Team 2.5
CyberSpectrum

STAGE 1

Overview :-

In today's interconnected and digital world, cybersecurity is a paramount concern for organizations of all sizes and industries. The project, "Enhancing Organizational Cybersecurity Resilience," aims to establish a robust cybersecurity framework to protect an organization's digital assets, data, and infrastructure from a wide range of cyber threats. The project's primary objective is to create a comprehensive and proactive approach to cybersecurity, aligning with the organization's business objectives and risk tolerance.

Key Project Steps and Objectives:-

- Cybersecurity Policy and Strategy Development: The project will begin by crafting a clear and well-defined cybersecurity policy and strategy. This strategic framework will serve as a guide for all cybersecurity initiatives, aligning them with the organization's overarching goals and risk management strategies.

- Risk Assessment and Mitigation: A thorough risk assessment will be conducted to identify potential cybersecurity threats and vulnerabilities specific to the organization. Risks will be prioritized based on their potential impact and likelihood of occurrence. Risk mitigation measures will be implemented, and a risk management plan will be created to address identified vulnerabilities.

- Access Control and Authentication: Strong access control measures will be put in place to ensure that only authorized personnel can access sensitive data and critical systems. Multi-factor authentication (MFA) will be implemented for an additional layer of security.

- Network Security: The project will deploy firewalls, intrusion detection/prevention systems (IDS/IPS), and secure gateways to monitor and control network traffic, ensuring that unauthorized access and malicious activities are promptly identified and blocked.

- Endpoint Security: Antivirus software, endpoint protection tools, and host-based firewalls will be installed on all devices to defend against malware and other threats at the device level, enhancing the security of endpoints.

- Data Encryption: Sensitive data will be encrypted both at rest and in transit to prevent unauthorized access and ensure data confidentiality, even in the event

of a breach.

- Patch Management: A systematic process will be established to apply security patches and updates promptly to all software, operating systems, and firmware to address known vulnerabilities and reduce the organization's exposure to threats.

- Incident Response Planning: The project will develop a well-defined incident response plan (IRP) to effectively handle cybersecurity incidents. This IRP will include guidelines for identifying, reporting, containing, eradicating, and recovering from security incidents, minimizing potential damage and downtime.

- Security Audits and Assessments: Regular internal and external security audits and assessments will be conducted to evaluate the organization's security posture and identify potential weaknesses or gaps. These evaluations will ensure that the cybersecurity framework remains effective and up-to-date.

- Monitoring and Logging: The project will implement centralized logging and real-time monitoring of network and system activities to detect and respond to suspicious activities promptly, minimizing the impact of potential security incidents.

List of teammates–

S.no	Name	College	Contact
1	Anondita Dutta	VIT Bhopal	Anondita.dutta2021@vitbhopal.ac.in
2	Hardik Kanane	VIT Bhopal	Hardik.kankane2021@vitbhopal.ac.in
3	Elisabeth Varghese	VIT Bhopal	Elisabeth.varghese2021@vitbhopal.ac.in

Website: www.testfire.net
IP Address: 65.61.137.117

List of Vulnerability Table

S.no	VulnerabilityName	CWE - No
1	SQL injection	89: Improper Neutralization of Special Elements used in an SQL Command
2	Brute Force Attack	1391: Use of Weak Credentials
3	Broken authentication	285: Improper Authorization
4	Improper Input Validation	132: Miscalculated Null Termination
5	Web server allows password auto-completion	CWE-310: Cryptographic Issues
6	Clickjacking	CWE-1021: Improper Restriction of Rendered UI Layers or Frames
7	HTML injection attack	CWE - 601: URL Redirection to Untrusted Site ('Open Redirect')
8	Cross site scripting (stored)	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
9	Cleartext Transmission of Sensitive Information	CWE-319: Cleartext Transmission of Sensitive Information
10	Insecure Direct object Reference	CWE-639: Authorization Bypass Through User-Controlled Key

REPORT:-

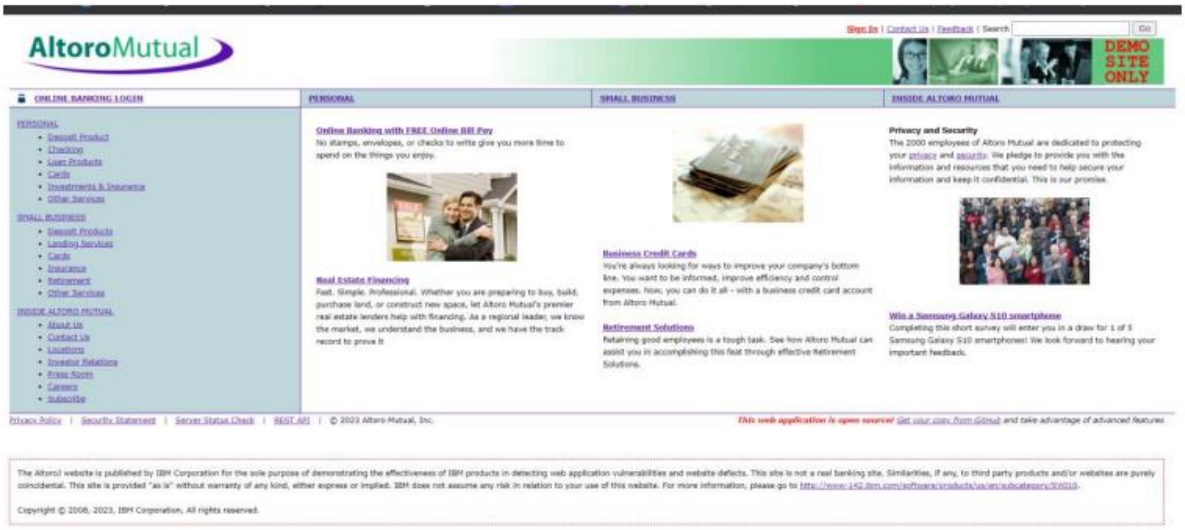
1. **Vulnerability name**: SQL injection
   CWE: 89

Description: The product constructs all or part of an SQL command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended SQL command when it is sent to a downstream component. Business Impact: In summary, it is crucial to underscore that CWE-89, known as SQL Injection, can exert a profound and diverse business impact. This encompasses critical facets such as data breaches, financial setbacks, harm to reputation, legal ramifications, and operational turmoil. Hence, the imperative of preventing and remedying SQL injection vulnerabilities cannot be overstated, as it is indispensable for fortifying the security and continuity of an organization's applications and data.

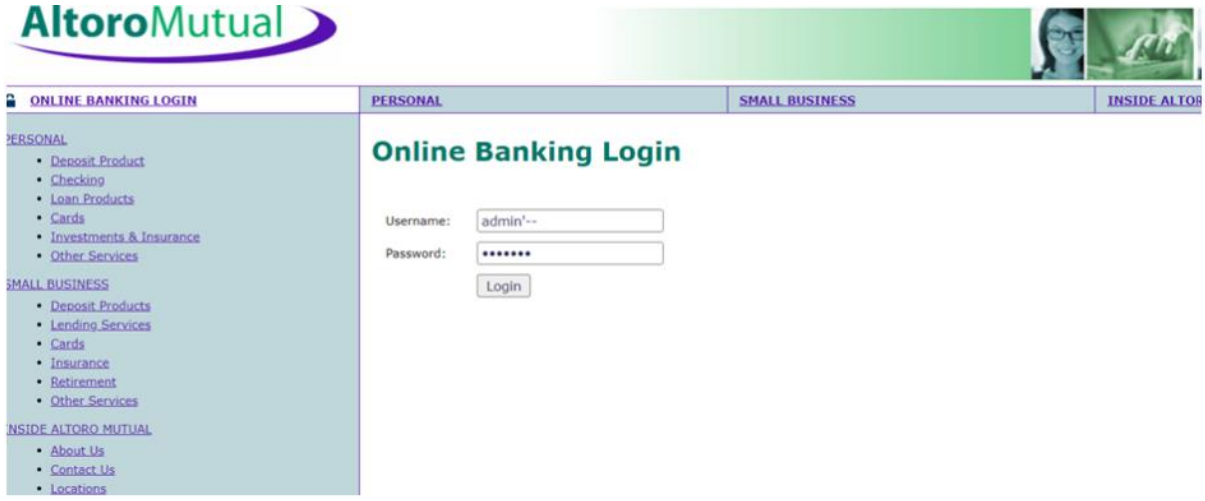
Vulnerability path: http://testfire.net/

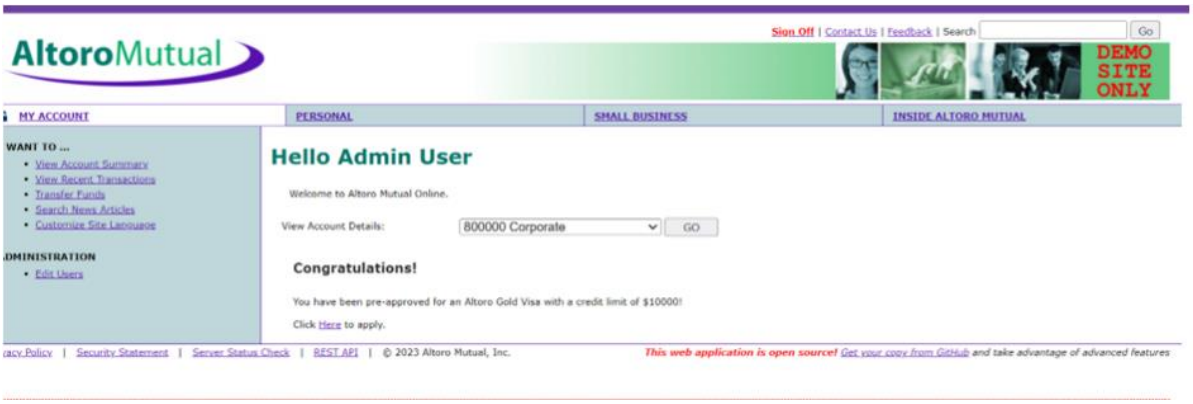
Steps to Reproduce:

Access the URL



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





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

Business Impact:

SQL injection attacks represent an extreme security danger to associations. A successful SQL injection assault can bring about confidential and important information being erased, edited or taken out for malicious uses. Other risks are sites being ruined, defaced or unapproved access to frameworks or accounts and, eventually, compromised machines or whole systems.

