Team 10.4

CyberSentinels

SmartInternz - AI for Cybersecurity with QRadar

AI-enhanced security analytics dashboard that provides real-time insights into security events, trends, and risks

Date: 04/11/2023

Team Members:

- Dev Mehta
- Diti Jain
- Aditi Rai
- Abhishek Kumar

This project aims to develop an AI-enhanced security analytics dashboard that goes beyond conventional security measures. This dashboard will provide real-time insights into security events, trends, and risks, empowering organizations to proactively defend against cyber threats.

This abstract outline the foundational aspects of the project, emphasizing the importance of clarity in scope, well-defined objectives, and a comprehensive execution plan. By strategically addressing these elements, we intend to create a robust and effective security analytics dashboard that can adapt to the dynamic nature of modern cybersecurity challenges.

The scope of the project includes:

● Data Collection and Integration: Gathering data from various sources, such as network logs, system logs, and security appliances, and integrating it into a unified platform.

● AI-Powered Analytics: Implementing advanced machine learning algorithms to analyze the collected data, identify anomalies, and detect potential security breaches in real-time.

● User-Friendly Dashboard: Developing an intuitive user interface that enables security professionals to easily access and interpret critical information.

● Trend Analysis: Providing historical data analysis and trend identification to anticipate potential security risks and vulnerabilities.

● Risk Assessment: Calculating risk scores based on data analysis to prioritize security events and incidents.

● Alerting and Reporting: Implementing automated alerting mechanisms and

customizable reporting features to notify security teams of critical incidents and provide comprehensive insights.

The objectives of the project are to:

Enhance Security Posture: Improve an organization's ability to detect and respond to security threats promptly, reducing the potential impact of security breaches.

Streamline Operations: Optimize the efficiency of security operations by automating repetitive tasks and providing actionable insights.

Foster Proactive Security: Shift from reactive security measures to proactive threat hunting and risk mitigation.

Enable Informed Decision-Making: Empower security professionals and decision-makers with data-driven insights for more effective cybersecurity strategies.

To ensure the successful execution of this project, we will adhere to a comprehensive plan that encompasses:

Requirements Gathering: Engaging stakeholders to clearly define their needs and expectations for the dashboard.

Technology Selection: Evaluating and selecting the most suitable AI and analytics technologies and tools.

Development and Testing: Building and rigorously testing the dashboard to ensure accuracy and reliability.

Deployment and Integration: Implementing the dashboard within the organization's existing security infrastructure.

Training and Adoption: Providing training and support to ensure that security teams can effectively utilize the dashboard.

Ongoing Monitoring and Maintenance: Continuously monitoring the dashboard's performance, updating algorithms, and addressing emerging threats

The Thought Behind the Project:

Step 1: Various Ideas

Step 2: Selecting some features and grouping them

Data Collection and Integration

- Explore various data sources, including IoT devices and cloud platforms.
- Investigate real-time data streaming technologies for efficient data integration.

Risk Assessment:

- Research industry-standard risk assessment frameworks (e.g., FAIR, NIST).
- Discuss methods to calculate dynamic risk scores based on evolving threats.

AI-Powered Analytics:

- Research cutting-edge machine learning algorithms for anomaly detection.
- Consider natural language processing for parsing security-related texts.

Trend Analysis

- Explore tools for predictive analytics to identify future trends.
- Brainstorm ways to visually represent historical data for trend analysis

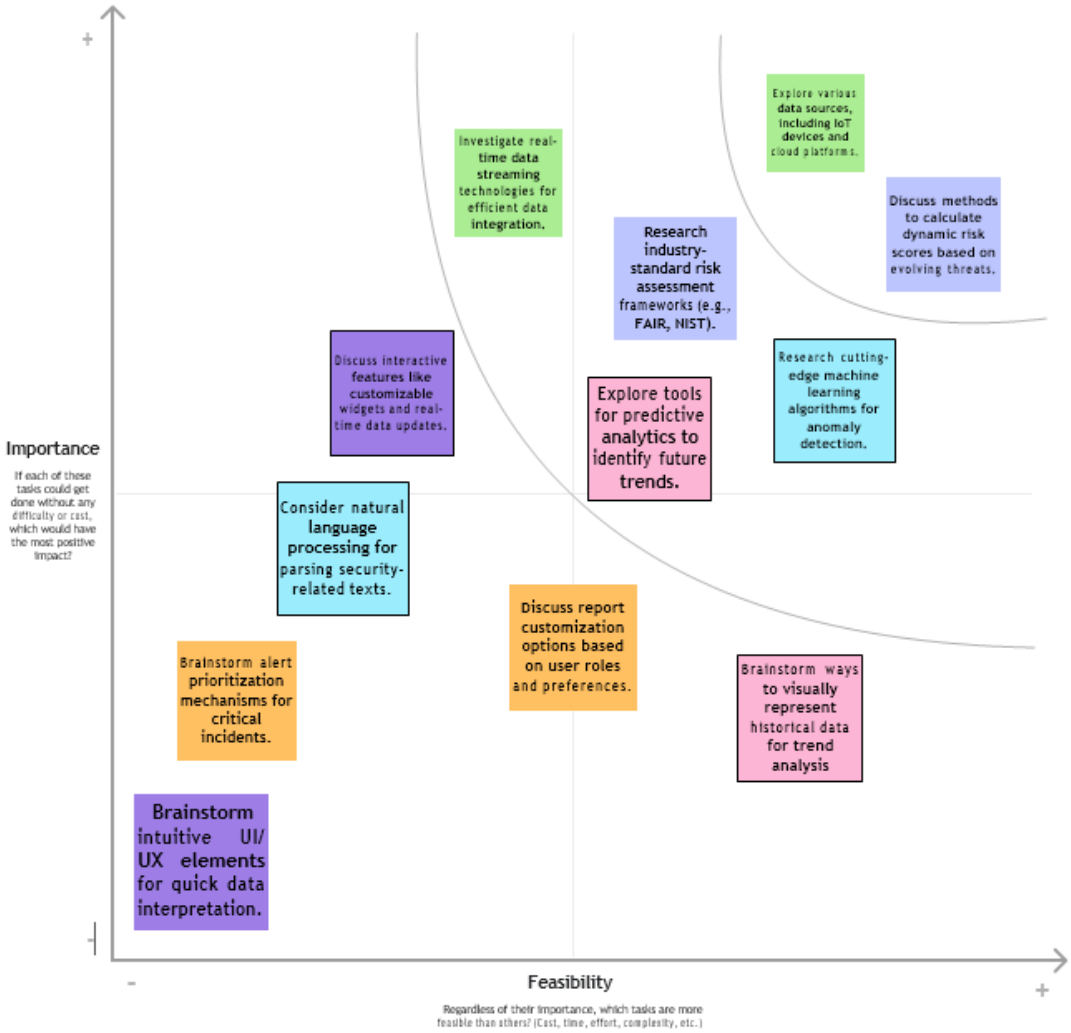
User-Friendly Dashboard:

- Brainstorm intuitive UI/UX elements for quick data interpretation.
- Discuss interactive features like customizable widgets and real-time data updates.

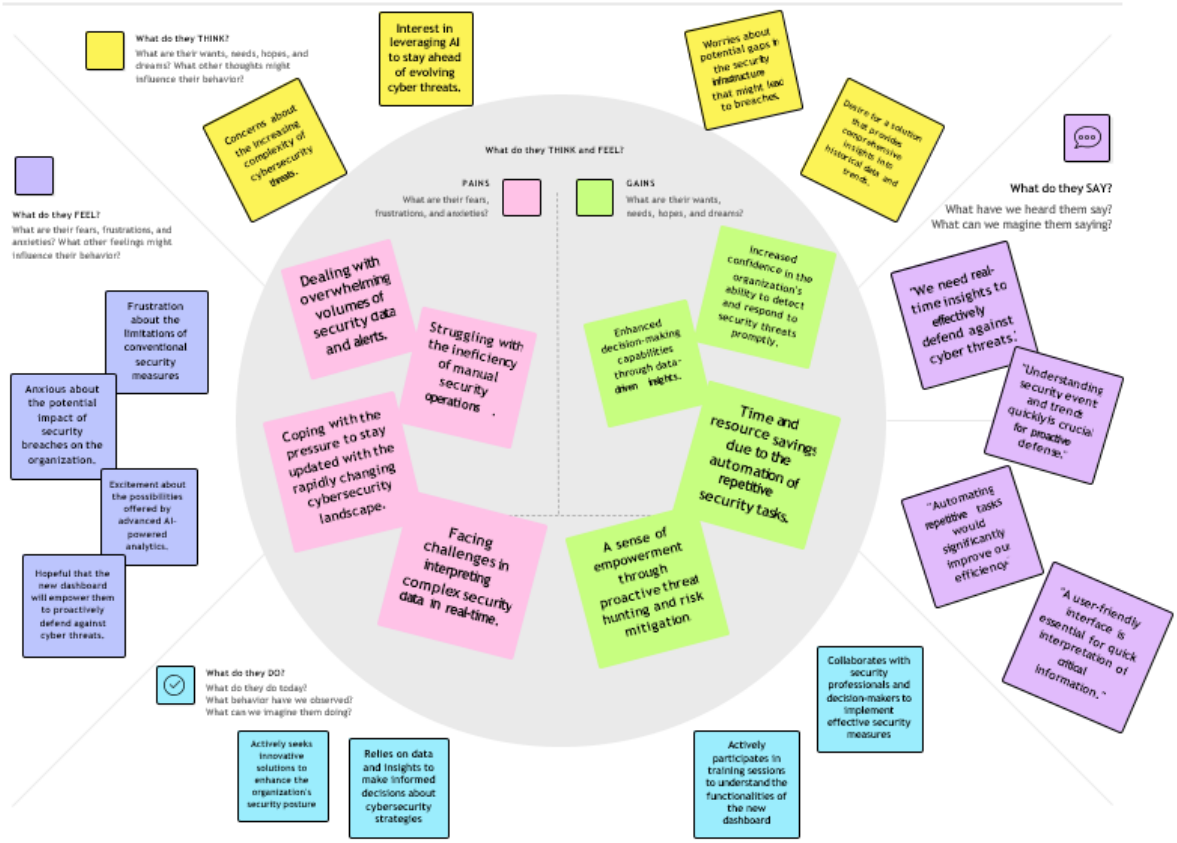
Alerting and Reporting

- Brainstorm alert prioritization mechanisms for critical incidents.
- Discuss report customization options based on user roles and preferences.

Step 3: Priority Chart



Step 4: Empathy Map



Project Planning:

Product Backlog, Sprint Schedule, and Estimation

Use the below template to create product backlog and sprint schedule

Sprint	Functional Requirement (Epic)	User Story Number	User Story / Task	Story Points	Priority	Team Members

Sprint-1	Data Collection	USN-1	Collect data from various cybersecurity websites.	5	High	Dev, Diti, Abhishek, Aditi
Sprint-1		USN-2	Use real-time APIs to fetch data	2	Medium	Dev, Diti, Abhishek, Aditi
Sprint-2		USN-3	Get various news about different kinds of cybersecurity vulnerabilities.	2	Low	Dev, Diti, Abhishek, Aditi
Sprint-1	Data Storage	USN-4	To store the various data collected into different database applications.	5	High	Dev, Diti, Abhishek, Aditi
Sprint-2	Preprocessing	USN-5	Use Apache Kafka for stream processing of the data	5	High	Dev, Diti, Abhishek, Aditi
Sprint-3		USN-6	Use Tensorflow libraries to work on the given data	4	High	Dev, Diti, Abhishek, Aditi
Sprint-2	User Interface	USN-7	Use various coding languages like React.js to create a simple yet	5	High	Dev, Diti, Abhis

			effective dashboard for the user.			hek, Aditi
Sprint-3		USN-8	Have separate login implemented for users to see dashboard particular to their content.	3	Mediu m	Dev, Diti, Abhis hek, Aditi
Sprint-3	Data Visualizati on	USN-9	Use tools like Kibana to show various data in a more readable format to the users.	5	High	Dev, Diti, Abhis hek, Aditi
Sprint-4		USN-10	Have a feature to ask users for their suggestions.	2	Low	Dev, Diti, Abhis hek, Aditi
Sprint-4	Scalability	USN-11	Use Docker to Scale the whole project.	5	High	Dev, Diti, Abhis hek, Aditi
Sprint-4		USN-12	Have a better Database system to store the real time and other various data.	5	High	Dev, Diti, Abhis hek, Aditi

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

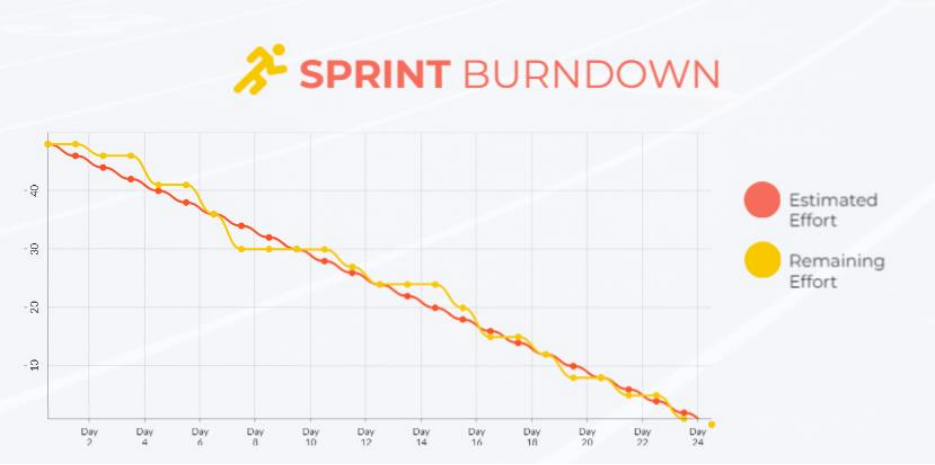
Sprint	**Total Story Points**	**Duration**	**Sprint Start Date**	**Sprint End Date (Planned)**	**Story Points Completed (as on Planned End Date)**	**Sprint Release Date (Actual)**
Sprint-1	12	6 Days	24 Oct 2023	29 Oct 2023	12	29 Oct 2023
Sprint-2	12	6 Days	31 Oct 2023	05 Nov 2023		
Sprint-3	12	6 Days	07 Nov 2023	12 Nov 2023		
Sprint-4	12	6 Days	14 Nov 2023	19 Nov 2023		

Velocity:

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

$$AV = \frac{\text{sprint duration}}{\text{Velocity}} = \frac{12}{6} = 2$$

Burndown Chart:



Proposed Solution Template:

Project team shall fill the following information in the proposed solution template.

S.No.	Parameter	Description
1.	Problem Statement (Problem to be solved)	AI-Enhanced Security Analytics Dashboard That Provides Real-Time Insights Into Security Events, Trends, And Risks.
2.	Idea / Solution description	The solution is an AI-Enhanced Security Analytics Dashboard (AISAD), which incorporates data from diverse sources such as network logs and system records. AISAD delivers real-time insights, analyses abnormalities, and detects possible security breaches using powerful machine learning algorithms. Its simple interface enables security experts to quickly access vital information. The dashboard analyses trends, predicts security threats, and provides risk scores to prioritise tasks. Rapid incident response is ensured via automated alerting and configurable reporting, increasing the organization's security posture. AISAD encourages proactive threat hunting, efficient operations, data-driven decision-making, and continual adaption to new threats.
3.	Novelty / Uniqueness	The distinctive aspect of our concept is AISAD's real-time predictive analytics, which estimate future risks based on existing data, providing proactive security measures. Its sophisticated risk assessment and automatic warnings prioritise replies, allowing for better event

		management. Natural language processing integration improves user contact, allowing for smooth communication with the system. AISAD distinguishes itself with its unique blend of predictive analysis, risk prioritisation, and user-friendly interaction, revolutionising cybersecurity methods with a new, forward-thinking approach.
4.	Social Impact / Customer Satisfaction	Our technology improves customer satisfaction by giving real-time security information, allowing for quick reaction to attacks, and ultimately preserving critical data. Furthermore, its proactive strategy reduces the potential effect of security breaches, promoting a safer digital environment. This not only assures organisational resilience, but also benefits society by raising general cybersecurity standards and fostering confidence in digital interactions.
5.	Business Model (Revenue Model)	The business strategy entails AISAD providing a subscription-based service with tiered pricing based on the amount of data processing and degree of support. Furthermore, revenue streams may be broadened through customised services, training programmes, and continuous maintenance contracts, assuring long-term income while delivering customised solutions to a wide clientele. Strategic alliances with cybersecurity service providers can help to broaden the company's reach and improve service offerings.
6.	Scalability of the Solution	The architecture of the system is built for smooth scalability, allowing it to handle rising data volumes and user needs without sacrificing performance. Its modular architecture enables for the simple integration of new features and technologies, enabling adaptation to changing cybersecurity requirements. AISAD can effectively grow to match the extent and complexity of any organization's security requirements, whether for small businesses or huge organisations.

Solution Architecture:

1. Data Collection and Integration Layer:

AISAD takes data from many sources such as network logs, system logs, and security appliances in this layer. APIs and data connections make seamless integration possible, allowing for real-time data intake. Data preparation techniques clean, transform, and aggregate raw data before it is analysed further.

2. Big Data Storage:

AISAD makes use of a scalable, distributed large data storage system, such as Apache Hadoop or Amazon S3. This storage system processes enormous amounts of organised and unstructured data effectively, maintaining stability and availability even during peak loads.

3. Real-time Data Processing and Analysis:

Real-time analysis is possible with data processed by stream processing engines such as Apache Kafka or Apache Flink. Data is processed by machine learning algorithms and anomaly detection models, which discover trends and possible dangers. Apache Spark may be used to do in-memory processing, which improves speed and accuracy.

4. Predictive Analytics and Trend Analysis:

For predictive analytics, AISAD uses machine learning frameworks such as TensorFlow or scikit-learn. Historical data is used to train trend analysis models, allowing the system to forecast future security risks and vulnerabilities. Deep learning algorithms may be used to recognise complicated patterns.

5. User Interface and Experience Layer:

AISAD's user-friendly web-based dashboard is designed using cutting-edge frontend technologies such as React.js and Angular. The interface includes dynamic visualisations, widgets that may be customised, and real-time updates. NLP APIs, which may be driven by Google's BERT or OpenAI's GPT, enable user interaction through voice commands and text inquiries.

6. Alerting and Reporting Engine:

Tools like Elasticsearch and Kibana are used to incorporate automated alerting methods, guaranteeing rapid alerts for significant security issues. Users may produce thorough reports and summaries based on certain criteria and time frames thanks to the implementation of customizable reporting options.

7. Security and Compliance:

Encryption mechanisms for data transfer and storage, as well as multi-factor authentication for user access, are among the security measures. Compliance with industry standards like GDPR and HIPAA is assured, and audit trails are kept for regulatory purposes.

