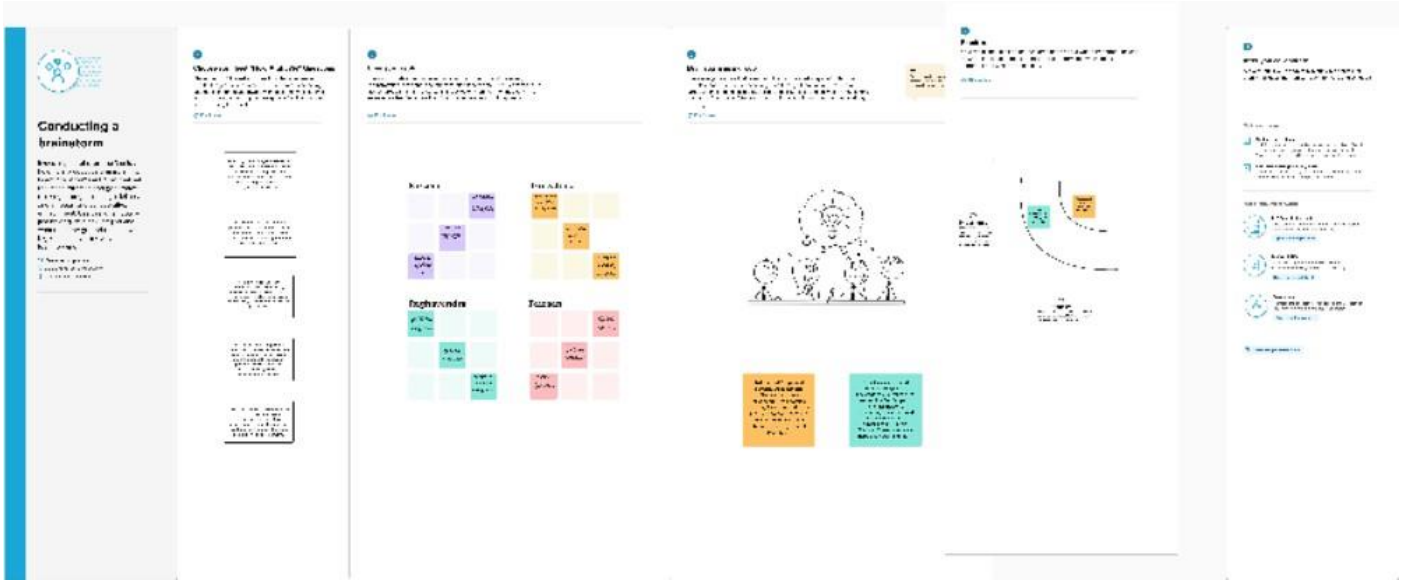
"Now that we've provided an abstract overview of our project's objectives, it's time to roll up our sleeves and dive into the Empathy Map. This tool will help us better understand the needs, perspectives, and pain points of cybersecurity teams, enabling us to design an AI-driven incident response platform that truly resonates with its users."

EMPATHY MAP:



"As we conclude the Empathy map, we'll now transition to the Brainstorming Phase. In this section, we will explore innovative concepts, technical considerations, and design strategies that will shape our AI-driven incident response platform."

BRAINSTORMING:



How might we?

How might we integrate advanced anomaly detection techniques to proactively identify potential security threats and vulnerabilities before they escalate into significant incidents?

How might we enhance the platform's user interface to ensure intuitive navigation and facilitate efficient incident management for cybersecurity teams?

How might we streamline the incident response workflow by automating routine tasks, allowing cybersecurity analysts to focus on critical analysis and decision-making processes?

How might we leverage data visualization and real-time analytics to provide comprehensive insights into the organization's security posture, enabling proactive decision-making and risk management strategies?

How might we encourage a culture of continuous learning and knowledge sharing within cybersecurity teams through the platform, fostering collaboration and expertise development?

Brainstorming Solo:

<u>Farzeen:</u>

Natural Language Processing (NLP) for Incident Reports
Allow team members to input incident details in natural language, which the AI can process and act upon.

Intelligent Workflow Automation
Create dynamic response playbooks that adapt to the specific incident context, allowing AI to recommend and even execute response actions in real-time.

Incident Playbooks:
Create a library of predefined incident response playbooks that can be customized and automated.
Allow teams to create and share their playbooks based on their organization's specific needs.

Greeshma:

Real-time Alert Analysis
Develop a feature that quickly analyzes and provides insights on incoming alerts, reducing the time taken for manual analysis.

Automated Triage
Implement an intelligent system that automatically prioritizes and categorizes incidents based on severity and potential impact.

Integration with Existing Tools
Ensure compatibility with other security tools commonly used in organizations, allowing for a seamless workflow and maximizing the platform's effectiveness.

Raghavendra:

Real-time Forensics and Data Analysis
Use AI for real-time data analysis to identify potential threats, malicious patterns, and vulnerabilities. Provide visualizations and reports for a quick understanding of the incident.

Enhanced Threat Detection
Utilize deep learning techniques to detect and predict emerging threats by analyzing network traffic, behavior anomalies, and new attack patterns.

Risk Assessment and Impact Analysis
Use AI to assess the potential impact of an incident on the organization, including financial and reputational risks.

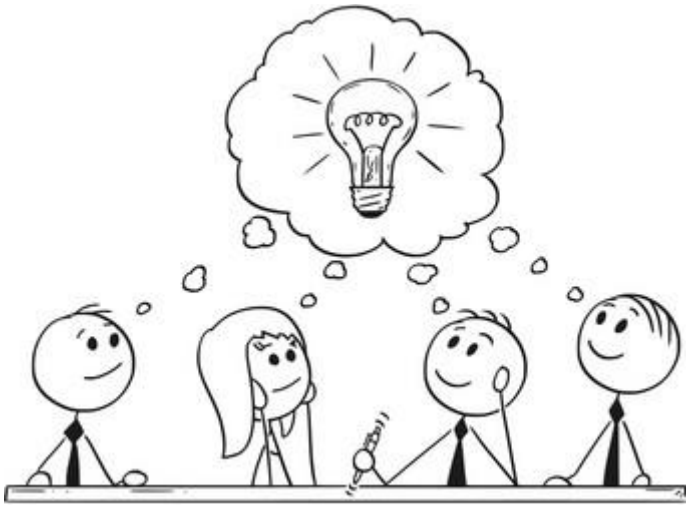
Faizaan:

Intelligent Workflow Automation
Create dynamic response playbooks that adapt to the specific incident context, allowing AI to recommend and even execute response actions in real time.

Knowledge Sharing Hub
Integrate a platform that allows cybersecurity teams to share insights, findings, and best practices, fostering collaboration and knowledge exchange.

Machine Learning for Incident Investigation
Employ machine learning algorithms to automatically cross-reference data from logs, network traffic, and endpoint information, accelerating the incident investigation process.

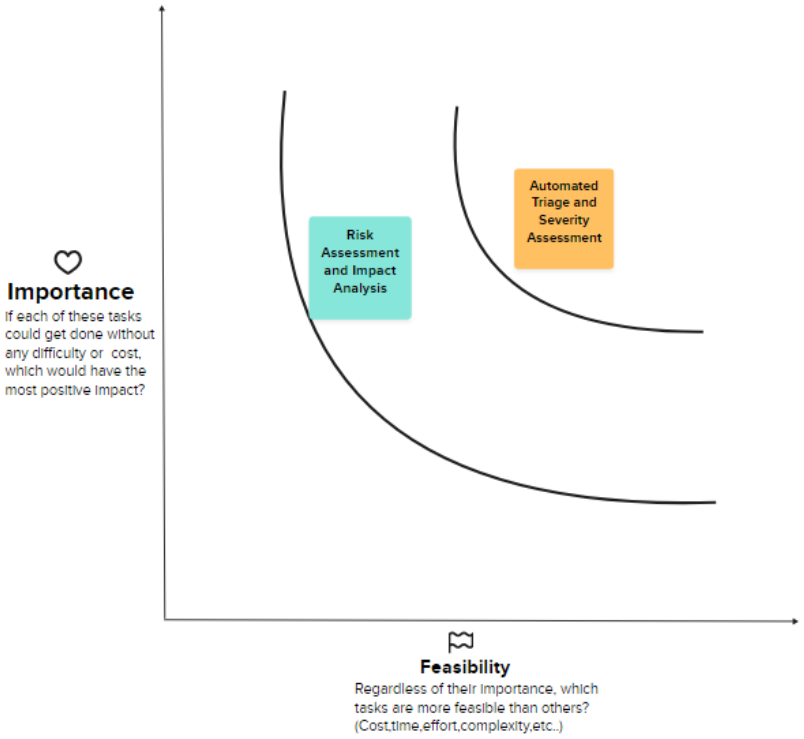
Brainstorming as a Group:



Automated Triage and Severity Assessment:
The platform uses advanced AI to prioritize security incidents, reducing manual effort and allowing swift attention to critical threats, ensuring prompt resolution.

Risk Assessment and Impact Analysis:
Leverage the Power of AI to Assess the Full Scope of Potential Incidents, Uncovering Their Profound Implications on the Organization - From Financial Consequences to Reputation-Defining Risks.

Prioritize:



"Now that we've gained valuable insights into the needs and experiences of cybersecurity teams through the Brainstorming, it's time to move forward and explore how our AI-driven incident response platform can leverage this understanding, with a closer look at the integration of a Nessus scan report for proactive threat assessment and response enhancement."

PROJECT PLANNING:

Sprint	Functional Requirement (Epic)	User Story Number	User Story / Task	Story Point	Priority	Team Member
Sprint 1	Incident Triage and Response	US001	As a cybersecurity analyst, I want to log in securely to access the system.	5	High	Raghavendra
Sprint 1	Incident Triage and Response	US002	As a cybersecurity analyst, I want to receive incidents from various sources.	8	High	Faizaan
Sprint 2	AI Analysis	US003	As a cybersecurity analyst, I want to leverage AI analysis to understand incident details.	13	High	Greeshma
Sprint 2	Incident Classification and Prioritization	US004	As a cybersecurity analyst, I want to classify and prioritize incidents based on AI analysis.	8	High	Farzeen
Sprint 3	Incident Response Automation	US005	As a cybersecurity analyst, I want to trigger automated responses for priority incidents.	10	High	Raghavendra
Sprint 3	Notification Service	US006	As a cybersecurity analyst, I want to receive notifications about incident status.	5	High	Faizaan
Sprint 4	Logging and Auditing	US007	As a cybersecurity analyst, I want system activities to be logged for auditing.	8	High	Greeshma
Sprint 4	System Management	US008	As an administrator, I want to manage system configurations and AI models.	13	High	Farzeen
Sprint 5	External System Integration	US009	As an external system, I want to receive incident response actions from the platform.	5	High	Raghavendra

Sprint 5	Reporting	US010	As a reporting user, I want to generate and receive detailed incident reports.	3	Low	Faizaan

"With a comprehensive project plan in place, we're now ready to unveil the proposed solution. In this section, we will detail how our AI-driven incident response platform will address the identified vulnerabilities and challenges, offering a holistic approach to automating incident triage and response tasks for cybersecurity teams."

Proposed Solution:

S.No.	Parameter	Description
1.	Problem Statement (Problem to be solved)	Create an AI-powered incident response platform that enhances the efficiency of cybersecurity teams by automating incident identification, classification, and initial response actions. This system should be capable of analyzing and prioritizing security incidents, recommending mitigation strategies, and providing real-time alerts to enable rapid and effective incident resolution. The platform should integrate with existing security tools and be designed to adapt to evolving threats, ultimately reducing response times, and minimizing the impact of security breaches.
2.	Idea / Solution description	The proposed AI-driven incident response platform will utilize machine learning and natural language processing algorithms to analyze incoming security alerts and events. It will prioritize incidents based on severity and potential impact, allowing for faster response to critical threats. The system will also suggest and, in some cases, automatically execute predefined response actions, reducing the burden on cybersecurity professionals. Real-time monitoring and alerts will keep the team informed about the incident's progress. Furthermore, the platform will continuously learn from historical data, adapting to emerging threats and improving its accuracy over time. Integrating with existing security tools, it will streamline the incident management process, enhance response times, and bolster the overall cybersecurity posture.
3.	Novelty / Uniqueness	This project is original and unique because it incorporates state-of-the-art AI and machine learning technologies that are specially designed for cybersecurity incident response. The platform will interpret and classify security occurrences using cutting edge natural language processing methods, even in intricate and quickly changing threat environments. To stay ahead of new dangers, it will also use adaptive learning methods to continuously improve its event analysis and reaction suggestions. Its unique feature of simplifying the frequently difficult and time-sensitive process of incident triage and response is its ability to seamlessly interface with current security solutions and offer a comprehensive, automated solution for incident management.

4.	Social Impact / Customer Satisfaction	Social Impact / Customer Satisfaction: The development and implementation of this AI-driven incident response platform can have a significant positive social impact and enhance customer satisfaction in several ways: 1. Improved Security Posture: By automating incident triage and response, organizations can more effectively protect their digital assets, customer data, and critical systems. This, in turn, enhances the overall security posture, reducing the risk of data breaches and cyberattacks. 2. Faster Response Times: The platform's ability to swiftly identify and respond to security incidents means that potential threats are mitigated more rapidly, minimizing the damage caused by cyberattacks and reducing downtime. This increased responsiveness leads to improved customer satisfaction, as services and data remain accessible and secure. 3. Reduced Workload for Cybersecurity Teams: By automating routine and time-consuming tasks, the platform alleviates the burden on cybersecurity professionals, allowing them to focus on more strategic and complex security challenges. This can lead to higher job satisfaction among cybersecurity teams. 4. Proactive Threat Mitigation: The platform's adaptive learning and continuous improvement capabilities enable it to anticipate and proactively address emerging threats. This results in fewer security incidents, less customer data exposure, and a higher level of trust from customers who see their information being better protected. 5. Compliance and Regulatory Benefits: The platform's ability to provide detailed incident response documentation can aid organizations in meeting compliance requirements. This not only helps avoid potential fines but also builds trust with customers who value strong data protection measures. In summary, this project can significantly improve the social impact and customer satisfaction by enhancing security, response times, and the overall quality of incident management in the cybersecurity domain.
5.	Business Model (Revenue Model)	1. The business model for the AI-driven incident response platform can incorporate several revenue streams: 2. Subscription Licensing: Offer tiered subscription plans based on the size and needs of organizations. Customers can pay a recurring fee to access the platform, with features and support varying by subscription level. 3. Per-Incident Fees: Charge a fee for each incident the platform successfully manages. This model could be suitable for smaller organizations or those with sporadic security incident needs. 4. Custom Development and Integration: Provide customization services to tailor the platform to the

		unique requirements of specific organizations. Charge for initial development and ongoing support. 5. Consulting and Training: Offer cybersecurity consulting and training services to help organizations maximize the platform's effectiveness. Charge for these services on a project or hourly basis. 6. Add-On Modules: Develop and sell add-on modules or features that enhance the platform's functionality, such as advanced threat intelligence feeds, reporting tools, or compliance-specific modules. 7. Data Analytics and Reporting: Charge for advanced analytics and reporting capabilities, allowing organizations to gain deeper insights into their incident data. 8. Volume Discounts: Incentivize large enterprises with significant incident response needs to subscribe by offering volume-based discounts. 9. Partnerships and Reseller Agreements: Collaborate with cybersecurity service providers, resellers, or managed security service providers (MSSPs) to expand the platform's reach and revenue through partnerships. This diverse revenue model allows for flexibility and scalability, accommodating a wide range of customer needs and budgets while capitalizing on the platform's unique capabilities.
6.	Scalability of the Solution	The scalability of the AI-driven incident response platform is a crucial aspect of its design and implementation. Here are key elements that contribute to its scalability: 1. Modular Architecture: The platform should be built with a modular architecture, allowing for easy addition or removal of components. New features and capabilities can be integrated without disrupting the existing system. 2. Cloud-Based Infrastructure: Leveraging cloud services enables the platform to scale horizontally by allocating more resources when needed. This flexibility ensures it can handle increased workloads during peak incident periods. 3. Elastic Computing: Implementing auto-scaling mechanisms allows the system to dynamically allocate computing resources in response to demand. This ensures efficient resource utilization and optimal performance. 4. Data Management: Scalable data storage and processing capabilities are critical. Using distributed databases and

		data warehouses can manage the growing volume of incident data efficiently. 5. Load Balancing: Load balancing techniques ensure that incoming incidents are distributed evenly across multiple processing nodes, preventing bottlenecks and maintaining system responsiveness. 6. API Integration: Providing robust APIs for integrating with other security tools and external systems allows for seamless expansion and integration with a variety of technologies. 7. User Management and Access Control: Scalability should extend to user management, allowing for the addition of new users and roles as the organization grows. 8. Monitoring and Reporting: Implementing scalable monitoring and reporting tools ensures that the platform can handle increased data analysis and reporting demands as the user base expands. 9. Training and Learning: The platform's AI algorithms should be adaptable and continue to learn, accommodating new threat patterns and evolving alongside the cybersecurity landscape. 10. Global Reach: Scalability should encompass geographic reach, supporting a distributed user base, and adhering to regional data privacy regulations. 11. Incorporating these scalability measures ensures that the incident response platform can grow and adapt to the evolving needs of cybersecurity teams and organizations of all sizes.

"Building upon the proposed solution for our AI-driven incident response platform, it's now crucial to delve into the solution architecture. This phase will outline how the proposed solution manifests into a comprehensive structure, detailing the system's design, components, and interactions to ensure a cohesive and effective incident response mechanism for cybersecurity teams."

Solution Architecture:

A comprehensive AI-driven incident response system is crucial for organizations to effectively detect, analyze, and mitigate security incidents. This solution architecture integrates advanced technologies and methodologies to ensure a proactive and efficient response to potential threats.

The project focuses on establishing a robust security infrastructure that leverages AI algorithms and machine learning to swiftly identify and categorize potential security incidents. Through the seamless integration of a Security Information and Event Management (SIEM) system, the solution captures and monitors security-related logs and events, providing a comprehensive view of the organization's security landscape.

- **Continuous Monitoring and Feedback Loop:** The system incorporates continuous monitoring and a feedback loop to evaluate the effectiveness of the incident response process. It collects data on the response actions taken and uses this information to refine and improve the overall incident response strategy and the performance of the AI algorithm.
- **SIEM (Security Information and Event Management):** The system initially captures and stores logs of all security-related events and incidents. It continuously monitors and analyzes these logs to detect any anomalies or potential threats.
- **Incident Tracking and Case Management:** The system tracks and manages all incidents through a centralized case management system, providing a comprehensive overview of the incident lifecycle, from detection to resolution. This aids in maintaining a systematic record of incidents for future reference and analysis.
- **AI Algorithm for Threat Detection:** If an incident is identified as new or unknown, it is passed through an AI algorithm specially designed for threat detection. This algorithm leverages machine learning and pattern recognition techniques to identify potential security threats or malicious activities.
- **Alert System and User Notification:** Upon confirming a threat, the system triggers an alert mechanism to notify the appropriate user or security personnel. The alert includes details about the nature of the threat, its severity, and any immediate actions required.
- **Classification and Reporting:** The incident is classified based on its severity and impact. A detailed report is generated, outlining the specifics of the incident, the affected systems, and the potential risks involved. This report is shared with the management and relevant stakeholders for further assessment and decision-making.
- **High-Risk Data Protection:** As soon as the alert is generated, the system activates protocols to protect high-risk and confidential information. This includes isolating sensitive data, restricting access to critical systems, and implementing additional security measures to prevent unauthorized access or data breaches.

Integrating these elements into the solution architecture will enable a streamlined and effective AI-driven incident response process, ensuring timely threat detection, notification, and protection of critical data assets.

Solution Architecture Diagram:

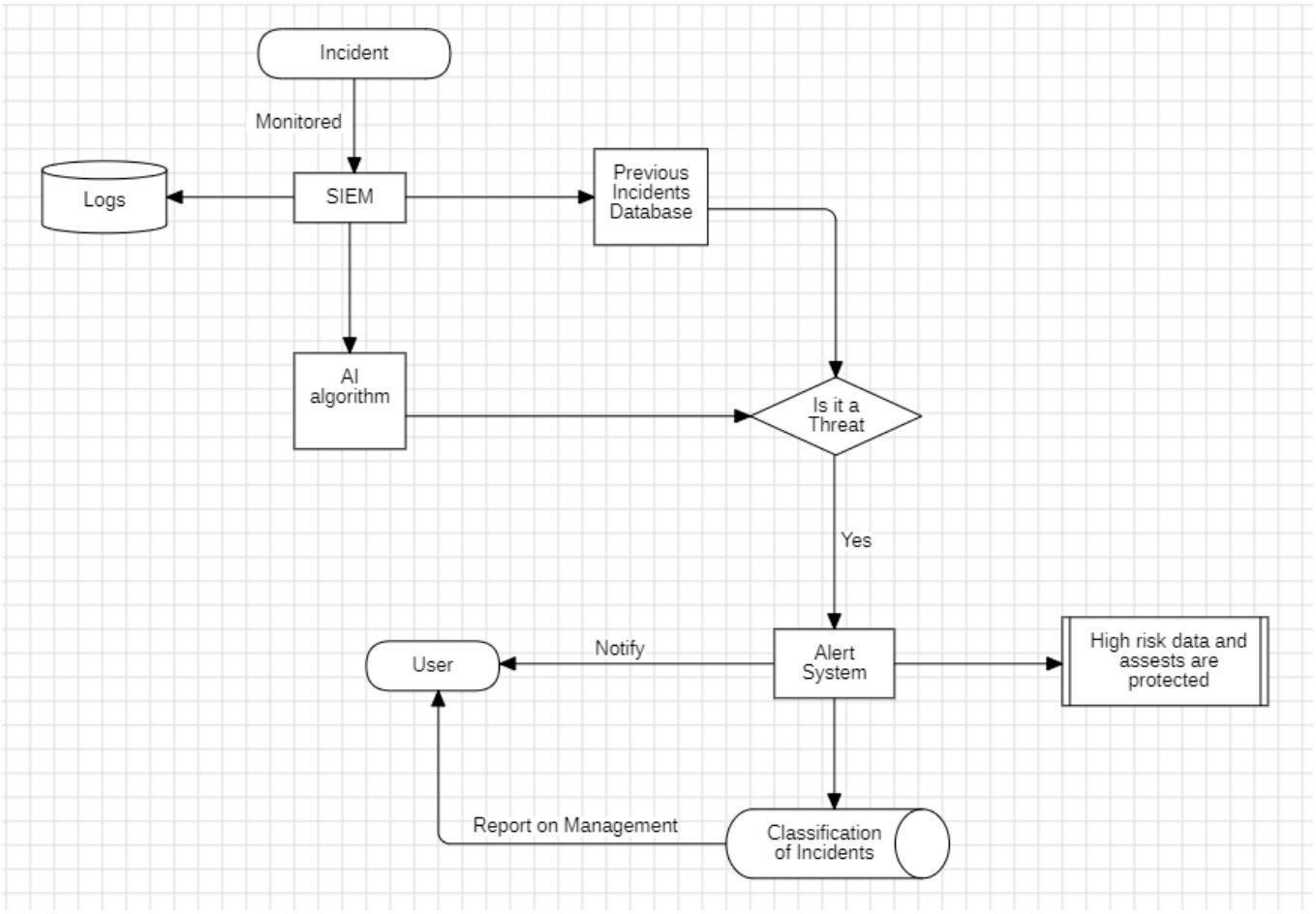


Figure 1: Architecture and data flow of the AI-Driven Incident Response Platform

Reference:

https://www.linkedin.com/pulse/leveraging-ai-enhanced-cyber-security-incident-novel-threat-drew/
https://medium.com/kmeanswhat/ai-automation-for-incident-management-c872ee10e833

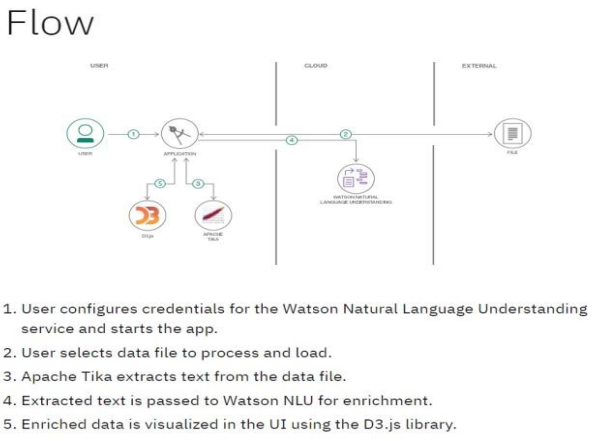
"Having established the foundation of our solution architecture, the next step is to visualize the practical implementation through data flow diagrams. These diagrams will provide a clear representation of how data and information traverse the system, offering insights into the operational aspects of our AI-driven incident response platform for cybersecurity teams.