2. **Vulnerability name**: Brute Force Attack

CWE-1391: Use of Weak Credentials

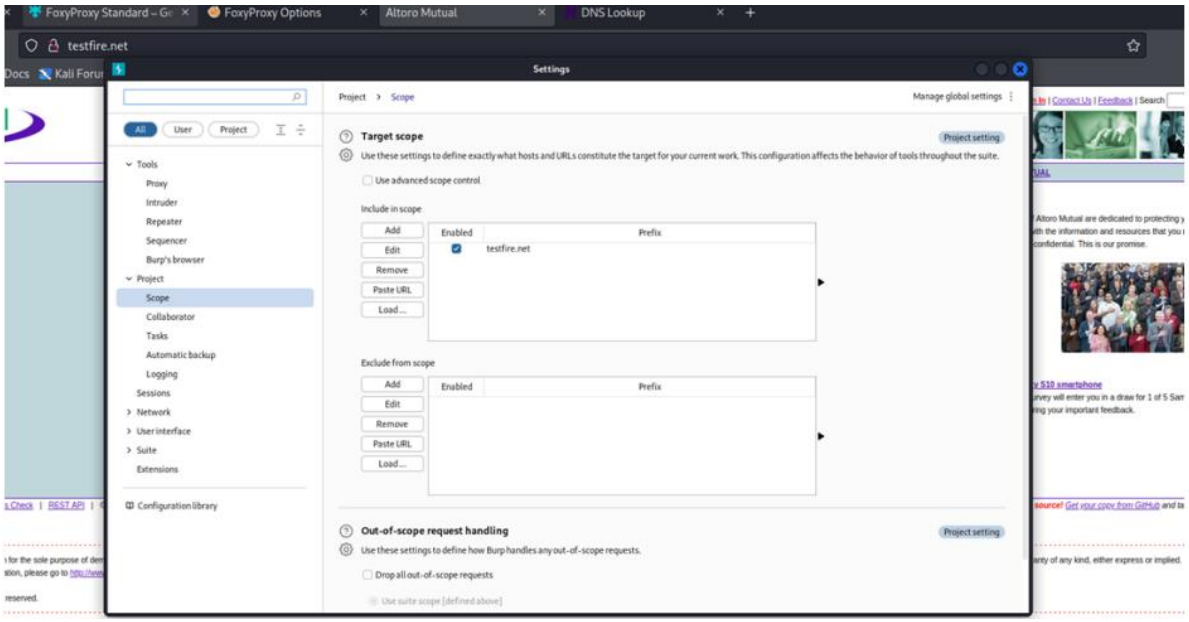
Description: The product uses weak credentials (such as a default key or hard-coded password) that can be calculated, derived, reused, or guessed by an attacker.

CWE-307: Improper Restriction of Excessive Authentication Attempts

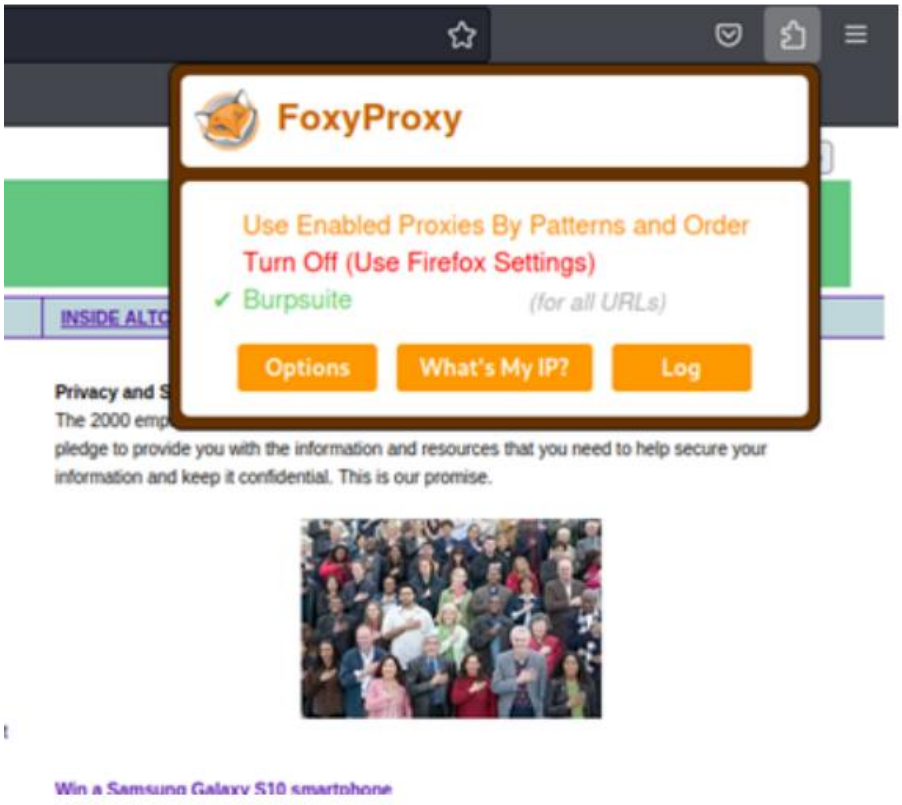
Description: The product does not implement sufficient measures to prevent multiple failed authentication attempts within a short time frame, making it more susceptible to brute force attacks.