8. Scalability and Deployment:

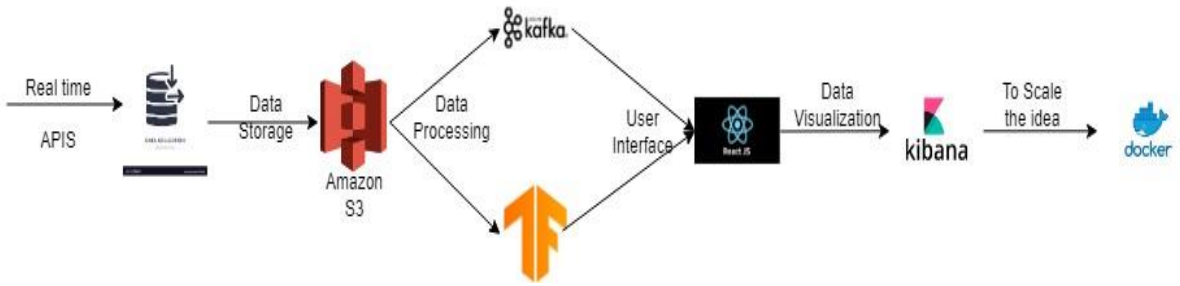
Docker containerization and Kubernetes orchestration improve scalability and deployment flexibility. AISAD can be installed on-premises, in private clouds, or on popular public cloud platforms like AWS or Azure, allowing for on-demand scalability.

9. Continuous Monitoring and Maintenance:

Monitoring technologies such as Prometheus and Grafana are incorporated to ensure optimal resource utilisation by monitoring system performance. Pipelines for continuous integration and deployment (CI/CD) automate updates and additions, ensuring that the system is constantly up to date and capable of handling emerging risks.

This comprehensive architecture ensures AISAD's ability to handle vast amounts of data, process it in real-time, provide actionable insights, and offer a seamless user experience while adhering to the highest standards of security and compliance.

Example - Solution Architecture Diagram:



Stage 1

Understanding various Vulnerabilities:

Top 5 Vulnerability Exploitation

1. Broken Access Control

Description

Broken Access Control is a vulnerability that allows unauthorized users to access protected resources or perform actions that they should not be able to perform. This can occur when there is a failure to properly authenticate and authorize users or when access control rules are not properly enforced.

For example, if a web application does not properly check user permissions when accessing certain pages or performing certain actions, an attacker could exploit this vulnerability to gain access to sensitive data or perform unauthorized actions. This could have serious business impact, such as loss of confidential information, reputational damage, financial loss, or legal liability.

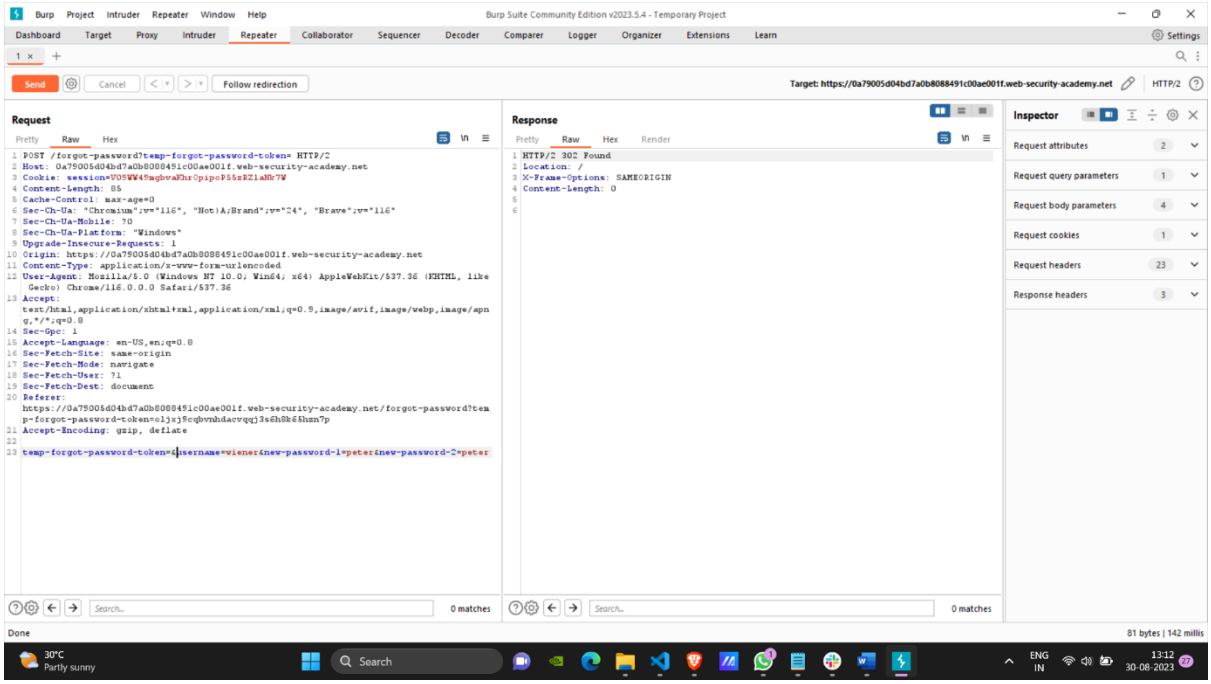
To perform this vulnerability, an attacker would attempt to bypass access control mechanisms by exploiting weaknesses in authentication and authorization mechanisms, such as brute-forcing passwords, exploiting session management flaws, or manipulating access control tokens. It is important to properly design and implement access control mechanisms to prevent this vulnerability and protect sensitive resources.

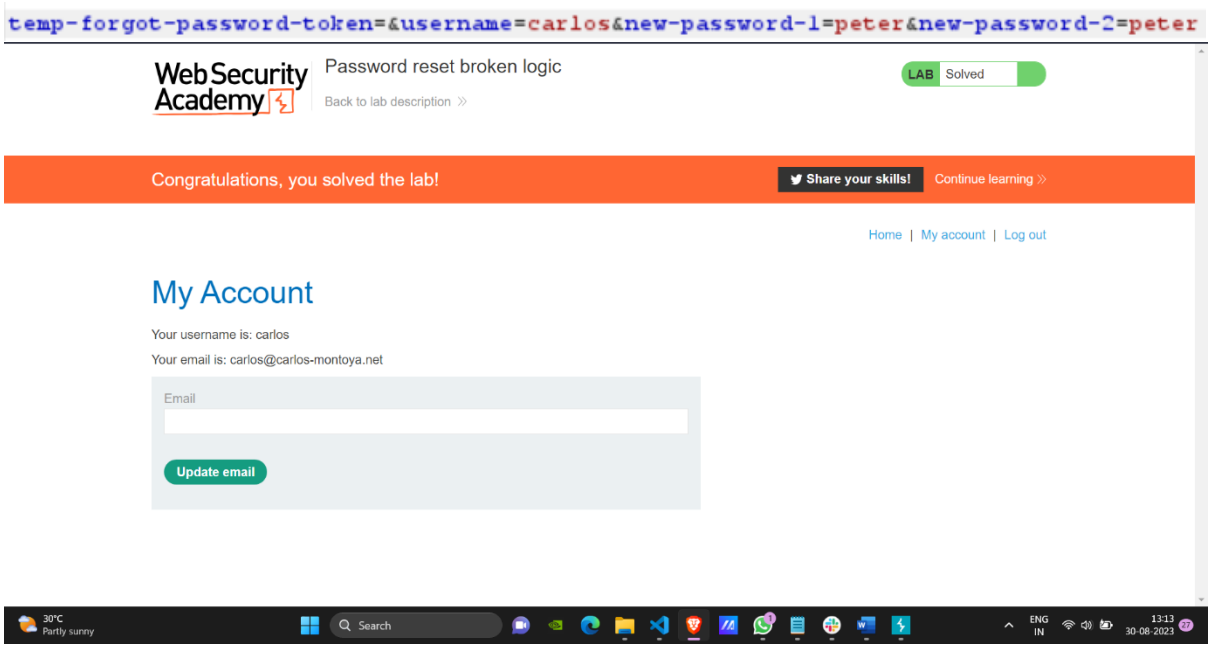
Business Impact

Broken Access Control can have serious business impact, such as loss of confidential information, reputational damage, financial loss, or legal liability. If an attacker gains unauthorized access to sensitive data or performs unauthorized actions, it could compromise the security of the entire system and lead to significant consequences for the organization. It is important to properly design and implement access control mechanisms to prevent this vulnerability and protect sensitive resources.

Performing the vulnerability

Using PortSwigger Lab we will try to access and change password for a user names carlos. Here, we *change the name in username parameter* while querying and posting, hence we can access a account names carlos





2. Cryptographic Failures

Description

Cryptographic failures are vulnerabilities that occur when the cryptographic mechanisms used to protect data are implemented incorrectly or are insufficiently strong. This can result in sensitive data being exposed or compromised.

Cryptographic failures can occur in many ways, such as using weak encryption algorithms, improperly storing cryptographic keys, or failing to properly authenticate digital signatures. These vulnerabilities can be exploited by attackers to bypass security controls and gain unauthorized access to sensitive information.

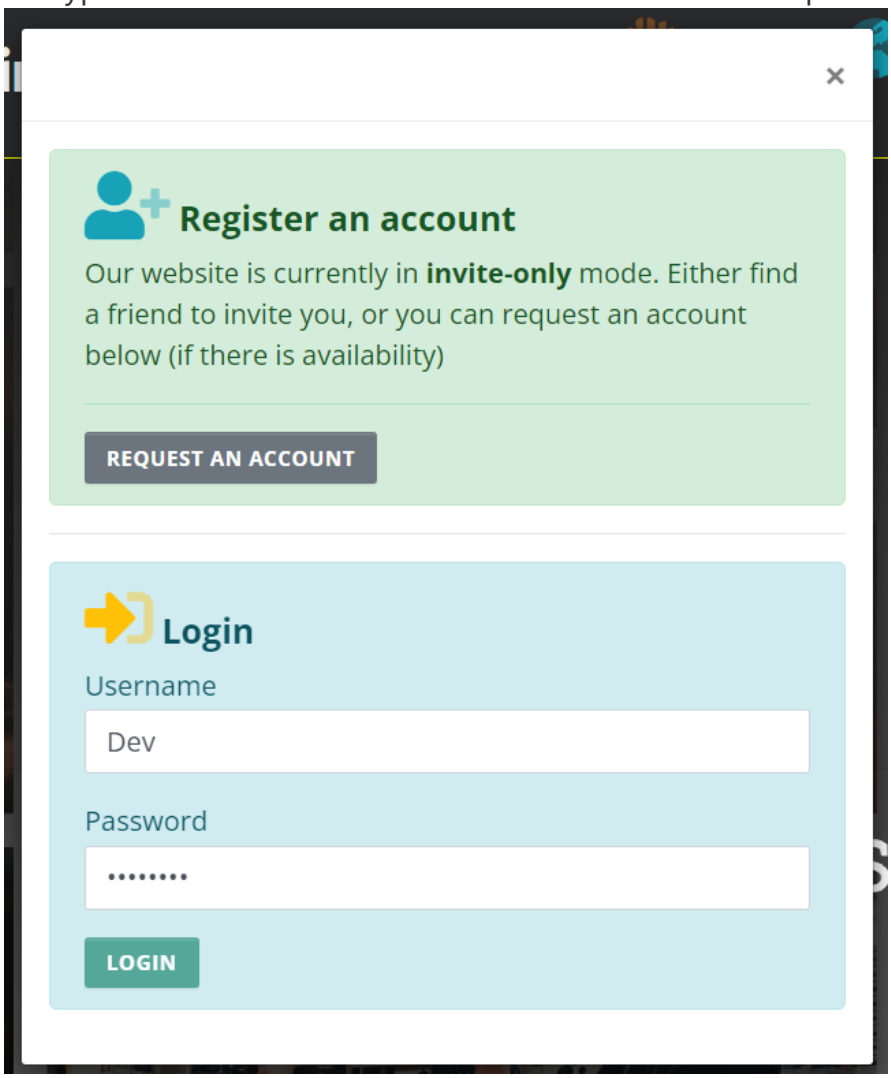
For example, if a web application uses weak encryption algorithms to protect sensitive data, an attacker may be able to easily decrypt the data and gain access to confidential information. Similarly, if cryptographic keys are not properly protected, attackers may be able to steal the keys and use them to access encrypted data.
To prevent cryptographic failures, it is important to properly implement strong cryptographic mechanisms, such as using up-to-date encryption algorithms, properly storing cryptographic keys, and using digital signatures to ensure the integrity of data.

Business Impact

Cryptographic failures can have serious business impact, such as loss of confidential information, reputational damage, financial loss, or legal liability. If an attacker is able to exploit a cryptographic vulnerability, they may be able to gain access to sensitive data and compromise the security of the entire system. It is important to properly implement strong cryptographic mechanisms to protect sensitive information.

Performing the vulnerability

This vulnerability takes place when important things like password are not stored after encryption but stored in direct normal text. For our example we use,



When I click on login and use burp suite intercept I can clearly see the password without any encryption which is a cryptographic failure

```
Pretty    Raw    Hex
1  POST /fastfoodhackings/index.php?act=login HTTP/1.1
2  Host: www.bugbountytraining.com
3  Content-Length: 30
4  Cache-Control: max-age=0
5  Sec-Ch-Ua: "Chromium";v="116", "Not)A;Brand";v="24", "Brave";v="116"
6  Sec-Ch-Ua-Mobile: ?0
7  Sec-Ch-Ua-Platform: "Windows"
8  Upgrade-Insecure-Requests: 1
9  Origin: https://www.bugbountytraining.com
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36
12 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
13 Sec-Gpc: 1
14 Accept-Language: en-US,en;q=0.8
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-User: ?1
18 Sec-Fetch-Dest: document
19 Referer: https://www.bugbountytraining.com/fastfoodhackings/index.php
20 Accept-Encoding: gzip, deflate
21 Connection: close
22
23 username=Dev&password=12345678
```

3. Injection

Description

Injection vulnerabilities occur when untrusted data is sent to an interpreter as part of a command or query. This can allow an attacker to execute malicious code or access sensitive information. Injection vulnerabilities can occur in many different contexts, such as SQL, LDAP, or XML.

For example, if a web application does not properly validate user input when constructing SQL queries, an attacker may be able to inject malicious SQL code into the query and gain access to sensitive data. Similarly, if an application uses untrusted data to construct LDAP queries, an attacker may be able to inject LDAP commands to gain unauthorized access to the system.

To prevent injection vulnerabilities, it is important to properly validate and sanitize all input data, and to use parameterized queries whenever possible. It is also important to limit the privileges of interpreters to reduce the impact of successful attacks.

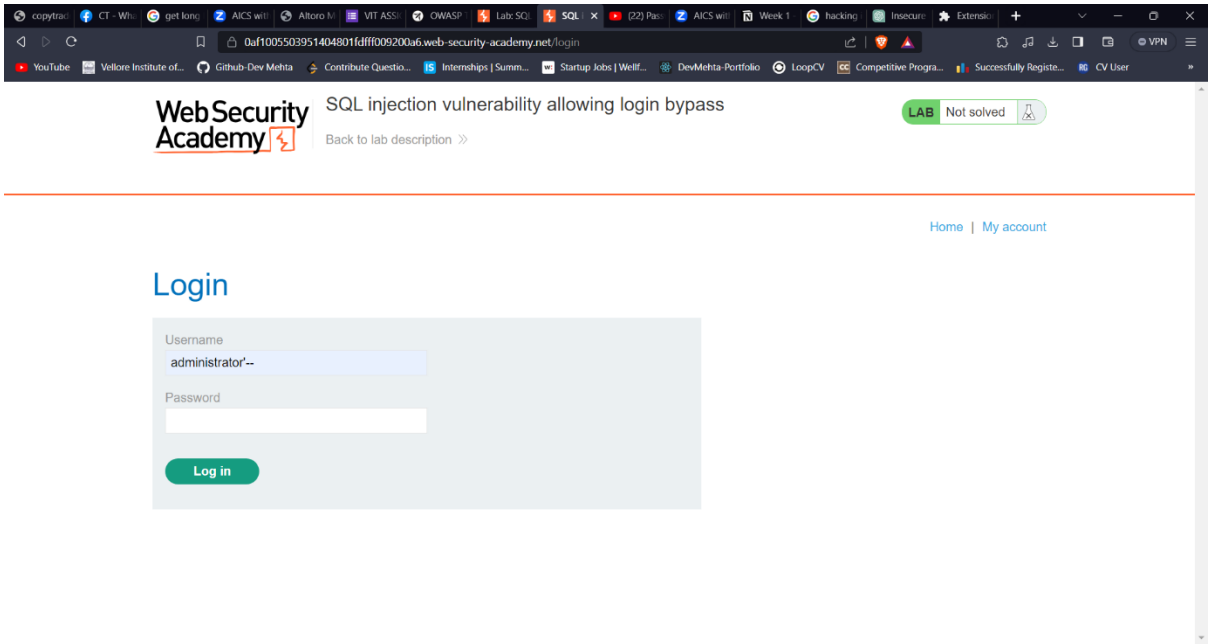
Business Impact

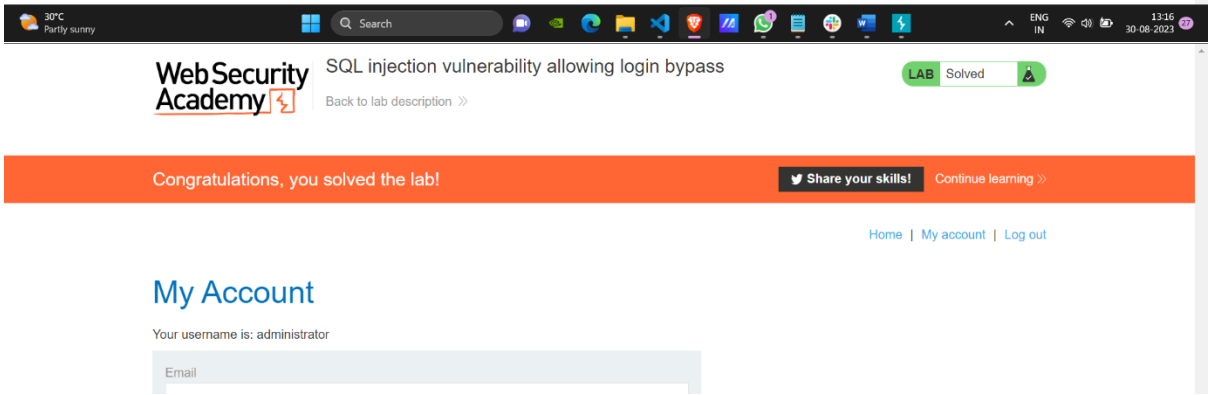
Injection vulnerabilities can have serious business impact, such as loss of confidential information, reputational damage, financial loss, or legal liability. If an attacker is able to exploit an injection vulnerability, they may be able to gain access to sensitive data or execute unauthorized commands, compromising the security of the entire system.