Data Flow Diagrams:

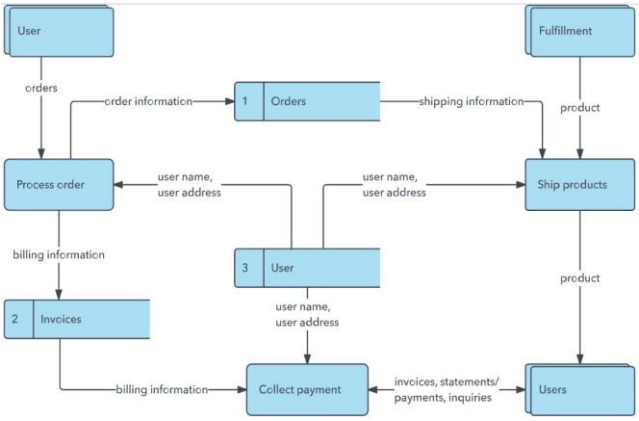
A Data Flow Diagram (DFD) is a traditional visual representation of the information flows within a system. A neat and clear DFD can depict the right amount of the system requirement graphically. It shows how data enters and leaves the system, what changes the information, and where data is stored.

Example: [(Simplified)]

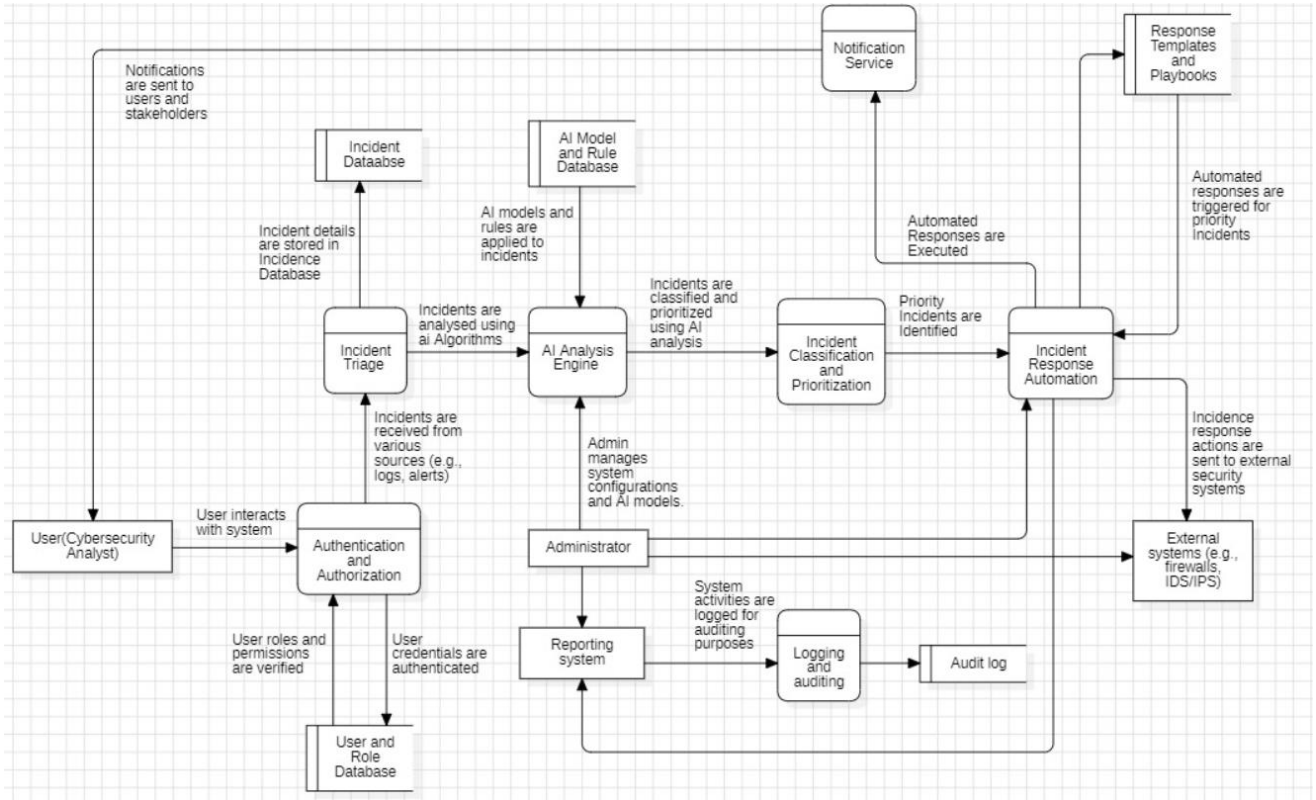
Example: DFD Level 0 (Industry Standard)



1. User configures credentials for the Watson Natural Language Understanding service and starts the app.
2. User selects data file to process and load.
3. Apache Tika extracts text from the data file.
4. Extracted text is passed to Watson NLU for enrichment.
5. Enriched data is visualized in the UI using the D3.js library.



DFD:



User Stories:

User Type	Functional Requirement (Epic)	User Story Number	User Story / Task	Acceptance criteria	Priority	Release
Cybersecurity Analyst	Incident Triage and Response	US001	As a cybersecurity analyst, I want to log in securely to access the system	User can enter valid credentials. Authentication is successful. User roles and permissions are verified.	HIGH	Sprint-1
Cybersecurity Analyst	Incident Triage and Response	US002	As a cybersecurity analyst, I want to receive incidents from various sources, including logs and alerts.	Incidents are received from external sources. Incidents are stored in the incident database.	HIGH	Sprint-1
Cybersecurity Analyst	AI Analysis	US003	As a cybersecurity analyst, I want to leverage AI analysis to understand incident details.	Incidents are analysed using AI algorithms. AI models and rules are applied to incidents.	HIGH	Sprint-2
Cybersecurity Analyst	Incident classification and prioritization.	US004	As a cybersecurity analyst, I want to classify and prioritize incidents based on AI analysis.	Incidents are classified and prioritized based on AI analysis.	HIGH	Sprint-2
Cybersecurity Analyst	Incident response Automation.	US005	As a cybersecurity analyst, I want to trigger automated responses for priority incidents.	Automated response actions are executed for priority incidents. Responses are based on predefined templates and playbooks.	HIGH	Sprint-3
Cybersecurity Analyst	Notification service	US006	As a cybersecurity analyst, I want to receive notifications about incident status and actions taken.	Notifications are sent to users and stakeholders.	HIGH	Sprint-3
Cybersecurity Analyst	Logging and Auditing	US007	As a cybersecurity analyst, I want system activities to be logged for auditing purposes.	System activities are logged in the Audit log.	HIGH	Sprint-4
Administrator	System management	US008	As and administrator, I want to manage system configurations and AI models.	The admin interface allows configuration management.	HIGH	Sprint-4
External system	External System integration	US009	As and external system, I want to receive incident response actions from the platform.	The platform can send incident response actions to external systems.	HIGH	Sprint-5

Reporting user	Reporting	US010	As a reporting user, I want to generate and receive detailed incident reports	Incident reports are generated and transmitted to the reporting system.	LOW	Sprint-5

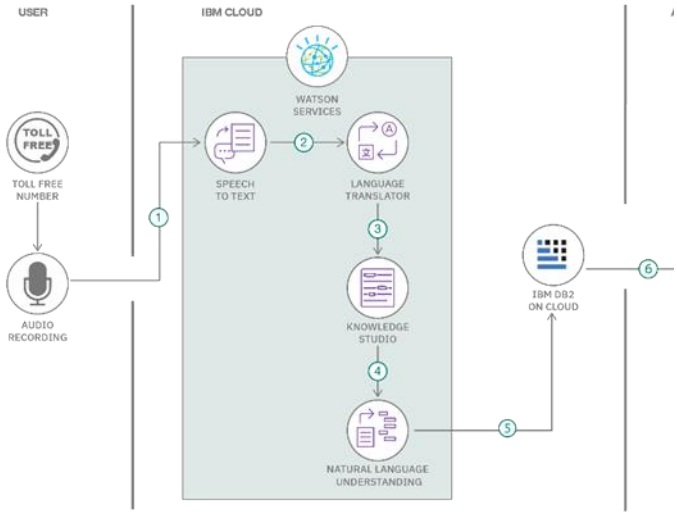
"With the data flow diagrams illustrating the system's operational intricacies, it's time to turn our attention to the technology track. In this section, we will map out the technical components and infrastructure required to facilitate the seamless flow of data within our AI-driven incident response platform for cybersecurity teams.

Technical Architecture:

The Deliverable shall include the architectural diagram as below and the information as per the table1 & table 2.

Example: Order processing during pandemics for offline mode

Reference: https://developer.ibm.com/patterns/ai-powered-backend-system-for-order-processing-during-pandemics/



Guidelines:

1. Include all the processes (As an application logic / Technology Block)
2. Provide infrastructural demarcation (Local / Cloud)
3. Indicate external interfaces (third-party API etc.)
4. Indicate Data Storage components/services
5. Indicate interface to machine learning models (if applicable)

Table-1: Components & Technologies:

S. No	Component	Description	Technology
1.	Incident Triage and Response System	Central component managing incident response	Programming Languages: Python, Java
2.	User Authentication and Authorization	Handles user authentication and authorization	Java / Python
3.	Incident Triage	Responsible for receiving and storing incidents	Programming Languages: Python, Java
4.	AI Analysis Engine	Analyses incidents using AI algorithms and rules	Machine Learning / AI: TensorFlow, Scikit-Learn
5.	Incident Classification and Prioritization	Classifies and prioritizes incidents	Programming Languages: Python, Java

6.	Incident Response Automation	Executes automated response actions	Programming Languages: Python, Java
7.	Notification Service	Sends notifications to users and stakeholders	Programming Languages: Python, Java
8.	Logging and Auditing	Records system activities for auditing	Data Storage: SQL Database (e.g., MySQL)
9.	Administrator	Component for system administrators	Programming Languages: Python, Java
10.	External Systems	Interfaces with external security systems	External API Integration: RESTful APIs
11.	Reporting System	Generates and transmits incident reports	Programming Languages: Python, Java

Table-2: Application Characteristics:

S. No	Characteristics	Description	Technology
1.	Scalability	Ability to scale based on incident volume	Cloud Computing, Load Balancing
2.	Security	Implementation of security measures	Encryption, Authentication
3.	Real-time	Capability to respond to incidents in real-time	Real-time Data Processing
4.	Accessibility	Accessible from various devices and locations	Web-Based Interface
5.	Usability	User-friendly and intuitive interface	User Experience (UX) Design
6.	Performance	High performance to handle incident data	Optimization, Caching
7,	Reliability	Ensuring minimal downtime and system reliability	Redundancy, Failover
8.	Integration	Ability to integrate with external systems	API Integration, Data Exchange
9.	Reporting	Generation of detailed incident reports	Reporting Tools, Data Visualization
10.	Compliance	Adherence to relevant cybersecurity regulations	Compliance Frameworks, Auditing

"Now that we've outlined the technology track, our next focus is on the critical phase of the main project task: test implementation. This pivotal stage involves rigorous testing of our AI-driven incident response platform to ensure its functionality, reliability, and efficacy in automating incident triage and response tasks for cybersecurity teams."

Stage – 1

Title:

AI-Driven Incident Response Platform That Assists Cybersecurity Teams in Automating Incident Triage and Response Tasks.

Overview:

The AI-Driven Incident Response Platform is a comprehensive solution designed to assist cybersecurity teams in automating incident triage and response tasks. The platform integrates advanced AI algorithms and machine learning techniques to enable swift and accurate identification, analysis, and mitigation of potential security threats. Its primary goal is to streamline the incident response process, ensuring a proactive and efficient approach to managing cybersecurity incidents.

The groundwork for the project involves a detailed analysis of the organization's existing incident response capabilities, identifying potential gaps and inefficiencies in the current process. This analysis serves as the foundation for defining the scope and objectives of the project, which include enhancing incident detection capabilities, automating response tasks, and optimizing the overall incident response workflow.

Key participants in the project include cybersecurity experts, AI specialists, IT professionals, and relevant stakeholders from various departments within the organization. Collaboration among these key stakeholders is essential for understanding specific organizational requirements, defining use cases, and aligning the project objectives with the overall business strategy.

The project's effective planning entails a structured approach towards the development and implementation of the AI-driven incident response platform. This includes establishing a clear roadmap for the project, defining key milestones, and allocating resources effectively. The planning phase also involves outlining the platform's key functionalities, such as automated incident triage, threat detection, real-time monitoring, and adaptive response orchestration.

Furthermore, the project emphasizes the importance of continuous feedback and collaboration between the cybersecurity team and AI specialists to refine and improve the platform's capabilities over time. The integration of external threat intelligence feeds and the implementation of a robust reporting and analytics framework are key components of the project, enabling the platform to adapt to evolving cybersecurity threats and provide actionable insights for informed decision-making.

Overall, the AI-Driven Incident Response Platform aims to establish a proactive, adaptive, and resilient incident response framework that empowers cybersecurity teams to effectively detect, analyze, and respond to security incidents in real time. Through effective planning and collaboration, the platform aims to enhance the organization's overall cybersecurity posture and ensure the protection of critical data assets.

Team Members:

Name	College	Contact
Raghavendra Reddy Orra	VIT Vellore	orraraghavendra.reddy2021@vitstudent.ac.in
Greeshma Reddy Basireddy	VIT Chennai	basireddygreeshma.reddy2021@vitstudent.ac.in
Shaik Muhammed Faizaan Ali	VIT Vellore	shaikmuhammed.faizaan2021@vitstudent.ac.in
Farzeen Niaz	VIT Vellore	farzeen.2021@vitstudent.ac.in

List of Vulnerability:

S. No.	Vulnerability Name	CWE No.
1.	Cross-site scripting (stored)	79
2.	Broken Access Control	285
3.	SQL Injection	89
4.	Broken Authentication	285
5.	Insecure Direct Object Reference	639
6.	Security Misconfiguration	732
7.	Cross-Site Request Forgery	352
8.	Cleartext Transmission of Sensitive Information	319
9.	ClickJacking	1021
10.	webserver allows password auto-completion	310
11.	Cross-site scripting (DOM-based XSS)	79
12.	JQuery 1.2 < 3.5.0 Multiple XSS	79
13.	Information Exposure (Web Server HTTP Header Internal IP Disclosure)	200
14.	Information Exposure (SSL (Multiple Issues))	200
15.	Information Exposure (HTTP (Multiple Issues))	200
16.	OS Identification Failed	200

Report:

1. **Vulnerability name:** Cross site scripting (stored)

   CWE: 79

   OWASP category: A03:2021 -Injections

   Description: It occurs when a malicious script is injected directly into a vulnerable web application. Reflected XSS involves the reflection of a malicious script of a web application, onto a user's browser.

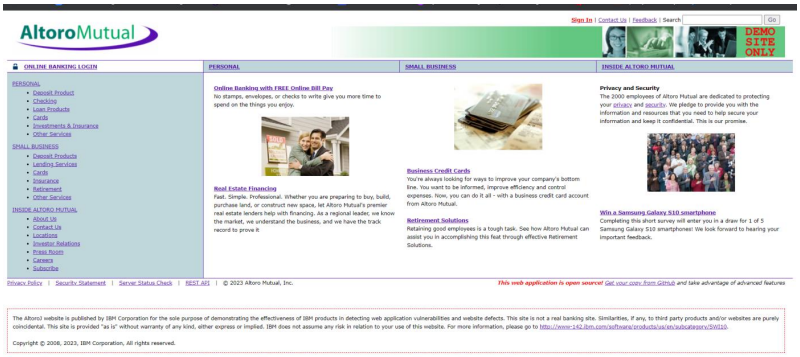
   Business Impact: The application stores dangerous data in a database, message forum, visitor log, or other trusted data store. Later, the dangerous data is subsequently read back into the application and included in dynamic content. From an attacker's perspective, the optimal place to inject malicious content is in an area that is displayed to either many users or particularly interesting users. Interesting users typically have elevated privileges in the application or interact with sensitive data that is valuable to the attacker. If one of these users executes malicious content, the attacker may be able to perform privileged operations on behalf of the user or gain access to sensitive data belonging to the user.

   Vulnerability path: http://testfire.net/

   Vulnerability parameter:
   http://testfire.net/search.jsp?query=%27%3E%3Cscript%3Ealert%28%27hacked%27%29%3C%2Fscript%3E

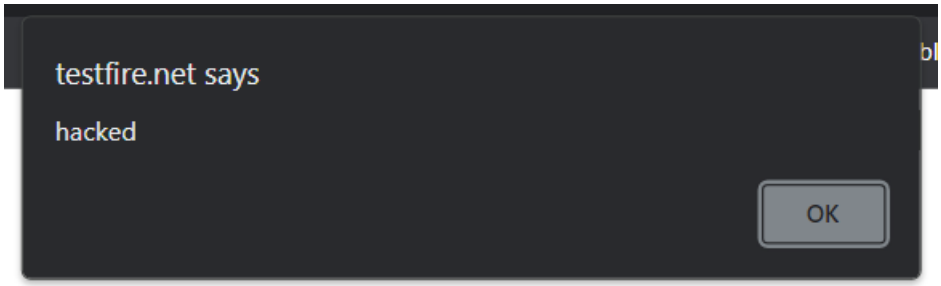
   Steps to Reproduce:

   - Access the URL



- In the search box we will input some code to perform the vulnerability.

- The Script we will be inputting is '><script>alert('hacked')</script>
- This displays a harmless pop up alert box with the text saying 'hacked'



Recommendation:

- When interacting with databases, use parameterized statements or prepared statements to avoid SQL injection, which can be a vector for XSS.
- Sanitize and validate all user inputs and ensure that any data displayed on the web page is properly encoded. Use output encoding libraries or functions to prevent script injection.

2. **Vulnerability name:** Broken access control

CWE: 285

Description: When access control checks are not applied consistently - or not at all - users are able to access data or perform actions that they should not be allowed to perform. This can lead to a wide range of problems, including information exposures, denial of service, and arbitrary code execution.

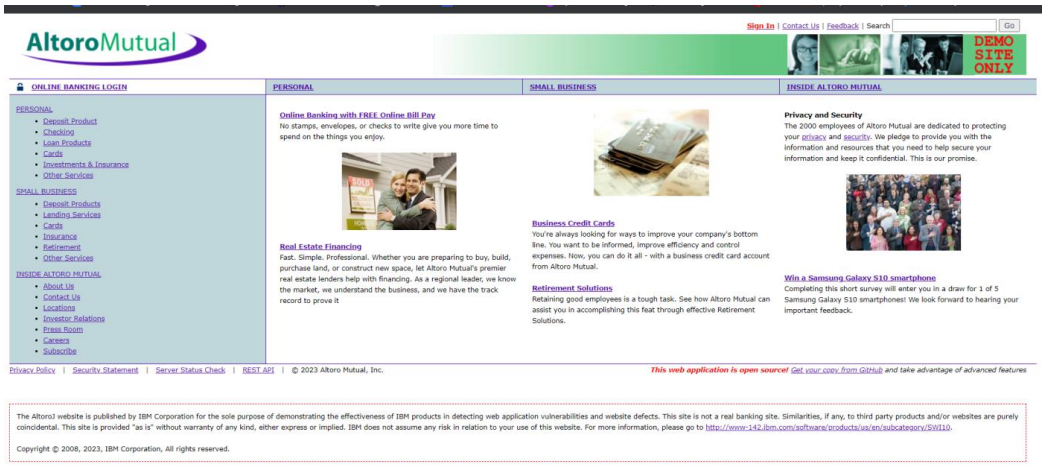
Business Impact: wide-ranging business impact, including financial losses, reputation damage, legal consequences, operational disruption, and loss of customer trust. Addressing this vulnerability is crucial to protect the organization and its stakeholders from these potential negative effects.

Vulnerability path: http://testfire.net/

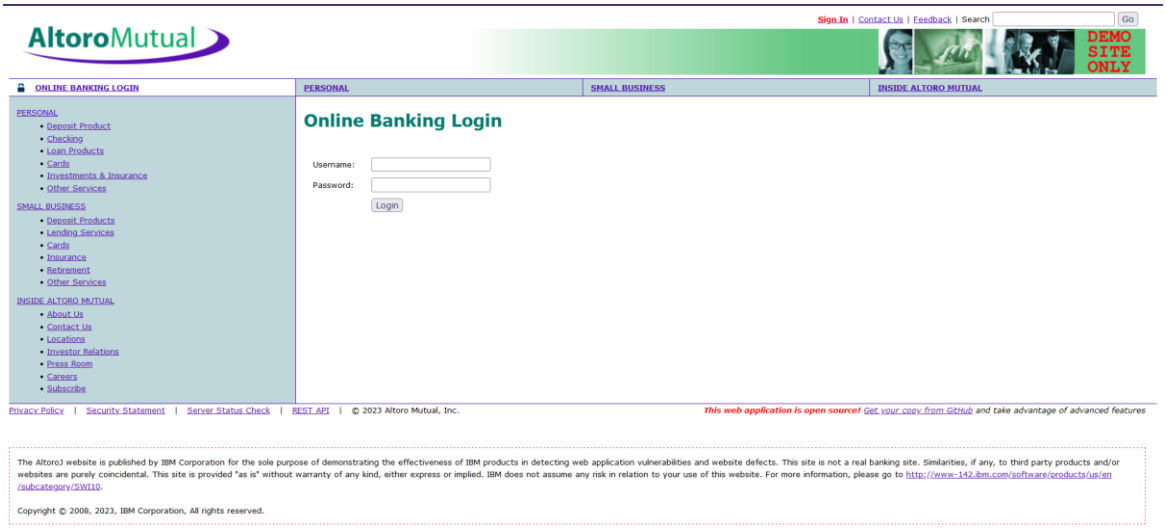
Vulnerability parameter: http://testfire.net/login.jsp

Steps to Reproduce:

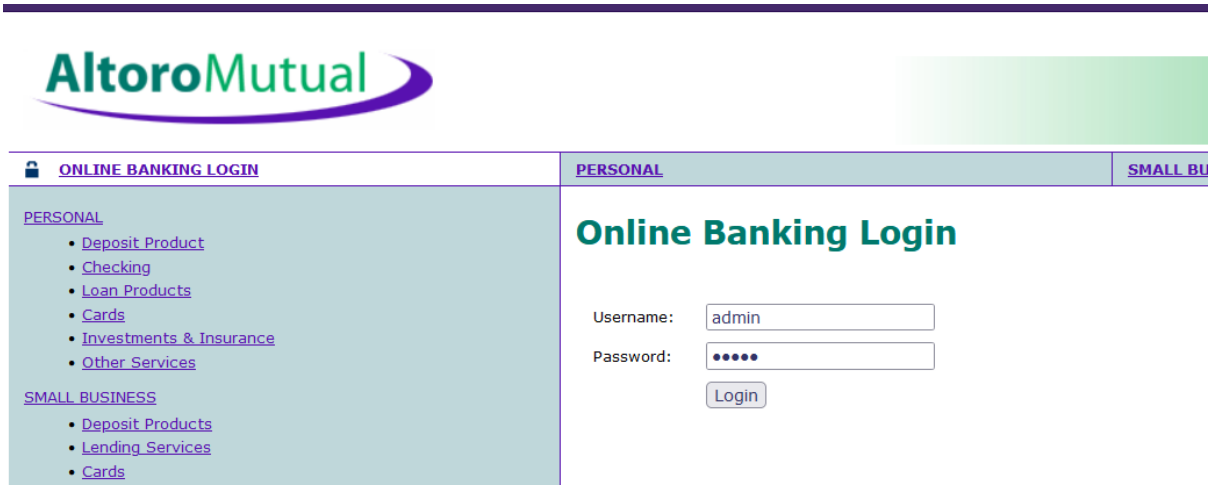
- Access the URL



- Now we will try to sign in to this website with admin privileges

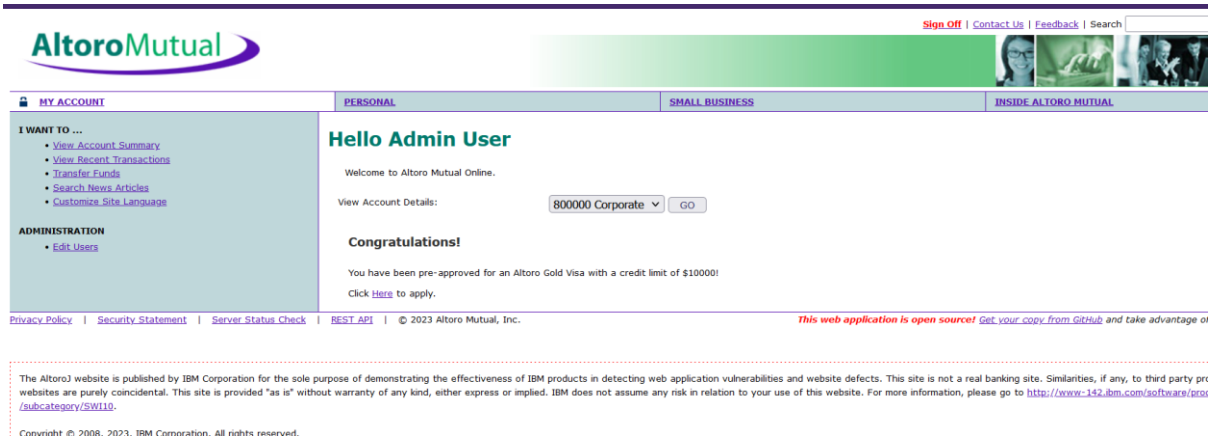


- Also, we will be using burp suite to get requests from the website and know additional information. We use 'admin' for the username and password.