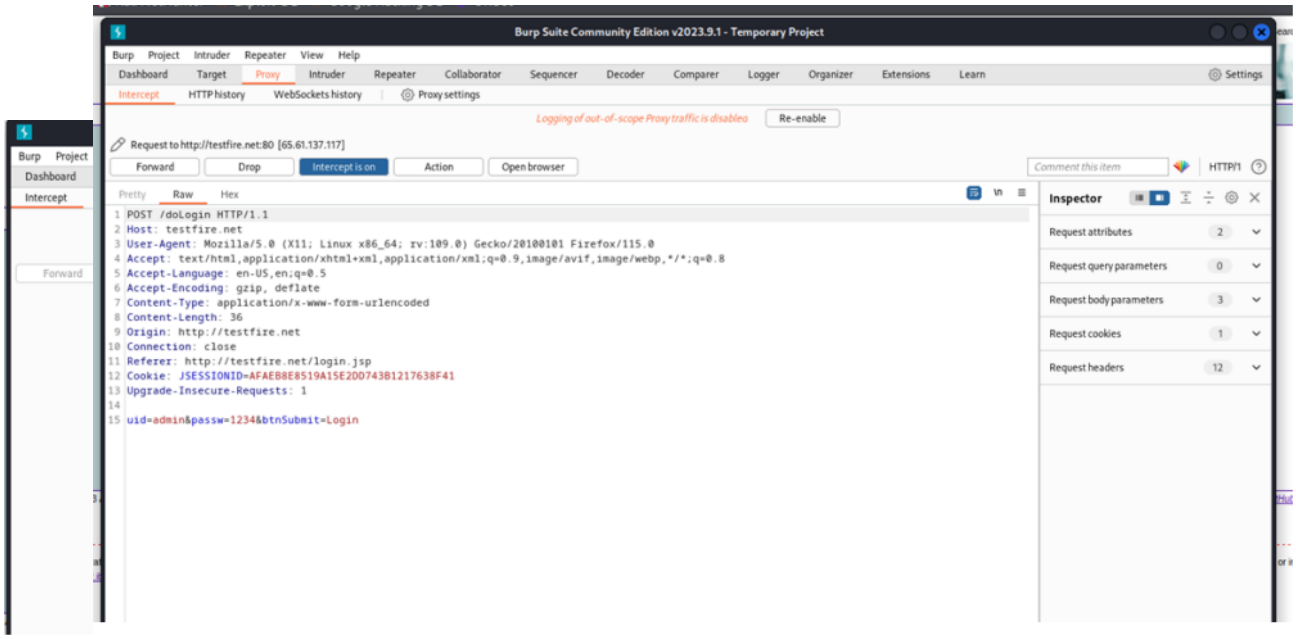
Steps to reproduce

Add the website by going to target tab -> add

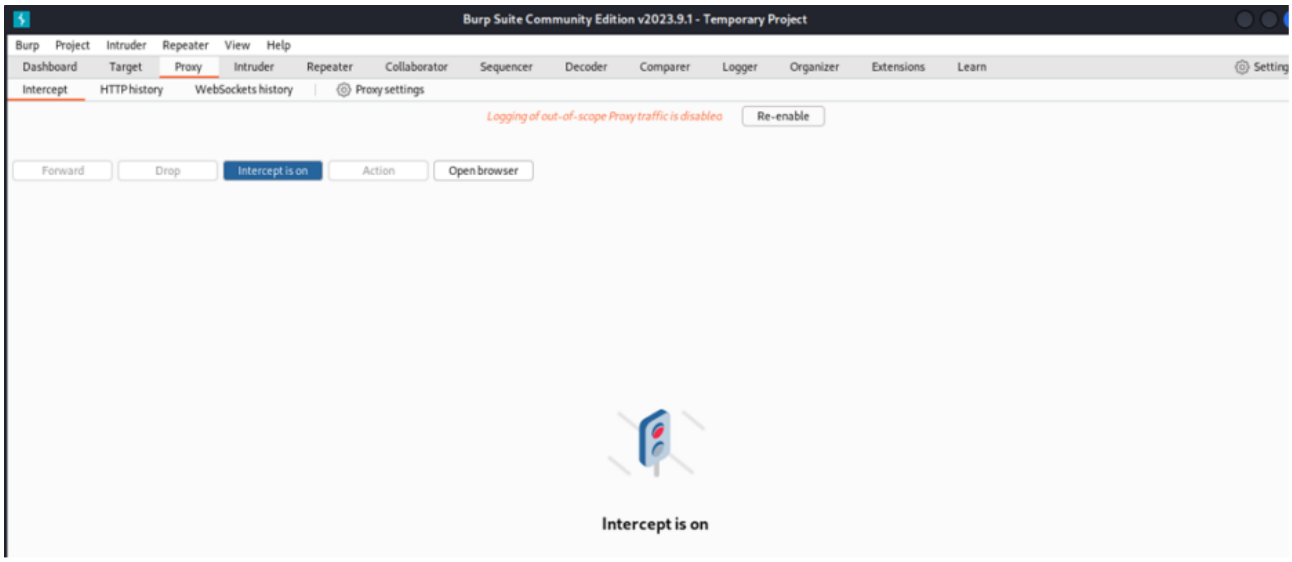


Choose burp as our default proxy on foxyproxy

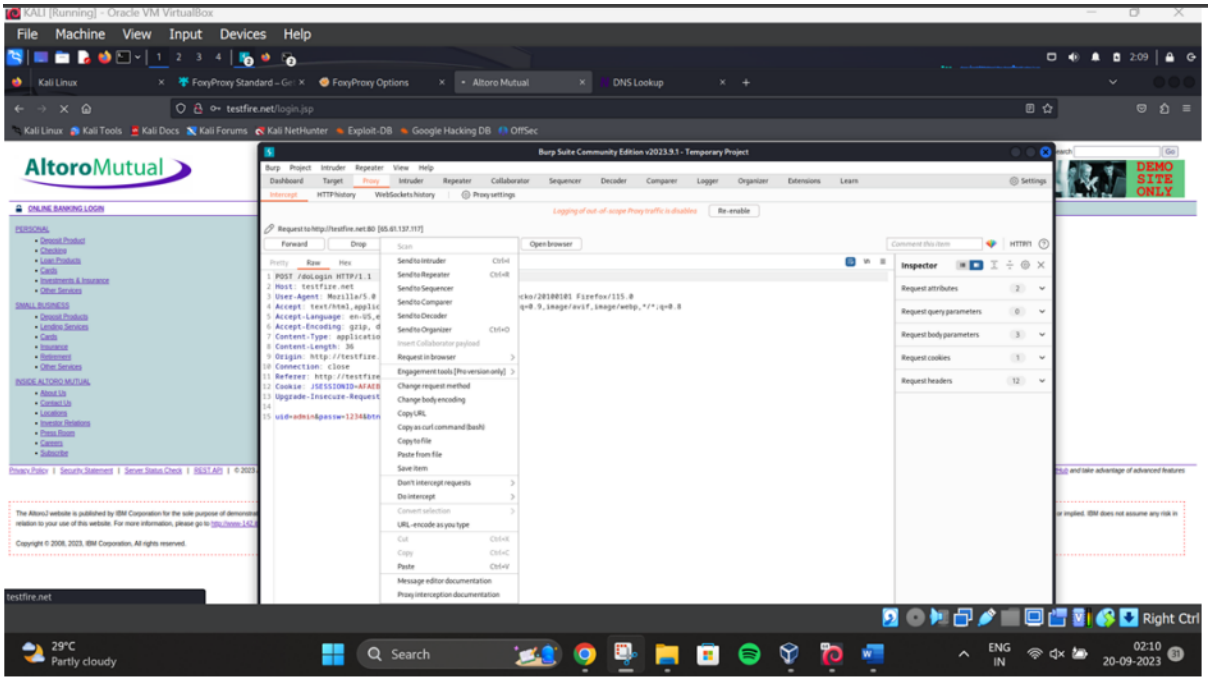


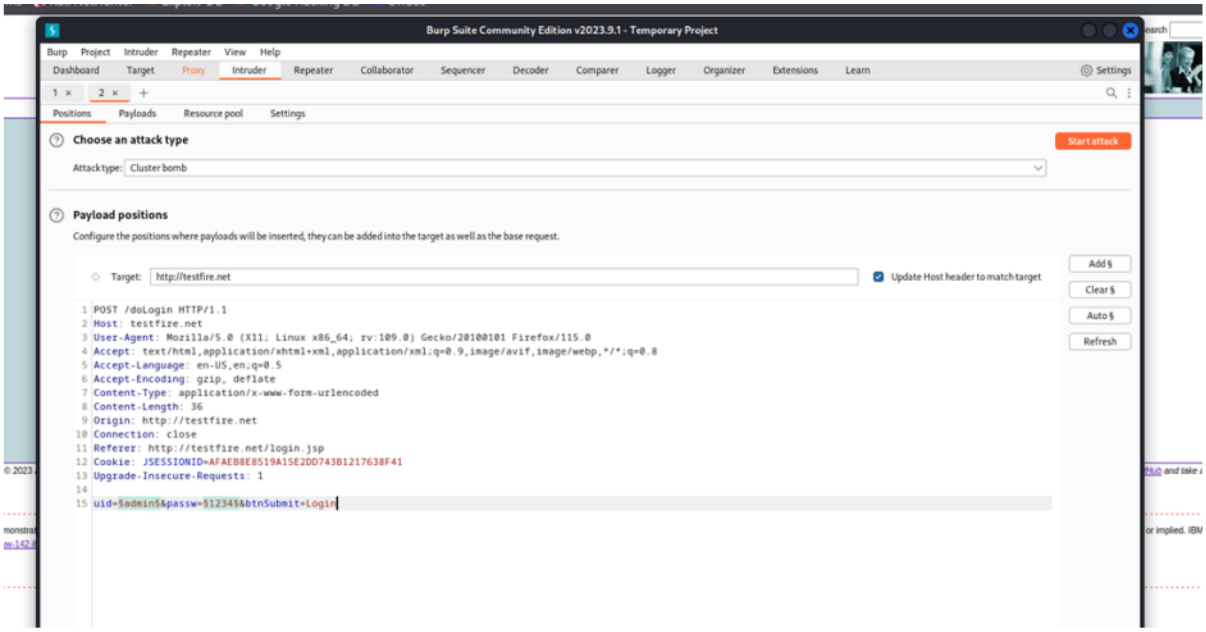


Go to proxy and turn on the intercept and then click on the login page of the website and give in random username and password.