Performing the vulnerability

Again using PortSwigger Labs we are able to show login bypass using SQL Injection!

We use ‘— which comments the password in a way and hence allows us to login





4. Insecure Design

Description

An insecure design vulnerability, often referred to as a security design flaw, is a type of software or system vulnerability that arises from poor or inadequate design choices in the architecture of a software application, system, or network. These design flaws can create pathways for attackers to exploit, compromise, or manipulate the system, potentially leading to unauthorized access, data breaches, service disruptions, or other security incidents.

Unlike more traditional vulnerabilities that stem from coding errors, insecure design vulnerabilities are rooted in fundamental architectural decisions. Examples of insecure design vulnerabilities include improper access controls, insufficient authentication mechanisms, lack of encryption for sensitive data, and improper handling of user inputs.

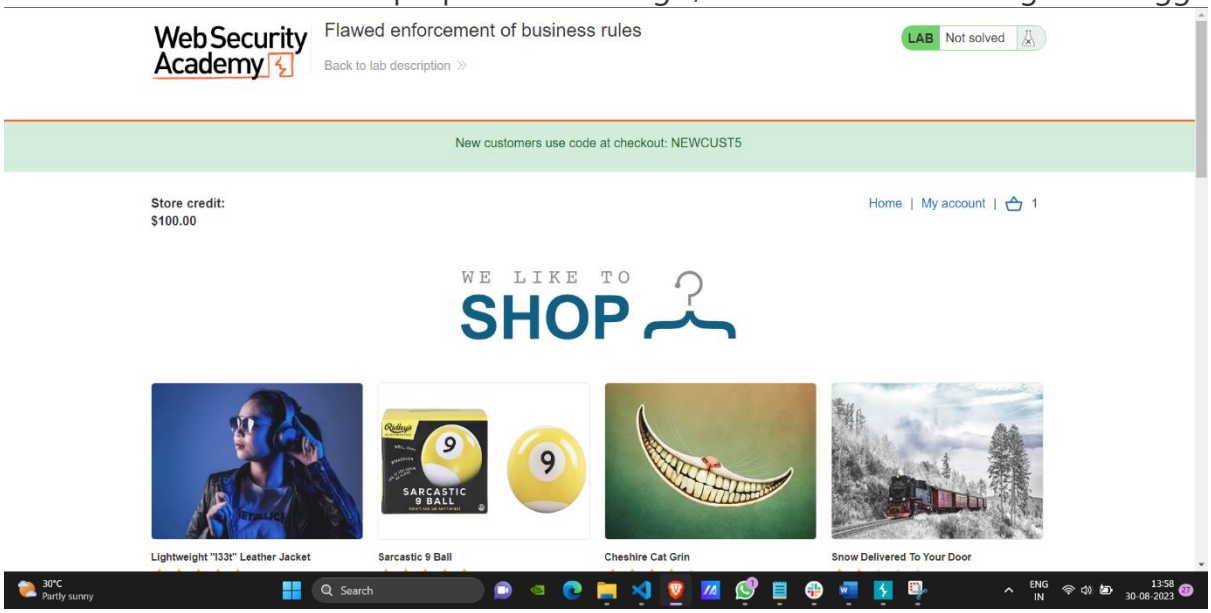
Business Impact

Insecure design vulnerabilities within software systems can have profound business implications, including the heightened risk of data breaches, eroded customer trust, financial losses from regulatory fines and legal actions, tarnished reputation leading to reduced customer acquisition and retention, operational disruptions causing downtime

and inefficiencies, and a competitive disadvantage as security concerns drive customers towards more secure alternatives. Addressing these vulnerabilities is crucial to safeguarding sensitive data, maintaining business continuity, and preserving the organization's reputation and bottom line.

Performing the vulnerability

A common issue here is no proper business logic, which we can see using PortSwigger Lab:



We see we can apply 2 coupons which is wrong business logic

5. Security Misconfiguration

Description

Security misconfiguration refers to the improper implementation or settings of security controls within software applications, systems, or networks. It occurs when default configurations, unnecessary features, or weak settings are left unchanged, creating vulnerabilities that attackers can exploit. These misconfigurations can expose sensitive data, grant unauthorized access, and weaken the overall security posture of an organization.

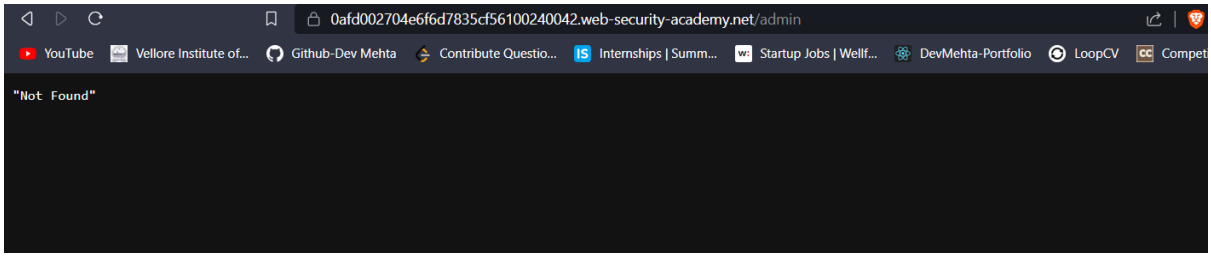
Business Impact

Security misconfigurations can lead to significant business impact, including unauthorized access to sensitive information, data breaches resulting in legal and financial liabilities, operational disruptions causing downtime and loss of productivity, reputation damage leading to customer loss and diminished trust, regulatory non-compliance leading to fines, and increased resource allocation for incident response and mitigation efforts. Proper configuration management and regular security assessments are essential to prevent these risks and maintain a strong security stance.

Performing the vulnerability

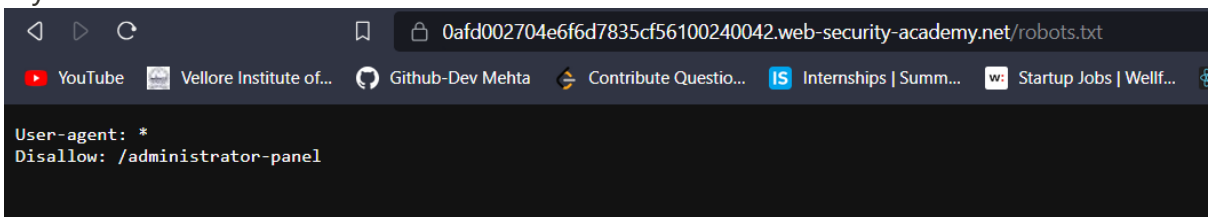
We try to get to admin panel which is a vulnerability, if the security is correct it wont allow us. We will again use PortSwigger Lab

Try 1:

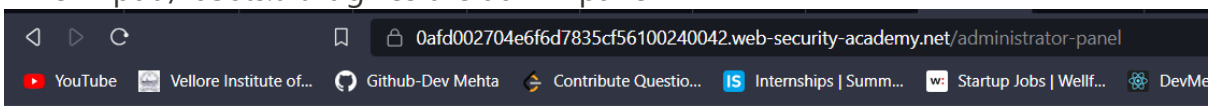


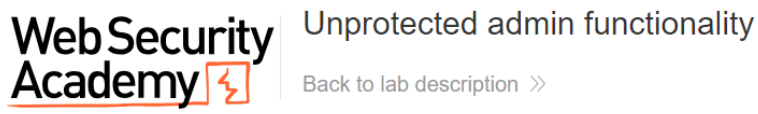
When I directly add */admin* in link it does not work

Try 2:



When I put */robots.txt* it gives the admin panel link





On adding */administrator-panel,* I get the access of admin shows security misconfiguration

Testing Vulnerabilities:

Practice Website 1:

1. Vulnerability Name: Login Page - Forgot Password exposed

OWASP Category: Insecure Design

Description: architectural flaws that are built-in right from the beginning of software development, if theappropriate security mitigations are not taken.

Business Impact:Lack of effective security controls in the design phase often results in an application being susceptible to many weaknesses, collectively known as insecure design vulnerabilities.

Vulnerability Path : http://4.246.191.90/good_food/

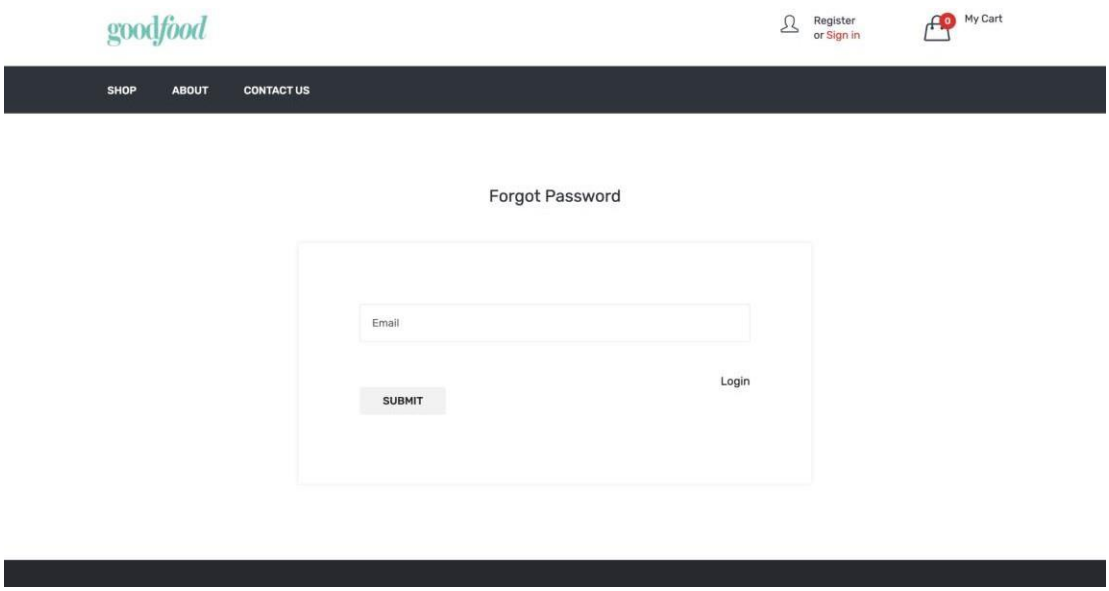
Vulnerability Parameter: **http://4.246.191.90/good_food/forget_password**

Steps to Reproduce :

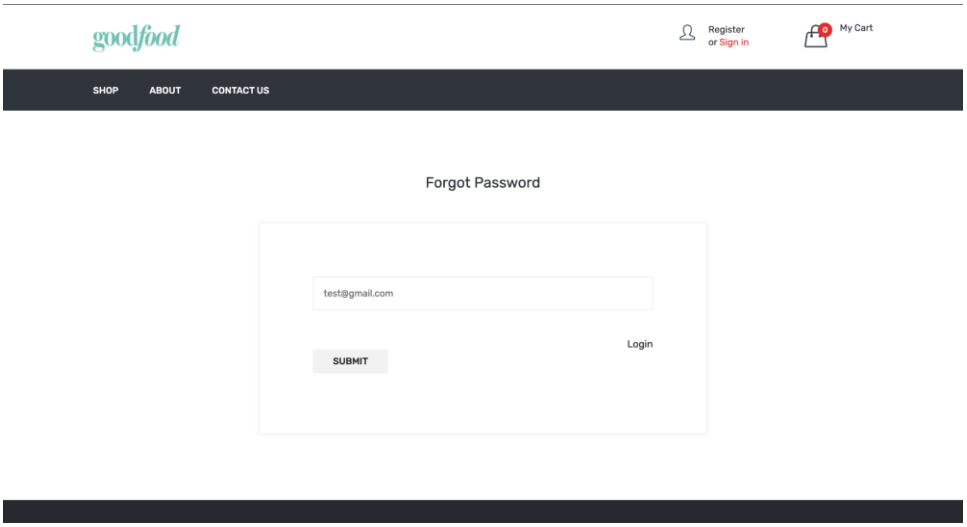
Step 1. Access the URL

Step 2:Then jump into the login page as shown.

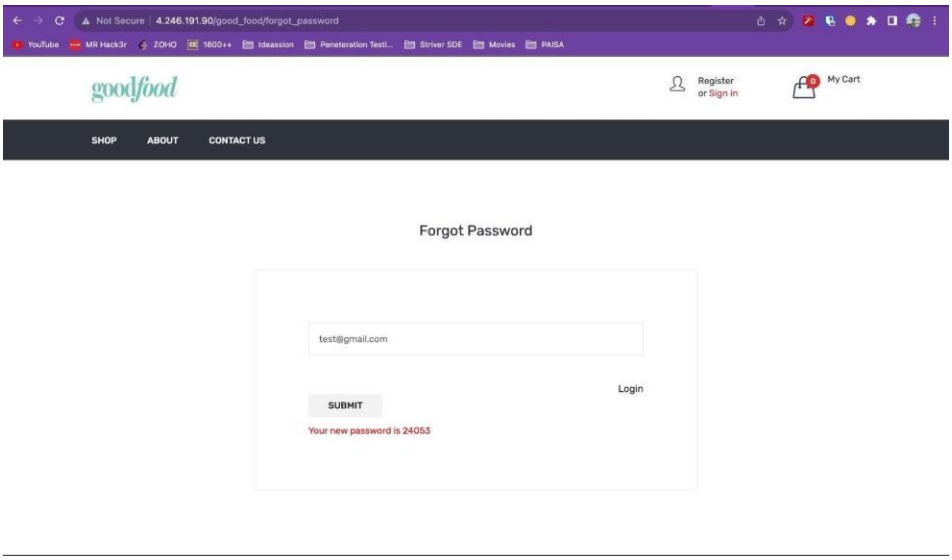
Step



3: then enter a random email you want to test which is present in the database.



Step 4: then you will find an auto generated password below the forgot password .



Recommendation:

- Establish and use a library of secure mechanism
- Strong validation process.

---

2. Vulnerability Name: Cross-site scripting (stored)

OWASP Category: Injections

Description: It occurs when a malicious script is injected directly into a vulnerable web application.

Reflected XSS involves the reflection of a malicious script off of a web application, onto a user's browser.

Business Impact: The application stores dangerous data in a database, message forum, visitor log, or other trusted data store. At a later time, the dangerous data is subsequently read back into the applicationand included in dynamic content. From an attacker's perspective, the optimal place to inject malicious

content is in an area that is displayed to either many users or particularly interesting users. Interesting users typically have elevated privileges in the application or interact with sensitive data that is valuable tothe attacker. If one of these users executes malicious content, the attacker may be able to perform

privileged operations on behalf of the user or gain access to sensitive data belonging to the user.

Vulnerability Path :http://4.246.191.90/good_food/contact_us

Step

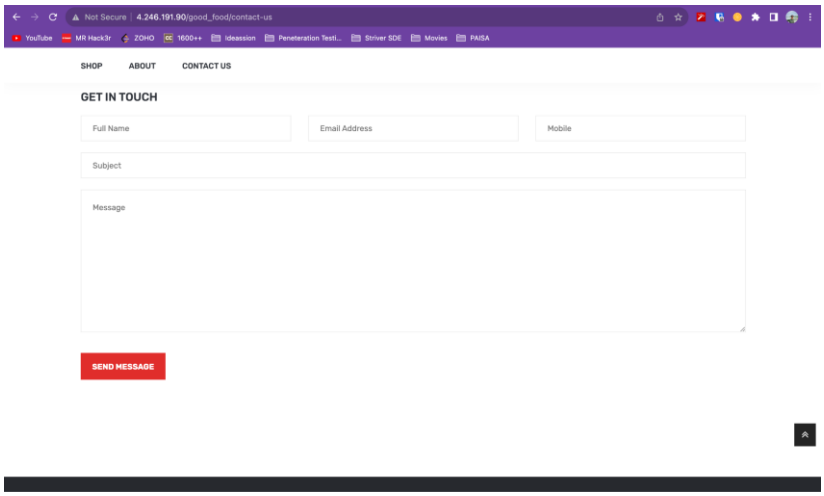
Vulnerability Parameter: http://4.246.191.90/good_food/admin/user.php

Steps to Reproduce :

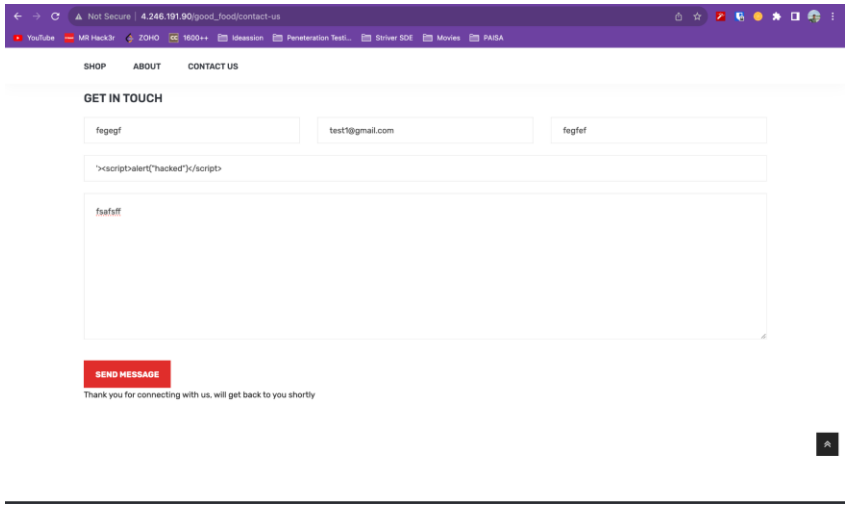
Step 1. Access the URL

Step 2: Then enter the credentials to the contact us page .

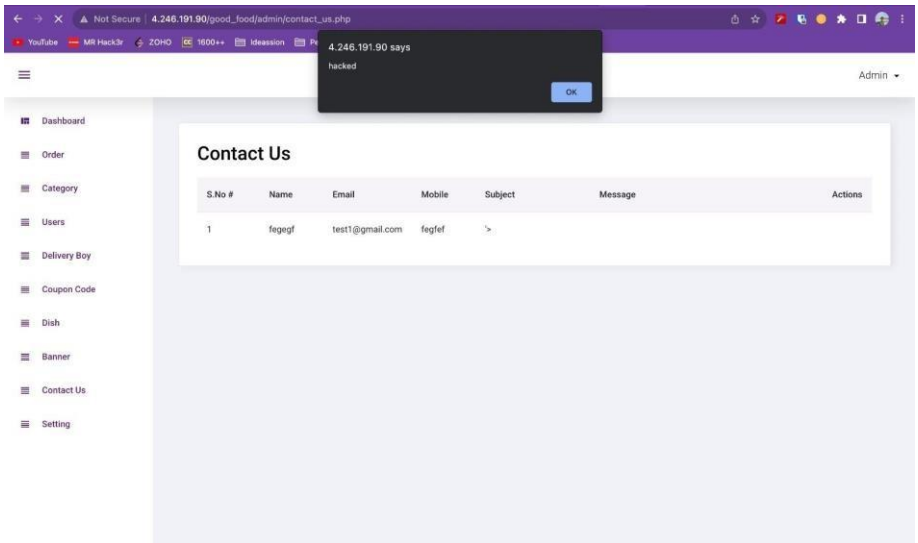
Step 3: inside the contact us page try to submit the message by filling the detail.