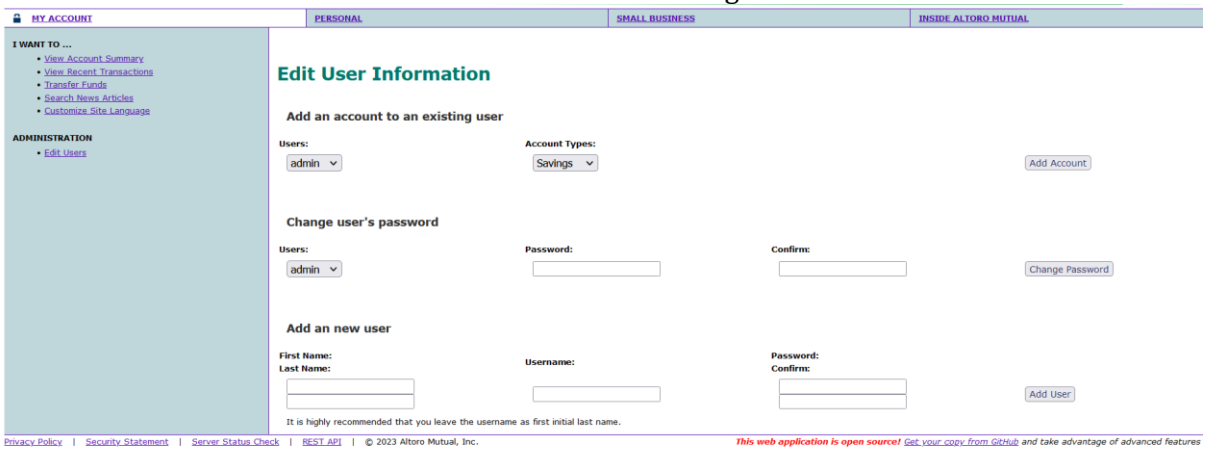


- This request has been received in the burp suite with the username and password as well in clear text.

- now we click on forward request in the burp suite and then we will be redirected to the admin user details.



- We can even edit the other users data and delete their login details as well.



Recommendations:

- Ensure that the application has a robust authentication and authorization mechanism in place. Users should be authenticated before any sensitive actions are performed, and authorization checks should be conducted to verify that users have the necessary permissions for the requested operation.
- Ensure that session management is secure. Use strong session IDs, enforce session timeouts, and regenerate session tokens after login. Implement session fixation protection to prevent session hijacking.

3. **Vulnerability name:** SQL injection

CWE: 89

Description: The product constructs all or part of an SQL command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended SQL command when it is sent to a downstream component.

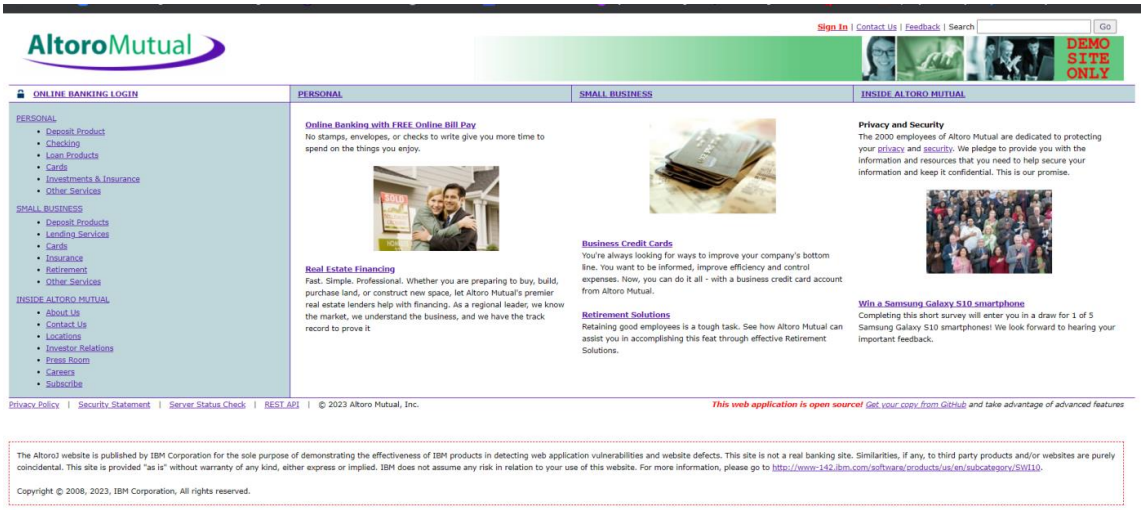
Business Impact: In summary, it is crucial to underscore that CWE-89, known as SQL Injection, can exert a profound and diverse business impact. This encompasses critical facets such as data breaches, financial setbacks, harm to reputation, legal ramifications, and operational turmoil. Hence, the imperative of preventing and remedying SQL injection vulnerabilities cannot be overstated, as it is indispensable for fortifying the security and continuity of an organization's applications and data.

Vulnerability path: http://testfire.net/

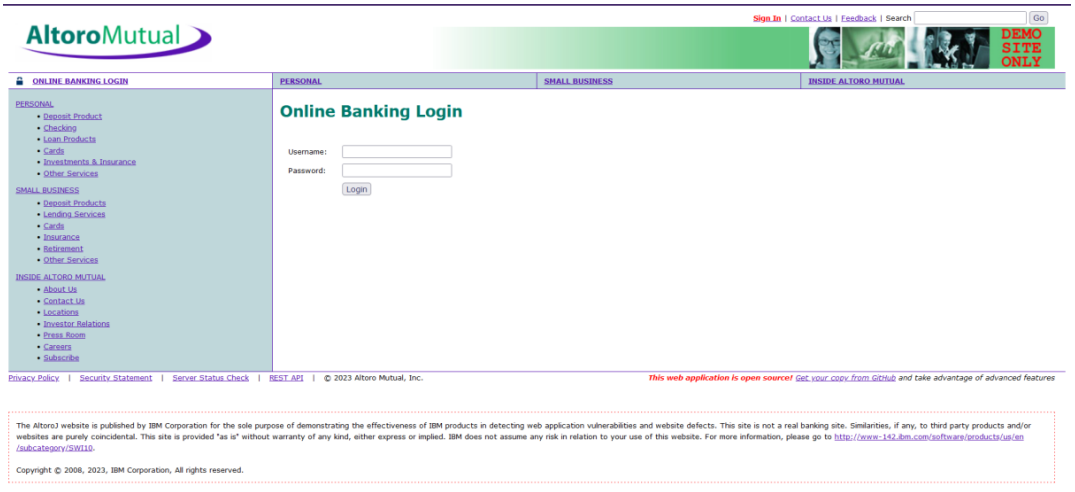
Vulnerability parameter: http://testfire.net/login.jsp

Steps to Reproduce:

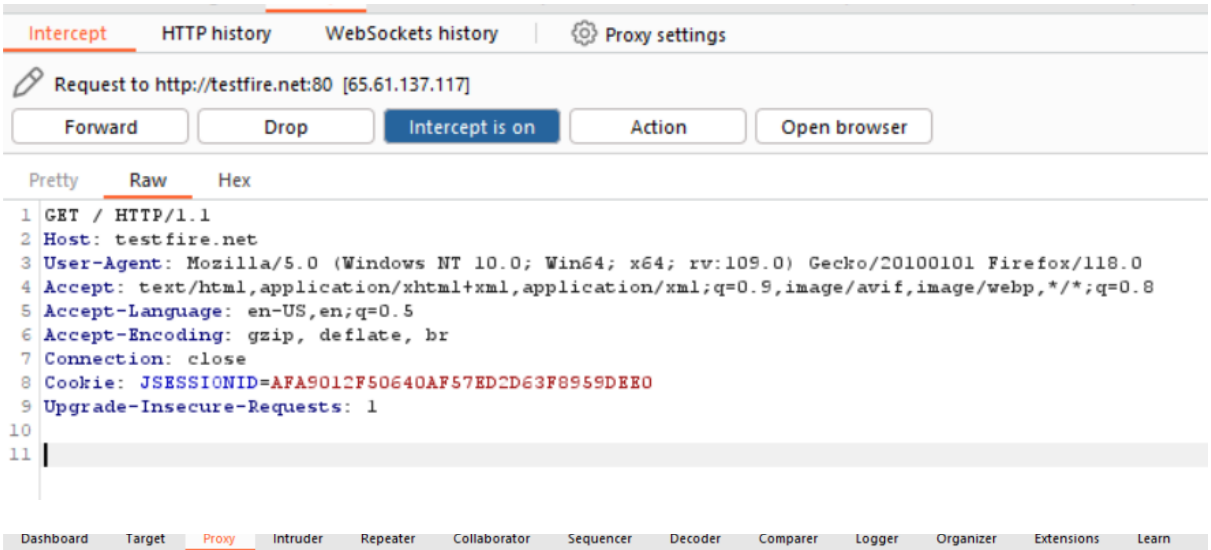
- Access the URL

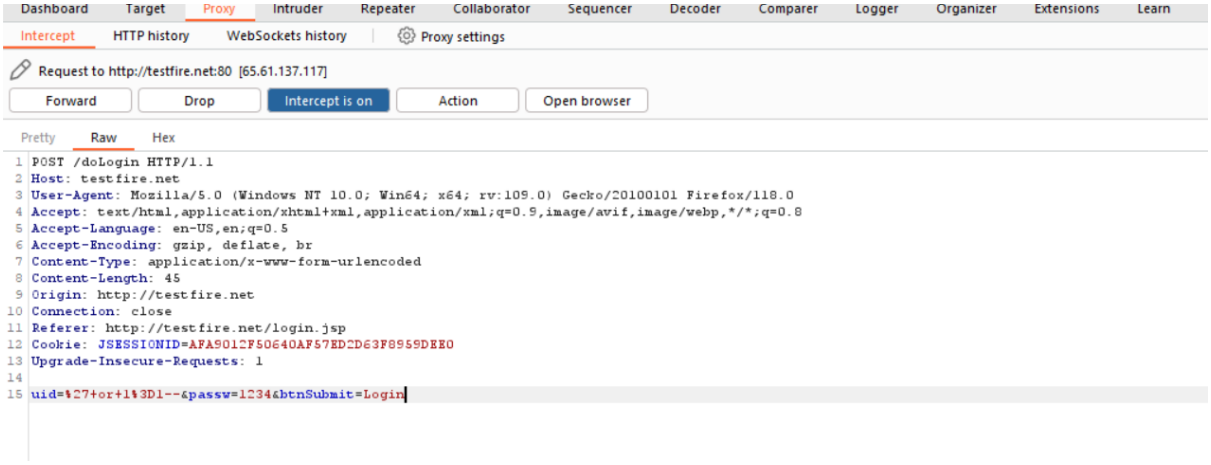


- Now we will try to sign in to this website with admin privileges but using SQL injection

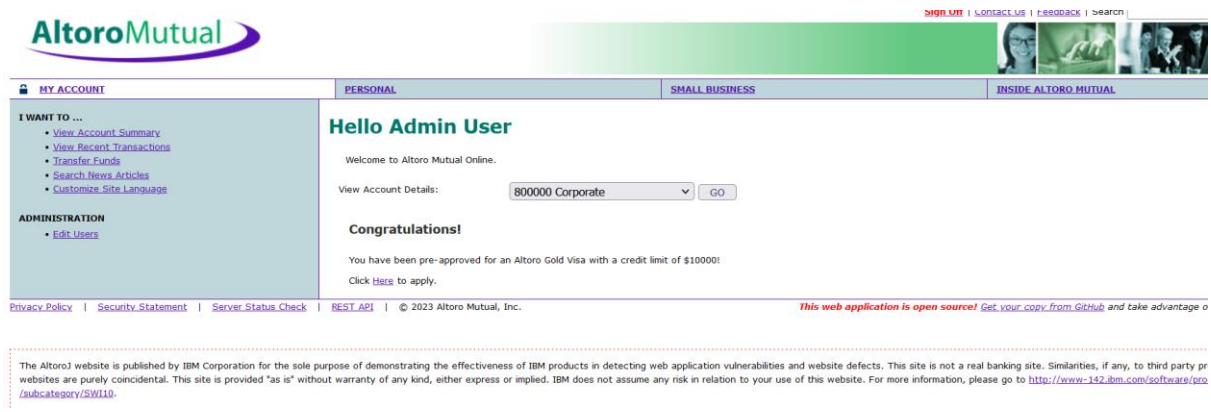


- Also, we will be using burp suite to get requests from the website and know additional information.





- Click forward request multiple times to proceed to the login page.



- With this we can know that sql injection worked and we got the admin privileges.

Recommendations:

- If parameterized statements are not feasible, use proper input validation and escaping mechanisms to sanitize user inputs before they are used in SQL queries. This helps prevent malicious code injection.
- Utilize stored procedures for database operations. This can help separate SQL code from application code and reduce the risk of SQL injection.
- Implement strict input validation for all user inputs, ensuring that data adheres to the expected format and structure.

4. **Vulnerability name:** Broken authentication

CWE: 285

Description: The system's authorization functionality does not prevent one user from gaining access to another user's data or record by modifying the key value identifying the data.

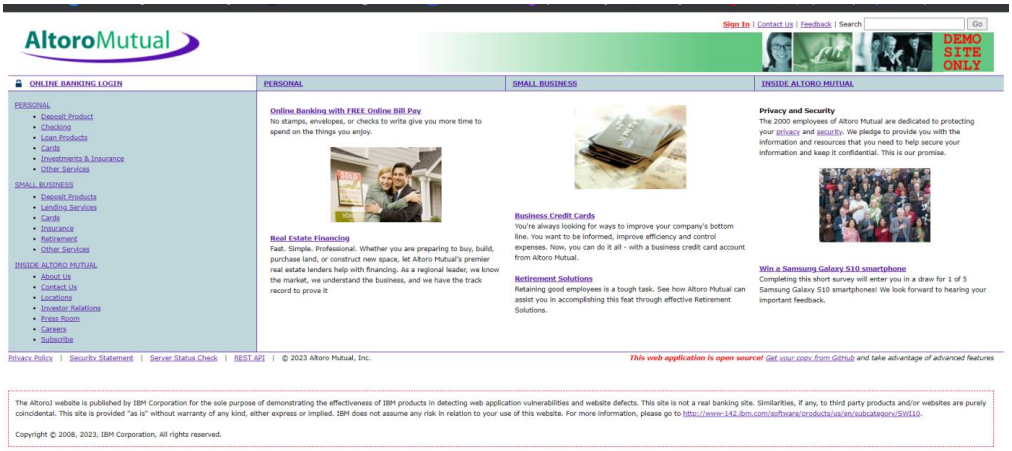
Business Impact: To effectively mitigate the business impact of CWE-285, it is imperative that organizations place a strong emphasis on bolstering their authentication and session management practices. This should encompass the adoption of multi-factor authentication, the secure storage of credentials, meticulous session handling, and a commitment to conducting routine security assessments and testing. The rectification of these vulnerabilities stands as a critical imperative, safeguarding sensitive data, user identities, and the organization's overarching security stature and reputation.

Vulnerability path: http://testfire.net/

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

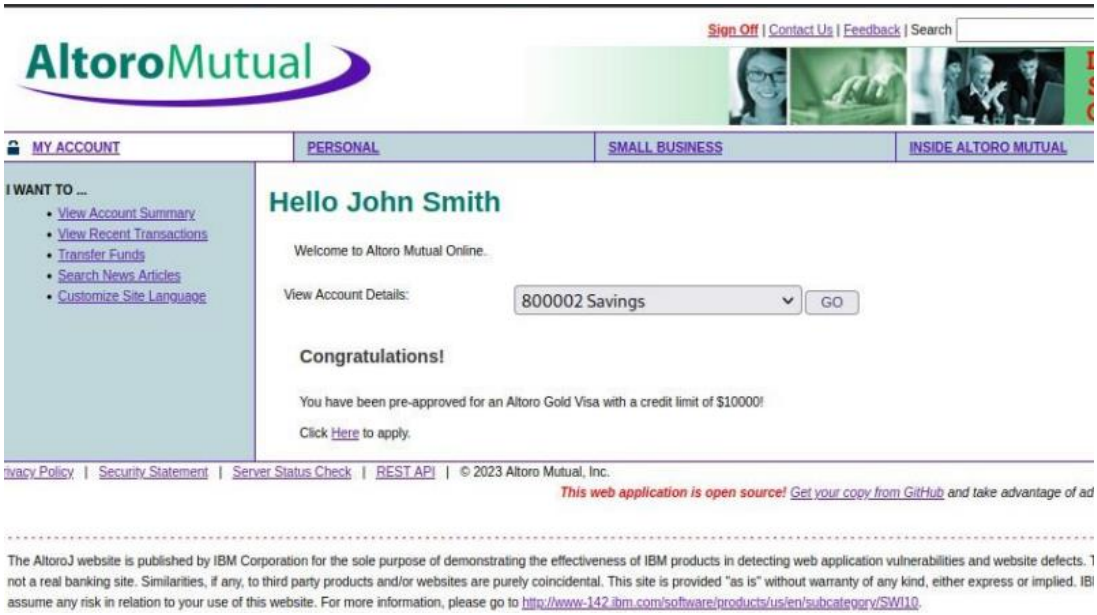
Steps to Reproduce:

- Access the URL



- Now we will try to login using some different approach.

- As we know which users are present in the database of this website by using the admin privileges. We can directly access a particular user by simply knowing their username; we will add some characters after his user name as a sql injection to simply bypass the password.



- This leads us to the details of this person's account.

Recommendations:

- Implement strong authentication mechanisms, such as multi-factor authentication (MFA) or two-factor authentication (2FA), to ensure that only authorized users can access the system.
- Implement proper authorization controls to ensure that users have the necessary permissions to access specific functions or data. Use role-based access control (RBAC) to manage user privileges effectively.
- Deploy intrusion detection and prevention systems (IDS/IPS) to monitor and block suspicious activities related to authentication and authorization.

5. **Vulnerability Name:** Insecure Direct object Reference

CWE: 639

OWASP Category: A01: Broken Access Control

Description:
Insecure Direct Object Reference (IDOR) is a vulnerability that arises when attackers can access or modify objects by manipulating identifiers used in a web application's URLs or parameters. It occurs due to missing access control checks, which fail to verify whether a user should be allowed to access specific data.

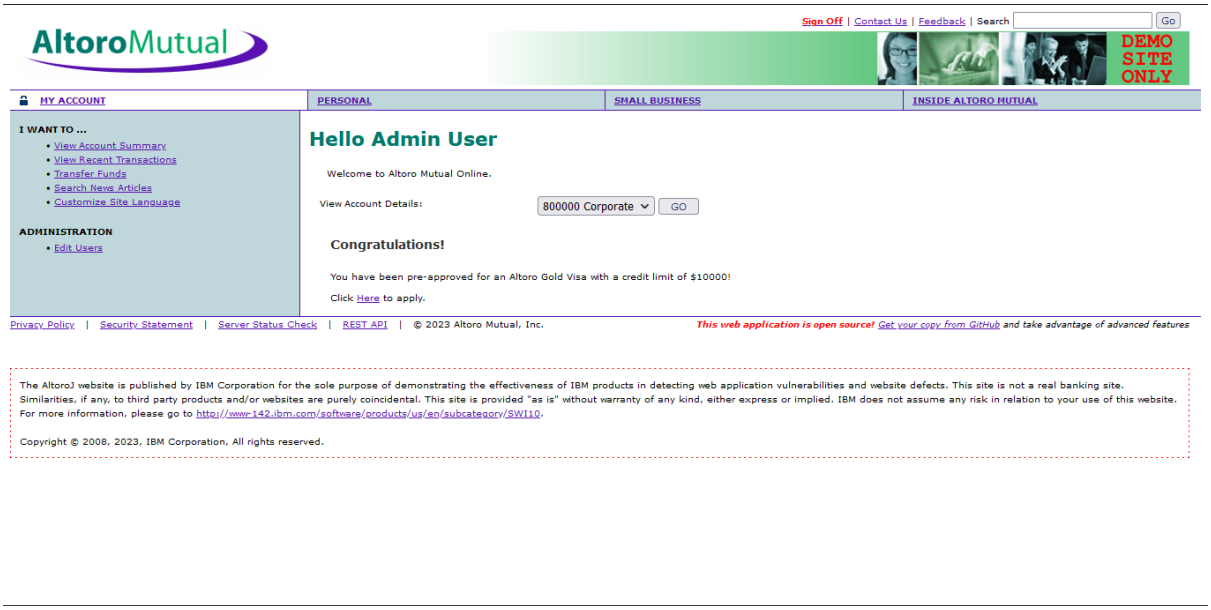
Business Impact:
To effectively mitigate the business impact of CWE-639, organizations must make it a top priority to fortify their access control and authorization mechanisms. This entails the implementation of robust security measures, the regular conduct of comprehensive security assessments, and the deployment of intrusion detection systems to promptly identify and counter unauthorized access attempts. These measures stand as absolutely critical in the defense of sensitive data, the overall security of systems, and the preservation of the organization's esteemed reputation.

Vulnerability Path: http://testfire.net

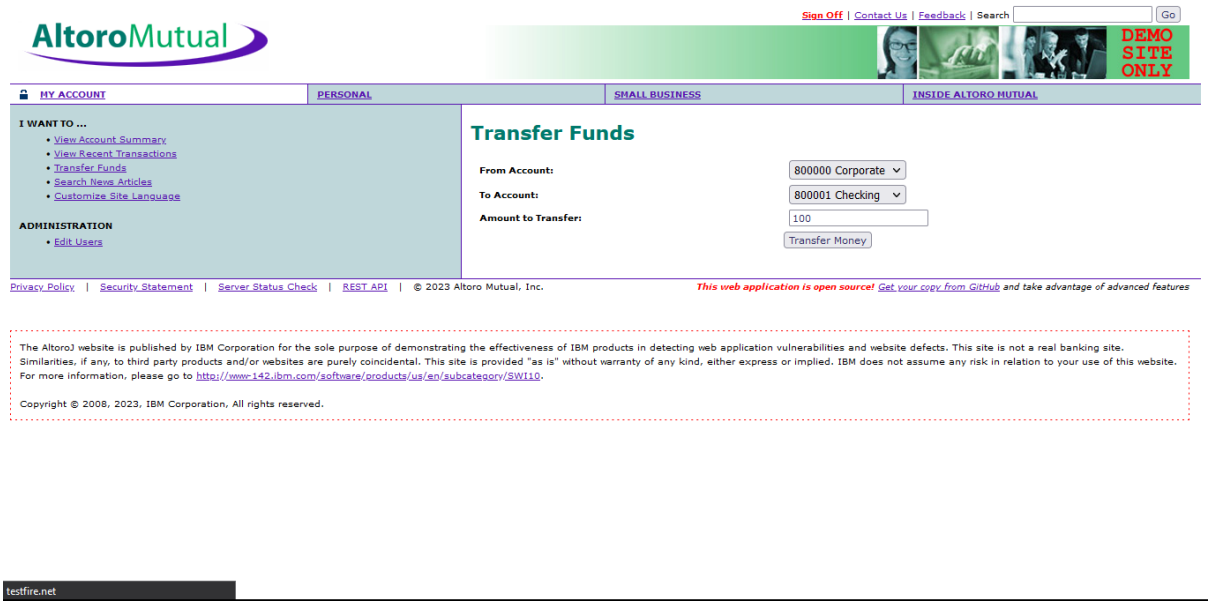
Vulnerability Parameter: http://testfire.net/bank/transfer.jsp

Steps to Reproduce:

- Go to the domain.
- Sign into the site.