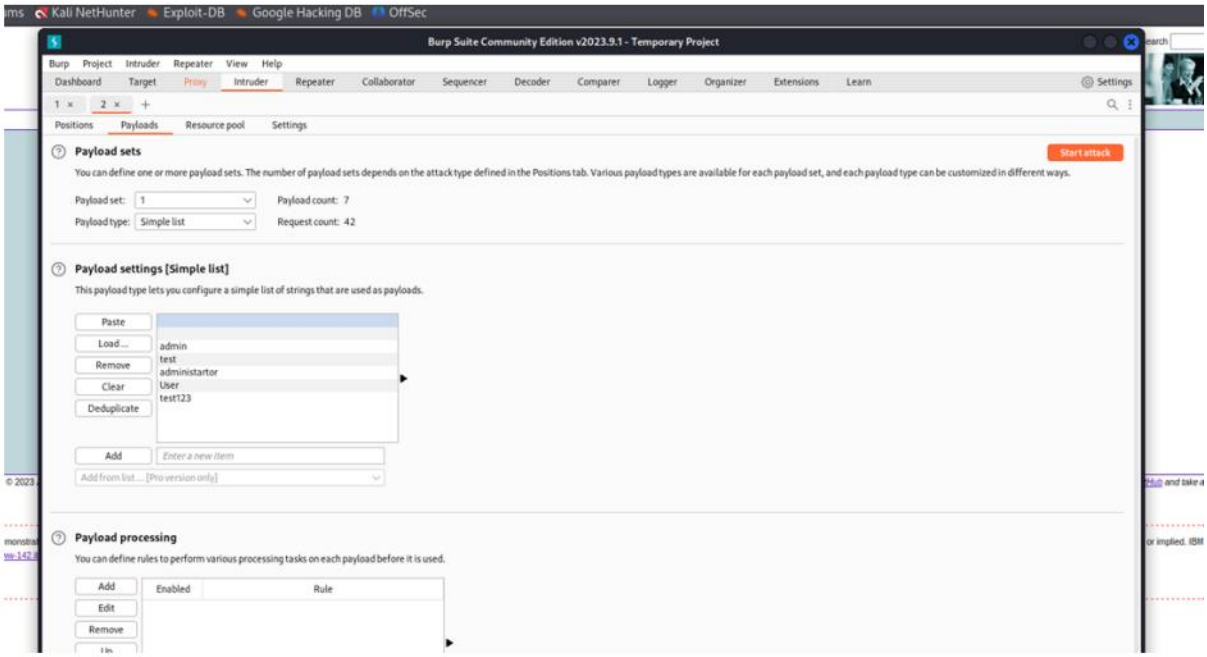


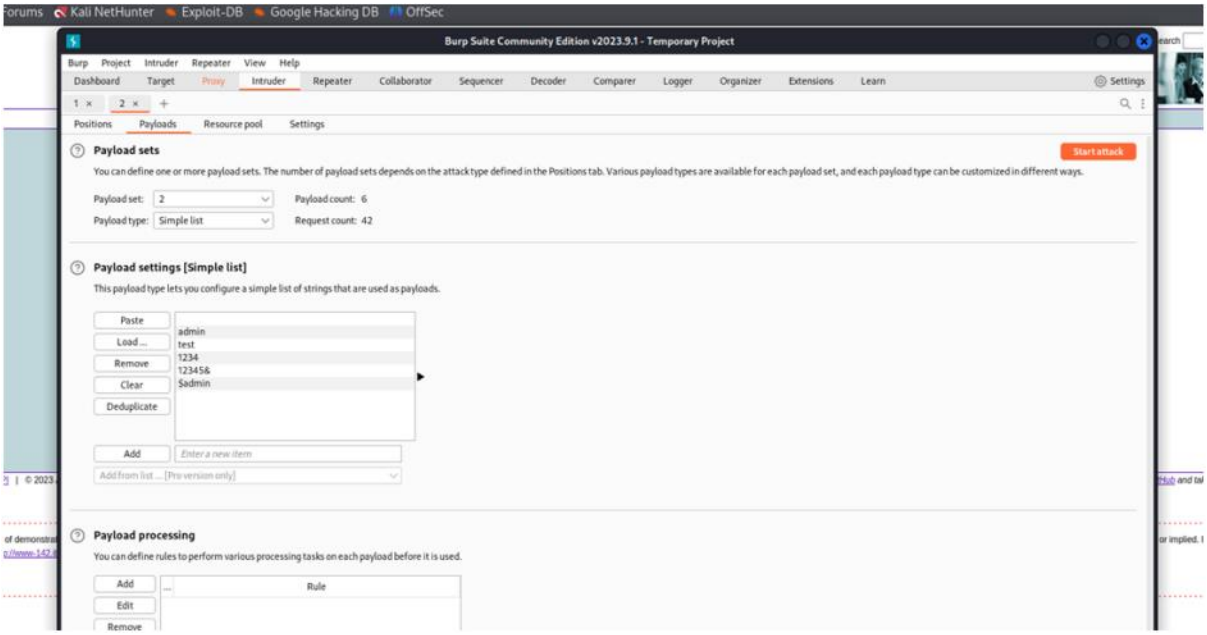
Then we sent it to intruder and go to positions tab choose cluster bomb attack and select the given input of username as payload 1 and given input of password as payload 2 by clicking on add.



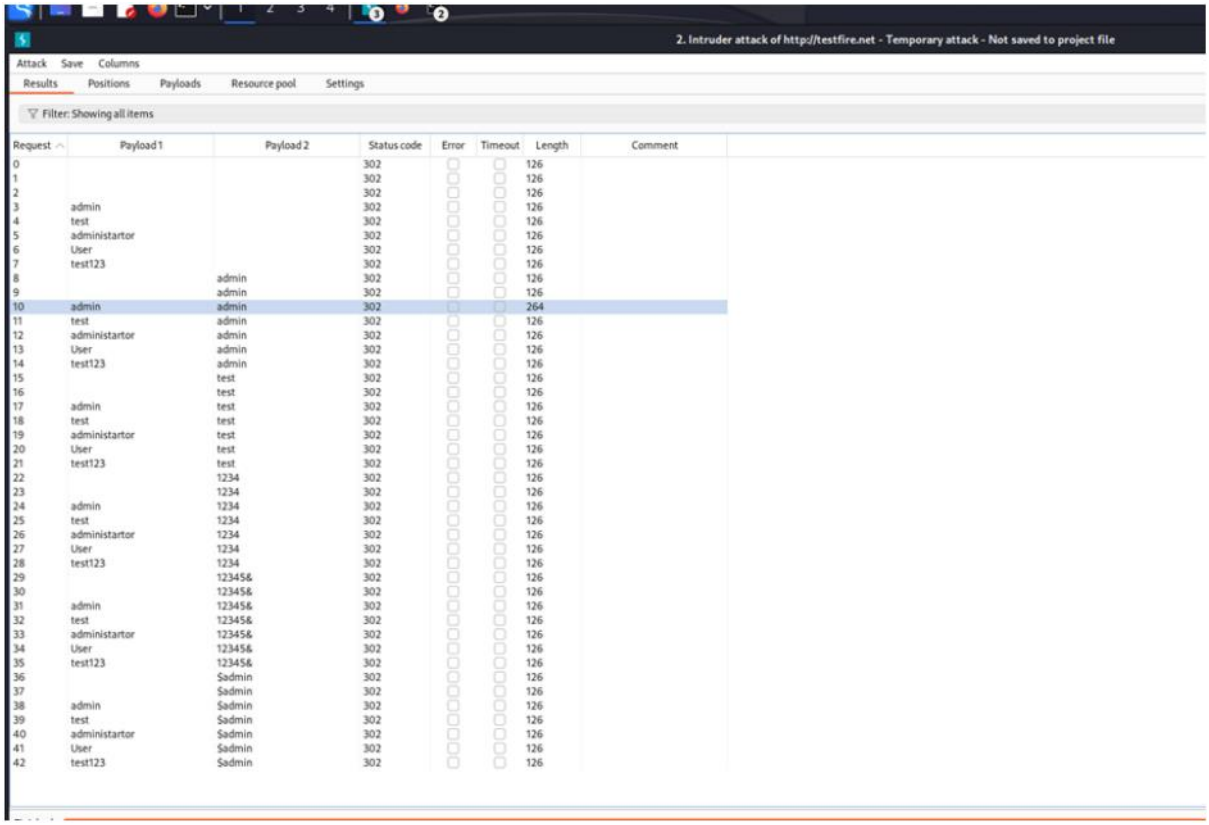


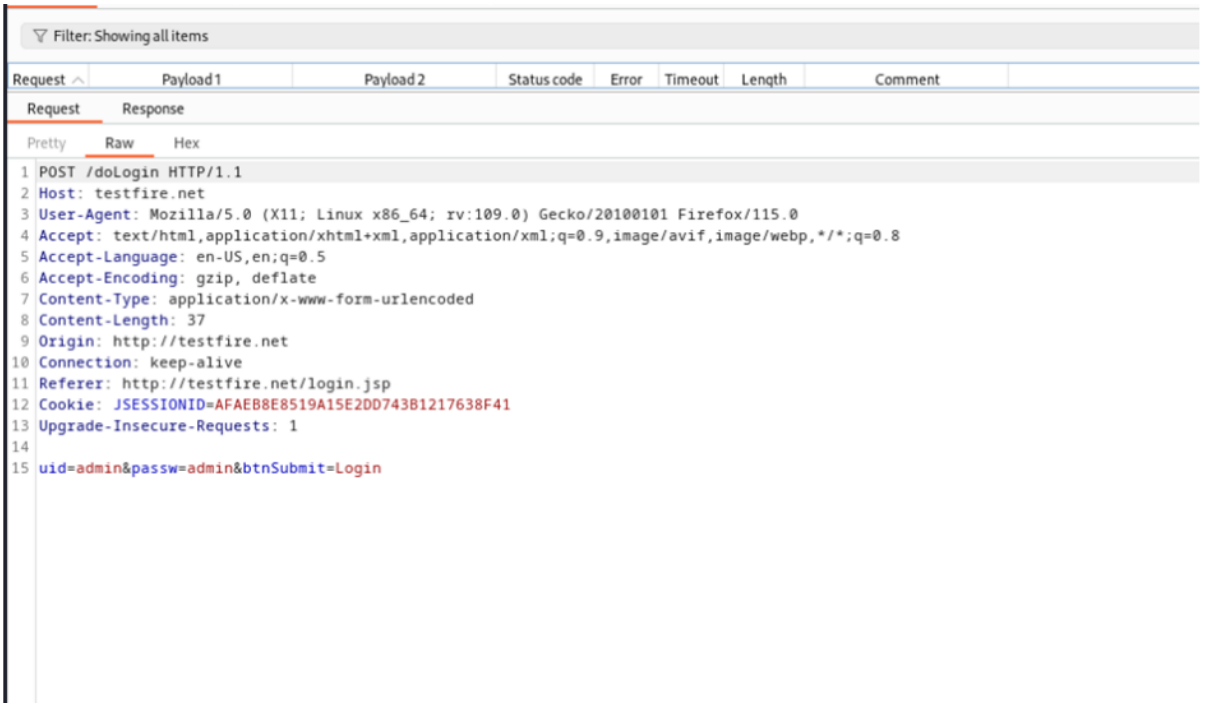
Then we go to the payloads tab and select payload 1 that is our username in this case and choose simple text and below give some random expected usernames. We can also upload a file here but since I do not have one I did it this way. We do the same for payload 2 which is our passwords and then start the attack.