4:-when you try to enter the details you will find the subject box that enters a script as shown.



Step 5:- then you will find something like this as shown below .



Recommendation:

- Note that proper output encoding, escaping, and quoting is the most effective solution for preventing XSS, although input validation may provide some defense-in-depth

3. Vulnerability Name : Register Page Lacking Input Validation

OWASP Category : Security Misconfiguration

Description : The Register Page on http://4.246.191.90/good_food/ is deficient in input validation, allowing for the submission of potentially malicious or incorrect data. Input validation safeguards are not in place to verify the accuracy and safety of user-provided information during the registration process.

Business Impact : This vulnerability introduces a significant security risk. Without proper input validation, malicious users could exploit the registration page to submit harmful data, potentially leading to various security issues, such as injection attacks or data corruption. This poses a threat to the integrity of the system and may result in reputation damage and data loss. Implementing input validation measures is essential to mitigate these risks and ensure the security of the registration process.

Vulnerability Path :http://4.246.191.90/good_food/

Step

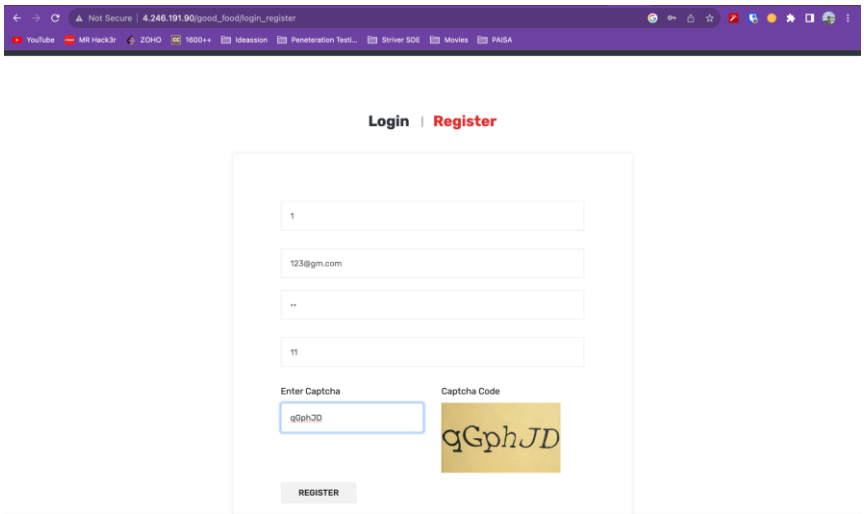
Vulnerability Parameter: http://4.246.191.90/good_food/login_register

Steps to Reproduce :

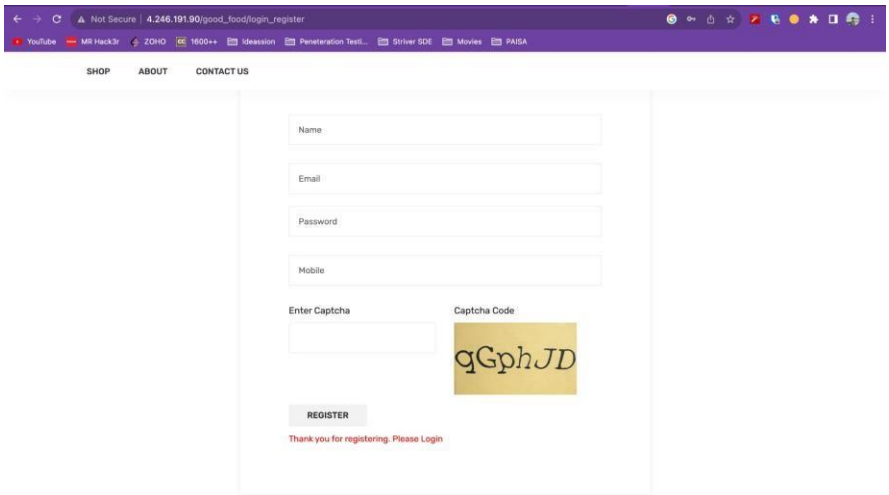
Step 1. Access the URL

Step 2: Then enter the details on register page .

Step 3: inside the fields on the page try to enter any single or double numbers/letters.



4: Then click on the register you will find that successfully registered.



4. Vulnerability Name : SSL encryption is not enabled

OWASP Category : Sensitive Data Exposure

Description : The absence of SSL encryption on the website at http://4.246.191.90/good_food/ means that data transmitted between the user's browser and the server is not secured, leaving it vulnerable to interception by unauthorized parties.

Business Impact : This vulnerability poses a significant risk as it could expose sensitive user data, including login credentials and personal information, to potential attackers. The lack of SSL encryption increases the likelihood of data breaches, erodes user trust, and can lead to regulatory compliance issues.

Vulnerability Path :http://4.246.191.90/good_food/

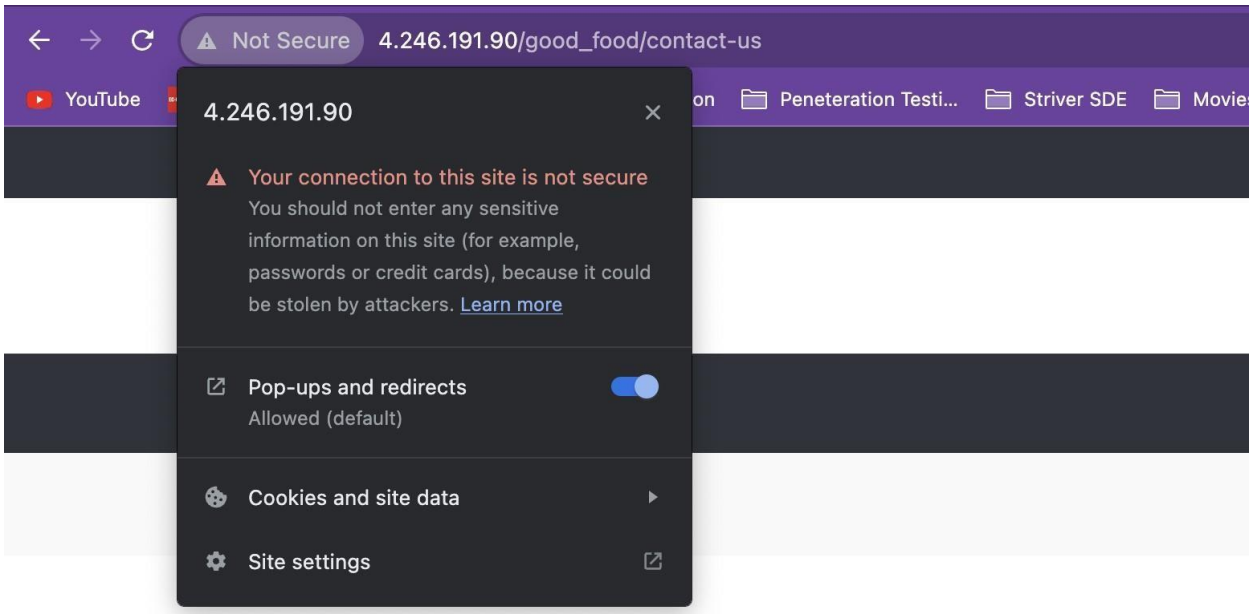
Vulnerability Parameter: **http://4.246.191.90/good_food/**

Steps to Reproduce :

Step 1. Access the URL

Step 2: Click on Not Secure

Step


Not Secure
4.246.191.90/good_food/contact-us
YouTube
Peneteration Testi...
Striver SDE
4.246.191.90
Your connection to this site is not secure
You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers. Learn more
Pop-ups and redirects
Allowed (default)
Cookies and site data
Site settings

5. Vulnerability Name : Clickjacking

OWASP Category : Security Misconfiguration

Description : The Clickjacking vulnerability is a security concern on the website located at http://4.246.191.90/good_food/. It allows malicious entities to potentially trick users into interacting with elements on the page without their knowledge or consent, often leading to unintended actions.

Business Impact : This vulnerability can have serious consequences. It could result in users inadvertently taking actions they didn't intend to, such as making unauthorized transactions or disclosing sensitive information. This not only threatens user trust but also exposes the business to potential legal and financial ramifications. Proper security measures are necessary to mitigate this risk.

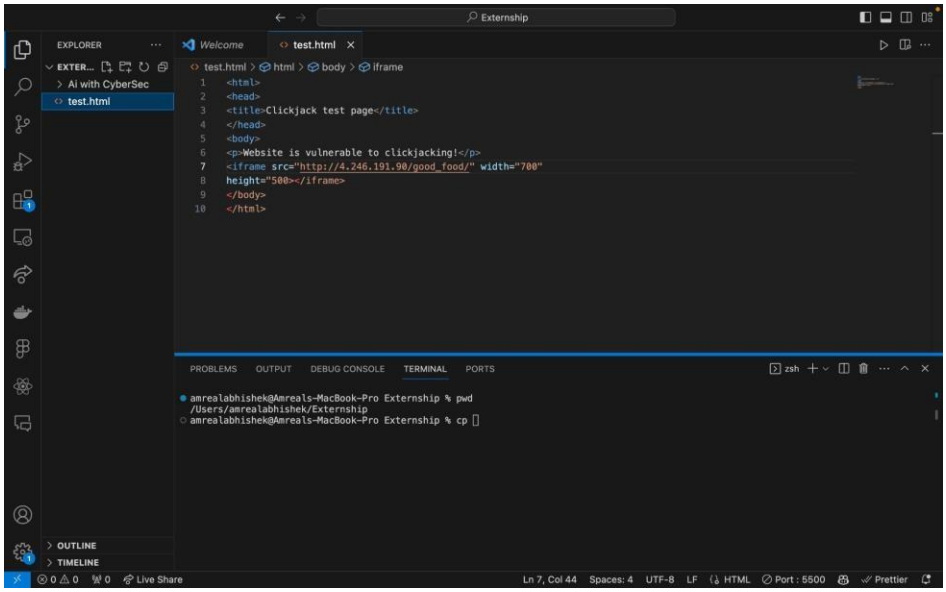
Vulnerability Path :http://4.246.191.90/good_food/

Vulnerability Parameter: **http://4.246.191.90/good_food/admin/user.php**

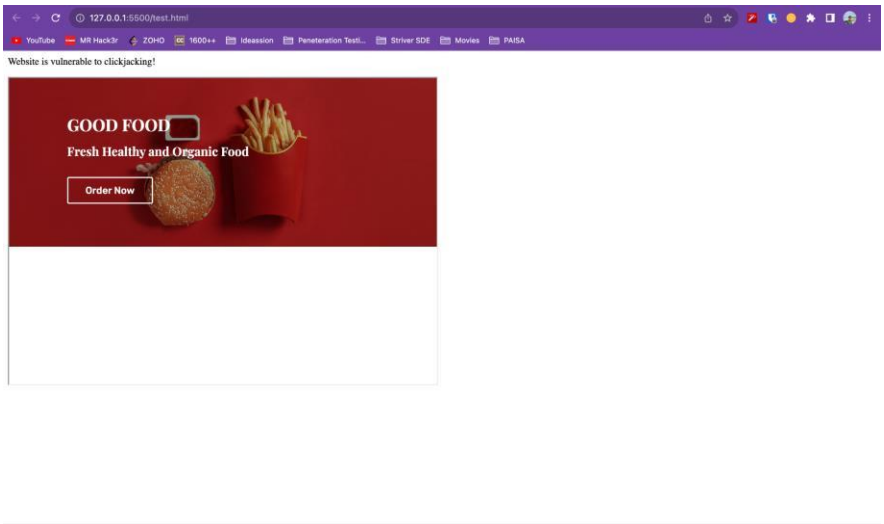
Steps to Reproduce :

Step 1. Write a script with your target url.

Step 2: Open it as a live server.



Step 3: Now you can see the results.



---

6. Vulnerability Name : SQLMAP dumping

OWASP Category : Injection

Description : The SQLMAP dumping vulnerability found on the website at http://4.246.191.90/good_food/ represents a serious injection risk. It allows malicious actors to exploit potential weaknesses in the application's code, potentially gaining unauthorized access to and extracting sensitive data stored in the underlying database.

Business Impact : This vulnerability can result in the unauthorized retrieval of critical and confidential information, such as customer data or financial records. The business impact includes potential data breaches, loss of trust, financial liability, and legal consequences, making it imperative to address and mitigate this risk promptly.

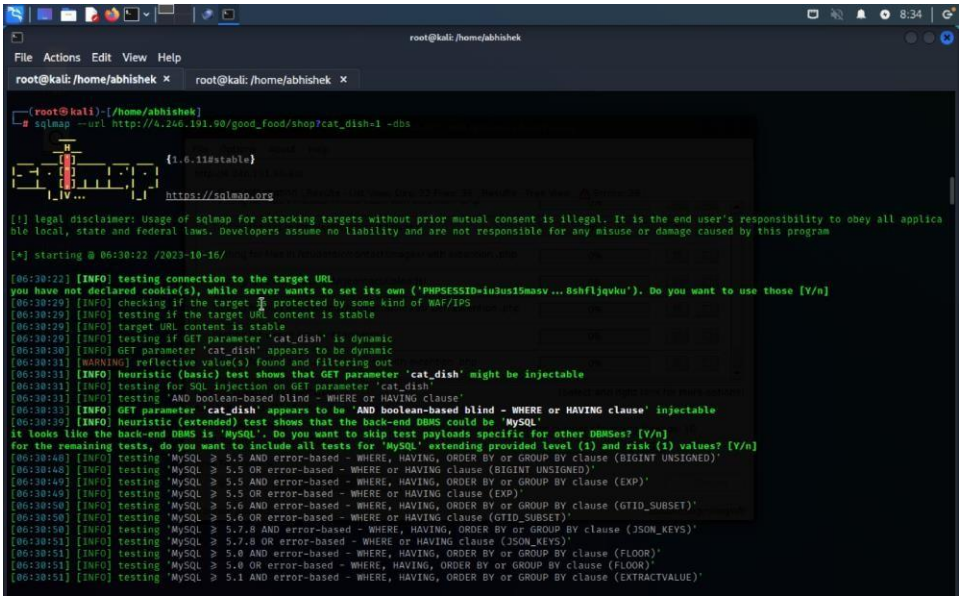
Vulnerability Path :http://4.246.191.90/good_food/

Vulnerability Parameter: **http://4.246.191.90/good_food/admin/user.php**

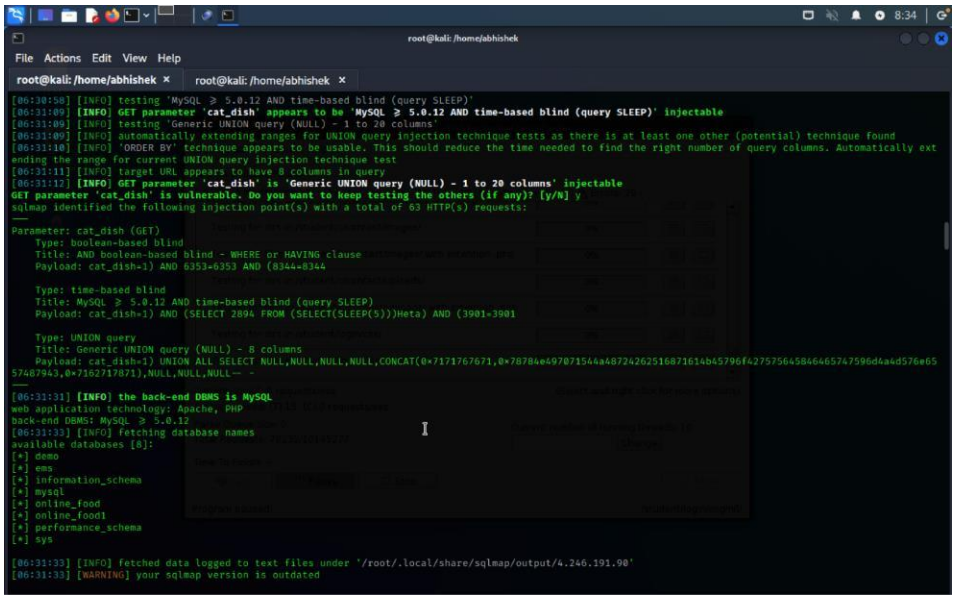
Steps to Reproduce :

Step 1. Open Kali Linux

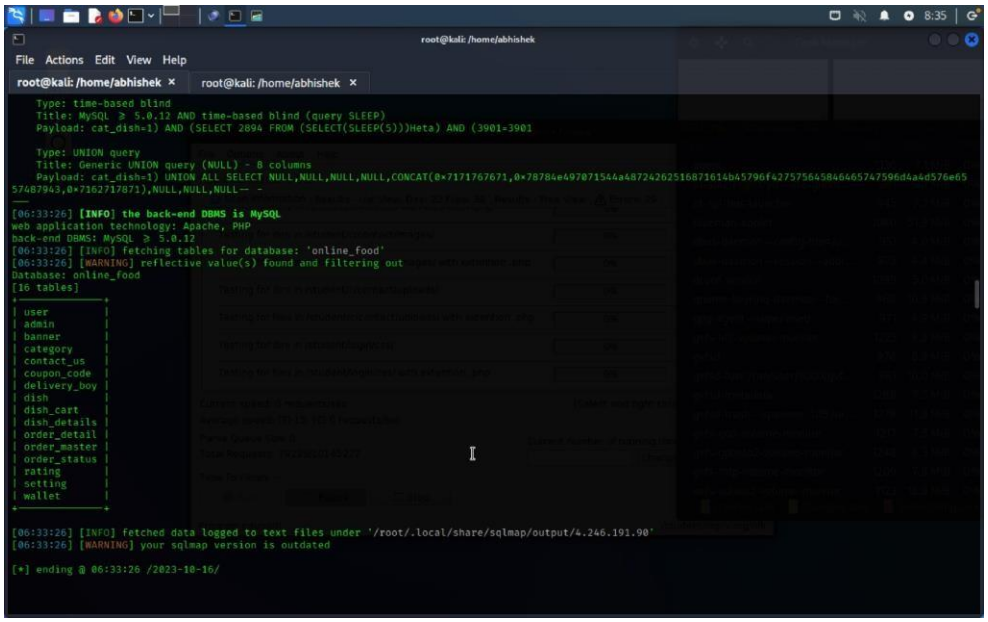
Step 2: Dumping the database by the command shown in Screenshots..