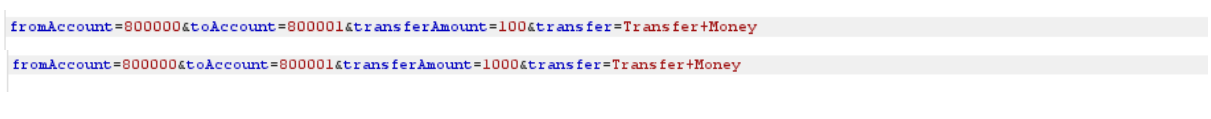
- Open “Transfer Money” on the left side and fill in the details. On the intercept and click transfer



testfire.net

- Open burp and notice the change.

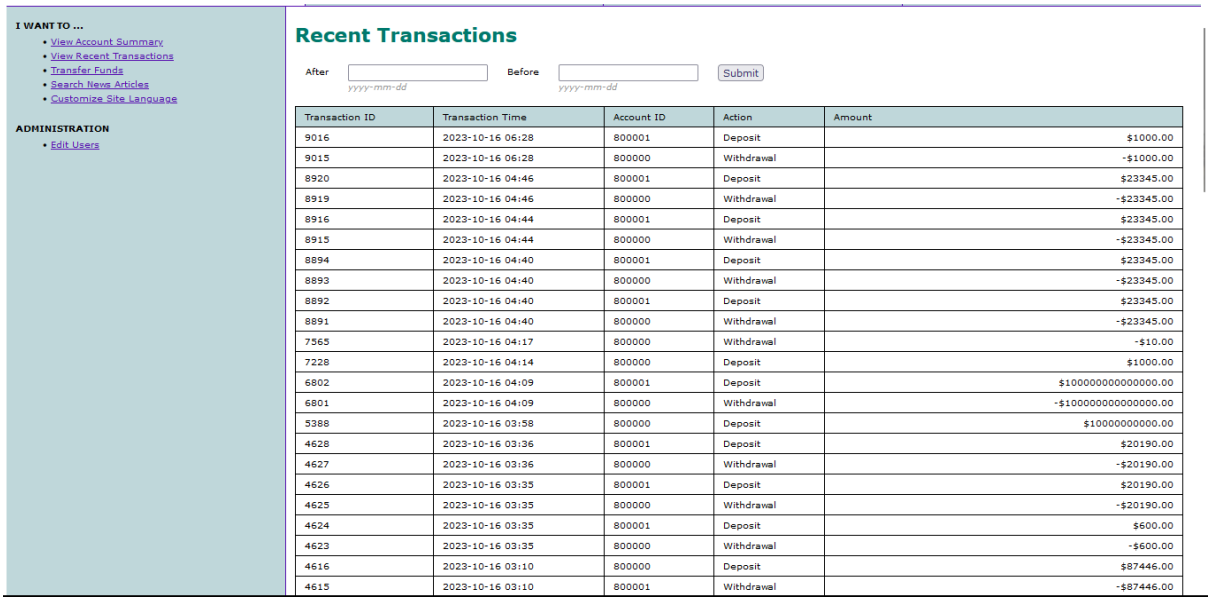
- In the 15th line change the amount from 100 to 1000 and click forward



```
Pretty   Raw   Hex
1 GET /v1/tiles HTTP/1.1
2 Host: contile.services.mozilla.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/119.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Te: trailers
8 Connection: close
9
10
```

- Look at the site, we can notice the msg that shows the transfer of 1000.

- Off the Intercept and open "View Recent Transactions".



Transaction ID	Transaction Time	Account ID	Action	Amount
9016	2023-10-16 06:28	800001	Deposit	$1000.00
9015	2023-10-16 06:28	800000	Withdrawal	-$1000.00
8920	2023-10-16 04:46	800001	Deposit	$23345.00
8919	2023-10-16 04:46	800000	Withdrawal	-$23345.00
8916	2023-10-16 04:44	800001	Deposit	$23345.00
8915	2023-10-16 04:44	800000	Withdrawal	-$23345.00
8894	2023-10-16 04:40	800001	Deposit	$23345.00
8893	2023-10-16 04:40	800000	Withdrawal	-$23345.00
8892	2023-10-16 04:40	800001	Deposit	$23345.00
8891	2023-10-16 04:40	800000	Withdrawal	-$23345.00
7565	2023-10-16 04:17	800000	Withdrawal	-$10.00
7228	2023-10-16 04:14	800000	Deposit	$1000.00
6802	2023-10-16 04:09	800001	Deposit	$100000000000000.00
6801	2023-10-16 04:09	800000	Withdrawal	-$100000000000000.00
5388	2023-10-16 03:58	800000	Deposit	$10000000000.00
4628	2023-10-16 03:36	800001	Deposit	$20190.00
4627	2023-10-16 03:36	800000	Withdrawal	-$20190.00
4626	2023-10-16 03:35	800001	Deposit	$20190.00
4625	2023-10-16 03:35	800000	Withdrawal	-$20190.00
4624	2023-10-16 03:35	800001	Deposit	$600.00
4623	2023-10-16 03:35	800000	Withdrawal	-$600.00
4616	2023-10-16 03:10	800000	Deposit	$87446.00
4615	2023-10-16 03:10	800001	Withdrawal	-$87446.00

Recommendation:

- Utilize parameterized queries or prepared statements when interacting with databases. This prevents user-controlled input from being executed as SQL code.
- Implement a Content Security Policy to mitigate the risk of cross-site scripting (XSS) attacks, which can be used to execute unauthorized queries.
- Implement account lockout mechanisms that temporarily suspend accounts after a specified number of unauthorized access attempts to prevent brute force attacks.

6. **Vulnerability name:** Security Misconfiguration

CWE:732

Description: The product specifies permissions for a security-critical resource in a way that allows that resource to be read or modified by unintended actors.

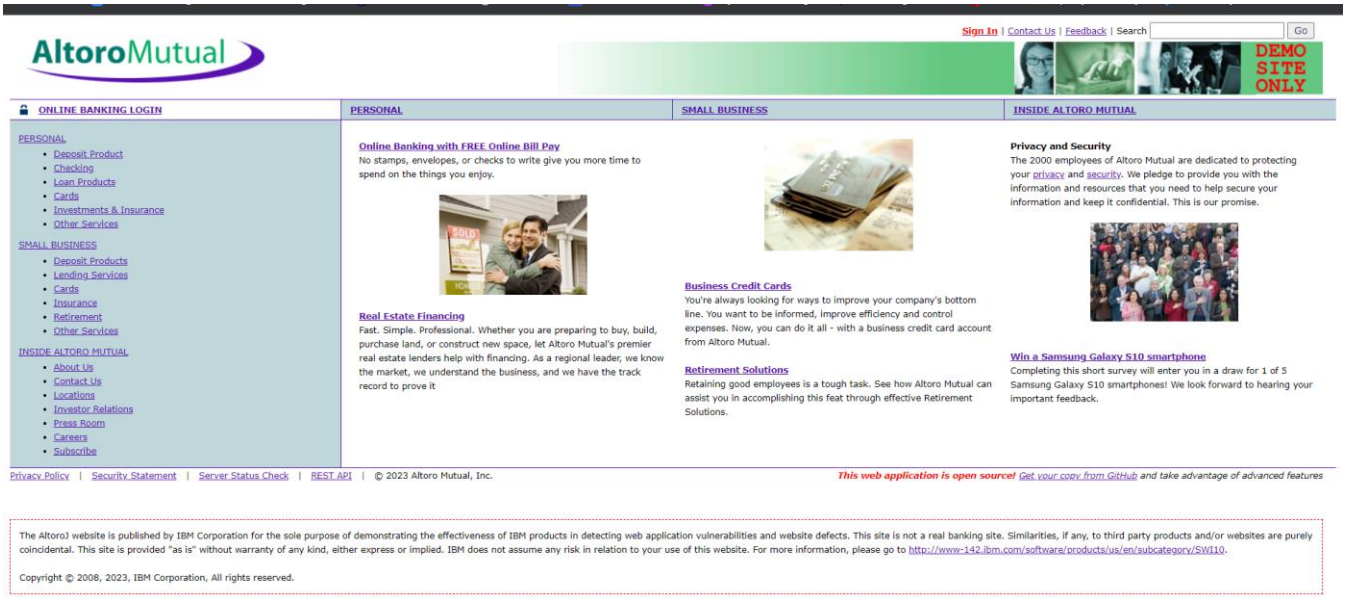
Business Impact: To effectively lessen the business consequences stemming from CWE-732, organizations must place a strong emphasis on bolstering their configuration management practices. This involves the establishment of secure default settings, the routine conduct of comprehensive security evaluations, and the deployment of intrusion detection systems to promptly detect and address misconfigurations and vulnerabilities. These actions are of paramount importance in safeguarding sensitive data, fortifying system security, and preserving the organization's esteemed reputation.

Vulnerability path: http://testfire.net/

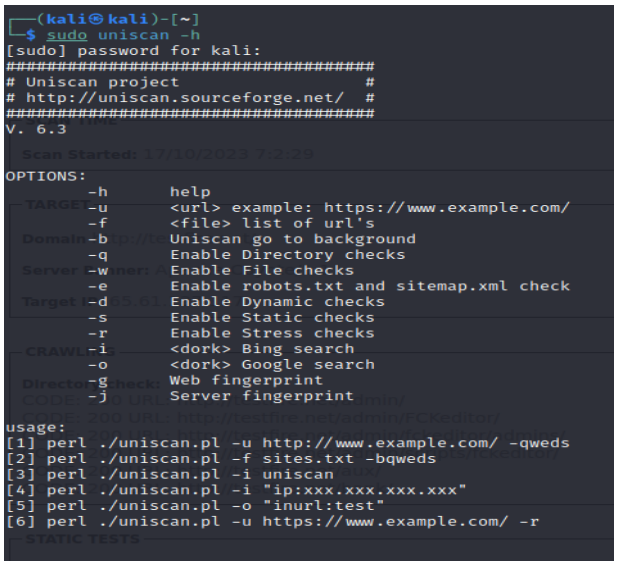
Vulnerability parameter: http://testfire.net/login.jsp

Steps to Reproduce:

- Access the URL



- We will be using the uniscan tool which is available in the kali.



- We will use this tool to scan for hidden directories that can be access due to poor security measures taken in this website.

```
┌──(kali㉿kali)-[~]
└─$ sudo uniscan -u http://testfire.net/ -qweds
[sudo] password for kali:
###################################
# Uniscan project                 #
# http://uniscan.sourceforge.net/ #
###################################
V. 6.3


Scan date: 17-10-2023 7:18:22
============================================================
| Domain: http://testfire.net/
| Server: Apache-Coyote/1.1
| IP: 65.61.137.117
============================================================
|
| Directory check:
| [+] CODE: 200 URL: http://testfire.net/admin/fckeditor/admins/
| [+] CODE: 200 URL: http://testfire.net/admin/
| [+] CODE: 200 URL: http://testfire.net/admin/scripts/fckeditor/
| [+] CODE: 200 URL: http://testfire.net/admin/FCKeditor/
| [+] CODE: 200 URL: http://testfire.net/aux/
| [+] CODE: 200 URL: http://testfire.net/bank/
============================================================
|
```

- We found directories that can be accessed easily. Also all the files that are present in the website has also been found.

```
| File check:
| [+] CODE: 200 URL: http://testfire.net/admin/account.asp
| [+] CODE: 200 URL: http://testfire.net/admin/account.html
| [+] CODE: 200 URL: http://testfire.net/admin/admin.php
| [+] CODE: 200 URL: http://testfire.net/admin/admin_phpinfo.php4
| [+] CODE: 200 URL: http://testfire.net/admin/account.php
| [+] CODE: 200 URL: http://testfire.net/admin/admin.shtml
| [+] CODE: 200 URL: http://testfire.net/admin/aindex.htm
| [+] CODE: 200 URL: http://testfire.net/admin/auth.php
| [+] CODE: 200 URL: http://testfire.net/admin/cfg/configscreen.inc.php+
| [+] CODE: 200 URL: http://testfire.net/admin/cfg/configsite.inc.php+
| [+] CODE: 200 URL: http://testfire.net/admin/cfg/configsql.inc.php+
| [+] CODE: 200 URL: http://testfire.net/admin/cfg/configtache.inc.php+
| [+] CODE: 200 URL: http://testfire.net/admin/cms/htmltags.php
| [+] CODE: 200 URL: http://testfire.net/admin/config.php
| [+] CODE: 200 URL: http://testfire.net/admin/contextAdmin/contextAdmin.html
| [+] CODE: 200 URL: http://testfire.net/admin/controlpanel.asp
| [+] CODE: 200 URL: http://testfire.net/admin/controlpanel.php
| [+] CODE: 200 URL: http://testfire.net/admin/controlpanel.html
| [+] CODE: 200 URL: http://testfire.net/admin/cplogfile.log
| [+] CODE: 200 URL: http://testfire.net/admin/cp.php
| [+] CODE: 200 URL: http://testfire.net/admin/cp.html
| [+] CODE: 200 URL: http://testfire.net/admin/database/wwForum.mdb
| [+] CODE: 200 URL: http://testfire.net/admin/credit_card_info.php
| [+] CODE: 200 URL: http://testfire.net/admin/datasource.asp
| [+] CODE: 200 URL: http://testfire.net/admin/db.php
| [+] CODE: 200 URL: http://testfire.net/admin/home.asp
| [+] CODE: 200 URL: http://testfire.net/admin/home.php
| [+] CODE: 200 URL: http://testfire.net/admin/index.asp
| [+] CODE: 200 URL: http://testfire.net/admin/index.html
| [+] CODE: 200 URL: http://testfire.net/admin/index.php
| [+] CODE: 200 URL: http://testfire.net/admin/phpinfo.php
| [+] CODE: 200 URL: http://testfire.net/admin/settings.inc.php+
| [+] CODE: 200 URL: http://testfire.net/admin/system_footer.php
| [+] CODE: 200 URL: http://testfire.net/admin/upload.php
| [+] CODE: 200 URL: http://testfire.net/admin/templates/header.php
| [+] CODE: 200 URL: http://testfire.net/admin/wg_user-info.ml
| [+] CODE: 200 URL: http://testfire.net/admin/script.php
| [+] CODE: 200 URL: http://testfire.net/login.jsp
============================================================
|
```

- Let us go through one webpage to see the vulnerability

- Here we can see the sensitive data of job applications which can help an attacker.

Recommendations:

- Implement a change management process to document and review all changes to system configurations. This helps prevent unauthorized or unintended alterations.
- Follow security guidelines provided by software and hardware vendors to ensure secure configurations.
- Regularly perform compliance checks against industry standards and regulations to ensure that configurations remain in compliance with security requirements.

7. **Vulnerability Name:** Cross-Site Request Forgery

CWS: 352

OWASP Category: A08: Cross-Site Request Forgery

Description:

Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated. With a little help of social engineering (such as sending a link via email or chat), an attacker may trick the users of a web application into executing actions of the attacker's choosing. If the victim is a normal user, a successful CSRF attack can force the user to perform state changing requests like transferring funds, changing their email address, and so forth. If the victim is an administrative account, CSRF can compromise the entire web application.

Business Impact:

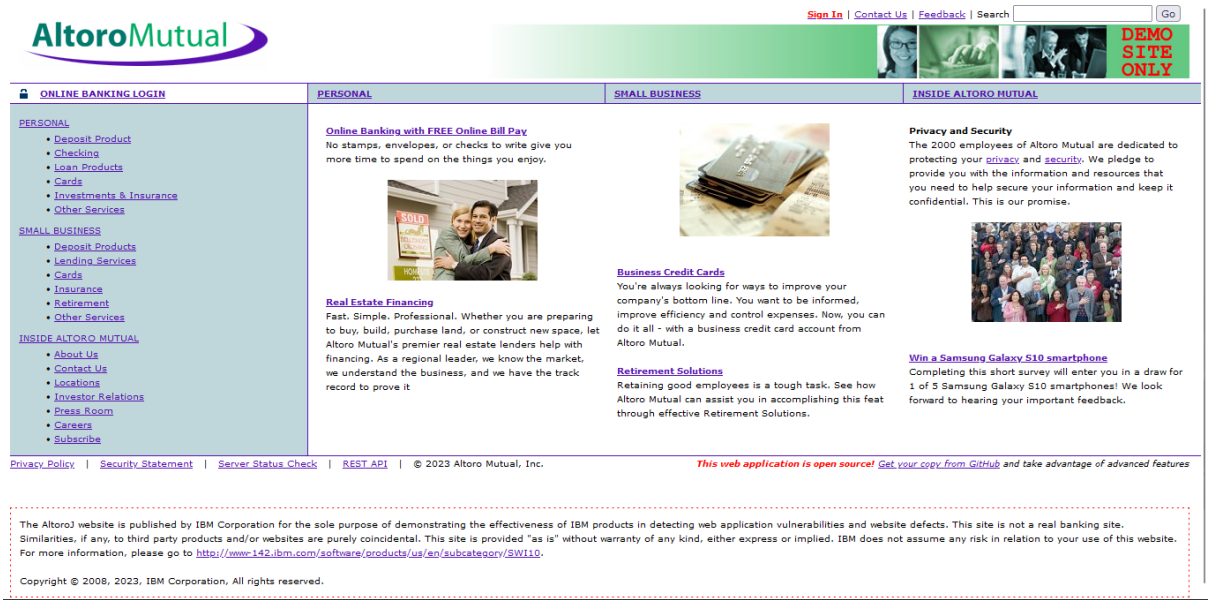
To effectively reduce the business repercussions of CWE-352, organizations must prioritize secure coding practices, including the incorporation of anti-CSRF tokens, while also conducting routine security assessments and testing to detect and rectify CSRF vulnerabilities. Furthermore, educating users on secure browsing practices is pivotal in preventing CSRF attacks. These actions are of paramount importance in the protection of data and in upholding the trust of customers and partners.

Vulnerability Path: http://testfire.net/

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

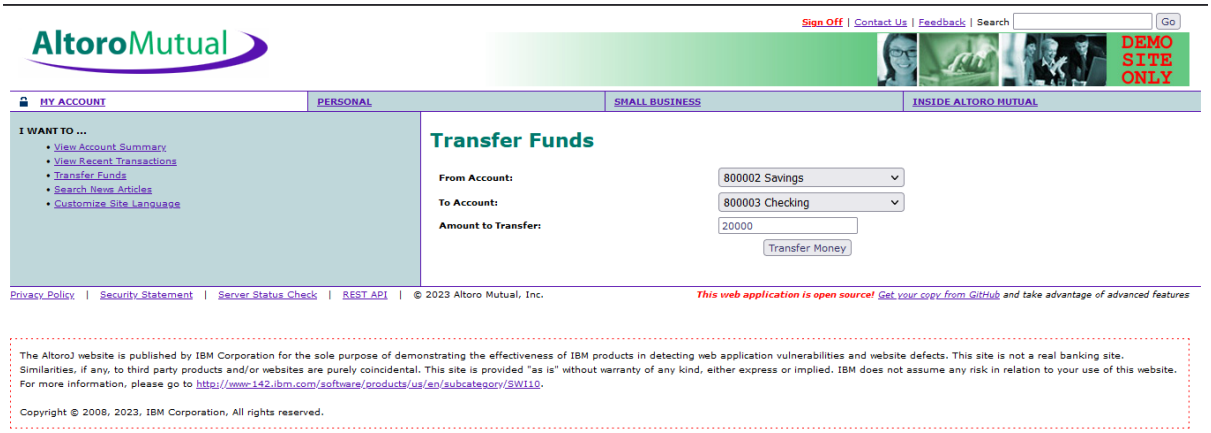
Steps to Reproduce:

- Open https://testfire.net/.

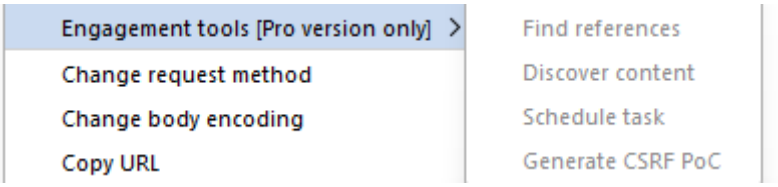


- Login to it using default credentials, and you will find two accounts.

- Capture the request in any Intercepting proxy (Burp Suite, Charles Proxy etc.) while transferring the amount from one account to another as shown in the below picture.



- Generate CSRF POC using Burp Suite Engagement tools (by modifying the account numbers accordingly)

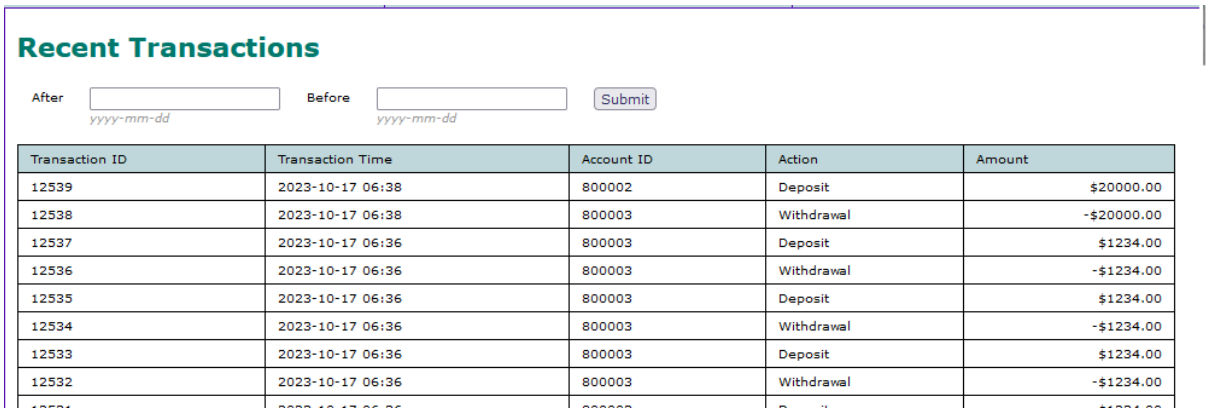


- As the victim is already logged-in to the site an attacker can send the crafted malicious form/URL to the user to his email/text/by any other means and trick the victim using his social engineering skills/techniques like below.

```
Limited Time Offer Get a $100 Gift Card Now!!  (Evil :P)
```

- User thinks, he could use a free $100 gift card! What could go wrong? You open the email and click the link/open the attachment.

- Once the user opens the form a transaction is automatically performed from his account without his knowledge as the user is already logged in.



Recent Transactions

After yyyy-mm-dd Before yyyy-mm-dd Submit

Transaction ID	Transaction Time	Account ID	Action	Amount
12539	2023-10-17 06:38	800002	Deposit	$20000.00
12538	2023-10-17 06:38	800003	Withdrawal	-$20000.00
12537	2023-10-17 06:36	800003	Deposit	$1234.00
12536	2023-10-17 06:36	800003	Withdrawal	-$1234.00
12535	2023-10-17 06:36	800003	Deposit	$1234.00
12534	2023-10-17 06:36	800003	Withdrawal	-$1234.00
12533	2023-10-17 06:36	800003	Deposit	$1234.00
12532	2023-10-17 06:36	800003	Withdrawal	-$1234.00

Recommendations:

- Implement Synchronizer Token Patterns to include unique, randomly generated tokens in each HTTP request and validate these tokens on the server side to verify the authenticity of the request.
- Utilize the SameSite attribute in cookies to restrict their usage to same-site requests only, preventing them from being sent along with cross-site requests and effectively mitigating CSRF attacks.