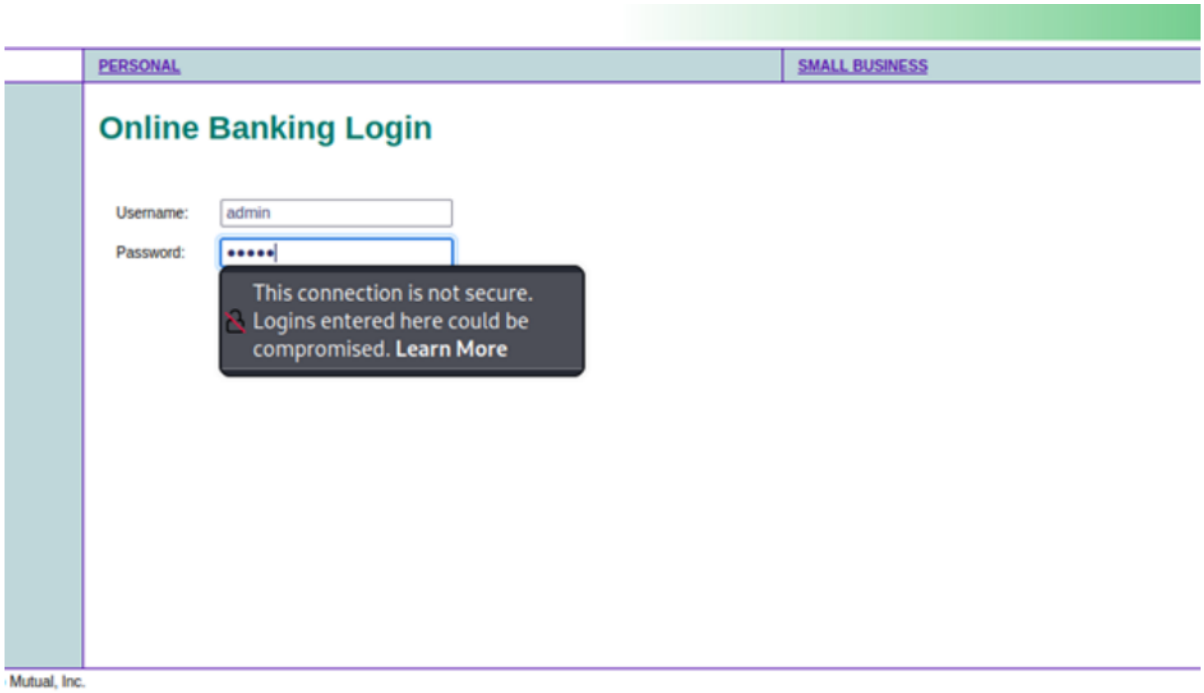


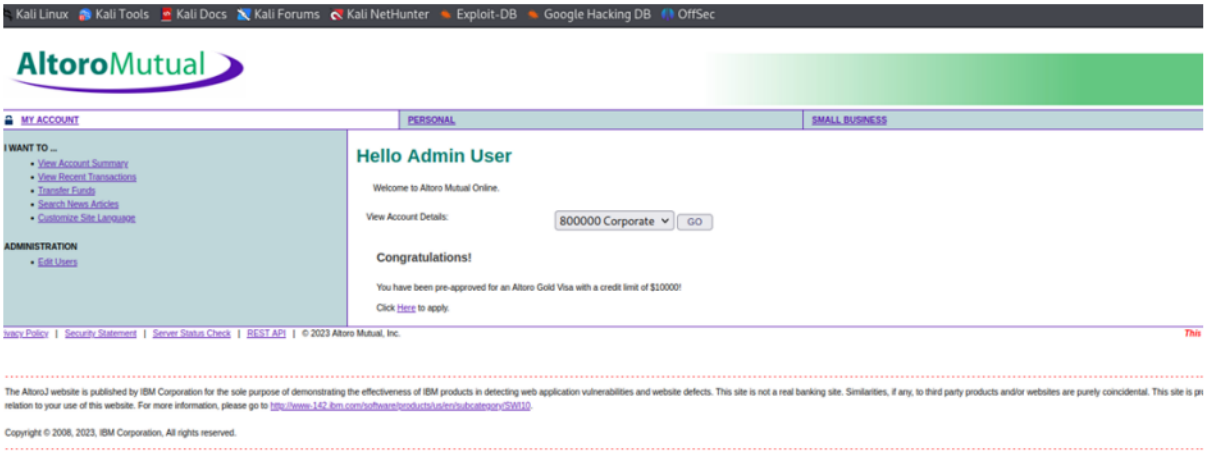
After the attack is finished we can see that the highlighted admin admin has different length from the others. Thus it can be a probable solution. Upon checking Request and response we can assure that this is working.





We then give the inputs in the login page and hence we are logged in





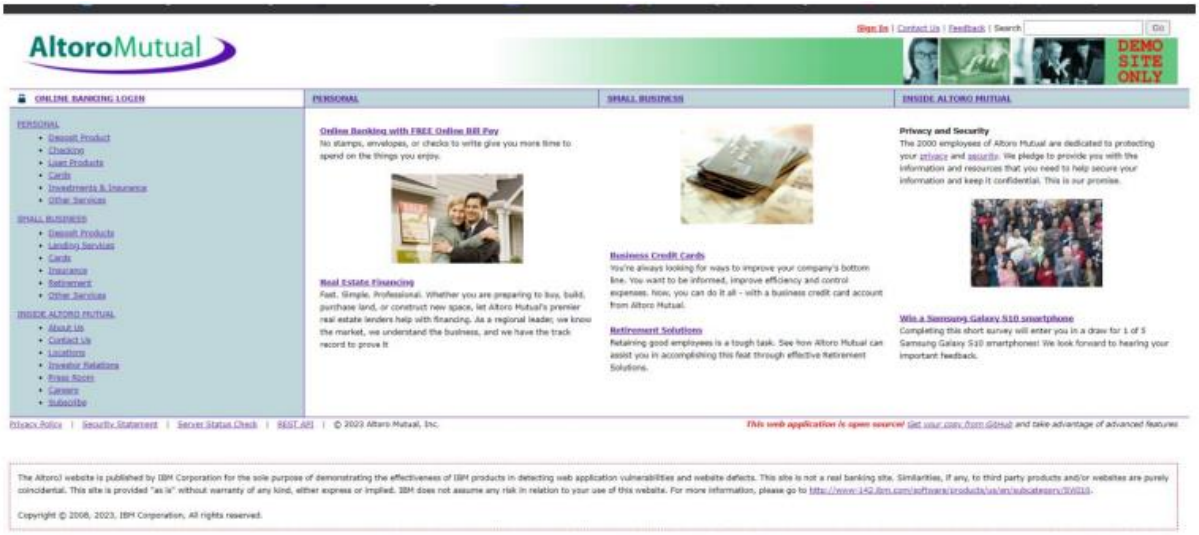
Business Impact:

A successful brute force attack on a business can result in unauthorized access, data loss or theft, financial losses, reputational damage, legal consequences, operational disruptions, increased security costs, loss of competitive advantage, damage to trust with customers and partners, and compliance issues, depending on the industry.

3. **Vulnerability name**: Broken authentication
   CWE: 285
   Description: The system's authorization functionality does not prevent one user from gaining access to another user's data or record by modifying the key value identifying the data.

Steps to reproduce:

Access the URL



Now we will try to login using some different approach.

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

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

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

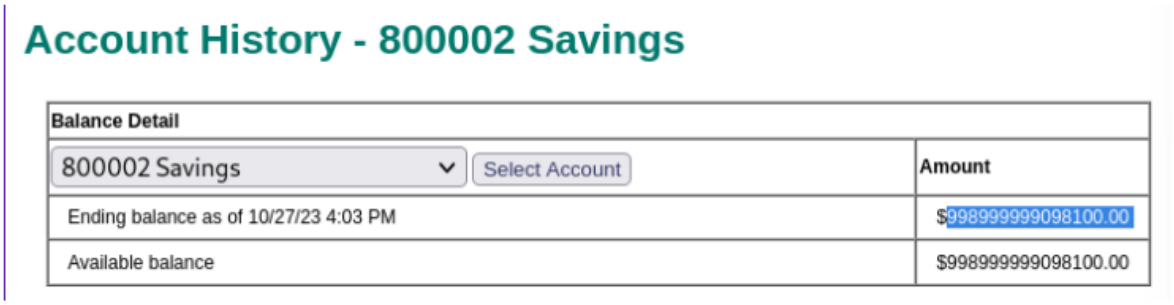
4. **Vulnerability Name**: Improper Input Validation (The website allows user to transfer amount greater than the user has in their account)

   CWE (Common Weakness Enumeration): CWE-132

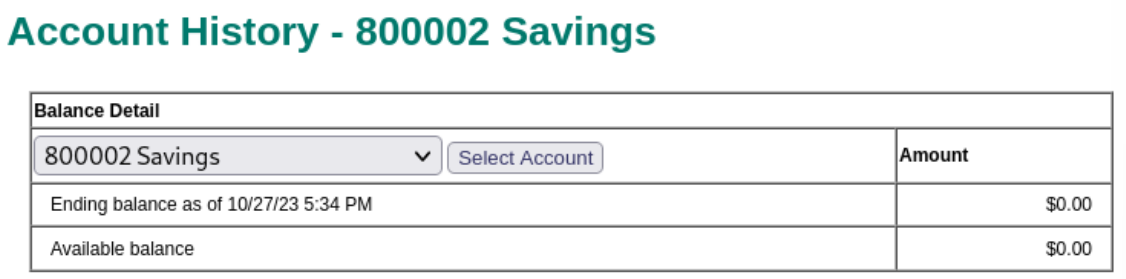
   Description: The product receives input or data, but it does not validate or incorrectly validates that the input has the properties that are required to process the data safely and correctly.