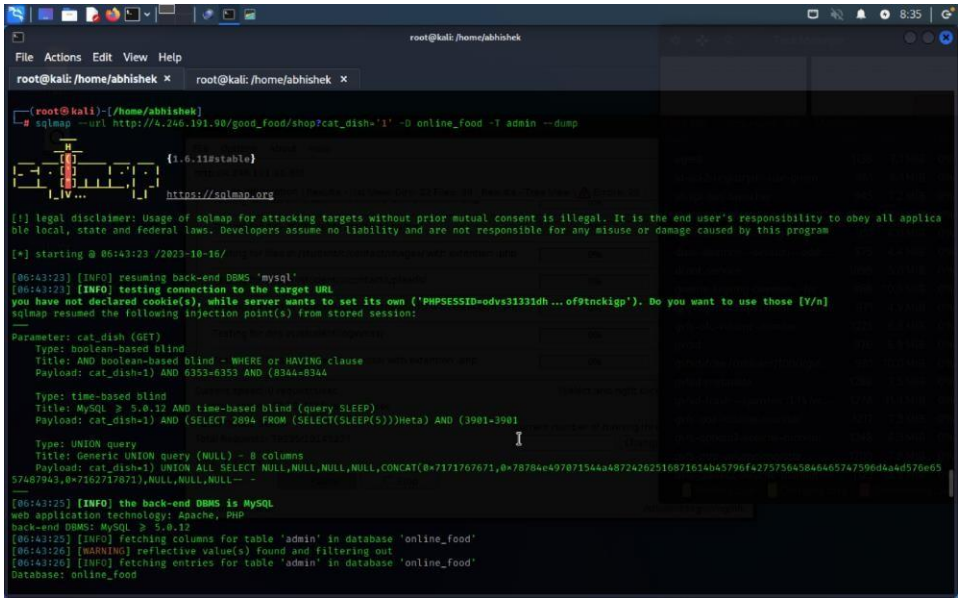
Step 3: Here we got all databases.

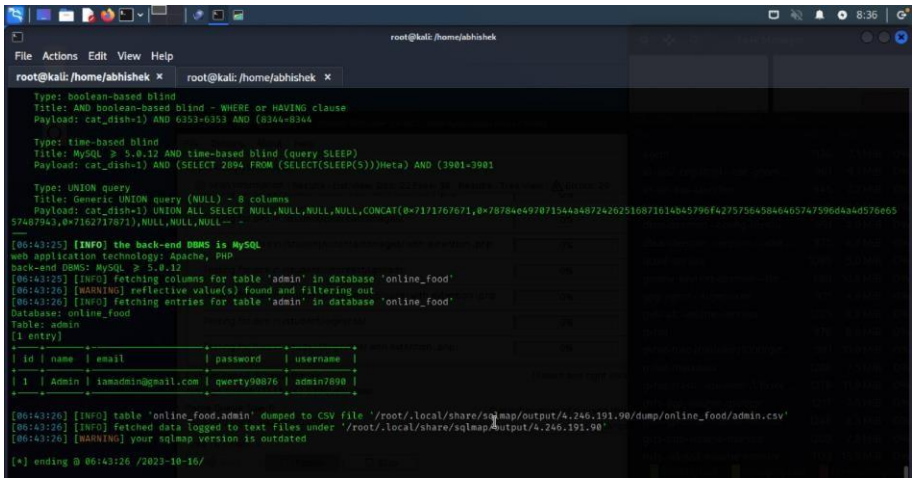


Step 4: Here we got all tables where the data is stored

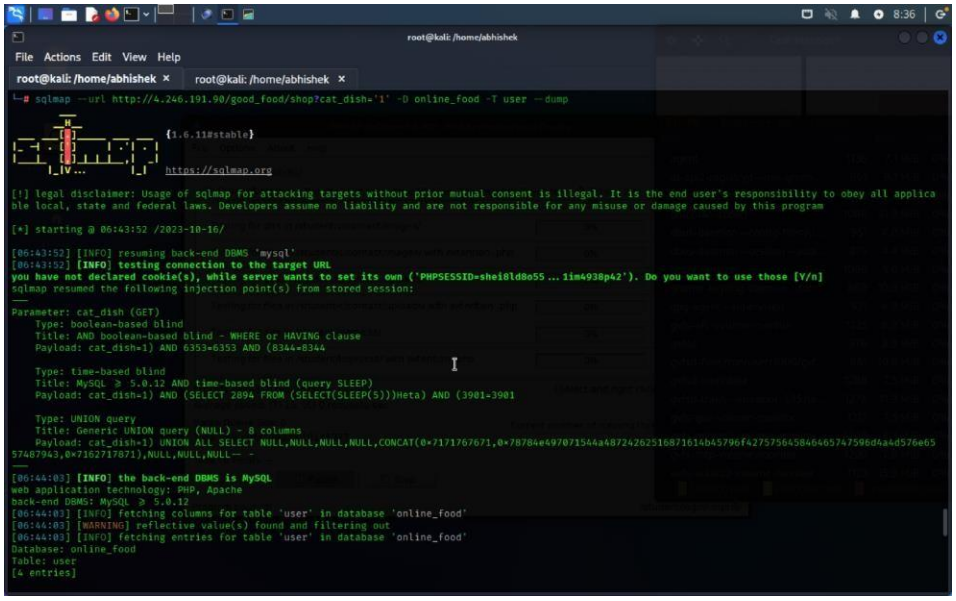


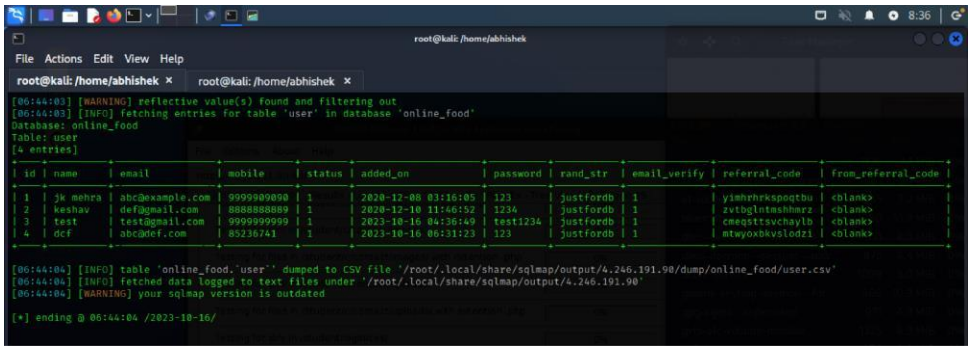
Step 5: Here we will dump the admin and will get all data like username and password of the admin.





Step 6: Here we will dump the users and others too where we can see all the credentials .





Finally after getting these admin and user credential we can login with different roles and permissions.

7. Vulnerability Name : Login page - Anti-CSRF token is missing

OWASP Category : Cross-Site Request Forgery (CSRF)

Description : The absence of an Anti-CSRF token on the login page of the website located at http://4.246.191.90/good_food/ poses a Cross-Site Request Forgery (CSRF) risk. This means that there is no protection against malicious entities potentially tricking users into making unauthorized actions without their consent.

Business Impact : This vulnerability could lead to unauthorized actions being taken on behalf of users, such as changing passwords, making unauthorized transactions, or revealing sensitive information. Such incidents can erode user trust, cause legal and financial consequences, and necessitate immediate attention to ensure user and business security.

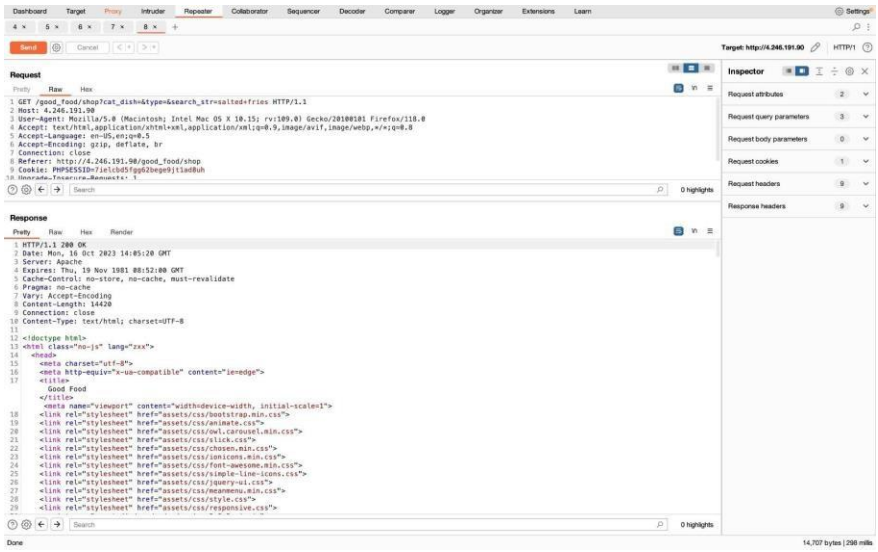
Vulnerability Path :http://4.246.191.90/good_food/

Vulnerability Parameter: **http://4.246.191.90/good_food/admin/user.php**

Steps to Reproduce :

Step 1. Access the URL

Step 2: Open the burpsuite.



Step 3: Turn on the intercept and capture the request.We can see there is no such Tokens generated.

---

8. Vulnerability Name : System information exposed - Version Exposure

OWASP Category : Sensitive Data Exposure

Description : The presence of system information exposed, specifically version details, on the website at http://4.246.191.90/good_food/ can potentially lead to Sensitive Data Exposure. This information may inadvertently reveal details about the website's underlying infrastructure and software.

Business Impact :This vulnerability may provide malicious actors with valuable insights into the website's technology stack, making it easier for them to identify and exploit vulnerabilities. The business impact includes potential security breaches, reputational damage, and financial losses. It's crucial to address this issue promptly to enhance the security and protect sensitive data.

Vulnerability Path :http://4.246.191.90/good_food/

Vulnerability Parameter: **http://4.246.191.90/good_food/admin/user.php**

Steps to Reproduce :

Step 1. Open the Terminal in kali Linux.

Step 2: Use nmap scanning tool to scan the host.

```
┌──(root㉿kali)-[/home/abhishek]
└─# nmap -sV 4.246.191.90
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-16 08:56 PDT
Nmap scan report for 4.246.191.90
Host is up (0.097s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE  SERVICE     VERSION
22/tcp   open   ssh         OpenSSH 8.2p1 Ubuntu 4ubuntu0.9 (Ubuntu Linux; protocol 2.0)
80/tcp   open   http        Apache httpd
443/tcp  closed https
8000/tcp open   http        Apache httpd 2.4.10 ((Debian) PHP/5.6.14)
8001/tcp closed vcom-tunnel
8080/tcp open   http        Apache httpd 2.4.7
Service Info: Host: localhost; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 31.50 seconds
```

Step 3: Here we got the versions of the services.

```
root@kali: /home/abhishek
File  Actions  Edit  View  Help
root@kali: /usr/share/wordlists/dirb ×   root@kali: /home/abhishek ×
Nmap done: 1 IP address (1 host up) scanned in 31.50 seconds

┌──(root㉿kali)-[/home/abhishek]
└─# nmap -A -sV 4.246.191.90
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-16 08:57 PDT
Nmap scan report for 4.246.191.90
Host is up (0.16s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE  SERVICE     VERSION
22/tcp   open   ssh         OpenSSH 8.2p1 Ubuntu 4ubuntu0.9 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 93188829b0c857614da42ba3e9586bfd (RSA)
|   256 35b6aa1322f74e453bda475e94f4d2eb (ECDSA)
|_  256 04696561abbe0a85e80cc5bf458a8545 (ED25519)
80/tcp   open   http        Apache httpd
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache
443/tcp  closed https
8000/tcp open   http        Apache httpd 2.4.10 ((Debian) PHP/5.6.14)
|_http-title: 403 Forbidden
|_http-server-header: Apache/2.4.10 (Debian) PHP/5.6.14
| http-methods:
|_  Potentially risky methods: TRACE
8001/tcp closed vcom-tunnel
8080/tcp open   http        Apache httpd 2.4.7
|_http-title: Index of /
|_http-server-header: Apache/2.4.7 (Ubuntu)
| http-ls: Volume /
| SIZE  TIME              FILENAME
| -     2023-06-13 14:03  xvwa/
|_
OS fingerprint not ideal because: Didn't receive UDP response. Please try again with -sSU
No OS matches for host
Network Distance: 5 hops
Service Info: Host: localhost; OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   25.92 ms 172.20.10.1
2   ... 4
5   55.10 ms 4.246.191.90
```

---

9. Vulnerability Name : Routes were exposed

OWASP Category : Sensitive Data Exposure

Description : The exposure of website routes, as identified on http://4.246.191.90/good_food/, can lead to Sensitive Data Exposure. This issue may unintentionally reveal the structure and functionality of the web application, including specific paths and endpoints.

Business Impact : This vulnerability can be exploited by malicious individuals to gain insights into the application's inner workings, potentially facilitating attacks or unauthorized access. The business impact includes the risk of security breaches, potential data exposure, and reputational harm. Addressing this issue is crucial to enhance the application's security and protect sensitive data.

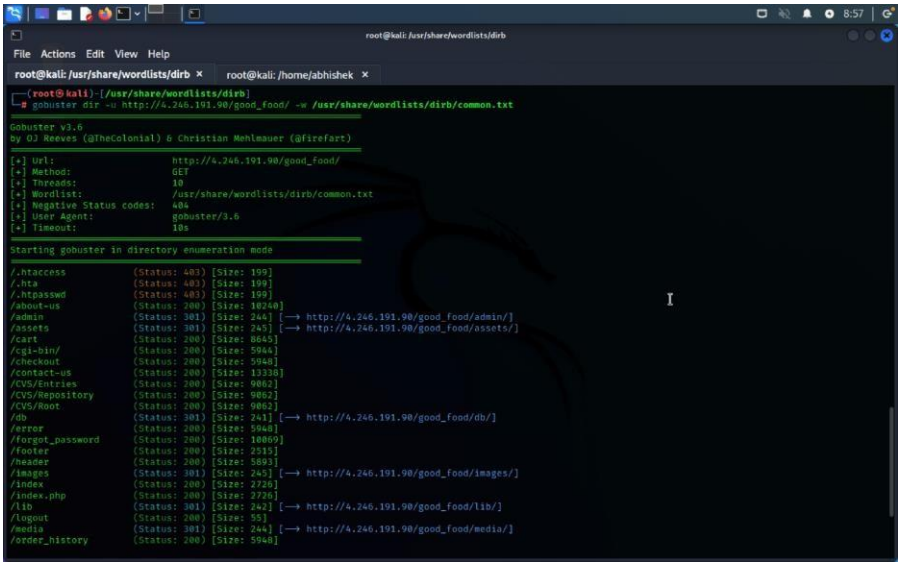
Vulnerability Path :http://4.246.191.90/good_food/

Vulnerability Parameter: **http://4.246.191.90/good_food/admin/user.php**

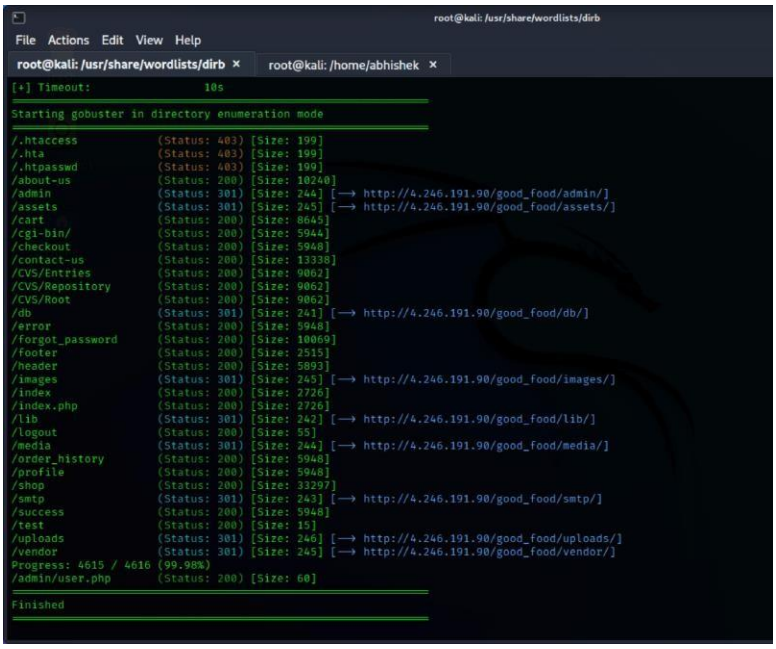
Steps to Reproduce :

Step 1. Open the Terminal

Step 2: use either dirbuster or Gobuster with the URL and choose any wordlist .



Step 3. Here we can see the **Status code=200** means all the routes are working.