- Utilize framework-specific protections and security features to prevent CSRF attacks. Many modern web frameworks have built-in mechanisms and libraries for handling CSRF vulnerabilities effectively.
- Implement a Content Security Policy to restrict the sources from which various types of content can be loaded. By specifying the trusted sources of content, you can minimize the risk of malicious code execution and reduce the likelihood of successful CSRF attacks.

8. **Vulnerability name:** Cleartext Transmission of Sensitive Information

   CWE: 319

   Description: The product transmits sensitive or security-critical data in cleartext in a communication channel that can be sniffed by unauthorized actors. Many communication channels can be "sniffed" (monitored) by adversaries during data transmission. For example, in networking, packets can traverse many intermediary nodes from the source to the destination, whether across the internet, an internal network, the cloud, etc. Some actors might have privileged access to a network interface or any link along the channel, such as a router, but they might not be authorized to collect the underlying data. As a result, network traffic could be sniffed by adversaries, spilling security-critical data.

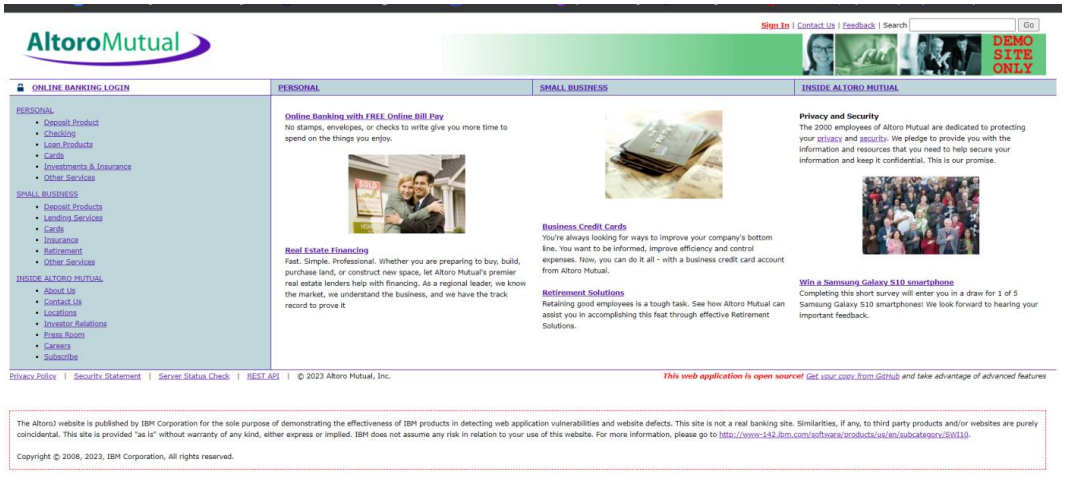
   Business Impact: To effectively reduce the business consequences associated with CWE-319, organizations must prioritize the adoption of secure data transmission practices. This includes the utilization of encryption and robust, secure protocols. The routine conduct of security assessments and testing is pivotal in pinpointing and remedying vulnerabilities linked to data transmission. Furthermore, the education of users on secure data handling practices plays a vital role in proactively preventing data exposure incidents. These actions are of paramount importance in the protection of sensitive data and in preserving the trust of both customers and partners.

   Vulnerability path: http://testfire.net/

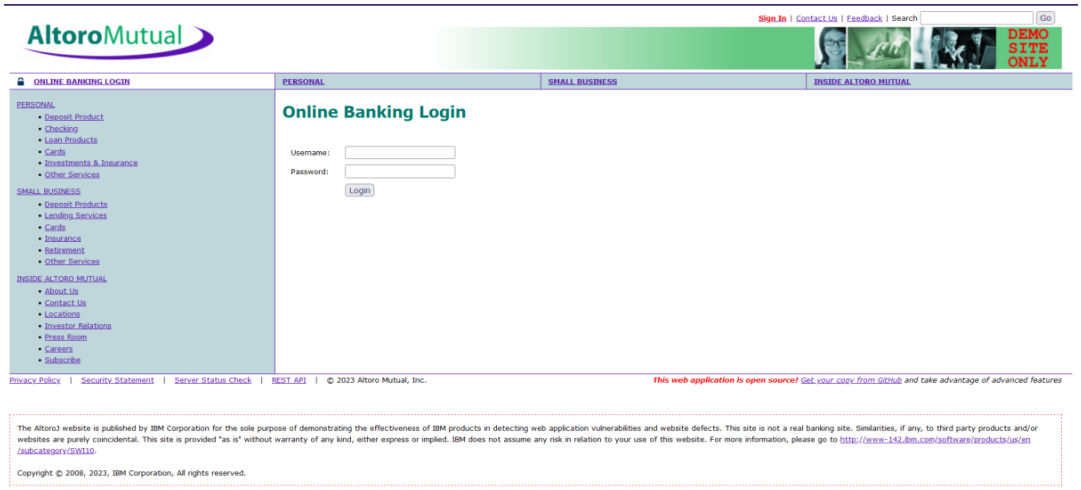
   Vulnerability parameter: http://testfire.net/login.jsp

   Steps to reproduce:

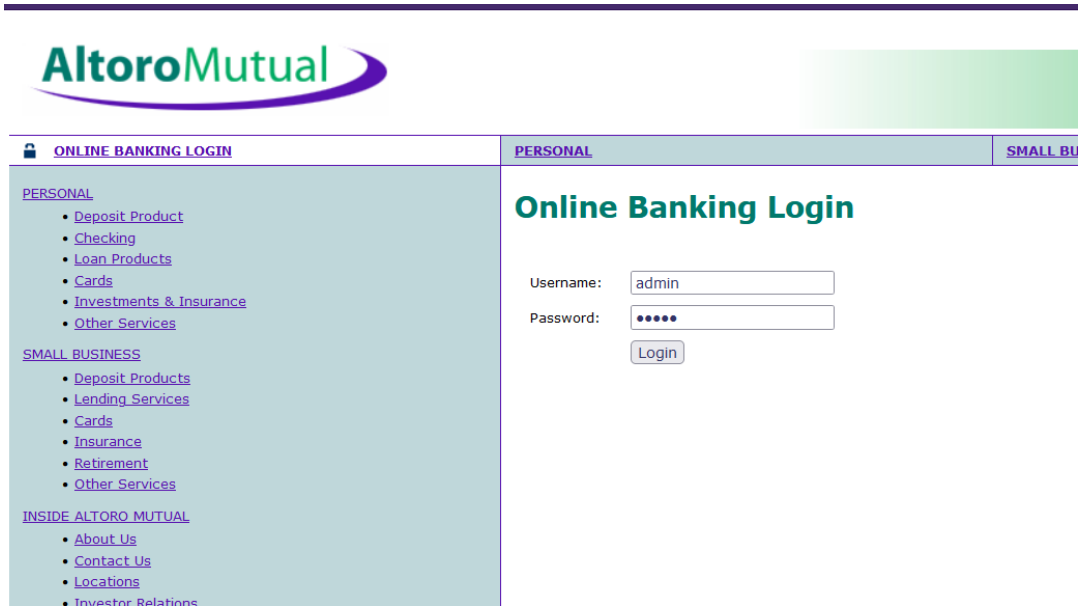
   - Access the URL



   - Now we will try to sign in to this website with admin privileges



- Also, we will be using burp suite to get requests from the website and know additional information.
- We use 'admin' for the username and password.



- This request has been received in the burp suite with the username and password as well in clear text.

- Now we click on forward request in the burp suite and then we will be redirected to the admin user details. Here in the burp suite, we can clearly see the login details in clear text. this is the clear indication of the vulnerability which can lead to data breach, monitored, and manipulated as well.

Recommendations:

- Educate users and employees on secure data handling practices, such as recognizing secure websites (look for "https") and avoiding insecure Wi-Fi networks.
- Employ data masking or redaction techniques to replace sensitive data with placeholders or cryptographic representations during transmission.
- Implement encryption for data in transit. Use secure encryption protocols such as TLS/SSL to protect sensitive information during transmission.

- Use secure communication protocols for transmitting data, such as HTTPS for web applications, and ensure that the selected protocols are kept up-to-date.

9. **Vulnerability name:** Click Jacking

   CWE: 1021

   Description: The web application does not restrict or incorrectly restricts frame objects or UI layers that belong to another application or domain, which can lead to user confusion about which interface the user is interacting with.

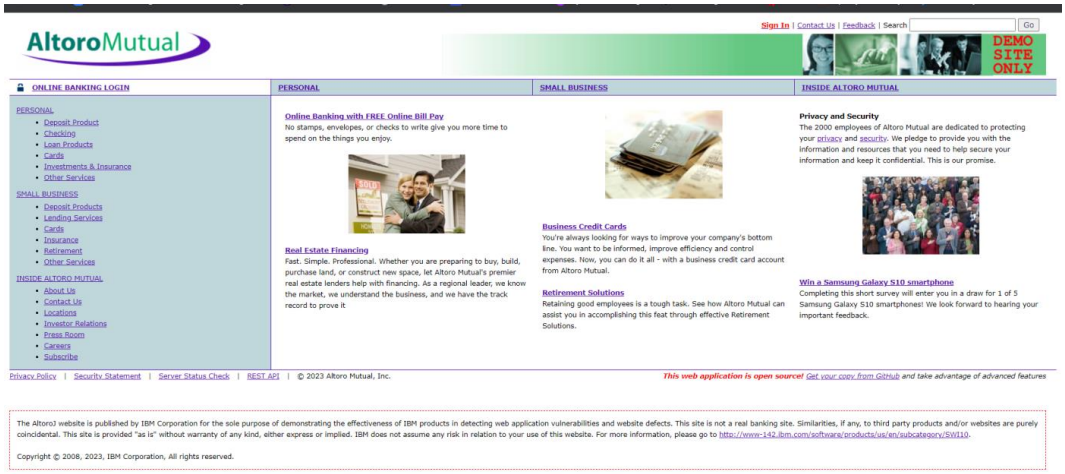
   Business Impact: To effectively reduce the business consequences resulting from CWE-1021, organizations must prioritize the implementation of protective measures, such as frame-busting code. Simultaneously, educating users on safe browsing practices plays a crucial role in preventing clickjacking incidents. Additionally, routine security assessments and testing are pivotal for identifying and mitigating vulnerabilities associated with clickjacking. These actions are of paramount importance in upholding user trust, ensuring data protection, and safeguarding the organization's reputation.

   Vulnerability path: http://testfire.net/

   Vulnerability parameter: http://testfire.net/

   Steps to reproduce:

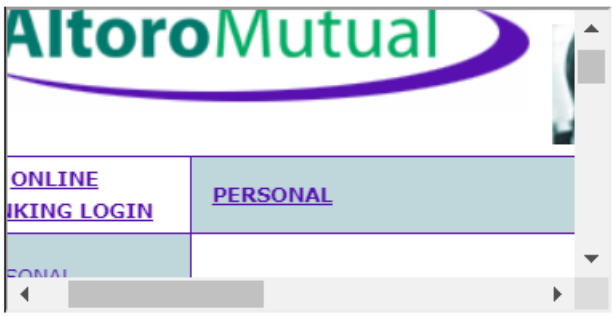
   - Access the URL



   - Then take the URL and use it for the html code
   - we will be writing some html code to perform this vulnerability. we will be writing the code in vs code for better flexibility and functionality.

```
<html>
<body>
<title>Click jacking vulnerability</title>
<h2>This website is vulnerable to clickjacking</h2>
<iframe  src="http://testfire.net/"></iframe>
</body>
</html>
```

   - After the code has been written then we will be executing the code in the browser.



- From this image we can see that the vulnerability has been found.

Recommendation:

- Set the X-Frame-Options HTTP response header to deny or same-origin to control how your site can be framed. This is supported by most modern browsers.
- Utilize frame-busting JavaScript code in web applications to prevent the embedding of your site within malicious iframes. This code can disrupt clickjacking attempts.
- Implement a Content Security Policy to restrict which domains can embed your site in iframes. This can help prevent unauthorized framing.
- Implement additional security controls to prevent UI redress attacks, such as clickjacking, within your web application.

10. **Vulnerability name:** web server allows password auto-completion

CWE: 310

Description:
Weaknesses in this category are related to the design and implementation of data confidentiality and integrity. Frequently these deal with the use of encoding techniques, encryption libraries, and hashing algorithms. The weaknesses in this category could lead to a degradation of the quality data if they are not addressed.

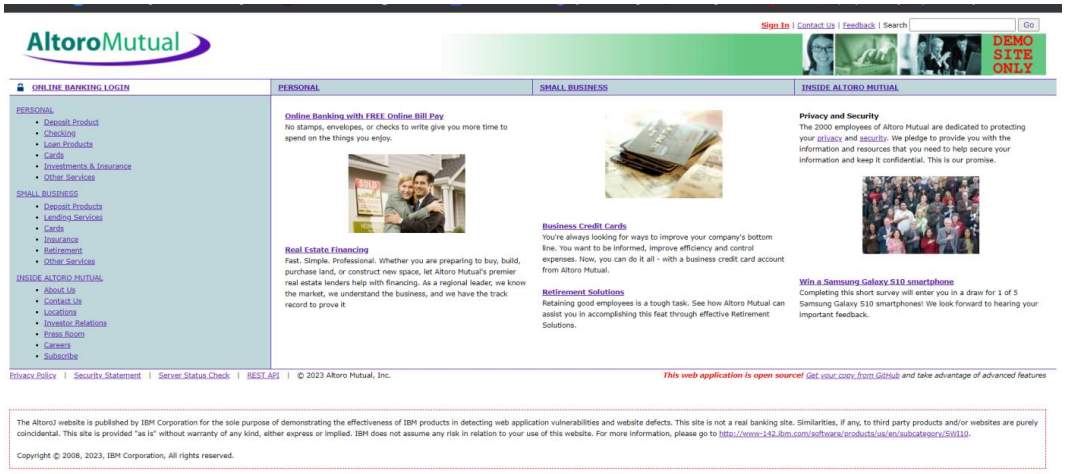
Business impact:
To effectively lessen the business consequences associated with CWE-310, organizations must prioritize the adoption of secure cryptographic practices. This entails ensuring proper password storage and robust encryption key management. Simultaneously, conducting routine security assessments and testing is pivotal in detecting and mitigating vulnerabilities related to cryptographic issues. Striving for compliance with pertinent data protection regulations and industry standards is equally essential. These actions are of paramount importance in the protection of sensitive data, the upholding of user trust, and the preservation of the organization's esteemed reputation.

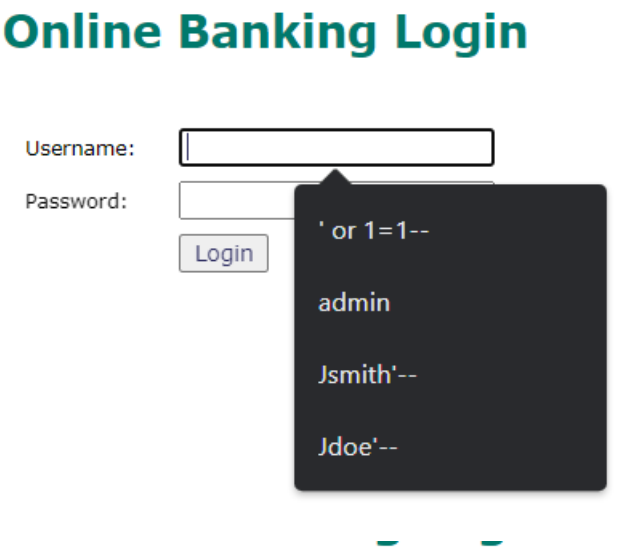
Vulnerability path: http://testfire.net/

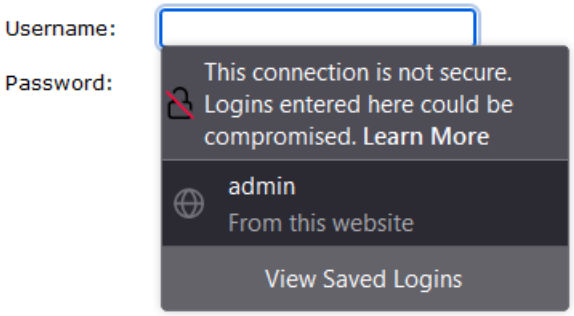
Vulnerability parameter: http://testfire.net/login.jsp

Steps to reproduce:

- Access the URL







- From this image we can see the usernames and the passwords getting auto filled. This is a potential vulnerability as this can be a doorway for attackers.

Responsibilities:

- Implement secure password storage mechanisms, such as using strong and salted cryptographic hashing algorithms like bcrypt or scrypt.
- Implement robust encryption key management practices, including secure key storage, key rotation, and access controls.
- Utilize well-established and proven cryptographic libraries and algorithms for encryption and decryption.
- Use secure encryption protocols, like TLS/SSL, for data transmission over networks to protect data in transit.

11. **Vulnerability name:** Cross-site scripting (DOM based XSS)

CWE: 79

OWASP category: A03: Injections

Description: It occurs when a malicious script is injected directly into a vulnerable web application. Reflected XSS involves the reflection of a malicious script of a web application, onto a user's browser.

DOM-XSS: DOM stands for Document Object Model and is a programming interface for HTML and XML documents. It represents that programs can change the document structure, style and content. A webpage is a document and this document can be either displayed in the browser window or as the HTML Source.

Business Impact: The application stores dangerous data in a database, message forum, visitor log, or other trusted data store. Later, the dangerous data is subsequently read back into the application and included in dynamic content. From an attacker's perspective, the optimal place to inject malicious content is in an area displayed to many users or particularly interesting users. Interesting users typically have elevated privileges in the application or interact with sensitive data that is valuable to the attacker. If one of these users executes malicious content, the attacker may be able to perform privileged operations on behalf of the user or gain access to sensitive data belonging to the user.

Vulnerability path: https://vit.ac.in/

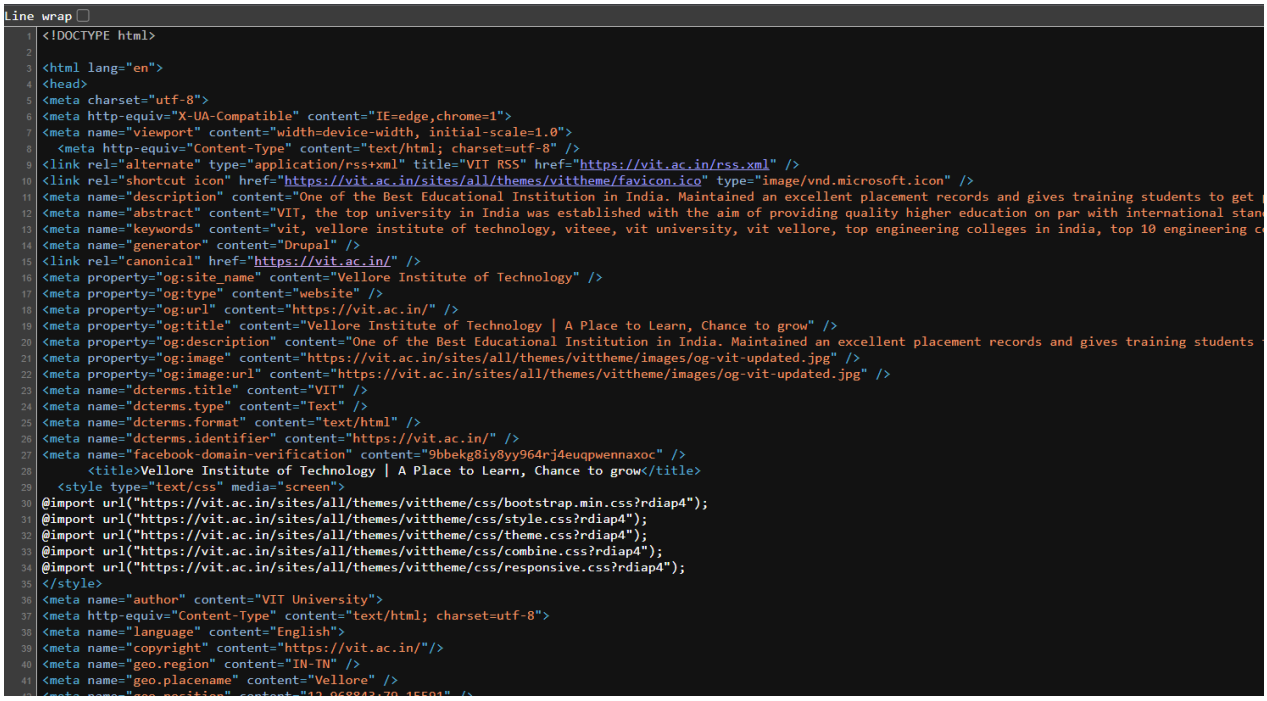
Vulnerability parameter: https://vit.ac.in/

Steps to Reproduce:

- Access the URL

- We will try to perform the DOM XSS attack which is displaying the source code of the webpage.

- Now we can access the source code of the webpage in two ways by clicking on the inspect option or by simply pressing Ctrl + U.



```
Line wrap
<!DOCTYPE html>

<html lang="en">
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
  <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<link rel="alternate" type="application/rss+xml" title="VIT RSS" href="https://vit.ac.in/rss.xml" />
<link rel="shortcut icon" href="https://vit.ac.in/sites/all/themes/vittheme/favicon.ico" type="image/vnd.microsoft.icon" />
<meta name="description" content="One of the Best Educational Institution in India. Maintained an excellent placement records and gives training students to get
<meta name="abstract" content="VIT, the top university in India was established with the aim of providing quality higher education on par with international stan
<meta name="keywords" content="vit, vellore institute of technology, viteee, vit university, vit vellore, top engineering colleges in india, top 10 engineering c
<meta name="generator" content="Drupal" />
<link rel="canonical" href="https://vit.ac.in/" />
<meta property="og:site_name" content="Vellore Institute of Technology" />
<meta property="og:type" content="website" />
<meta property="og:url" content="https://vit.ac.in/" />
<meta property="og:title" content="Vellore Institute of Technology | A Place to Learn, Chance to grow" />
<meta property="og:description" content="One of the Best Educational Institution in India. Maintained an excellent placement records and gives training students
<meta property="og:image" content="https://vit.ac.in/sites/all/themes/vittheme/images/og-vit-updated.jpg" />
<meta property="og:image:url" content="https://vit.ac.in/sites/all/themes/vittheme/images/og-vit-updated.jpg" />
<meta name="dcterms.title" content="VIT" />
<meta name="dcterms.type" content="Text" />
<meta name="dcterms.format" content="text/html" />
<meta name="dcterms.identifier" content="https://vit.ac.in/" />
<meta name="facebook-domain-verification" content="9bbekg8iy8yy964rj4euqpwennaxoc" />
      <title>Vellore Institute of Technology | A Place to Learn, Chance to grow</title>
  <style type="text/css" media="screen">
@import url("https://vit.ac.in/sites/all/themes/vittheme/css/bootstrap.min.css?rdiap4");
@import url("https://vit.ac.in/sites/all/themes/vittheme/css/style.css?rdiap4");
@import url("https://vit.ac.in/sites/all/themes/vittheme/css/theme.css?rdiap4");
@import url("https://vit.ac.in/sites/all/themes/vittheme/css/combine.css?rdiap4");
@import url("https://vit.ac.in/sites/all/themes/vittheme/css/responsive.css?rdiap4");
</style>
<meta name="author" content="VIT University">
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<meta name="language" content="English">
<meta name="copyright" content="https://vit.ac.in/"/>
<meta name="geo.region" content="IN-TN" />
<meta name="geo.placename" content="Vellore" />
```

- Many programs can help to alter this source code to find vulnerable spots.

- So, getting access to the source code of the webpage can lead to potential vulnerabilities as attackers can abuse the loop holes, exploits, vulnerabilities in the code and act accordingly.

Recommendation:

- When interacting with databases, use parameterized statements or prepared statements to avoid SQL injection, which can be a vector for XSS.
- Sanitize and validate all user inputs and ensure that any data displayed on the web page is properly encoded. Use output encoding libraries or functions to prevent script injection.
- Avoid using DOM manipulation methods that can introduce vulnerabilities. Be cautious with inner HTML, document. Write, and other methods that can execute scripts.
- Consider using well-established JavaScript frameworks and libraries that include built-in security features to prevent DOM XSS.