   Steps to reproduce:

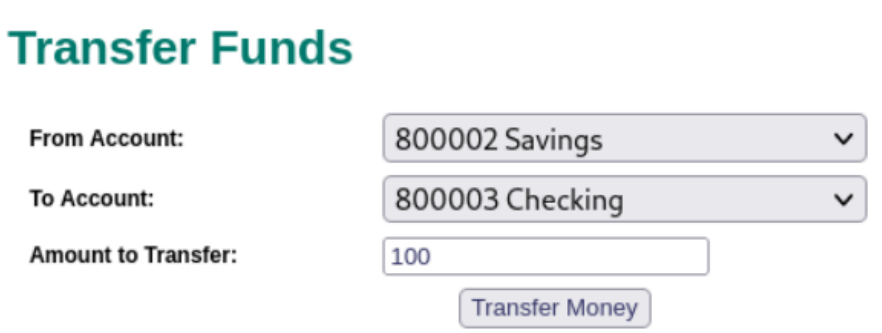
Wearing off the account 800002.

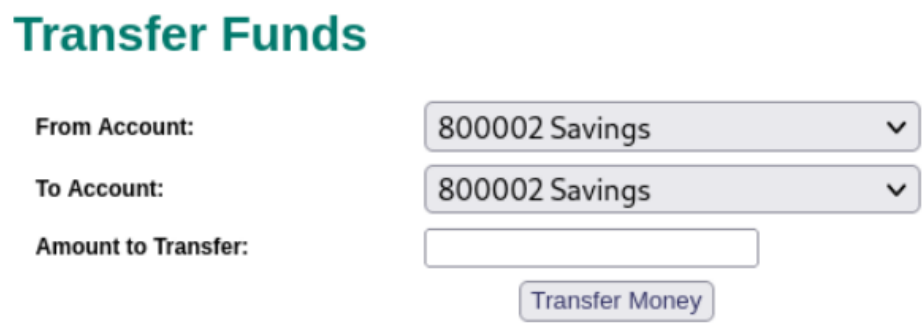


Amount to be debited to make the account balance empty is 998999999098100



Now trying to transfer amount even after the balance has worn out.





The transfer is successful as shown and the amount is credited in the respective account.

Business Impact:
-Financial losses: Unauthorized transfers could result in substantial financial losses for both the business and affected users.
- Reputation damage: Such a security flaw can erode user trust and damage the reputation of the company

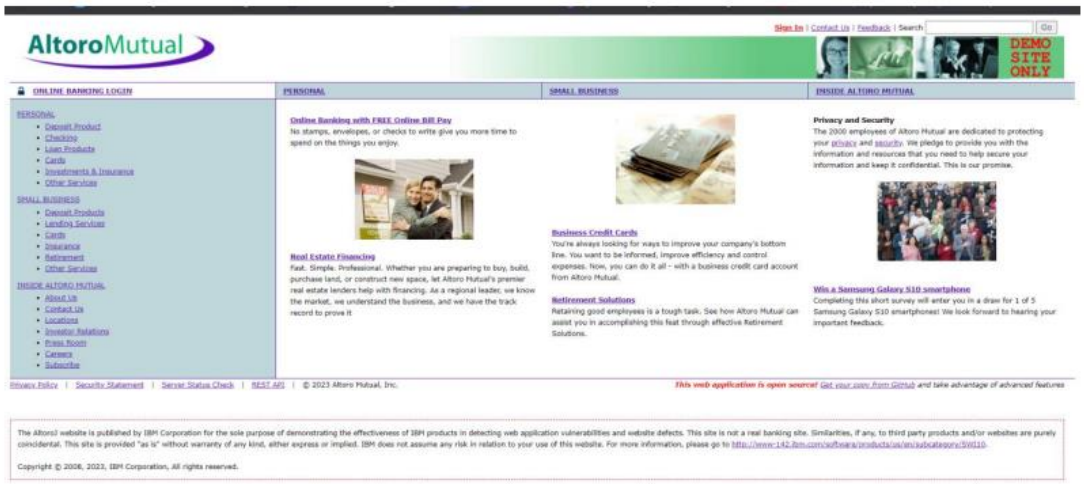
5. **Vulnerability name:** Web server allows password auto-completion

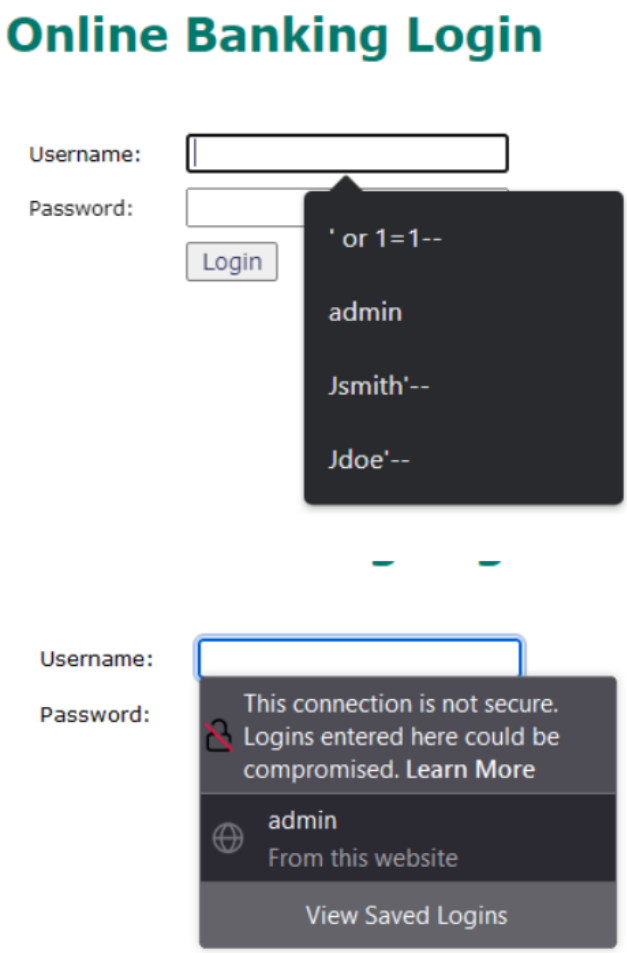
CWE: 310

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

Steps to reproduce:

Access the URL



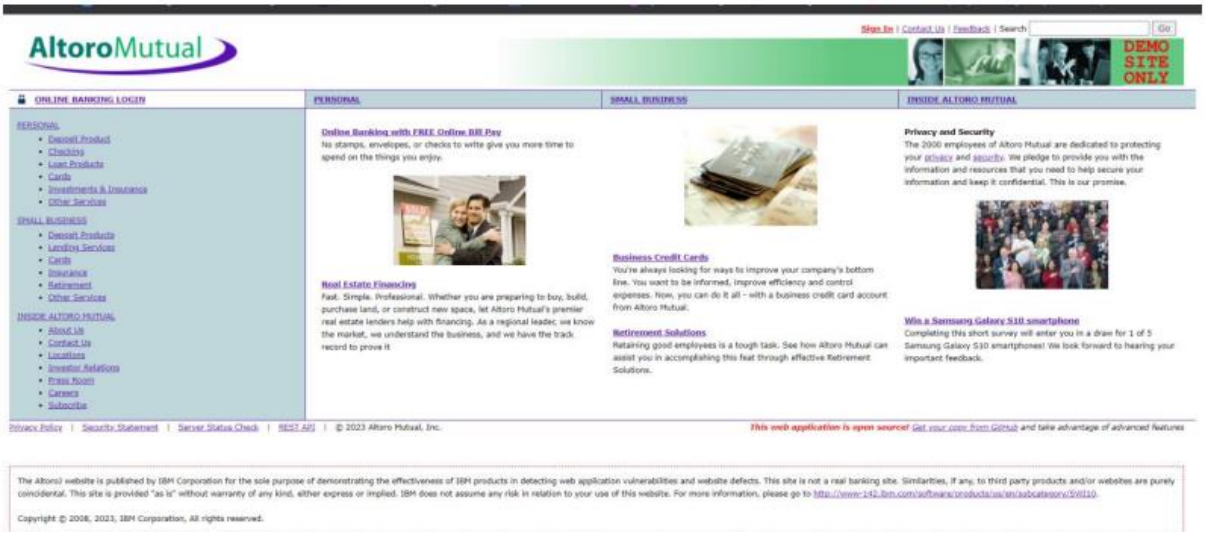


From this image we can see the usernames and the passwords getting auto filled. This is a potential vulnerability as this can be a doorway for attackers.