10. Vulnerability Name : Parameter Tampering

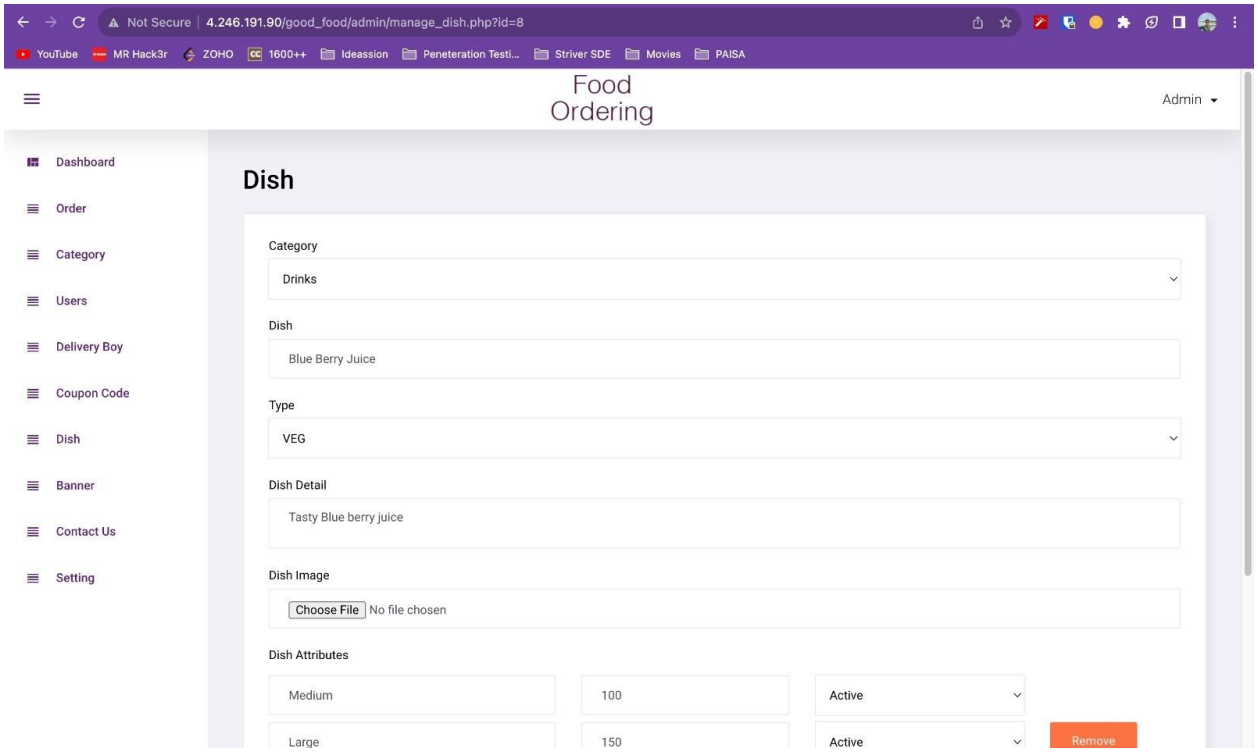
OWASP Category : File inclusion

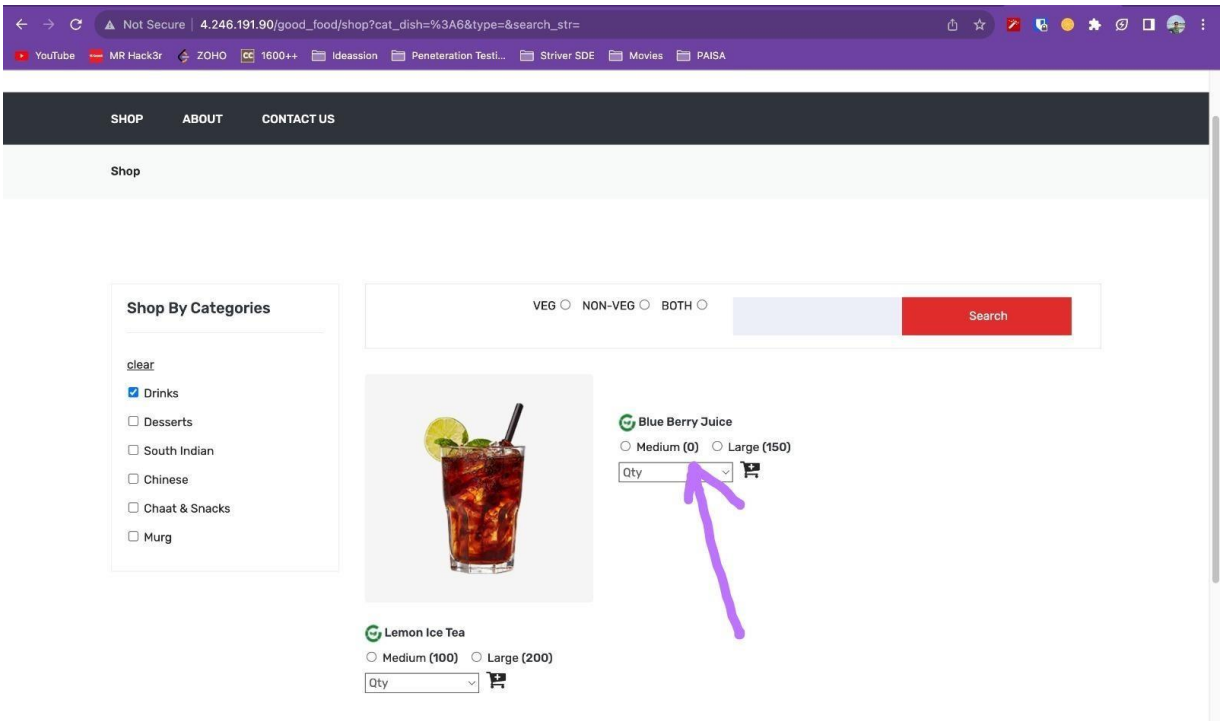
Description : The Web Parameter Tampering attack is based on the manipulation of parameters exchanged between client and server in order to modify application data, such as user credentials and permissions, price and quantity of products, etc. Usually, this information is stored in cookies, hidden form fields, or URL Query Strings, and is used to increase application functionality and control.

Business Impact : This vulnerability allows user to change the price of the food items which will result in Financial Loss to the business.

Vulnerability Path :http://4.246.191.90/good_food/

Vulnerability Parameter: **http://4.246.191.90/good_food/admin/user.php**





Practice Website 2:

1. SQL injection vulnerability in WHERE clause allowing retrieval of hidden data.

Query : - ‘+OR+1=1—

Explanation: - In SQL (Structured Query Language), the '=' operator is used to compare values. When you enter '+OR+1=1—' as part of a query, it is attempting to exploit a vulnerability in the system by injecting a condition that always evaluates to true.

Output:-

2. SQL injection vulnerability allowing login bypass

Query : - administrator’--

Explanation: - In SQL, the single quote (') is used to delimit string values. By appending '--' after the single quote, the intention is to comment out the remainder of the SQL statement. This technique is often used in SQL injection attacks to manipulate the behavior of the query.

Output:-

3. **SQL injection UNION attack, determining the number of columns returned by the query**

Query : - ‘+UNION+SELECT+NULL,NULL--

Explanation: - In SQL, the UNION operator allows you to combine the result sets of two or more SELECT statements. It is often used to retrieve data from different tables or columns. However, when used maliciously, it can be used to extract sensitive information or perform unauthorized actions.

Output:-

4. **SQL injection UNION attack, finding a column containing text**

Query : - '+UNION+SELECT+NULL, 'iJhkab',NULL--

Explanation: - The attacker is selecting a NULL value for the first and third columns, while introducing the string 'iJhkab' as the value for the second column in the result set. This could be an attempt to inject arbitrary data into the result set or exploit a specific vulnerability related to the 'iJhkab' value.

Output:-

Lab: SQL injection UNION attack, finding a column containing text

PRACTITIONER
LAB Solved

5. **SQL injection UNION attack, retrieving data from other tables**

Query : - '+UNION+SELECT+username,+password+FROM+users--

Explanation: - This attack attempts to retrieve the values from the "username" and "password" columns of the "users" table. By selecting these specific columns, the attacker may gain access to sensitive user information, such as usernames and passwords.

Output:-

Lab: SQL injection UNION attack, retrieving data from other tables

PRACTITIONER
LAB Solved

6. **SQL injection UNION attack, retrieving multiple values in a single column**

Query:'+UNION+SELECT+NULL,username||'~'||password+FROM
+users--

Explanation: - This attack attempts to retrieve the concatenated values of the "username" and "password" columns from the "users" table, using the "~" symbol as a separator. This technique is often employed to retrieve sensitive data, such as usernames and passwords, from a compromised database.

Output:-

Lab: SQL injection UNION attack, retrieving multiple values in a single column

PRACTITIONER
LAB Solved

7. **SQL injection with filter bypass via XML encoding**

Query : - <storeId>1 UNION SELECT NULL</storeId>

Explanation: - The attack seems to be injecting a malicious payload into the "<storeId>" XML element, attempting to exploit the application's handling of the data. However, the provided payload "1 UNION SELECT NULL" resembles a SQL injection attack rather than an XML injection.

Output:-

Lab: SQL injection with filter bypass via XML encoding

PRACTITIONER
LAB Solved

8. **HTTP request smuggling, confirming a CL.TE vulnerability via differential responses**

Explanation: HTTP request smuggling is a security vulnerability arising from discrepancies in how various components in a web application handle HTTP headers, specifically Content-Length (CL) and Transfer- Encoding (TE). While HTTP specifications deem it invalid for a request to include both headers, variations in header interpretation across components can lead to inconsistencies. Exploiting a CL.TE vulnerability involves crafting a malicious request with conflicting headers, passing it through components like a front-end proxy and backend server, and observing how each interprets the headers. The attacker then exploits the differences to manipulate processing, potentially allowing for unauthorized access or bypassing security controls. Confirming the vulnerability requires observing differential responses from these components. Responsible disclosure involves reporting the issue and implementing mitigation measures, such as configuring consistent header handling and updating

software. Ethical guidelines must be followed, ensuring activities are conducted with explicit permission to avoid legal consequences.

9. User role controlled by request parameter

Explanation: User role controlled by request parameters refers to a scenario in web applications where the privileges or permissions assigned to a user are determined based on values provided within the HTTP request parameters. Typically, a user's role dictates the actions they are authorized to perform within the application. In this context, the user role is dynamically set or modified by parameters included in the request, such as through URL parameters or form fields. This approach allows for flexibility in assigning different roles to users without requiring explicit changes in user profiles or settings. However, if not properly validated and secured, it poses a security risk, as an attacker might manipulate these parameters to gain unauthorized access or escalate privileges within the system. It is essential for developers to validate and sanitize user inputs, especially those influencing user roles, to prevent potential security vulnerabilities and unauthorized access.

10. Password reset broken logic

Explanation: Password reset broken logic refers to vulnerabilities or flaws in the design and implementation of the password reset functionality in a system. This security issue arises when there are inadequacies in the logic that governs the password reset process, potentially allowing attackers to manipulate or bypass the reset mechanism. Common issues include insufficient authentication checks, weak verification methods, or predictable tokens or links used in the reset process. For instance, if the reset link or token is easily guessable, an attacker might be able to gain unauthorized access to an account. Similarly, if the system lacks proper checks to ensure that the person initiating the password reset is indeed the legitimate account owner, it could lead to unauthorized access or account takeover. Ensuring a robust and secure password reset process is crucial for safeguarding user accounts, and developers should implement strong

authentication mechanisms and employ secure token generation to mitigate the risk of broken logic in password reset functionality.

Main Website:

1. Vulnerability Name: Sensitive Data Exposer

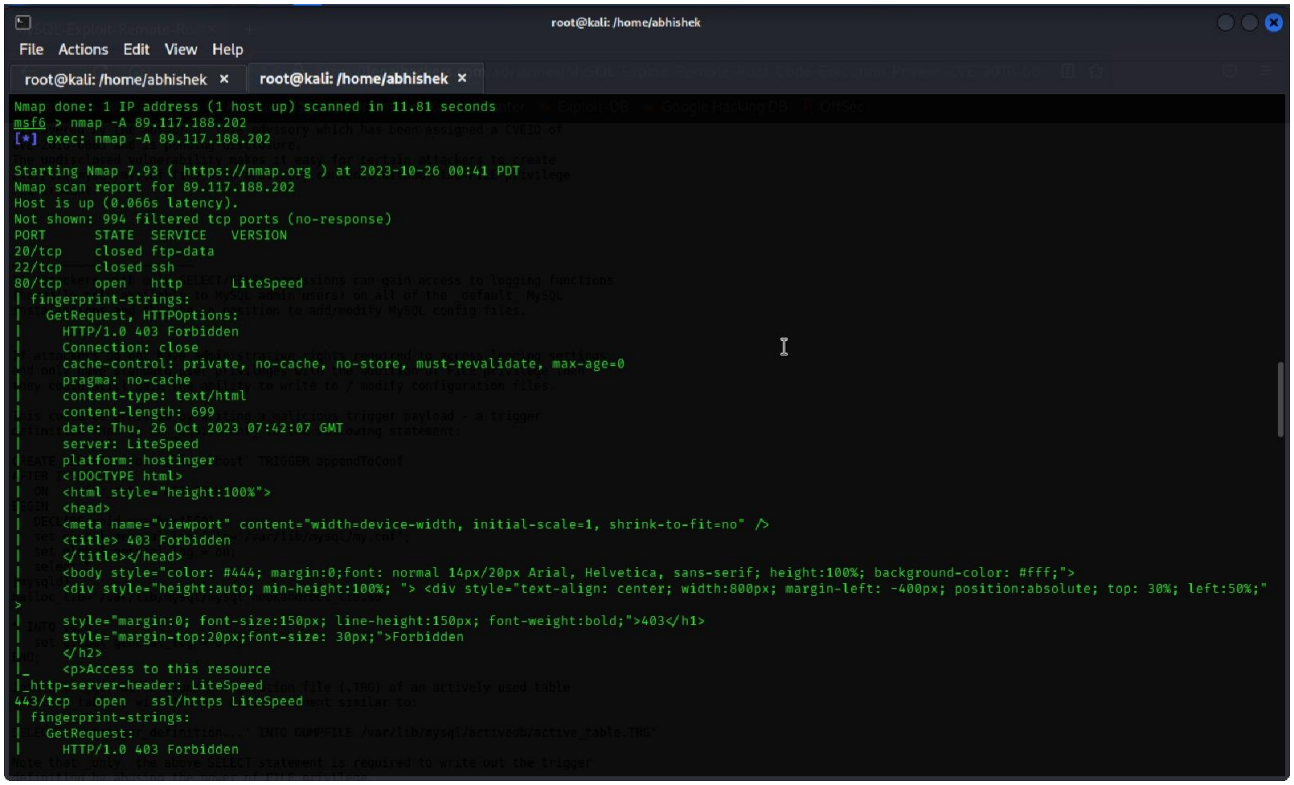
OWASP Category: Inadequate Data Protection

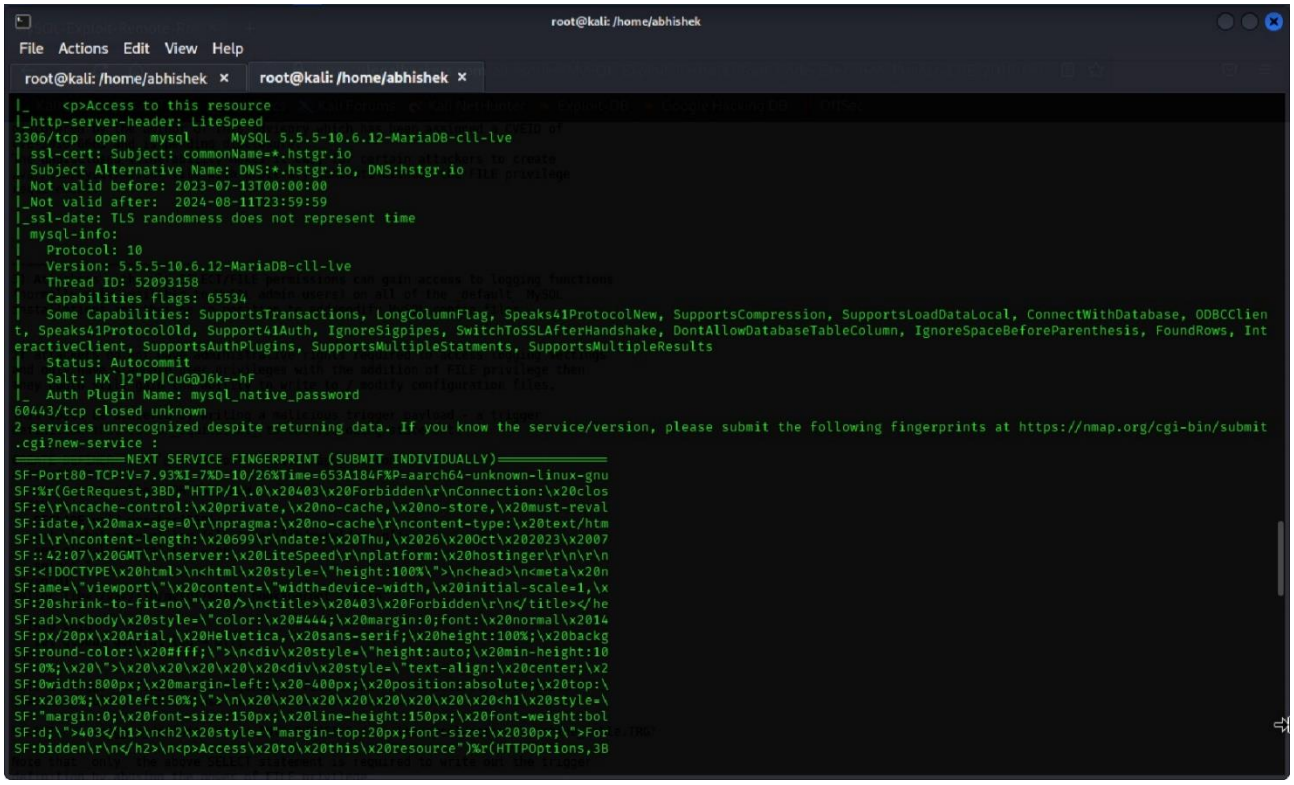
Description: The "Sensitive Data Exposer" vulnerability is a critical security flaw in web applications that puts confidential and personal information at risk. It occurs when sensitive data, such as credit card numbers or personal identification details, is not adequately protected. This can result from weak encryption, poor access controls, or insufficient data storage safeguards. Exploiting this vulnerability can lead to data breaches, financial loss, legal repercussions, and a tarnished reputation for the affected organization. Protecting against this vulnerability requires robust security measures and careful handling of sensitive data to prevent unauthorized access and disclosure.

Business Impact: The impact of a "Sensitive Data Exposer" vulnerability can be severe. It can lead to data breaches, identity theft, financial loss, legal consequences, reputational damage, and loss of customer trust. In addition, organizations may incur costs related to incident response and mitigation.

Vulnerability Path: The vulnerability path for a "Sensitive Data Exposer" can vary widely based on the specific implementation and circumstances of the application. It may involve multiple stages, including data collection, data storage, data transmission, and data access.

Vulnerability Parameter: The vulnerability parameter for a "Sensitive Data Exposer" depends on the specific data and context but can include various parameters where sensitive information is handled. These parameters can be things like input fields, database tables, file storage, APIs, and network communication channels.