12. **Vulnerability name:** JQuery 1.2 < 3.5.0 Multiple XSS

CWE: 79

OWASP category: A03: Injections

Description: It occurs when a malicious script is injected directly into a vulnerable web application. Reflected XSS involves the reflection of a malicious script of a web application, onto a user's browser.

Stored XSS (Persistent XSS): In this type of attack, the malicious script is permanently stored on a server or in a database, often in user-generated content like comments or forum posts. When other users view the affected content, the script executes in their browsers, potentially compromising their data or sessions.

Reflected XSS: Reflected XSS occurs when the malicious script is embedded in a URL and immediately executed when a victim clicks on a manipulated link. The script is not stored on a server but is reflected off a web application, making it a one-time attack.

DOM-based XSS: DOM stands for Document Object Model and is a programming interface for HTML and XML documents. It represents that programs can change the document structure, style and content. A webpage is a document and this document can be either displayed in the browser window or as the HTML Source.

Business Impact: The application stores dangerous data in a database, message forum, visitor log, or other trusted data store. Later, the dangerous data is subsequently read back into the application and included in dynamic content. From an attacker's perspective, the optimal place to inject malicious content is in an area displayed to many users or particularly interesting users. Interesting users typically have elevated privileges in the application or interact with sensitive data that is valuable to the attacker. If one of these users executes malicious content, the attacker may be able to perform privileged operations on behalf of the user or gain access to sensitive data belonging to the user.

Vulnerability path: https://vit.ac.in/

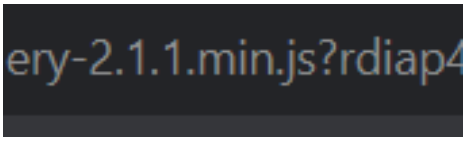
Vulnerability parameter: https://vit.ac.in/sites/all/themes/vittheme/js/jquery-2.1.1.min.js?rdiap4

Steps to Reproduce:

- Access the URL

- Try to access the URL https://vit.ac.in/sites/all/themes/vittheme/js/jquery- . This will lead us to the webpage with jquery script in it.

- We can also see the jquery version that has been used in the website



- We can access the source code of the jquery script that has been used in making the website, which can lead to multiple potential threats

Recommendation:

- The most important recommendation is to update to the latest version of jQuery. Newer versions typically include security patches, bug fixes, and performance improvements.
- Stay vigilant about jQuery updates and security announcements. Subscribe to relevant security mailing lists or forums to receive notifications about new releases.
- A Content Security Policy (CSP) can help mitigate various types of client-side vulnerabilities, including Cross-Site Scripting (XSS). Consider implementing a CSP in your web application to restrict the sources from which scripts can be loaded.
- If updating jQuery is not immediately possible, review your code for potential security issues. Ensure that you are escaping or sanitizing user inputs and that you are using safe coding practices to prevent XSS and other security vulnerabilities.

13. **Vulnerability name:** Information Exposure (Web Server HTTP Header Internal IP Disclosure)

CWE: 200

Description: The product exposes sensitive information to an actor that is not explicitly authorized to have access to that information.

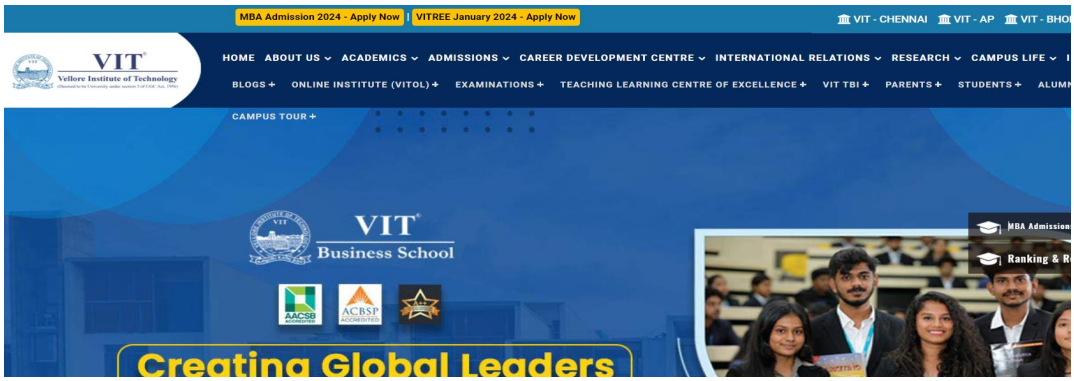
Business Impact: To effectively reduce the business consequences associated with CWE-200, organizations must prioritize the implementation of robust data access controls, secure data handling practices, and privacy protection measures. Regular security assessments and testing are instrumental in detecting and rectifying vulnerabilities related to information exposure. Furthermore, strict adherence to data protection regulations and industry standards is indispensable. These actions are of paramount importance in the protection of sensitive data, the preservation of user trust, and the upholding of the organization's esteemed reputation.

Vulnerability path: https://vit.ac.in/

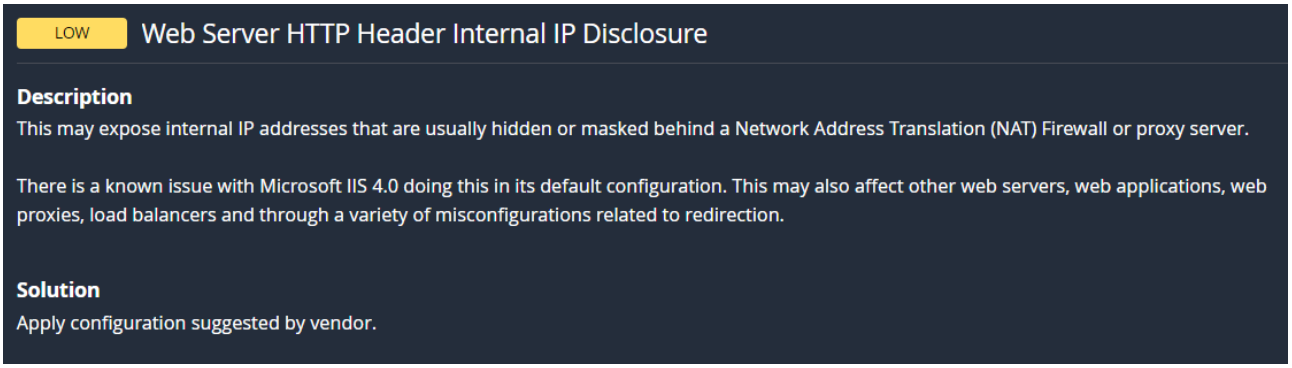
Vulnerability parameter: https://vit.ac.in/

Steps to Reproduce:

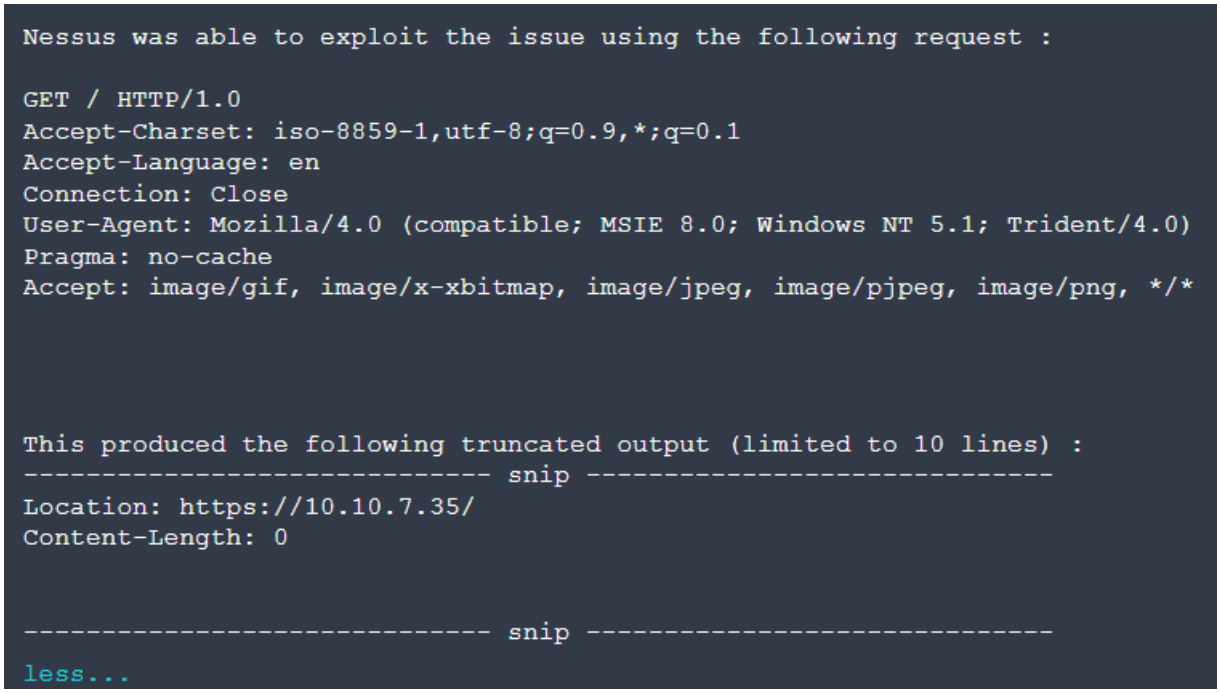
- Access the URL



- We will be using a tool to perform a scan on this website. (Nessus Scanner)



- Through this tool we can see the vulnerability in the scan along with detailed information regarding that vulnerability.



- Now this image tells us the internal IP address of the target website, the attackers can easily exploit the website using the ip address.

Recommendation:

- Carefully review your web server's configuration files (e.g., Apache's httpd.conf, Nginx's nginx.conf) to identify anywhere internal IP addresses are inadvertently included in HTTP response headers.
- Remove or replace any internal IP addresses in the server configuration files with appropriate placeholders or public IP addresses.
- If you use proxy servers or load balancers, ensure that they are configured to hide internal IP addresses and only expose public IP addresses instances in HTTP headers.
- Review and configure HTTP response headers (e.g., Server, X-Powered-By) to limit the exposure of server and technology details, reducing the potential for disclosing internal IP addresses.

14. **Vulnerability name:** Information Exposure (SSL (Multiple Issues))

CWE: 200

Description: The product exposes sensitive information to an actor that is not explicitly authorized to have access to that information.

Business Impact: To effectively reduce the business consequences arising from SSL issues, organizations must give utmost priority to establishing a secure SSL/TLS configuration, conducting frequent security assessments and testing. Adhering to data protection regulations and industry standards is imperative. These actions play a pivotal role in safeguarding sensitive data, upholding user trust, and safeguarding the organization's esteemed reputation.

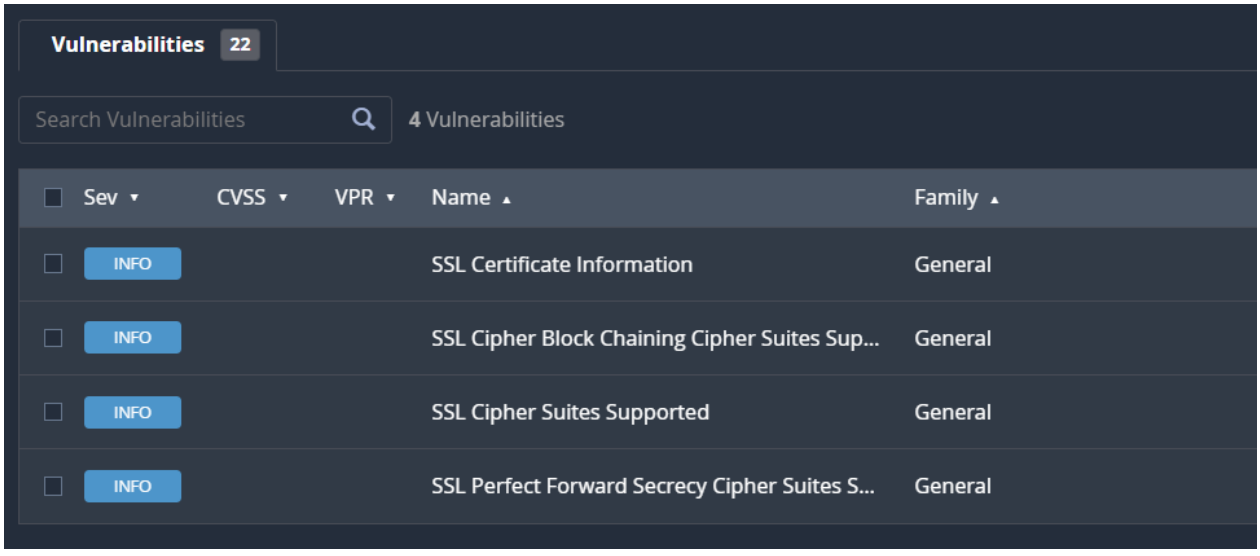
Vulnerability path: https://vit.ac.in/

Vulnerability parameter: https://vit.ac.in/

Steps to Reproduce:

- Access the URL

- We will be using a tool to perform a scan on this website. (Nessus Scanner)



- Through this tool we can see the vulnerability in the scan along with detailed information regarding that vulnerability.

INFO SSL Certificate Information

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Output

```
Subject Name:

Common Name: *.vit.ac.in

Issuer Name:

Country: GB
State/Province: Greater Manchester
Locality: Salford
Organization: Sectigo Limited
Common Name: Sectigo RSA Domain Validation Secure Server CA

Serial Number: 46 53 67 B6 23 C5 BE EE B9 6E E2 C0 5F 46 C9 F7

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Sep 04 00:00:00 2023 GMT
Not Valid After: Aug 03 23:59:59 2024 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
```

- Now this image tells us the type of encryption used in the target website with the public key details as well.

INFO SSL Cipher Block Chaining Cipher Suites Supported

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

INFO SSL Cipher Suites Supported

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

INFO SSL Perfect Forward Secrecy Cipher Suites Supported

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

- Through this we can understand what different types of encryptions are used in the website.

```
Here is the list of SSL CBC ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX          Auth     Encryption             MAC
    ----------------------        ----------        ---          ----     --------------------   ---
    ECDHE-RSA-CAMELLIA-CBC-128    0xC0, 0x76        ECDH         RSA      Camellia-CBC(128)      SHA256
    ECDHE-RSA-CAMELLIA-CBC-256    0xC0, 0x77        ECDH         RSA      Camellia-CBC(256)      SHA384
    DHE-RSA-AES128-SHA            0x00, 0x33        DH           RSA      AES-CBC(128)           SHA1
    DHE-RSA-AES256-SHA            0x00, 0x39        DH           RSA      AES-CBC(256)           SHA1
    DHE-RSA-CAMELLIA128-SHA       0x00, 0x45        DH           RSA      Camellia-CBC(128)      SHA1
    DHE-RSA-CAMELLIA256-SHA       0x00, 0x88        DH           RSA      Camellia-CBC(256)      SHA1
    DHE-RSA-SEED-SHA              0x00, 0x9A        DH           RSA      SEED-CBC(128)          SHA1
    ECDHE-RSA-AES128-SHA          0xC0, 0x13        ECDH         RSA      AES-CBC(128)           SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14        ECDH         RSA      AES-CBC(256)           SHA1
    AES128-SHA                    0x00, 0x2F        RSA          RSA      AES-CBC(128)           SHA1
    AES256-SHA                    0x00, 0x35        RSA          RSA      AES-CBC(256)           SHA1
    CAMELLIA128-SHA               0x00, 0x41        RSA          RSA      Camellia-CBC(128)      SHA1
    CAMELLIA256-SHA               0x00, 0x84        RSA          RSA      Camellia-CBC(256)      SHA1
    SEED-SHA                      0x00, 0x96        RSA          RSA      SEED-CBC(128)          SHA1
    DHE-RSA-AES128-SHA256         0x00, 0x67        DH           RSA      AES-CBC(128)           SHA256
    DHE-RSA-AES256-SHA256         0x00, 0x6B        DH           RSA      AES-CBC(256)           SHA256
    DHE-RSA-CAMELLIA128-SHA256    0x00, 0xBE        DH           RSA      Camellia-CBC(128)      SHA256
    DHE-RSA-CAMELLIA256-SHA256    0x00, 0xC4        DH           RSA      Camellia-CBC(256)      SHA256
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27        ECDH         RSA      AES-CBC(128)           SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28        ECDH         RSA      AES-CBC(256)           SHA384
    RSA-AES128-SHA256             0x00, 0x3C        RSA          RSA      AES-CBC(128)           SHA256
    RSA-AES256-SHA256             0x00, 0x3D        RSA          RSA      AES-CBC(256)           SHA256
    RSA-CAMELLIA128-SHA256        0x00, 0xBA        RSA          RSA      Camellia-CBC(128)      SHA256
    RSA-CAMELLIA256-SHA256        0x00, 0xC0        RSA          RSA      Camellia-CBC(256)      SHA256
```

Recommendation:

- Configure your web server to use the latest and strongest encryption protocols, such as TLS 1.2 or higher. Disable outdated and insecure protocols like SSLv3.
- Implement Perfect Forward Secrecy to ensure that even if the private key is compromised, previously recorded encrypted traffic remains secure.
- Safeguard your private keys by storing them securely and ensuring they are not accessible to unauthorized parties.

15. **Vulnerability name:** Information Exposure (HTTP (Multiple Issues))

CWE: 200

Description: The product exposes sensitive information to an actor that is not explicitly authorized to have access to that information.

Business Impact: To effectively reduce the business repercussions of HTTP issues, organizations must place a strong emphasis on ongoing monitoring and enhancement of their web services. Consistent performance testing and security assessments, coupled with proactive maintenance, are indispensable to ensure a seamless and secure online presence. Furthermore, offering timely and helpful customer support and transparent communication when HTTP issues arise is instrumental in mitigating adverse effects on user trust and satisfaction.

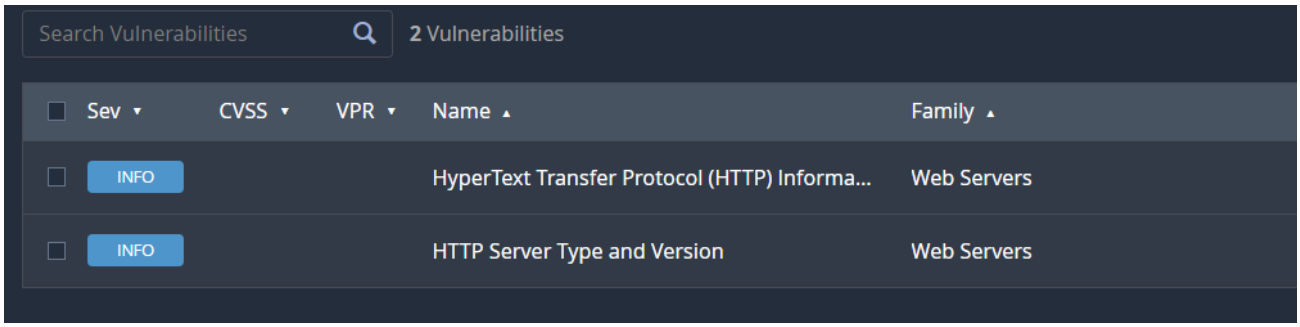
Vulnerability path: https://vit.ac.in/

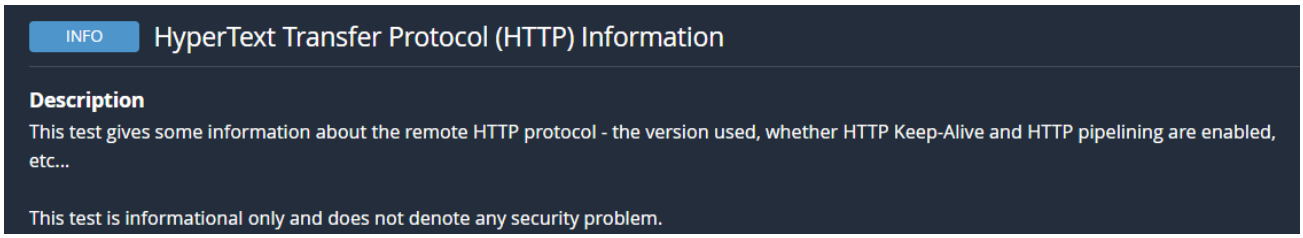
Vulnerability parameter: https://vit.ac.in/

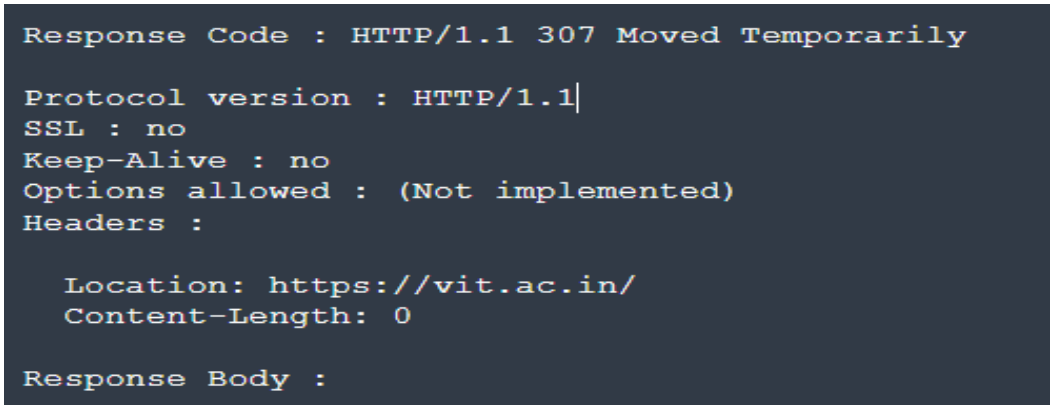
Steps to Reproduce:

- Access the URL

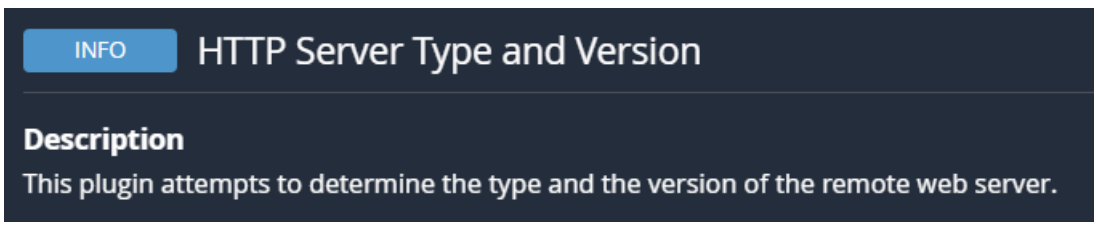
- We will be using a tool to perform a scan on this website. (Nessus Scanner)

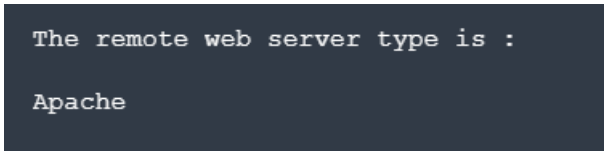






- From the above image we can see the details of protocol version of the website and its status.





- We can see the type of remote webserver here.
- All this information can lead to multiple potential threats such as data breaches by hackers.

Recommendation:

- Minimize the use of unnecessary redirects as they can increase page load times. Use 301 (permanent) redirects for consistent content.
- Regularly check for broken links (404 errors) and fix them to ensure users find the content they are looking for.
- Properly configure CORS to control which domains are allowed to make requests to your server.
- Migrate your website from HTTP to HTTPS to ensure secure data transmission. This is essential for user trust and search engine ranking.

16. **Vulnerability name:** OS Identification Failed

CWE: 200

Description: OS identification failed refers to the inability of a system or software to accurately recognize the operating system running on a device or network. This issue can result from various factors such as misconfigurations, network issues, or compatibility problems. The failure to identify the OS correctly can lead to security vulnerabilities, hindered software updates, and potential operational disruptions. Resolving this issue promptly is crucial to ensure accurate security measures and the smooth functioning of the system or network.

Business Impact: It may lead to operational inefficiencies, potential security vulnerabilities, non-compliance with industry regulations, and a possible loss of customer trust. Such failures could result in downtime, compromised data security, regulatory penalties, and damage to the company's reputation, potentially leading to financial losses and decreased market competitiveness. Resolving this issue promptly is crucial to mitigate these risks and maintain the smooth functioning of the organization.