Business impact:

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

6. **Vulnerability name**: Clickjacking
   CWE: 1021
   Description: The web application does not restrict or incorrectly restricts frame objects or UI layers that belong to another application or domain, which can lead to user confusion about which interface the user is interacting with
   Steps to reproduce:



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

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

Executing the code in the browser

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

Business Impact:

To effectively reduce the business consequences resulting from CWE-1021, organizations must prioritize the implementation of protective measures, such as frame-busting code. Simultaneously, educating users on safe browsing practices plays a crucial role in preventing clickjacking incidents. Additionally, routine security assessments and testing are pivotal for identifying and mitigating vulnerabilities associated with clickjacking. These actions are of

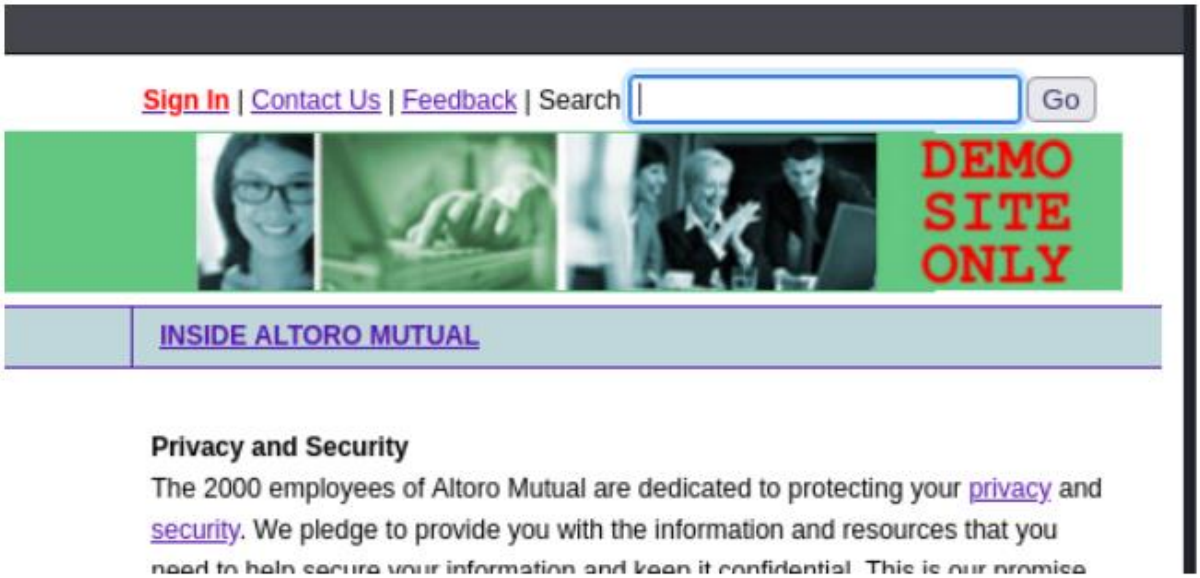
paramount importance in upholding user trust, ensuring data protection, and safeguarding the organization's reputation.

7. **Vulnerability Name:** HTML injection attack

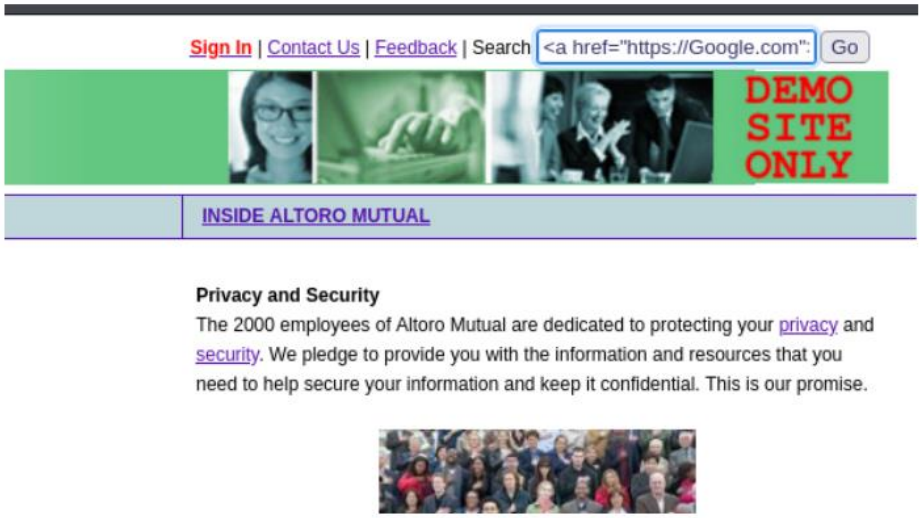
   CWE: 601 (URL Redirection to untrusted site('Open Redirect')

   Description: A web application accepts a user-controlled input that specifies a link to an external site, and uses that link in a Redirect. This simplifies phishing attacks.

   Steps to reproduce:



   HTML payload: Click her to login
   This payload's href link can be modified in certain way that it redirects to the malicious login page



   Executing the payload gives the following result.

When the click here to login hyperlink is clicked, we are redirected to the website that is linked to it.

Business Impact:
The impact of CWE-601 (Open Redirect) includes loss of trust, data breaches, financial loss, legal consequences, brand damage, and operational disruption. Here a combination of man in the middle attack and html injection can be used to inject an html payload that can return a link to a malicious copy of the login page of the legitimate website seeking the credentials from the user.

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

   CWE: 79

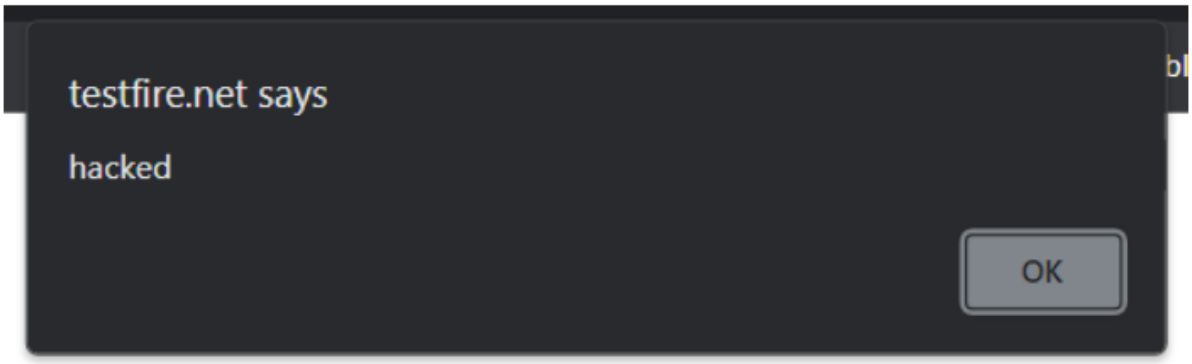
   OWASP category: A03:2021 -Injections

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

   Steps to reproduce:

In the search box we will input some code to perform the vulnerabilit

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



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

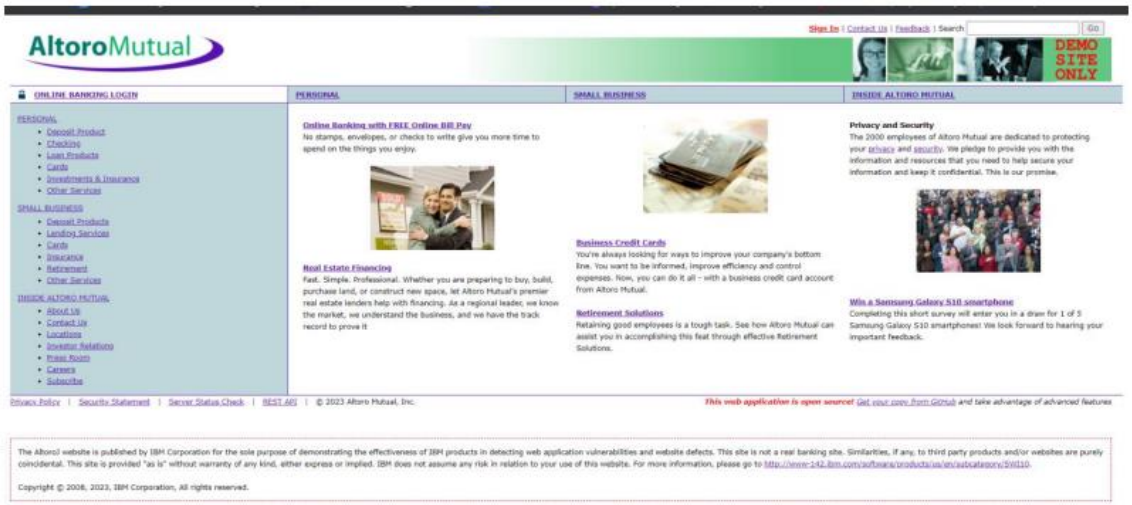
9. **Vulnerability name**: Cleartext Transmission of Sensitive Information

   CWE: 319

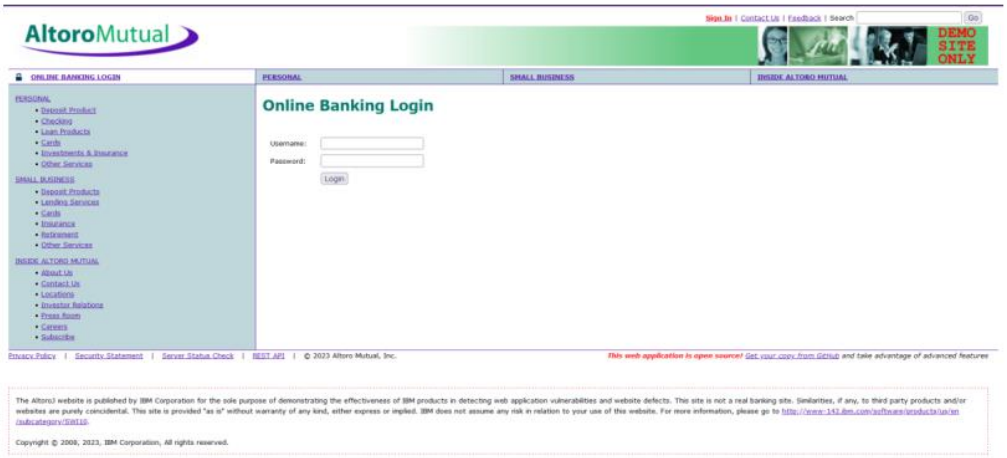
   Description: The product transmits sensitive or security-critical data in cleartext in a communication channel that can be sniffed by unauthorized actors. Many communication channels can be "sniffed" (monitored) by adversaries during data transmission. For example, in networking, packets can traverse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