2. Vulnerability Name: Hidden URL Discovery

OWASP Category: Unauthorized Access,

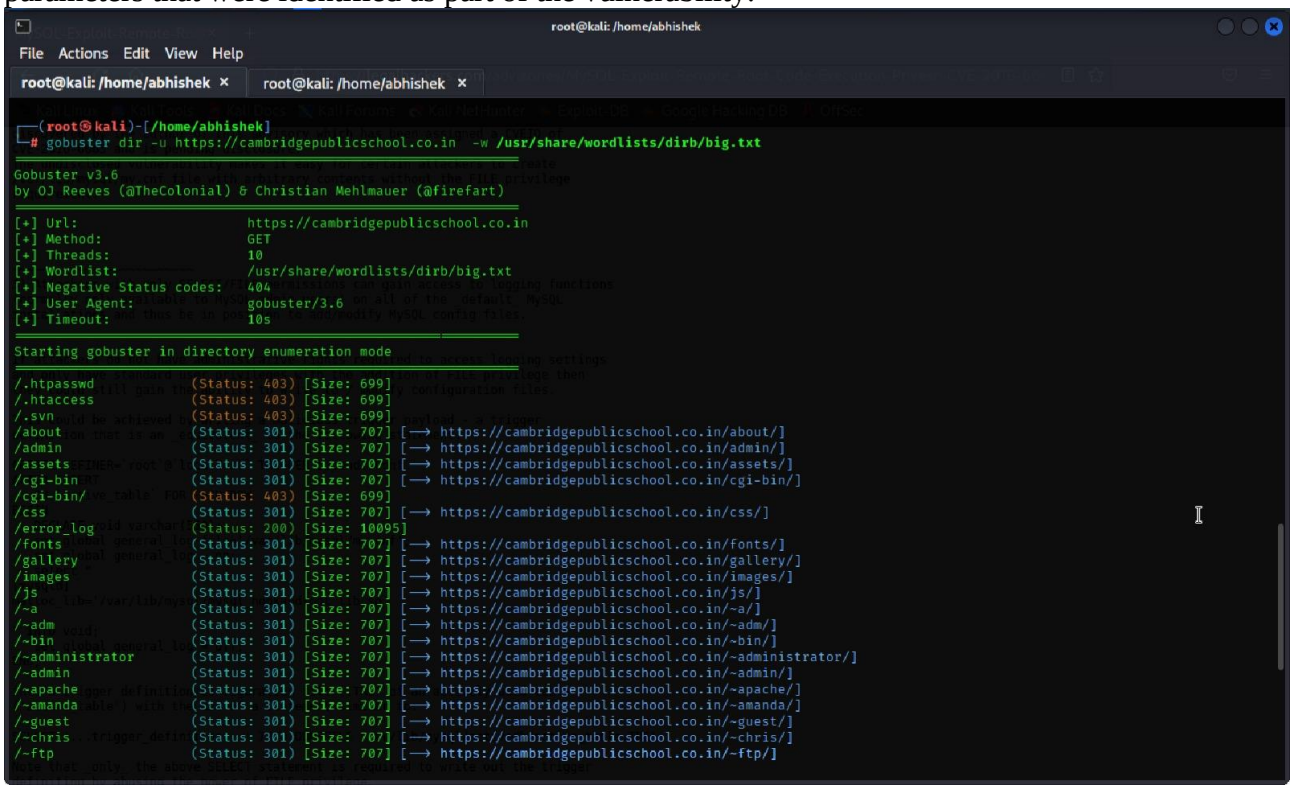
Description: This situation involves the discovery of URLs that were not publicly linked or disclosed but can be accessed through directory and file enumeration. It may occur when a

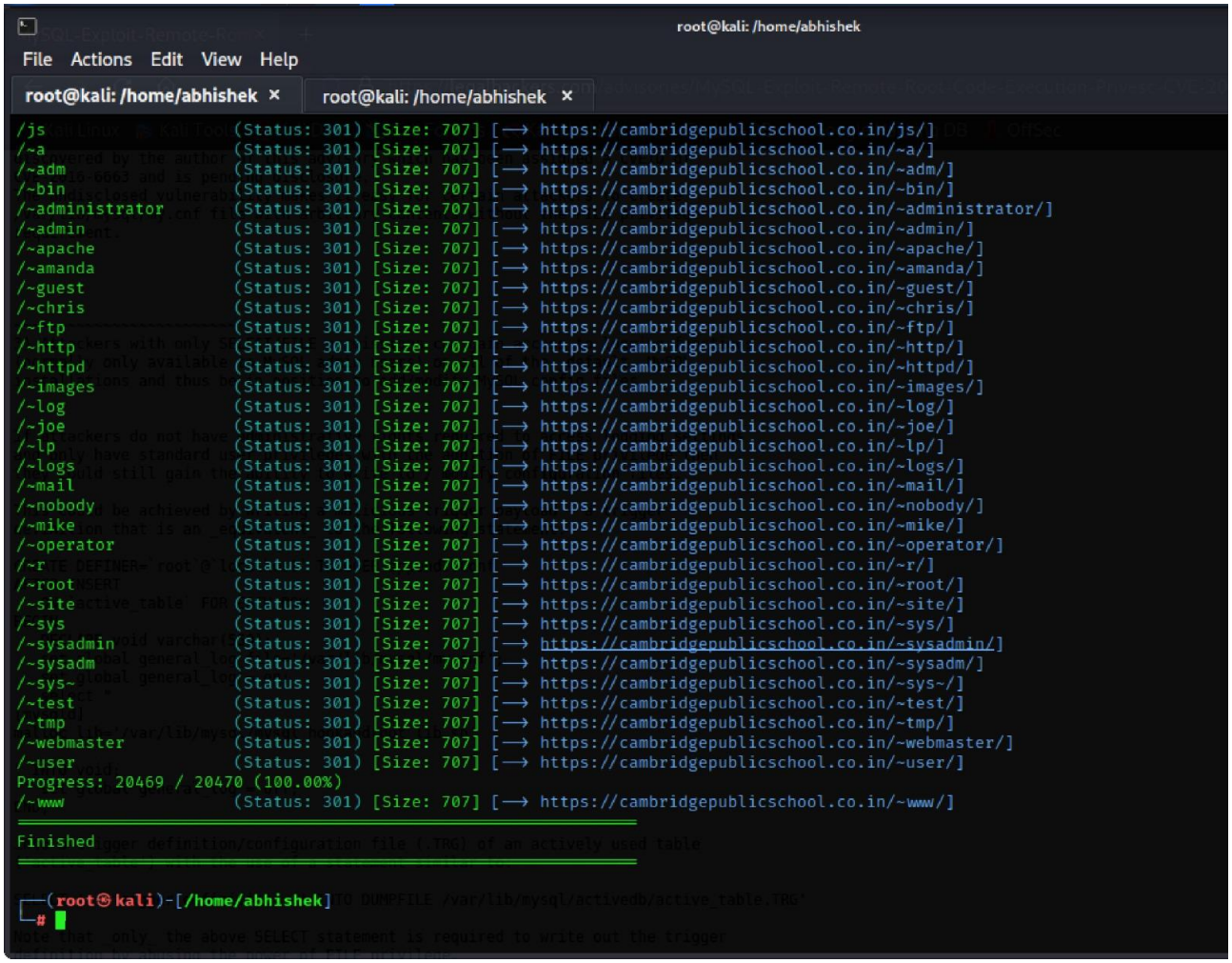
web application exposes URLs or files that should be hidden from public access, which could lead to unauthorized access or information disclosure.

Business Impact: The impact can vary widely depending on what is discovered. It could potentially lead to unauthorized access to sensitive information, data exposure, or other security issues. The impact can range from minimal to severe, depending on what can be accessed and the nature of the web application.

Vulnerability Path: The vulnerability path involves the use of a tool like DirBuster or other directory and file enumeration techniques to discover hidden URLs. The path typically includes running the tool against the web application, analyzing the results, and attempting to access the discovered URLs.

Vulnerability Parameter: The vulnerability parameter would be the specific URLs or files discovered during the enumeration process. These URLs or files can be considered the parameters that were identified as part of the vulnerability.





3.Vulnerability Name: SQL Admin Vulnerability

OWASP Category: Inadequate Security Configuration" or "Insecure Access Control

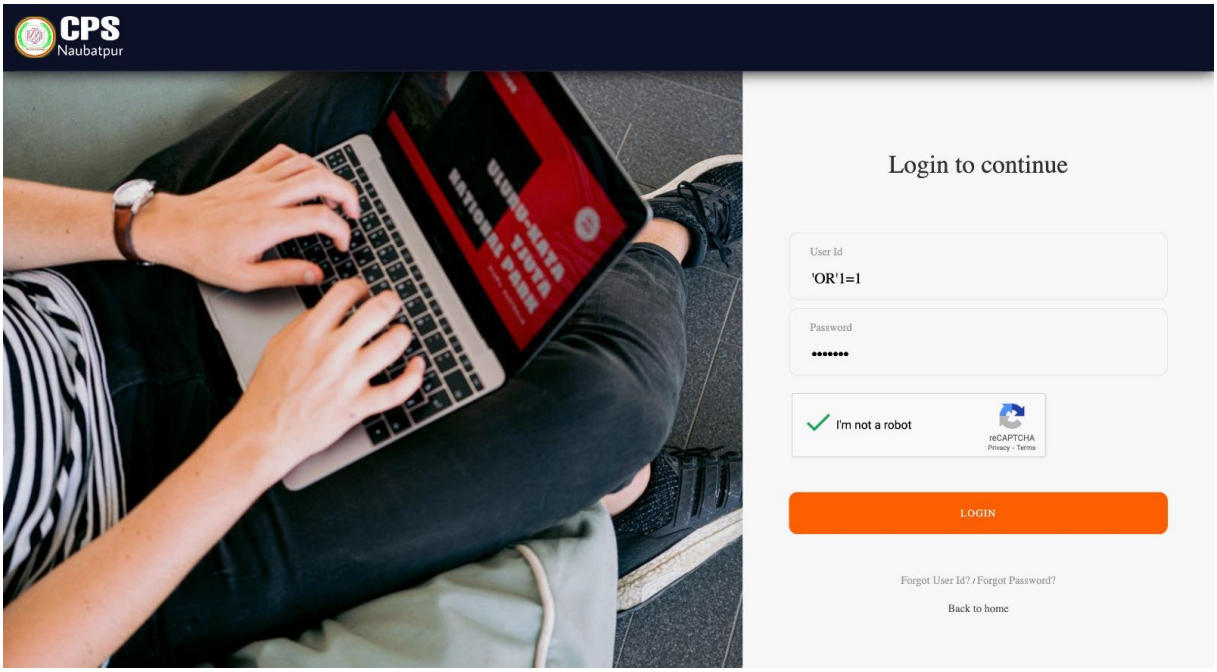
Description: The SQL Admin Vulnerability refers to a situation where the administrative interfaces or configurations of an SQL database are inadequately secured. This may include weak passwords, default credentials, or improper access controls, allowing unauthorized individuals to gain access to the database's administrative features.

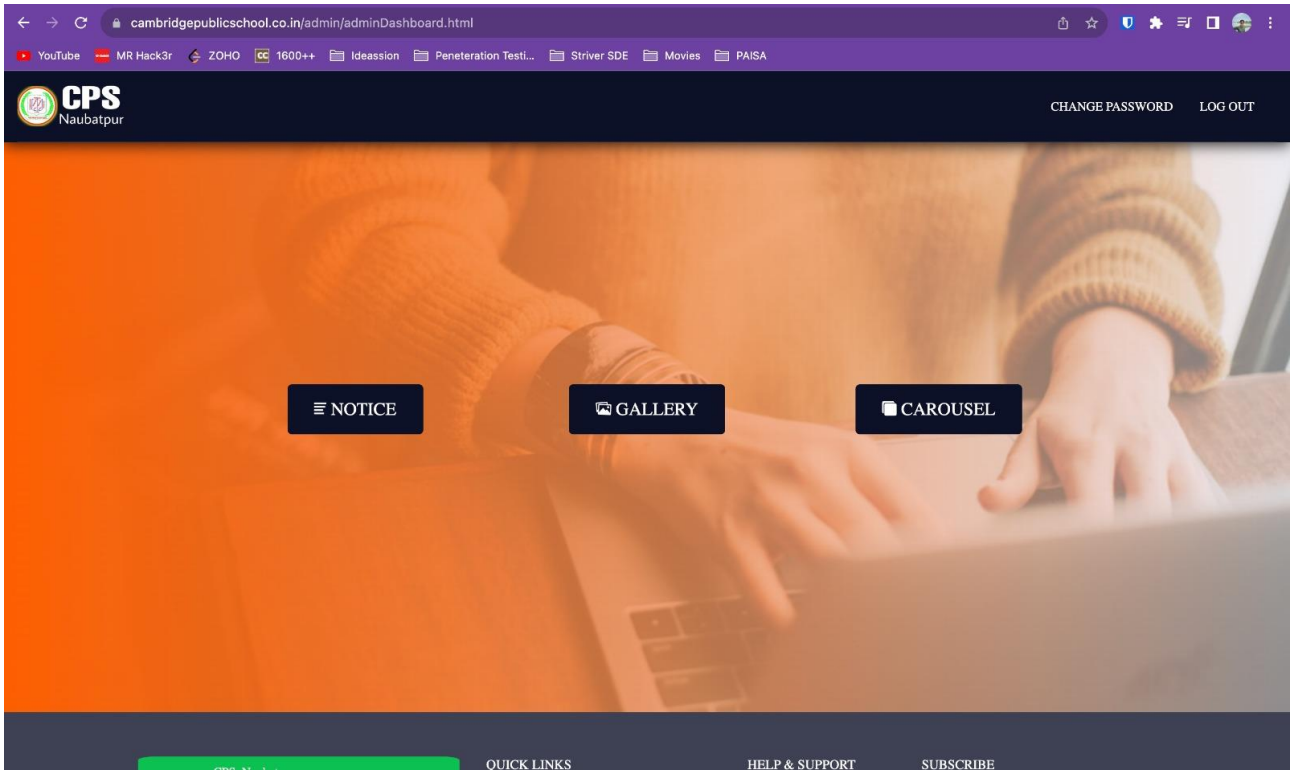
Business Impact: The impact of this vulnerability can be significant. Unauthorized access to the SQL database's administrative functions can lead to data breaches, data manipulation, or even complete database compromise. This can result in data loss, financial loss, reputational damage, and legal consequences.

Vulnerability Path: The vulnerability path involves the identification and exploitation of weak or misconfigured administrative access points. Attackers may attempt to guess passwords, exploit known vulnerabilities, or leverage misconfigurations to gain unauthorized access to the SQL database's admin interfaces.

Vulnerability Parameter: The vulnerability parameters would be the specific administrative interfaces, settings, or configurations that are found to be improperly secured. These could

include login pages, authentication settings, password policies, and access control lists related to SQL administration.





4.Vulnerability Name: SWEET32

OWASP Category: In the OWASP Top Ten, SWEET32 would not have a specific category since it's primarily a cryptographic vulnerability related to outdated encryption algorithms and SSL/TLS.

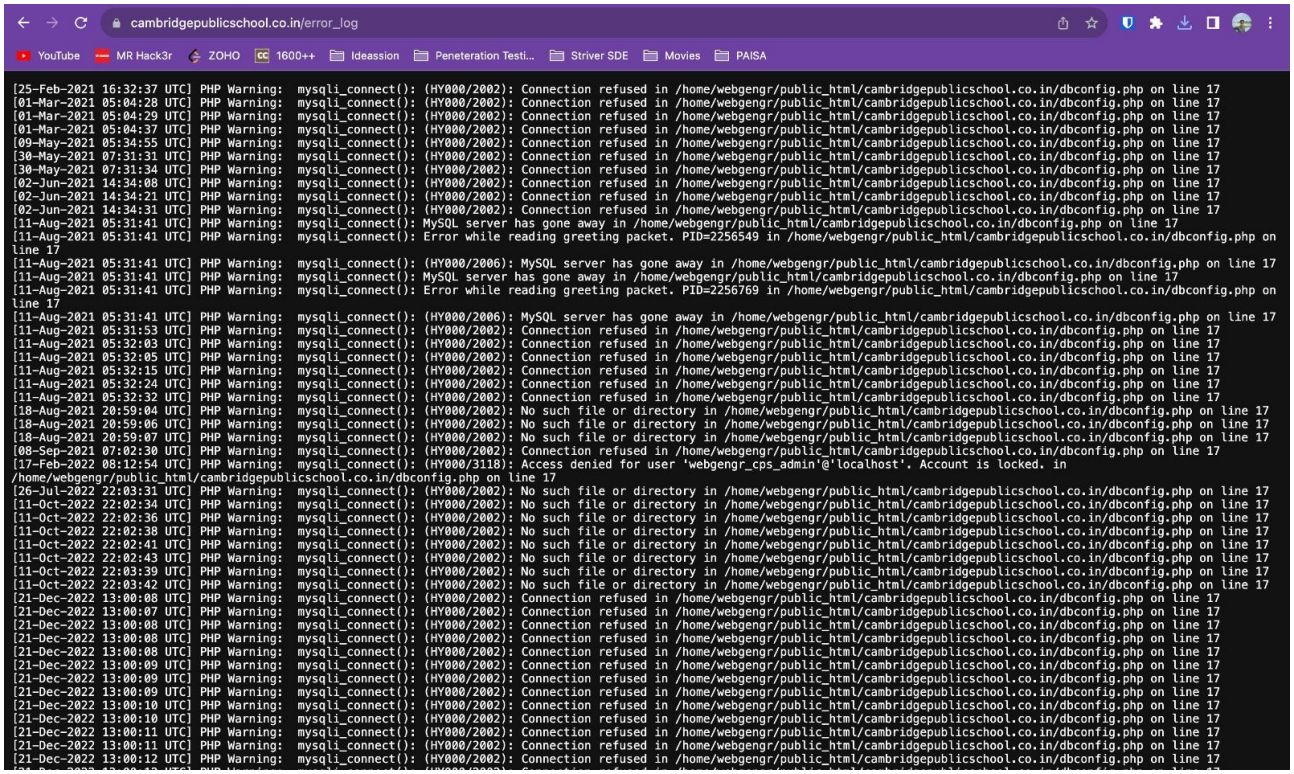
Description: SWEET32 is a vulnerability that arises from the continued use of outdated cryptographic protocols like 3DES in SSL/TLS encryption. It stands for "Security of Web Encryption using Encryption over Triple-DES" and highlights the security implications of maintaining support for these weak encryption algorithms, which can be exploited by attackers.

Business Impact: The impact of SWEET32 is the potential for attackers to carry out a "birthday attack" and decrypt SSL/TLS-encrypted data, potentially exposing sensitive information. This can lead to data breaches, data exposure, and a loss of confidentiality and privacy.

Vulnerability Path: The vulnerability path typically involves attackers exploiting the continued use of 3DES in SSL/TLS to initiate a birthday attack. This may involve eavesdropping on encrypted communication and collecting a sufficient amount of data to carry out the attack.

Vulnerability Parameter: The vulnerability parameters in the context of SQL administration might involve the configuration of the SQL database server, including how it communicates with clients and the encryption protocols it supports. If the SQL database uses SSL/TLS encryption and supports outdated ciphers like 3DES, it could be vulnerable to SWEET32.

To mitigate SWEET32, it's essential to disable the use of weak encryption algorithms like 3DES and ensure that strong, modern encryption protocols are in place for all encrypted communications, including those involving SQL database connections. This vulnerability is not specific to SQL admin vulnerabilities, but securing the underlying infrastructure, including cryptographic protocols, is crucial to overall web application security.