Vulnerability path: https://vit.ac.in/

Vulnerability parameter: https://vit.ac.in/

Steps to Reproduce:

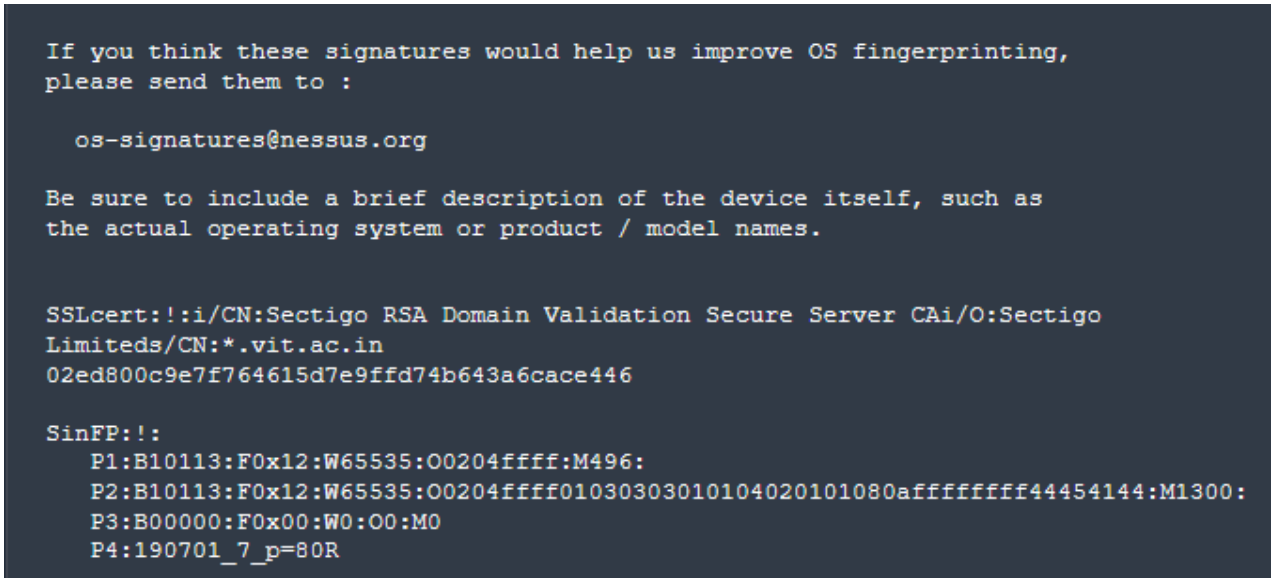
- Access the URL

- We will be using a tool to perform a scan on this website. (Nessus Scanner)

INFO **OS Identification Failed**

Description

Using a combination of remote probes (TCP/IP, SMB, HTTP, NTP, SNMP, etc), it was possible to gather one or more fingerprints from the remote system. Unfortunately, though, Nessus does not currently know how to use them to identify the overall system.



```
If you think these signatures would help us improve OS fingerprinting,
please send them to :

  os-signatures@nessus.org

Be sure to include a brief description of the device itself, such as
the actual operating system or product / model names.


SSLcert:!:i/CN:Sectigo RSA Domain Validation Secure Server CAi/O:Sectigo
Limiteds/CN:*.vit.ac.in
02ed800c9e7f764615d7e9ffd74b643a6cace446

SinFP:!:
   P1:B10113:F0x12:W65535:O0204ffff:M496:
   P2:B10113:F0x12:W65535:O0204ffff010303030101040201010 80affffffff44454144:M1300:
   P3:B00000:F0x00:W0:O0:M0
   P4:190701_7_p=80R
```

- From the above image, we can see the details of SSL Certificate Information and SinFP Information.
- If it is released without proper authorization, it can lead to serious consequences such as increased vulnerability to cyberattacks, potential data breaches, privacy violations, and legal repercussions.
- All this information can lead to multiple potential threats such as data breaches by hackers.

Recommendations:

- Employ robust data encryption methods for both data in transit and at rest.
- Implement strict access controls and authentication protocols to limit unauthorized access.
- Use secure communication channels, such as encrypted email and file transfer protocols.
- Provide comprehensive training to employees on data security best practices.
- Conduct regular security audits and assessments to identify and address vulnerabilities promptly.
- Ensure compliance with relevant data protection regulations and have a well-defined incident response plan in place.

NESSUS SCAN REPORT:

testfire.net

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	3	1	24

Vulnerabilities Total: 28

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	6.5	-	142960	HSTS Missing From HTTPS Server (RFC 6797)
MEDIUM	6.5	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	157288	TLS Version 1.1 Protocol Deprecated
LOW	3.7	4.5	83875	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
INFO	N/A	-	46180	Additional DNS Hostnames
INFO	N/A	-	39446	Apache Tomcat Detection
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	84502	HSTS Missing From HTTPS Server
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	-	11936	OS Identification
INFO	N/A	-	10919	Open Port Re-check
INFO	N/A	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	10863	SSL Certificate Information
INFO	N/A	-	95631	SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)
INFO	N/A	-	70544	SSL Cipher Block Chaining Cipher Suites Supported

INFO	N/A	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	94761	SSL Root Certification Authority Certificate Information
INFO	N/A	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	121010	TLS Version 1.1 Protocol Detection
INFO	N/A	-	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	-	10287	Traceroute Information

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

vit.ac.in

0	0	1	1	26
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 28

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	6.1	5.7	136929	JQuery 1.2 < 3.5.0 Multiple XSS
LOW	3.1	2.2	10759	Web Server HTTP Header Internal IP Disclosure
INFO	N/A	-	48204	Apache HTTP Server Version
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	106658	JQuery Detection
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	42823	Non-compliant Strict Transport Security (STS)
INFO	N/A	-	50350	OS Identification Failed
INFO	N/A	-	66334	Patch Report
INFO	N/A	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	10863	SSL Certificate Information
INFO	N/A	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	94761	SSL Root Certification Authority Certificate Information
INFO	N/A	-	156899	SSL/TLS Recommended Cipher Suites

INFO	N/A	-	22964	Service Detection
INFO	N/A	-	42822	Strict Transport Security (STS) Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	84821	TLS ALPN Supported Protocol Enumeration
INFO	N/A	-	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	100669	Web Application Cookies Are Expired
INFO	N/A	-	10386	Web Server No 404 Error Code Check
INFO	N/A	-	10302	Web Server robots.txt Information Disclosure

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

"With the Nessus scan report now at our disposal, we're equipped with critical data on the existing vulnerabilities and potential threats. This invaluable information will serve as a foundation for our project planning phase, as we chart the course to develop our AI-driven incident response platform with a well-informed strategy and timeline."

Stage – 2

Overview: -

An overview of a Nessus scan typically involves the following key steps and aspects:

1. Preparation: Define Objectives: Determine the scope and objectives of the scan. What systems or networks do you want to assess, and what specific vulnerabilities are you looking for?

   System Access: Ensure that you have the necessary permissions and access rights to scan the target systems or networks.

2. Configuration: Set Up Scan Policy: Create a scan policy that defines the parameters of the scan, such as the types of vulnerabilities to check for, scanning frequency, and specific configurations.

   Define Target Assets: Specify the IP addresses, hostnames, or network ranges of the systems you want to scan.

3. Scanning: Initiate Scan: Start the Nessus scan using the configured policy and target assets. Nessus will systematically scan the target systems for vulnerabilities based on its plugins and policies.

4. Vulnerability Identification: Nessus performs a comprehensive assessment, checking for vulnerabilities, misconfigurations, open ports, and other security issues. As the scan progresses, it categorizes vulnerabilities by severity, making it easier to prioritize remediation efforts.

5. Reporting: Nessus generates detailed reports that list the vulnerabilities discovered during the scan. Reports typically include information about the severity of each vulnerability, recommended actions for remediation, and supporting evidence. These reports can be customized and exported in various formats, such as PDF, HTML, or CSV.

6. Remediation: Review Findings: IT and security teams review the Nessus scan reports to prioritize and address the identified vulnerabilities.

   Remediation Steps: Take corrective actions to fix or mitigate the vulnerabilities. This may involve applying patches, changing configurations, or implementing security measures.

7. Follow-up: Regular Scanning: Conduct periodic Nessus scans to continuously monitor the security posture of the systems and networks. This helps identify new vulnerabilities and track progress in mitigating existing ones.

   Integration: Integrate Nessus with other security tools or workflows to automate the vulnerability management process and streamline the response to new findings.

8. Compliance Auditing (if applicable): If compliance checks are part of your scan policy, review compliance results and take actions to ensure systems meet the required standards and regulations.

9. Documentation: Maintain records of scan results, remediation efforts, and compliance checks for audit and reporting purposes.

10. User Training: Ensure that your IT and security teams are trained in using Nessus effectively and interpreting scan results.

Nessus scans are a critical component of proactive security, helping organizations identify and address vulnerabilities in their IT infrastructure to reduce the risk of security breaches and data compromises. The frequency and depth of scans can vary depending on an organization's security strategy and requirements.

Nessus is a popular vulnerability scanning tool used for identifying security weaknesses in computer systems and networks. It is widely utilized by security professionals and organizations to assess the security posture of

their systems and to proactively identify potential vulnerabilities that could be exploited by attackers. Here's what I understand about Nessus scans:

1. Vulnerability Assessment: Nessus performs a vulnerability assessment by scanning target systems or networks to identify security issues, such as missing patches, misconfigurations, weak passwords, and other potential weaknesses that could be exploited by attackers.

2. Network Scanning: Nessus can scan a wide range of network devices, including servers, routers, switches, firewalls, and more. It examines network services, open ports, and software running on target systems.

3. Plugin Architecture: Nessus uses a plugin-based architecture, allowing it to check for a wide variety of vulnerabilities. These plugins are regularly updated to include the latest security checks and support for new vulnerabilities.

4. Compliance Auditing: It can also be used to assess systems against various compliance standards and regulatory requirements, helping organizations ensure that their systems meet specific security standards, like PCI DSS or CIS benchmarks.

5. Customization: Nessus scans can be customized to suit the specific needs of an organization. Users can define scan policies, select the target systems, and specify the types of vulnerabilities to scan for.

6. Reporting: Nessus provides detailed reports that highlight vulnerabilities, their severity, and remediation recommendations. These reports are essential for IT and security teams to prioritize and address vulnerabilities.

7. Scanning Frequency: Organizations often perform regular Nessus scans to continuously monitor and improve their security posture. This is crucial for staying ahead of evolving threats and vulnerabilities.

8. Integration: Nessus can be integrated with other security tools and platforms, allowing organizations to automate the scanning process and streamline their vulnerability management.

9. Licensing: Nessus offers both free and commercial versions. The free version is limited in its functionality, while the commercial version provides more features and support.

10. User-Friendly Interface: Nessus offers an easy-to-use web-based interface, making it accessible to a wide range of users, from security experts to less experienced IT professionals.

It's important to note that Nessus is a valuable tool for identifying vulnerabilities, but it doesn't fix these vulnerabilities itself. It's up to the organization's IT and security teams to take the necessary steps to remediate the identified issues to enhance their security.

S. No	Vulnerability Name	Severity	Plugins
1.	Cross-site scripting (stored)	Low	Web application Scanner
2.	Broken Access Control	Medium	SSH weak HMAC Algorithms Supported
3.	SQL Injection	Medium	N/A
4.	Broken Authentication	Low	HSTS Missing from Server
5.	Insecure Direct Object Reference	Info	Service Detection
6.	Security Misconfiguration	Low	SSL cipher Block Chaining cipher suites
7.	Cross-Site Request Forgery	Low	HTTP Form- Based Authentication Detected
8.	Cleartext Transmission of Sensitive Information	Medium	Cleartext Transmission of Sensitive Information over HTTP
9.	ClickJacking	Info	HTML Rendering Layer Vulnerability

10.	webserver allows password auto-completion	Low	SSL/TLS Diffie-Hellman Modulus<=1024 bits(Logjam)

Target Website: testfire.net

Target IP Address: 54.83.41.36

Report:

1. **VULNERABILITY NAME:** Cross site scripting (stored)

   SEVERITY: Low

   PLUGIN: web application scanner

   PORT: N/A

   DESCRIPTION: It occurs when a malicious script is injected directly into a vulnerable web application. Reflected XSS involves the reflection of a malicious script of a web application, onto a user's browser.

   SOLUTION:
   - When interacting with databases, use parameterized statements or prepared statements to avoid SQL injection, which can be a vector for XSS.
   - Sanitize and validate all user inputs and ensure that any data displayed on the web page properly encoded. Use output encoding libraries or functions to prevent script injection.

   BUSINESS IMPACT: The application stores dangerous data in a database, message forum, visitor log, or other trusted data store. Later, the dangerous data is subsequently read back into the application and included in dynamic content. From an attacker's perspective, the optimal place to inject malicious content is in an area that is displayed to either many users or particularly interesting users. Interesting users typically have elevated privileges in the application or interact with sensitive data that is valuable to the attacker. If one of these users executes malicious content, the attacker may be able to perform privileged operations on behalf of the user or gain access to sensitive data belonging to the user.

2. **VULNERABILITY NAME:** Broken access control

   SEVERITY: medium

   PLUGIN: SSH weak HMAC Algorithms supported

   PORT: N/A

   DESCRIPTION: When access control checks are not applied consistently - or not at all - users are able to access data or perform actions that they should not be allowed to perform. This can lead to a wide range of problems, including information exposures, denial of service, and arbitrary code execution.

   SOLUTION:

- Ensure that the application has a robust authentication and authorization mechanism in place. Users should be authenticated before any sensitive actions are performed, and authorization checks should be conducted to verify that users have the necessary permissions for the requested operation.
- Ensure that session management is secure. Use strong session IDs, enforce session timeouts, and regenerate session tokens after login. Implement session fixation protection to prevent session hijacking.

BUSINESS IMPACT: wide-ranging business impact, including financial losses, reputation damage, legal consequences, operational disruption, and loss of customer trust. Addressing this vulnerability is crucial to protect the organization and its stakeholders from these potential negative effects.

3. **VULNERABILITY NAME:** SQL injection

   SEVERITY: medium

   PLUGIN: N/A (typically would be a security testing tool)

   PORT: port 80/443

   DESCRIPTION: The product constructs all or part of an SQL command using externally influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended SQL command when it is sent to a downstream component.

   SOLUTION:
   - If parameterized statements are not feasible, use proper input validation and escaping mechanisms to sanitize user inputs before they are used in SQL queries. This helps prevent malicious code injection.
   - Utilize stored procedures for database operations. This can help separate SQL code from application code and reduce the risk of SQL injection.
   - Implement strict input validation for all user inputs, ensuring that data adheres to the expected format and structure.

   BUSINESS IMPACT: In summary, it is crucial to underscore that CWE-89, known as SQL Injection, can exert a profound and diverse business impact. This encompasses critical facets such as data breaches, financial setbacks, harm to reputation, legal ramifications, and operational turmoil. Hence, the imperative of preventing and remedying SQL injection vulnerabilities cannot be overstated, as it is indispensable for fortifying the security and continuity of an organization's applications and data.

4. **VULNERABILITY NAME:** Broken authentication

   SEVERITY: Low

   PLUGIN: HSTS Missing from HTTPS Server (plugin id:142960)

   PORT: port 443

DESCRIPTION: The system's authorization functionality does not prevent one user from gaining access to another user's data or record by modifying the key value identifying the data.

SOLUTION:

- Implement strong authentication mechanisms, such as multi-factor authentication (MFA) or two-factor authentication (2FA), to ensure that only authorized users can access the system.
- Implement proper authorization controls to ensure that users have the necessary permissions to access specific functions or data. Use role-based access control (RBAC) to manage user privileges effectively.
- Deploy intrusion detection and prevention systems (IDS/IPS) to monitor and block suspicious activities related to authentication and authorization.

BUSINESS IMPACT: To effectively mitigate the business impact of CWE-285, it is imperative that organizations place a strong emphasis on bolstering their authentication and session management practices. This should encompass the adoption of multi-factor authentication, the secure storage of credentials, meticulous session handling, and a commitment to conducting routine security assessments and testing. The rectification of these vulnerabilities stands as a critical imperative, safeguarding sensitive data, user identities, and the organization's overarching security stature and reputation.

5. **VULNERABILITY NAME:** Insecure Direct object Reference

SEVERITY: Info

PLUGIN: Service Detection (plugin id:22964)

PORT: port 80/443

DESCRIPTION: Insecure Direct Object Reference (IDOR) is a vulnerability that arises when attackers can access or modify objects by manipulating identifiers used in a web application's URLs or parameters. It occurs due to missing access control checks, which fail to verify whether a user should be allowed to access specific data.

SOLUTION:

- Utilize parameterized queries or prepared statements when interacting with databases. This prevents user-controlled input from being executed as SQL code.
- Implement a Content Security Policy to mitigate the risk of cross-site scripting (XSS) attacks, which can be used to execute unauthorized queries.
- Implement account lockout mechanisms that temporarily suspend accounts after a specified number of unauthorized access attempts to prevent brute force attacks.

BUSINESS IMPACT: To effectively mitigate the business impact of CWE-639, organizations must make it a top priority to fortify their access control and authorization mechanisms. This entails the implementation of robust security measures, the regular conduct of comprehensive security assessments, and the deployment of intrusion detection systems to promptly identify and counter unauthorized access attempts. These measures stand as critical in the defence of sensitive data, the overall security of systems, and the preservation of the organization's esteemed reputation.

6. **VULNERABILITY NAME:** Security Misconfiguration

SEVERITY: low

PLUGIN: SSL cipher Block chaining cipher suites

PORT: port 443

DESCRIPTION: The product specifies permissions for a security-critical resource in a way that allows that resource to be read or modified by unintended actors.

SOLUTION:

- Implement a change management process to document and review all changes to system configurations. This helps prevent unauthorized or unintended alterations.
- Follow security guidelines provided by software and hardware vendors to ensure secure configurations.
- Regularly perform compliance checks against industry standards and regulations to ensure that configurations remain in compliance with security requirements.

BUSINESS IMPACT: To effectively lessen the business consequences stemming from CWE-732, organizations must place a strong emphasis on bolstering their configuration management practices. This involves the establishment of secure default settings, the routine conduct of comprehensive security evaluations, and the deployment of intrusion detection systems to promptly detect and address misconfigurations and vulnerabilities. These actions are of paramount importance in safeguarding sensitive data, fortifying system security, and preserving the organization's esteemed reputation.

7. **VULNERABILITY NAME:** Cross-Site Request Forgery

SEVERITY: Low

PLUGIN: HTTP Form-Based Authentication Detected

PORT: port 8080/443

DESCRIPTION: Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated. With a little help of social engineering (such as sending a link via email or chat), an attacker may trick the users of a web application into executing actions of the attacker's choosing. If the victim is a normal user, a successful CSRF attack can force the user to perform state changing requests like transferring funds, changing their email address, and so forth. If the victim is an administrative account, CSRF can compromise the entire web application.

SOLUTION:

- Implement Synchronizer Token Patterns to include unique, randomly generated tokens in each HTTP request and validate these tokens on the server side to verify the authenticity of the request.
- Utilize the Same Site attribute in cookies to restrict their usage to same-site requests only, preventing them from being sent along with cross-site requests and effectively mitigating CSRF attacks.

- Utilize framework-specific protections and security features to prevent CSRF attacks. Many modern web frameworks have built-in mechanisms and libraries for handling CSRF vulnerabilities effectively.
- Implement a Content Security Policy to restrict the sources from which various types of content can be loaded. By specifying the trusted sources of content, you can minimize the risk of malicious code execution and reduce the likelihood of successful CSRF attacks.

BUSINESS IMPACT: To effectively reduce the business repercussions of CWE-352, organizations must prioritize secure coding practices, including the incorporation of anti-CSRF tokens, while also conducting routine security assessments and testing to detect and rectify CSRF vulnerabilities. Furthermore, educating users on secure browsing practices is pivotal in preventing CSRF attacks. These actions are of paramount importance in the protection of data and in upholding the trust of customers and partners.

8. **VULNERABILITY NAME:** Cleartext Transmission of Sensitive Information

SEVERITY: Medium

PLUGIN: Cleartext Transmission of Sensitive Information over HTTP

PORT: port 443

DESCRIPTION: The product transmits sensitive or security-critical data in cleartext in a communication channel that can be sniffed by unauthorized actors. Many communication channels can be "sniffed" (monitored) by adversaries during data transmission. For example, in networking, packets can traverse many intermediary nodes from the source to the destination, whether across the internet, an internal network, the cloud, etc. Some actors might have privileged access to a network interface or any link along the channel, such as a router, but they might not be authorized to collect the underlying data. As a result, network traffic could be sniffed by adversaries, spilling security-critical data.

SOLUTION:
- Educate users and employees on secure data handling practices, such as recognizing secure websites (look for "https") and avoiding insecure Wi-Fi networks.
- Employ data masking or redaction techniques to replace sensitive data with placeholders or cryptographic representations during transmission.
- Implement encryption for data in transit. Use secure encryption protocols such as TLS/SSL to protect sensitive information during transmission.
- Use secure communication protocols for transmitting data, such as HTTPS for web applications, and ensure that the selected protocols are kept up to date.

BUSINESS IMPACT: To effectively reduce the business consequences associated with CWE-319, organizations must prioritize the adoption of secure data transmission practices. This includes the utilization of encryption and robust, secure protocols. The routine conduct of security assessments and testing is pivotal in pinpointing and remedying vulnerabilities linked to data transmission. Furthermore, the education of users on secure data handling practices plays a vital role in proactively preventing data exposure incidents. These actions are of paramount importance in the protection of sensitive data and in preserving the trust of both customers and partners.

9. **VULNERABILITY NAME:** Clickjacking

SEVERITY: Info

PLUGIN: HTML Rendering Layer Vulnerability

PORT: port 80/443

DESCRIPTION: The web application does not restrict or incorrectly restricts frame objects or UI layers that belong to another application or domain, which can lead to user confusion about which interface the user is interacting with.

SOLUTION:

- Set the X-Frame-Options HTTP response header to deny or same-origin to control how your site can be framed. This is supported by most modern browsers.
- Utilize frame-busting JavaScript code in web applications to prevent the embedding of your site within malicious frame's. This code can disrupt clickjacking attempts.
- Implement a Content Security Policy to restrict which domains can embed your site in iframes. This can help prevent unauthorized framing.
- Implement additional security controls to prevent UI redress attacks, such as clickjacking, within your web application.

BUSINESS IMPACT: To effectively reduce the business consequences resulting from CWE-1021, organizations must prioritize the implementation of protective measures, such as frame-busting code. Simultaneously, educating users on safe browsing practices plays a crucial role in preventing clickjacking incidents. Additionally, routine security assessments and testing are pivotal for identifying and mitigating vulnerabilities associated with clickjacking. These actions are of paramount importance in upholding user trust, ensuring data protection, and safeguarding the organization's reputation.

10. **VULNERABILITY NAME:** web server allows password auto-completion

SEVERITY: Low

PLUGIN: SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)

PORT: port 443

DESCRIPTION: Weaknesses in this category are related to the design and implementation of data confidentiality and integrity. Frequently these deal with the use of encoding techniques, encryption libraries, and hashing algorithms. The weaknesses in this category could lead to a degradation of the quality data if they are not addressed.

SOLUTION:

- Implement secure password storage mechanisms, such as using strong and salted cryptographic hashing algorithms like crypt or script.
- Implement robust encryption key management practices, including secure key storage, key rotation, and access controls.
- Utilize well-established and proven cryptographic libraries and algorithms for encryption and decryption.

- Use secure encryption protocols, like TLS/SSL, for data transmission over networks to protect data in transit

BUSINESS IMPACT: To effectively lessen the business consequences associated with CWE-310, organizations must prioritize the adoption of secure cryptographic practices. This entails ensuring proper password storage and robust encryption key management. Simultaneously, conducting routine security assessments and testing is pivotal in detecting and mitigating vulnerabilities related to cryptographic issues. Striving for compliance with pertinent data protection regulations and industry standards is equally essential. These actions are of paramount importance in the protection of sensitive data, the upholding of user trust, and the preservation of the organization's esteemed reputation.