5. Vulnerability Name: Unauthorized Access to Admin URL

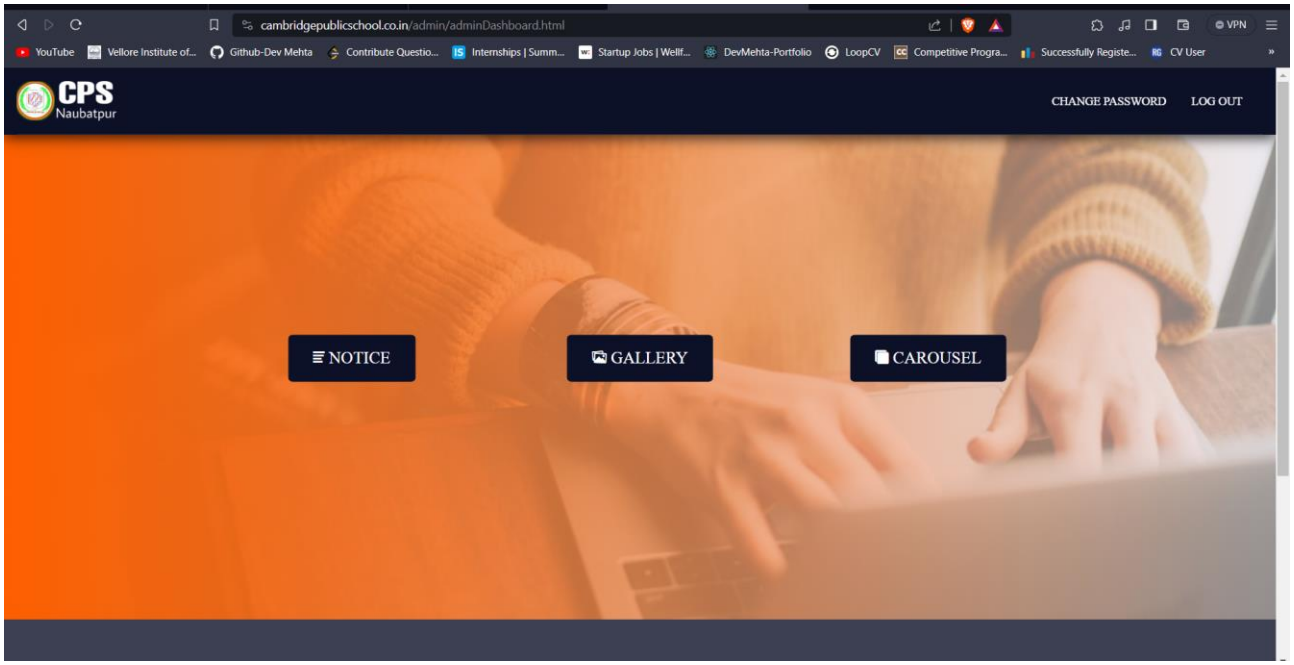
OWASP Category: A5 - Security Misconfiguration

Description: This vulnerability allows an attacker to access the admin URL of a website without the need for proper authentication. Attackers can exploit misconfigured access controls or weak authentication mechanisms to directly access sensitive administrative functionalities or pages reserved for authorized personnel.

Business Impact: Unauthorized access to admin functionalities can lead to unauthorized data manipulation, theft, or deletion. Attackers could potentially disrupt the normal functioning of the website, compromise user data, or deface the site, leading to reputational damage and loss of customer trust.

Vulnerability Path: The vulnerability occurs due to misconfigured access controls or weak authentication mechanisms. It can also result from improper URL handling or lack of proper authorization checks on the server side.

Vulnerability Parameter: The vulnerable parameter in this case is the lack of proper authentication and authorization checks for accessing the admin URL.



On searching this *URL*, it directly opens admin settings without asking for login details.

Stage 2:

Nessus Scans:

Firetable Results

Sun, 01 Jan 2023 00:00:00 +0000 – Sun, 31 Dec 2023 23:59:59 +0000

Project

Firetable v1.0.0 (Firetable/1.0.0)

Tags for CHANGES

Tags for CHANGES

Tag: v1.0.0 (v1.0.0)

Scanned with Firetable v1.0.0 Results 1 – 1 of 1 Sort: Severity

7.1.50.40

Critical	High	Medium	Low	Info
0	0	0	0	1

Host Characteristics

Hostname 7.1.50.40 (rdns)
Operating System Linux 2.6 (Ubuntu 10.04)
Scan Time Mon Jan 01 00:00:00 2023

Port Summary & Vulnerabilities

Port / Service Severity Plugin Name
80 / tcp / www Info Web Server No 404 Response

Info | 80 / tcp / www | Web Server No 404 Response

Synopsis

The remote web server does not return a 404 response for unknown URLs.

Description

The remote web server does not return a 404 response for requests for non-existent URLs. This forces Nessus to rely on other heuristics to determine which URLs are valid on the server.

See Also

http://www.w3.org/Protocols/rfc2616.txt

Solution

Configure the remote web server to return a 404 response for requests for non-existent URLs.

Risk Factor

None

Plugin Information

Plugin ID: 10386
Plugin Family: Web Servers

Plugin Output

```
No 404 response was received to query for a random URL.
Enclosed is the response received to the request:
GET /.nsr HTTP/1.1 ~ Accept: text/plain, text/*, */* ~ User-Agent: mozilla/5.0 (compatible; nessus) ~ Host: 7.1.50.40 ~ Connection: close ~ Pragma: no-cache ~ Content-Type: application/x-www-form-urlencoded ~ Content-Length: 0 ~ ~
HTTP/1.1 200 OK ~ Date: Mon, 01 Jan 2023 00:00:00 GMT ~ Server: Apache/2.2.14 (Ubuntu) ~ Vary: Accept-Encoding,User-Agent ~ Content-Length: 1 ~ Connection: close ~ Content-Type: text/plain ~ ~ 1
```

Postman Sandbox

Sandbox Overview

Sandbox Scripts

- Request Scripts
- Response Scripts
- Sandbox Overview
- Sandbox Variables
- Sandbox Modules
- Sandbox Built-in Libraries
- Sandbox Timeout
- Sandbox Memory Limit
- Sandbox Execution Limits
- Sandbox Network Access
- Sandbox Error Handling
- Sandbox Debugging
- Sandbox Performance Tips
- Sandbox Security Model
- Sandbox Limitations
- Sandbox Quick Reference
- Sandbox Troubleshooting
- Sandbox Frequently Asked Questions
- Sandbox Glossary

Sandbox Overview

Postman Sandbox

Sandbox Overview

Postman Sandbox is a secure execution environment that runs your pre-request scripts and test scripts. Your code runs in a sandbox that limits what it can access for security and stability.

Sandbox Variables

Sandbox Variables

Sandbox variables are temporary variables that exist only during the execution of your pre-request scripts and test scripts. They are cleared after each request completes.

Sandbox Modules

Sandbox Modules

Sandbox modules are built-in libraries that provide functionality for your scripts. Some modules are available by default, while others require explicit imports.

Sandbox Built-in Libraries

Sandbox Built-in Libraries

Sandbox built-in libraries are modules that are available by default in your scripts. They provide common functionality for data processing, cryptography, and more.

Sandbox Timeout

Sandbox Timeout

Sandbox timeout is the maximum time your scripts can run before they are terminated. This prevents infinite loops and long-running scripts from blocking the system.

Sandbox Memory Limit

Sandbox Memory Limit

Sandbox memory limit is the maximum amount of memory your scripts can use. This prevents memory leaks and ensures system stability.

Sandbox Execution Limits

Sandbox Execution Limits

Sandbox execution limits are the maximum number of operations your scripts can perform. This prevents infinite loops and ensures system performance.

Sandbox Network Access

Sandbox Network Access

Sandbox network access allows your scripts to make HTTP requests to external APIs. This is limited for security and performance.

Sandbox Error Handling

Sandbox Error Handling

Sandbox error handling provides ways to catch and handle errors in your scripts. Proper error handling ensures your scripts work reliably.

Sandbox Debugging

Sandbox Debugging

Sandbox debugging provides tools to help you find and fix issues in your scripts. Use console.log() and console.error() to output debug information.

Sandbox Performance Tips

Sandbox Performance Tips

Sandbox performance tips help you write efficient scripts that run quickly and use resources wisely.

Sandbox Security Model

Sandbox Security Model

Sandbox security model ensures your scripts run safely and cannot access sensitive system resources.

Sandbox Limitations

Sandbox Limitations

Sandbox limitations are the restrictions that prevent your scripts from accessing sensitive system resources.

Sandbox Quick Reference

Sandbox Quick Reference

Sandbox quick reference provides a quick overview of the most commonly used sandbox features.

Sandbox Troubleshooting

Sandbox Troubleshooting

Sandbox troubleshooting provides solutions to common problems you may encounter when using the sandbox.

Sandbox Frequently Asked Questions

Sandbox Frequently Asked Questions

Sandbox frequently asked questions provides answers to common questions about the sandbox.

Sandbox Glossary

Sandbox Glossary

Sandbox glossary provides definitions of terms used in the sandbox.

Zomato-1

Thu, 26 Oct 2023 11:20:24 India Standard Time

TABLE OF CONTENTS

Vulnerabilities by Plugin

- 11219 (2) - Nessus SYN scanner
- 10107 (1) - HTTP Server Type and Version
- 10287 (1) - Traceroute Information
- 11936 (1) - OS Identification
- 10053 (1) - Host Fully Qualified Domain Name (FQDN) Resolution
- 19506 (1) - Nessus Scan Information
- 22964 (1) - Service Detection
- 24260 (1) - HyperText Transfer Protocol (HTTP) Information
- 25220 (1) - TCP/IP Timestamps Supported
- 45590 (1) - Common Platform Enumeration (CPE)
- 54615 (1) - Device Type

Vulnerabilities by Plugin

Collapse All | Expand All

11219 (2) - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

23.206.173.42 (tcp/80/www)

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

23.206.173.42 (tcp/443)

```
Port 443/tcp was found to be open
```

10107 (1) - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

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

Plugin Output

23.206.173.42 (tcp/80/www)

```
The remote web server type is :
AkamaiGHost
```

10287 (1) - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/11/27, Modified: 2023/06/26

Plugin Output

23.206.173.42 (udp/0)

```
For your information, here is the traceroute from 192.168.1.3 to 23.206.173.42 :
192.168.1.2

An error was detected along the way.

An error was detected along the way.
10.10.10.1
100.71.128.1
100.64.0.253
125.98.55.253
?
103.77.108.22
?
23.206.173.42

Hop Count: 10
```

11936 (1) - OS Identification

Synopsis

It is possible to guess the remote operating system.

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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2022/03/09

Plugin Output

23.206.173.42 (tcp/0)

```
Remote operating system : Linux Kernel 2.6
Confidence level : 65
Method : SinFP

The remote host is running Linux Kernel 2.6
```

10053 (1) - Host Fully Qualified Domain Name (FQDN) Resolution

Synopsis

It was possible to resolve the name of the remote host.

Description

Nessus was able to resolve the fully qualified domain name (FQDN) of the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/02/11, Modified: 2017/04/14

Plugin Output

23.206.173.42 (tcp/0)

```
23.206.173.42 resolves as a23-206-173-42.deploy.static.akamaitechnologies.com.
```

19506 (1) - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

23.206.173.42 (tcp/0)

```
Information about this scan :

Nessus version : 10.6.1
Nessus build : 20003
Plugin feed version : 202310240550
Scanner IP : 192.168.1.3
Scanner OS : WINDOWS
Scanner Port Range : win-x86-64
Ping RTT : 10.610 ms
Thorough tests : no
Parallel hosts : 5
Plugin debugging enabled : no
Paranoia level : 1
It is frequent : 0
Safe checks : yes
Optimize the test : yes
Disable confirmed tests : no
Path Mondrian check : None
Display superseded patches : yes (supersedence plugin launched)
Number of IPs : 1
Web application tests : disabled
Port range : all
Max checks : 5
Max hosts : 30
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2023/10/26 11:09 India Standard Time
Scan duration : 1 sec
Scan for malware : no
```

22964 (1) - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2023/07/10

Plugin Output

23.206.173.42 (tcp/80/www)

```
A web server is running on this port.
```

24260 (1) - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

23.206.173.42 (tcp/80/www)

```
Response Code : HTTP/1.0 400 Bad Request

Protocol version : HTTP/1.0
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Server: AkamaiGHost
  Mime-Version: 1.0
  Content-Type: text/html
  Content-Length: 215
  Expires: Thu, 26 Oct 2023 06:44:39 GMT
  Date: Thu, 26 Oct 2023 05:44:39 GMT
  Connection: close

  Response Body :

  <HTML><HEAD>
  <TITLE>Invalid URL</TITLE>
  </HEAD><BODY>
  <H1>Invalid URL</H1>
  The requested URL&#91;&#93;, rqst&#32;URL&#61;&#91;&#93;, is invalid.<p>
  Reference&#32;&#45;&#45;&#46;&#46;&#46
```

Stage 3:

Understanding SOC, SIEM and QRadar:

1. Introduction to SOC

An organization's centralized unit in charge of keeping an eye on, evaluating, and protecting its information systems and assets is known as a Security Operations Centre (SOC). Keeping the organization's networks, data, and IT infrastructure secure against online attacks is its main goal. A SOC's primary duties consist of:

- `Monitoring` Constantly keeping an eye on user behaviour, system activity, and network traffic for any odd trends that could point to a security concern.
- `Incident Detection` Identifying and categorizing security occurrences via monitored data analysis is known as incident detection. To identify abnormalities, it's necessary to understand what typical behaviour looks like.
- `Incident Response` Creating and putting into practice plans to prevent and quickly address security problems. This can entail deploying fixes, deleting malware, and isolating the afflicted systems.
- `Forensics` Investigating security incidents to determine the type and scale of an attack, assisting in strengthening security protocols, and averting further occurrences are referred to as forensics.

By offering continuous monitoring and quick reaction, SOCs play a critical role in an organization's cybersecurity strategy by reducing the effect of security breaches and preserving the confidentiality, integrity, and availability of data and systems.

2. SIEM Systems

Modern cybersecurity relies heavily on Security Information and Event Management (SIEM) systems because they allow businesses to gather, analyze, and correlate security data from diverse sources in real-time. Effective security threat monitoring and response are made possible for organizations by SIEM through:

- `Log Collection` The process of collecting log data from host systems, apps, and other elements of the organization's IT infrastructure.
- `Correlation` It is the process of comparing recorded security events to find trends, possible dangers, or vulnerabilities. Correlation makes it easier to spot complex assaults that individual event analysis could miss.
- `Alerting` Instantaneous notification of security administrators when a predetermined security incident takes place. These warnings allow for an immediate reaction to possible security problems.
- `Compliance Reporting` Creating reports to demonstrate that the organization's security procedures are in place and operating as intended, in accordance with internal rules and industry laws.

3. QRadar Overview

IBM QRadar is a leading SIEM solution that provides advanced security intelligence and analytics. Key features and benefits of IBM QRadar include:

- `Advanced Analytics` To identify advanced threats and atypical activity in real-time, QRadar uses behavioral analytics and machine learning.
- `Comprehensive Log Management` Gathers and examines log data from a range of sources, such as network devices, security appliances, operating systems, and applications.
- `Incident Forensics` Provides in-depth insight into security occurrences, assisting in thorough forensic examination.
- `User Behaviour Analytics` Analyzing user behaviour helps to spot compromised accounts and insider threats by tracking user actions and behaviours.
- `Cloud and On-Premises Deployment` QRadar offers flexibility by supporting both on-premises and cloud-based deployments, allowing businesses to select the one that best meets their needs and infrastructure.

4. Use Cases

Here are some actual use scenarios and illustrations of how a SOC may utilise a SIEM system like IBM QRadar to identify and react to security incidents:

- `Detecting Malware` QRadar can be used to detect malware infections by analyzing security logs for suspicious activity, such as unusual file access or network traffic patterns.
- `Detecting data breaches` QRadar can be used to detect data breaches by analyzing security logs for suspicious activity, such as unauthorized access to sensitive data or large-volume data transfers.
- `Detecting insider threats` QRadar can be used to detect insider threats by analyzing security logs for suspicious activity by users with privileged access or users who are accessing unusual data or systems.
- `Investigating security incidents` QRadar can be used to investigate security incidents by providing analysts with a centralized view of all relevant security data. This helps analysts to quickly understand the scope of the incident and identify the root cause.
- `Responding to security incidents` QRadar can be used to respond to security incidents by providing analysts with tools to quarantine infected systems, block malicious traffic, and notify appropriate personnel.

Overall, SIEM systems like IBM QRadar are essential tools for SOCs to *detect, investigate, and respond to security incidents effectively.*

Conclusion:

In conclusion, the development of the AI-enhanced security analytics dashboard outlined in this project abstract holds immense promise for revolutionizing how organizations approach cybersecurity. By focusing on key aspects such as data collection, AI-powered analytics, user-friendly interface, trend analysis, risk assessment, alerting mechanisms, and comprehensive reporting, the project aims to empower security professionals with real-time insights into security events, trends, and risks. The emphasis on enhancing security posture, streamlining operations, fostering proactive security measures, and enabling data-driven decision-making underscores the project's strategic importance in the realm of cybersecurity.

The meticulous planning outlined in the abstract, from requirements gathering to ongoing monitoring and maintenance, demonstrates a comprehensive approach that ensures the successful execution and integration of the security analytics dashboard into an organization's existing infrastructure. Through collaboration with stakeholders, careful technology selection, rigorous development and testing, seamless deployment, thorough training, and continuous monitoring, the project is poised to significantly enhance the cybersecurity landscape for the organization.

Future Scope:

Looking ahead, there are several avenues for future development and enhancement of the AI-enhanced security analytics dashboard:

1. **Continuous Innovation:** Embrace emerging technologies and advancements in artificial intelligence and machine learning to continuously improve the dashboard's analytical capabilities. Regular updates to algorithms and incorporating new data sources can enhance the accuracy and effectiveness of threat detection.
2. **Integration with Threat Intelligence:** Integrate the dashboard with external threat intelligence feeds to enrich the analysis. By leveraging external data sources, the dashboard can provide a more comprehensive view of potential threats and vulnerabilities, enabling organizations to stay ahead of evolving cyber threats.
3. **Predictive Analytics:** Explore the implementation of predictive analytics to forecast potential security threats based on historical data patterns. Predictive modeling can help organizations anticipate future attacks and vulnerabilities, allowing for proactive mitigation strategies.
4. **Behavioral Analytics:** Incorporate behavioral analytics to analyze user and entity behavior within the network. By identifying deviations from normal behavior patterns, the dashboard can detect insider threats and compromised accounts, enhancing the organization's overall security posture.
5. **Collaborative Security:** Enable collaborative features within the dashboard, allowing security teams to share threat intelligence and collaborate on incident response. Facilitating communication and information sharing among security professionals can lead to faster response times and more effective threat mitigation.

6. **Enhanced User Experience:** Continuously refine the user interface and user experience based on feedback from security professionals. An intuitive and user-friendly dashboard ensures that security teams can easily interpret complex data, enabling quick and informed decision-making during critical security incidents.
7. **Compliance and Reporting:** Extend the dashboard's capabilities to facilitate compliance management by automating regulatory compliance checks and reporting. This feature would be invaluable for organizations operating in highly regulated industries, ensuring adherence to legal and industry-specific security requirements.

By exploring these future avenues, the AI-enhanced security analytics dashboard can evolve into a sophisticated, adaptive, and indispensable tool for organizations aiming to fortify their cybersecurity defenses in the face of ever-evolving cyber threats.