S. NO	VULNERABILITY NAME	SEVERITY	PLUGINS
1.	Cross-site scripting (DOM based XSS)	Medium	Multiple XSS
2.	jQuery 1.3<3.5.0 Multiple XSS	Medium	CGI Abuse: XSS
3.	Information exposure (web server HTTP header internal IP disclosure)	Low	Webserver HTTP Header Internal IP Disclosure
4.	Information exposure (SSL (Multiple Issues))	Info	SSL Certificate Information
5.	Information exposure (HTTP (Multiple Issues))	Info	HTTP Information
6.	OS identification failed	Info	TCP/IP Remote Probing

TARGET WEBSITE: vit.ac.in

TARGET IP ADDRESS: 122.184.65.22

Report:

1. **VULNERABILITY NAME:** Cross-site scripting (DOM based XSS)

   SEVERITY: Medium

   PLUGIN: Multiple XSS

   PORT: port 443

   DESCRIPTION: It occurs when a malicious script is injected directly into a vulnerable web application. Reflected XSS involves the reflection of a malicious script of a web application, onto a user's browser. DOM-XSS: DOM stands for Document Object Model and is a programming interface for HTML and XML documents. It represents that programs can change the document structure, style and content. A webpage is a document, and this document can be either displayed in the browser window or as the HTML Source.

SOLUTION:

- When interacting with databases, use parameterized statements or prepared statements to avoid SQL injection, which can be a vector for XSS.
- Sanitize and validate all user inputs and ensure that any data displayed on the web page is properly encoded. Use output encoding libraries or functions to prevent script injection.
- Avoid using DOM manipulation methods that can introduce vulnerabilities. Be cautious with inner HTML, document. Write, and other methods that can execute scripts.
- Consider using well-established JavaScript frameworks and libraries that include built-in security features to prevent DOM XSS.

BUSINESS IMPACT: The application stores dangerous data in a database, message forum, visitor log, or other trusted data store. Later, the dangerous data is subsequently read back into the application and included in dynamic content. From an attacker's perspective, the optimal place to inject malicious content is in an area displayed to many users or particularly interesting users. Interesting users typically have elevated privileges in the application or interact with sensitive data that is valuable to the attacker. If one of these users executes malicious content, the attacker may be able to perform privileged operations on behalf of the user or gain access to sensitive data belonging to the user.

2. **VULNERABILITY NAME:** jQuery 1.2 < 3.5.0 Multiple XSS

SEVERITY: Medium

PLUGIN: CGI Abuse: XSS

PORT: port 443

DESCRIPTION: It occurs when a malicious script is injected directly into a vulnerable web application. Reflected XSS involves the reflection of a malicious script of a web application, onto a user's browser. Stored XSS (Persistent XSS): In this type of attack, the malicious script is permanently stored on a server or in a database, often in user-generated content like comments or forum posts. When other users view the affected content, the script executes in their browsers, potentially compromising their data or sessions. Reflected XSS: Reflected XSS occurs when the malicious script is embedded in a URL and immediately executed when a victim clicks on a manipulated link. The script is not stored on a server but is reflected off a web application, making it a one-time attack. DOM-based XSS: DOM stands for Document Object Model and is a programming interface for HTML and XML documents. It represents that programs can change the document structure, style and content. A webpage is a document, and this document can be either displayed in the browser window or as the HTML Source.

SOLUTION:

- The most important recommendation is to update to the latest version of jQuery. Newer versions typically include security patches, bug fixes, and performance improvements.
- Stay vigilant about jQuery updates and security announcements. Subscribe to relevant security mailing lists or forums to receive notifications about new releases.
- A Content Security Policy (CSP) can help mitigate various types of client-side vulnerabilities, including Cross-Site Scripting (XSS). Consider implementing a CSP in your web application to restrict the sources from which scripts can be loaded.

- If updating jQuery is not immediately possible, review your code for potential security issues. Ensure that you are escaping or sanitizing user inputs and that you are using safe coding practices to prevent XSS and other security vulnerabilities.

BUSINESS IMPACT: The application stores dangerous data in a database, message forum, visitor log, or other trusted data store. Later, the dangerous data is subsequently read back into the application and included in dynamic content. From an attacker's perspective, the optimal place to inject malicious content is in an area displayed to many users or particularly interesting users. Interesting users typically have elevated privileges in the application or interact with sensitive data that is valuable to the attacker. If one of these users executes malicious content, the attacker may be able to perform privileged operations on behalf of the user or gain access to sensitive data belonging to the user.

3. **VULNERABILITY NAME:** Information Exposure (Web Server HTTP Header Internal IP Disclosure)

   SEVERITY: Low

   PLUGIN: Web Server HTTP Header Internal IP Disclosure

   PORT: port 80

   DESCRIPTION: The product exposes sensitive information to an actor that is not explicitly authorized to have access to that information.

   SOLUTION:
   - Carefully review your web server's configuration files (e.g., Apache's httpd.conf, Nginx's nginx.conf) to identify anywhere internal IP addresses are inadvertently included in HTTP response headers.
   - Remove or replace any internal IP addresses in the server configuration files with appropriate placeholders or public IP addresses.
   - If you use proxy servers or load balancers, ensure that they are configured to hide internal IP addresses and only expose public IP addresses instances in HTTP headers.
   - Review and configure HTTP response headers (e.g., Server, X-Powered-By) to limit the exposure of server and technology details, reducing the potential for disclosing internal IP addresses.

   BUSINESS IMPACT: To effectively reduce the business consequences arising from SSL issues, organizations must give utmost priority to establishing a secure SSL/TLS configuration, conducting frequent security assessments and testing. Adhering to data protection regulations and industry standards is imperative. These actions play a pivotal role in safeguarding sensitive data, upholding user trust, and safeguarding the organization's esteemed reputation.

4. **VULNERABILITY NAME:** Information Exposure (SSL (Multiple Issues))

   SEVERITY: Info

   PLUGIN: SSL certificate Information

   PORT: port 443

DESCRIPTION: The product exposes sensitive information to an actor that is not explicitly authorized to have access to that information.

SOLUTION:

- Configure your web server to use the latest and strongest encryption protocols, such as TLS 1.2 or higher. Disable outdated and insecure protocols like SSLv3.
- Implement Perfect Forward Secrecy to ensure that even if the private key is compromised, previously recorded encrypted traffic remains secure.
- Safeguard your private keys by storing them securely and ensuring they are not accessible to unauthorized parties.

BUSINESS IMPACT: To effectively reduce the business consequences arising from SSL issues, organizations must give utmost priority to establishing a secure SSL/TLS configuration, conducting frequent security assessments and testing. Adhering to data protection regulations and industry standards is imperative. These actions play a pivotal role in safeguarding sensitive data, upholding user trust, and safeguarding the organization's esteemed reputation.

5. **VULNERABILITY NAME:** Information Exposure (HTTP (Multiple Issues))

SEVERITY: Info

PLUGIN: HTTP information

PORT: port 80 /443

DESCRIPTION: The product exposes sensitive information to an actor that is not explicitly authorized to have access to that information

SOLUTION:

- Minimize the use of unnecessary redirects as they can increase page load times. Use 301 (permanent) redirects for consistent content.
- Regularly check for broken links (404 errors) and fix them to ensure users find the content they are looking for.
- Properly configure CORS to control which domains are allowed to make requests to your server.
- Migrate your website from HTTP to HTTPS to ensure secure data transmission. This is essential for user trust and search engine ranking.

BUSINESS IMPACT: To effectively reduce the business repercussions of HTTP issues, organizations must place a strong emphasis on ongoing monitoring and enhancement of their web services. Consistent performance testing and security assessments, coupled with proactive maintenance, are indispensable to ensure a seamless and secure online presence. Furthermore, offering timely and helpful customer support and transparent communication when HTTP issues arise is instrumental in mitigating adverse effects on user trust and satisfaction.

6. **VULNERABILITY NAME:** OS Identification Failed

SEVERITY: Info

PLUGIN: TCP/IP remote probing

PORT: N/A

DESCRIPTION: OS identification failed refers to the inability of a system or software to accurately recognize the operating system running on a device or network. This issue can result from various factors such as misconfigurations, network issues, or compatibility problems. The failure to identify the OS correctly can lead to security vulnerabilities, hindered software updates, and potential operational disruptions. Resolving this issue promptly is crucial to ensure accurate security measures and the smooth functioning of the system or network.

SOLUTION:

- Minimize the use of unnecessary redirects as they can increase page load times. Use 301 (permanent) redirects for consistent content.
- Regularly check for broken links (404 errors) and fix them to ensure users find the content they are looking for.
- Properly configure CORS to control which domains are allowed to make requests to your server.
- Migrate your website from HTTP to HTTPS to ensure secure data transmission. This is essential for user trust and search engine ranking.

BUSINESS IMPACT: It may lead to operational inefficiencies, potential security vulnerabilities, non-compliance with industry regulations, and a possible loss of customer trust. Such failures could result in downtime, compromised data security, regulatory penalties, and damage to the company's reputation, potentially leading to financial losses and decreased market competitiveness. Resolving this issue promptly is crucial to mitigate these risks and maintain the smooth functioning of the organization.

Stage – 3

Title:

The SOC/SIEM Cycle: Empowering Security Teams to Detect, Respond, and Recover from Cyberattacks

- **SOC (Security Operations Center)**
  A security operations center (SOC) is a centralized team of security professionals responsible for monitoring and protecting an organization's IT infrastructure from cyberattacks. SOCs use a variety of tools and technologies to collect and analyze security data, identify threats, and respond to incidents.
  SOCs are an essential part of any organization's security posture. They help to protect organizations from a wide range of cyber threats, including malware, phishing attacks, and denial-of-service attacks. SOCs also play a vital role in incident response, helping organizations to mitigate the damage from cyberattacks and recover as quickly as possible.

- **SOC Cycle**

The SOC cycle is a continuous process of detecting, responding, and recovering from cyberattacks. It typically consists of the following steps:

1. Data collection: SOCs collect data from a variety of sources, including network devices, security appliances, and application servers. This data may include network traffic logs, firewall logs, and application logs.
2. Data aggregation and normalization: The collected data is aggregated and normalized so that it can be easily analyzed. This involves converting the data to a common format and structure.
3. Log analysis: SOCs use a variety of tools and techniques to analyze the collected data to identify potential threats and security incidents. This may involve using signature-based detection, anomaly detection, and machine learning.
4. Threat detection: When a threat is detected, the SOC team investigates the incident to determine the scope and impact of the threat. This may involve collecting additional data and analyzing the threat using a variety of tools and techniques.
5. Incident response: Once the SOC team has a good understanding of the threat, they will take steps to mitigate the damage and prevent the threat from spreading. This may involve isolating the affected systems, patching vulnerabilities, and notifying users of the incident.
6. Recovery: After the incident has been mitigated, the SOC team will take steps to help the organization recover. This may involve restoring data from backups, reimaging systems, and implementing new security controls.

- **SIEM (Security Information and Event Management)**

Security Information and Event Management (SIEM) is a security solution that helps organizations collect, analyze, and respond to security events from various sources. It provides a centralized view of security data, making it easier for security teams to identify and investigate potential threats.
SIEM systems collect data from a variety of sources, including:

1. Network devices, such as firewalls, routers, and switches
2. Security appliances, such as intrusion detection systems (IDS) and intrusion prevention systems (IPS)
3. Application servers
4. Operating systems
5. Databases

SIEM systems then analyze the collected data to identify potential threats. This analysis may involve using a variety of techniques, including:

1. Signature-based detection: SIEM systems can match collected data against known threat signatures to identify known threats.
2. Anomaly detection: SIEM systems can identify anomalous behavior in the collected data that may indicate a threat.
3. Machine learning: SIEM systems can use machine learning to identify patterns in the collected data that may indicate a threat.

- SIEM Cycle

The SIEM cycle is like the SOC cycle, but it focuses on the collection, analysis, and management of security data. The SIEM cycle typically consists of the following steps:

1. Data collection: SIEMs collect data from a variety of sources, including network devices, security appliances, and application servers.
2. Data normalization: The collected data is normalized so that it can be easily analyzed.
3. Log correlation: SIEMs correlate events from different sources to identify patterns and anomalies that may indicate a threat.
4. Alert generation: SIEMs generate alerts when they detect potential threats.
5. Incident response: SIEMs can be integrated with other security tools to help SOC teams respond to incidents.
6. Reporting and dashboards: SIEMs can generate reports and dashboards that provide SOC teams with insights into their security posture.

- MISP (Malware Information Sharing Platform)

1. MISP (Malware Information Sharing Platform) is an open-source threat intelligence platform that allows organizations to share and collaborate on threat information. MISP can be used to share information about malware, vulnerabilities, and other threats.
2. MISP is a valuable tool for organizations of all sizes. It can help organizations to:
3. Improve their security posture by identifying and responding to threats more quickly and effectively.
4. Reduce the risk of cyberattacks by detecting and blocking threats before they can cause damage.
5. Improve their compliance with security regulations, such as the General Data Protection Regulation (GDPR).
6. Reduce downtime caused by cyberattacks by responding to incidents quickly and effectively.
7. Improve customer confidence by demonstrating that they are taking steps to protect their data.

- Your college network information

Vellore Institute of Technology (VIT) has a large and complex network that supports over 40,000 students, faculty, and staff. The network includes a variety of devices and technologies, including:

- Core routers and switches
- Distribution routers and switches
- Access switches
- Wireless access points
- Firewalls
- Intrusion detection systems
- Load balancers
- Content filters

- VPN servers

The VIT network is designed to be highly reliable and available. The core network is redundant, with multiple paths between devices. The network is also monitored 24/7 by a team of network engineers.
The VIT network provides a variety of services to students, faculty, and staff, including:

- Internet access
- Email
- Wireless access
- File sharing
- Voice over IP (VoIP)

Access to campus resources, such as the library and student information system
The VIT network is a critical asset to the university. It supports the teaching, learning, and research activities of students, faculty, and staff.

- **How you think you deploy SOC in your college**

To deploy a SOC in VIT college, you would need to start by identifying the specific needs of the institution. This would involve considering the size and complexity of your network, the types of threats you are most concerned about, and your budget.
Once you have identified your needs, you would need to develop a plan for deploying and managing a SOC. This plan would need to include the following:

1. Identifying the resources, you need: This would include personnel, tools, and technology.
2. Developing a process for collecting, analysing, and responding to security data: This would include developing procedures for incident response and threat intelligence sharing.
3. Integrating your SOC with other security tools: This would include integrating your SIEM with other security tools, such as firewalls and intrusion detection systems.

- **Threat intelligence**

Threat intelligence is information about existing and potential cyber threats. It can be used by organizations to improve their security posture by helping them to identify, prioritize, and mitigate threats.
Threat intelligence can come from a variety of sources, including:

1. Open-source intelligence (OSINT): OSINT is information that is publicly available, such as news reports, social media posts, and security blogs.
2. Closed-source intelligence (CSINT): CSINT is information that is not publicly available, such as information from government agencies and security vendors.
3. Human intelligence (HUMINT): HUMINT is information that is collected from human sources, such as informants and undercover operatives.

Threat intelligence can be used for a variety of purposes, including:

1. Identifying new threats: Threat intelligence can be used to identify new threats that are not yet known to the security community.
2. Understanding threat actors: Threat intelligence can be used to understand the motivations, capabilities, and tactics of threat actors.
3. Prioritizing threats: Threat intelligence can be used to prioritize threats based on their likelihood and impact.
4. Mitigating threats: Threat intelligence can be used to mitigate threats by implementing appropriate security controls.

- **Incident response**

Incident response is the process of detecting, responding to, and recovering from cyberattacks. It is a continuous process that involves a variety of activities, including:

1. Detection: Identifying and assessing the scope of a cyberattack.
2. Containment: Stopping the attack from spreading and causing further damage.
3. Eradication: Removing the malicious code or threat from the affected systems.
4. Recovery: Restoring the affected systems to their original state.
5. Post-incident review: Learning from the incident and improving the organization's security posture.

Incident response is a critical part of any organization's security program. It helps organizations to minimize the damage caused by cyberattacks and get back to business as quickly as possible.
Here are some of the benefits of having an incident response plan:

1. Reduced downtime: Incident response plans help organizations to reduce downtime caused by cyberattacks. This is because they provide a clear and concise roadmap for responding to incidents.
2. Reduced risk of data breaches: Incident response plans help organizations to reduce the risk of data breaches. This is because they help organizations to identify and contain incidents quickly and effectively.
3. Compliance: Incident response plans can help organizations to comply with security regulations, such as the General Data Protection Regulation (GDPR). This is because they require organizations to have a plan in place for responding to data breaches.
4. Improved customer confidence: Incident response plans can help to improve customer confidence by demonstrating that the organization is taking steps to protect their data.

- QRadar

IBM QRadar is a security information and event management (SIEM) platform that helps organizations collect, analyze, and respond to security threats. It uses a variety of technologies, including machine learning and artificial intelligence, to identify and prioritize threats, as well as provide insights into security trends.
QRadar is a modular platform that can be customized to meet the specific needs of an organization. It includes a variety of features, such as:

1. Log collection and aggregation: QRadar collects logs from a variety of sources, including network devices, security appliances, and applications. It then aggregates the logs into a single repository for analysis.
2. Log analysis and correlation: QRadar uses a variety of techniques to analyze and correlate logs, including machine learning and artificial intelligence. This allows it to identify patterns and anomalies that may indicate a security threat.
3. Alerting and reporting: QRadar generates alerts when it detects a potential threat. It also provides a variety of reports that can be used to track security trends and identify areas for improvement.
4. Incident response: QRadar can be integrated with other security tools to help organizations respond to security incidents. For example, it can be integrated with a security orchestration, automation, and response (SOAR) platform to automate the incident response process.

- Understanding about the tool

QRadar is a security information and event management (SIEM) platform that helps organizations collect, analyze, and respond to security threats. It is a powerful tool that can be used to improve an organization's security posture by detecting threats early, prioritizing threats, responding to threats quickly, and improving security posture.
Here are some of the key things to understand about QRadar:

1. It is a modular platform: QRadar is a modular platform that can be customized to meet the specific needs of an organization. This means that organizations can choose the features and modules that they need, and they can also scale QRadar to meet their growing needs.
2. It uses a variety of technologies: QRadar uses a variety of technologies, including machine learning and artificial intelligence, to identify and prioritize threats. This allows QRadar to be more effective at detecting and responding to threats than traditional SIEM solutions.
3. It provides insights into security trends: QRadar generates reports that can be used to track security trends and identify areas for improvement. This information can be used to improve the organization's security posture and reduce the risk of future security incidents.
4. It can be integrated with other security tools: QRadar can be integrated with other security tools, such as firewalls, intrusion detection systems, and security orchestration, automation, and response (SOAR) platforms. This integration allows QRadar to provide a more comprehensive view of the organization's security posture and to automate the incident response process.

Conclusion:

Stage 1: In conclusion, web application testing is a crucial process that ensures the security, functionality, and reliability of web-based software. It involves a comprehensive evaluation of various aspects, including user interface, functionality, performance, and security to identify and rectify issues before they impact end-users. This process not only enhances the quality of web applications but also bolsters their resilience against potential threats and vulnerabilities. In an age where online services and applications are integral to our daily lives, effective web application testing is essential to deliver a seamless and secure user experience.

Stage 2: The Nessus report for the specific website has highlighted key security insights. It identified vulnerabilities, categorized by severity, with a focus on critical and high-risk issues that need immediate attention. Recommendations for addressing these vulnerabilities include patching, reconfiguration, and other security measures, with a priority on actions that can have the most significant impact. Compliance with industry standards and best practices is considered, ensuring alignment with recognized security benchmarks like OWASP guidelines. The report underscores the need for continuous monitoring, regular updates, and ongoing security efforts to maintain a strong security posture. In summary, the Nessus report offers a clear view of the website's security state, provides guidance on mitigating vulnerabilities, and stresses the importance of sustained vigilance against evolving threats.

Stage 3:

- A SOC (Security Operations Center) is pivotal for an organization's cybersecurity, continuously monitoring, detecting, and responding to threats.
- SOC operates in a cycle, employing SIEM (Security Information and Event Management) solutions for data collection, analysis, and incident response.
- The SIEM cycle includes data collection, normalization, analysis, detection, alerting, investigation, and reporting.
- QRadar, an IBM SIEM tool, offers a comprehensive security view with its dashboard, presenting critical information, alerts, and analytics.
- Effective utilization of SOC, SIEM, and QRadar is essential for maintaining a strong security posture and safeguarding an organization's digital assets.

Future Scope:

Stage 1: future scope of web application testing

The future scope of web application testing is promising and evolving rapidly, driven by the continuous growth of the internet and web-based applications.

Here are some key aspects of its future scope:

- Increased Demand: As more businesses and services move online, the demand for web applications continues to grow. This, in turn, increases the demand for web application testing to ensure security, reliability, and functionality.
- Advanced Technologies: The complexity of web applications is rising with the integration of advanced technologies like AI, IoT, and blockchain. Testing these cutting-edge applications will require specialized skills and tools.
- Security Emphasis: With the growing number of cyber threats and data breaches, security testing for web applications will become even more critical. Testers will need to focus on vulnerabilities, data protection, and compliance with regulations like GDPR.
- Mobile and Cross-Browser Testing: Mobile usage is on the rise, and web applications must be responsive and functional on various devices and browsers. Testing for cross-compatibility will be essential.
- Performance Testing: As user expectations for speed and performance increase, load testing, stress testing, and other performance testing types will be crucial to ensure web applications can handle traffic spikes.

Stage 2: future scope of the testing process you understood.

The future scope of the web application testing process, particularly in terms of identifying vulnerabilities, is exceedingly promising due to the continuous growth of digital platforms, the escalating importance of cybersecurity, and the ever-evolving threat landscape. Here are some key aspects that highlight the prospective scope of web application testing for vulnerability discovery:

- AI-Driven Testing: The integration of artificial intelligence (AI) and machine learning (ML) into web application testing tools will revolutionize the way vulnerabilities are identified. AI algorithms can swiftly scan vast amounts of code and data to pinpoint vulnerabilities that might elude human testers.
- IoT and Mobile App Testing: With the proliferation of Internet of Things (IoT) devices and the increasing usage of mobile applications, the scope of web application testing will extend to encompass these areas. Ensuring the security of IoT devices and the interfaces they use will become critical.
- Blockchain and Cryptocurrency Security: As blockchain technology and cryptocurrencies continue to gain traction, security testing will be imperative to safeguard transactions and digital assets. Ensuring the robustness of blockchain-based applications will be a specialized niche in web application testing. Serverless Architectures: With the adoption of serverless computing, web application testing will need to adapt to assess the security of serverless functions and APIs. Ensuring that serverless components are free from vulnerabilities will be paramount.
- Container Security: As containerization technologies like Docker and Kubernetes become ubiquitous, web application testing will extend to cover container security. This includes ensuring that container images and orchestration configurations are free from vulnerabilities.

Stage 3: future scope of SOC / SEIM

The outlook for Security Operations Centre (SOC) and Security Information and Event Management (SIEM) systems is exceptionally promising, driven by the ever-changing threat landscape, expanding digitalization, and the increasing significance of cybersecurity.

Here are some pivotal aspects regarding the prospective scope of SOC/SIEM:

- Advanced Threat Detection: SOC/SIEM will increasingly rely on cutting-edge technologies such as artificial intelligence (AI) and machine learning (ML) to enhance their ability to detect and respond to intricate and ever-evolving cyber threats.
- Cloud Security: As a growing number of organizations shift their operations to the cloud, SOC/SIEM must adapt to ensure the security of cloud-based infrastructures and applications. The prevalence of cloud-native SIEM solutions is expected to rise.
- IoT and OT Security: With the proliferation of Internet of Things (IoT) devices and operational technology (OT) systems, SOC/SIEM will broaden its purview to monitor and safeguard these areas, recognizing their vulnerability to potential cyberattacks.
- Compliance and Privacy: Escalating regulatory demands related to data protection and privacy, exemplified by regulations like GDPR and CCPA, will necessitate SOC/SIEM to ensure compliance and safeguard sensitive data.

Topics Explored:

1. SOC
2. SOC Cycle
3. SIEM
4. SIEM Cycle
5. MISP
6. College Network Information
7. Deployment of SOC in the College
8. Threat Intelligence
9. Incident Response

Tools Explored:

- Nessus Scanner
- IBM Qradar