   Steps to reproduce:

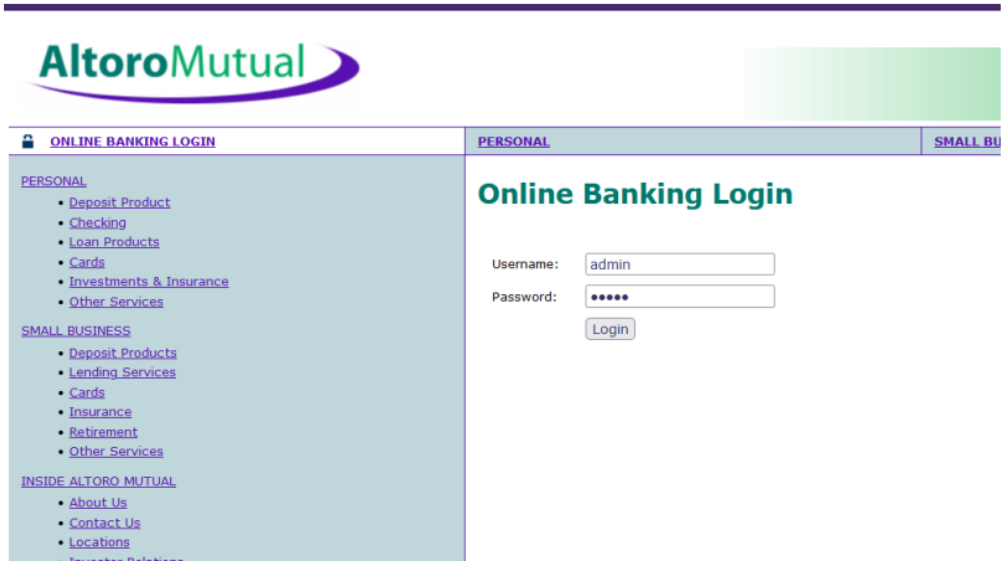
Access the URL



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



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



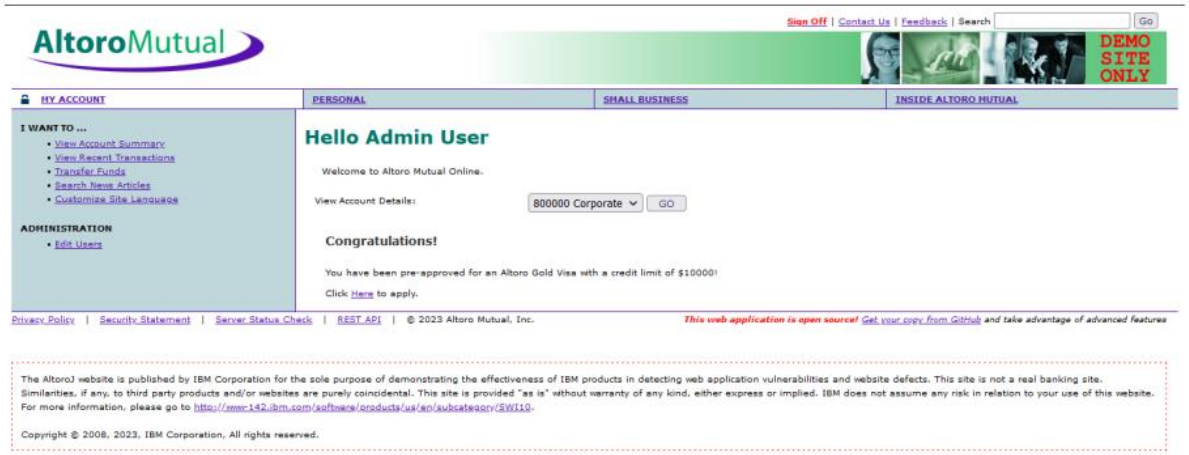
This request has been received in the burp suite with the username and password as well in clear text.

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

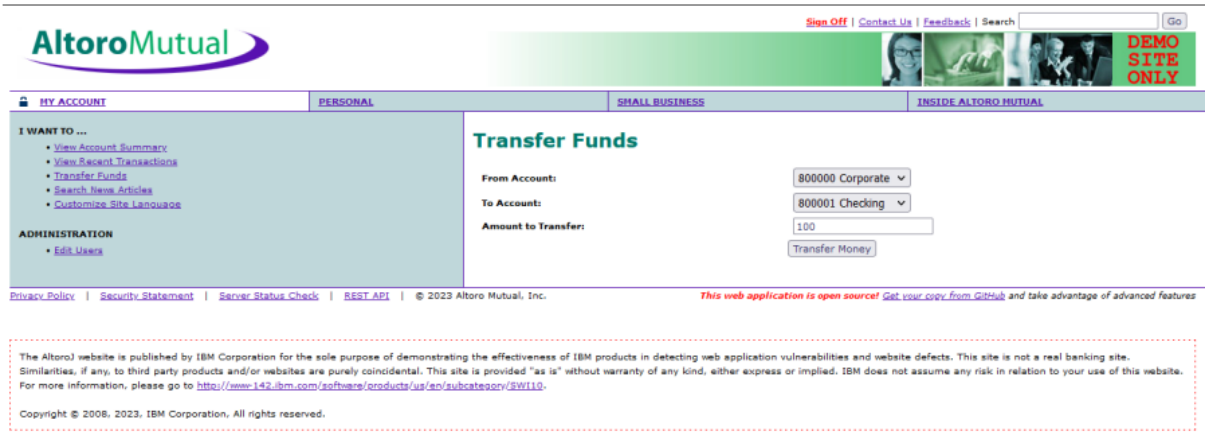
Business Impact:

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

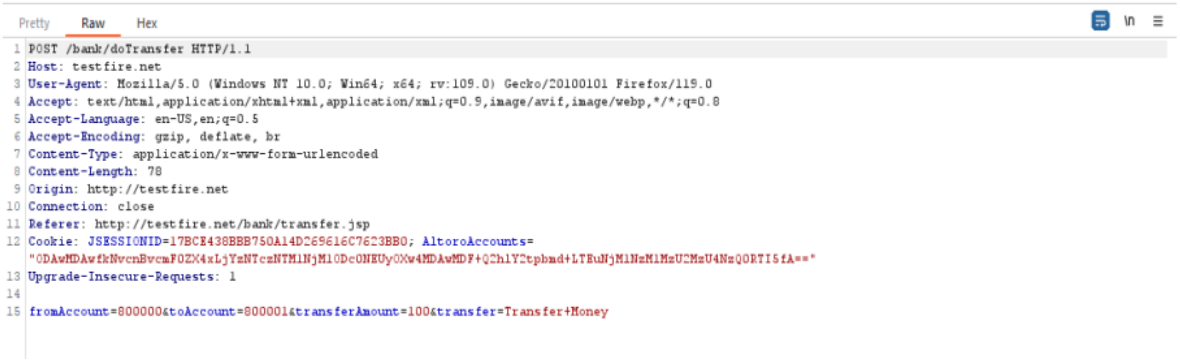
10. **Vulnerability Name:** Insecure Direct object Reference
    CWE: 639
    OWASP Category: A01: Broken Access Control
    Description: Insecure Direct Object Reference (IDOR) is a vulnerability that arises when attackers can access or modify objects by manipulating identifiers used in a web application's URLs or parameters. It occurs due to missing access control checks, which fail to verify whether a user should be allowed to access specific data.
    Steps to reproduce:



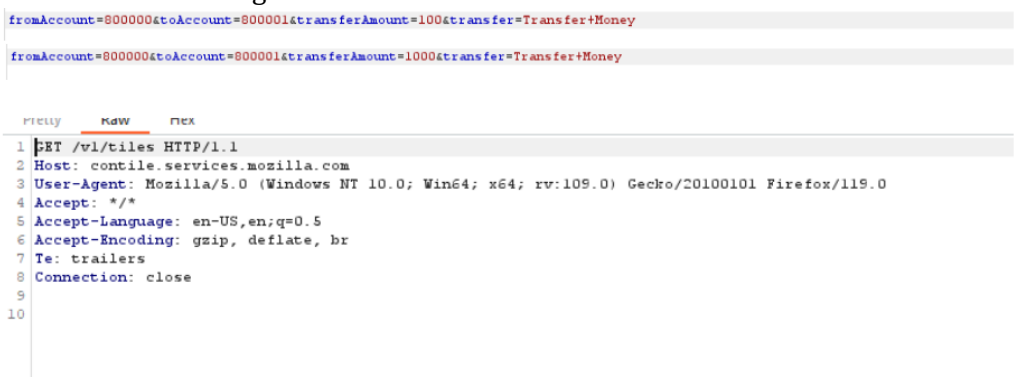
Open “Transfer Money” on the left side and fill in the details. On the intercept and click transfer



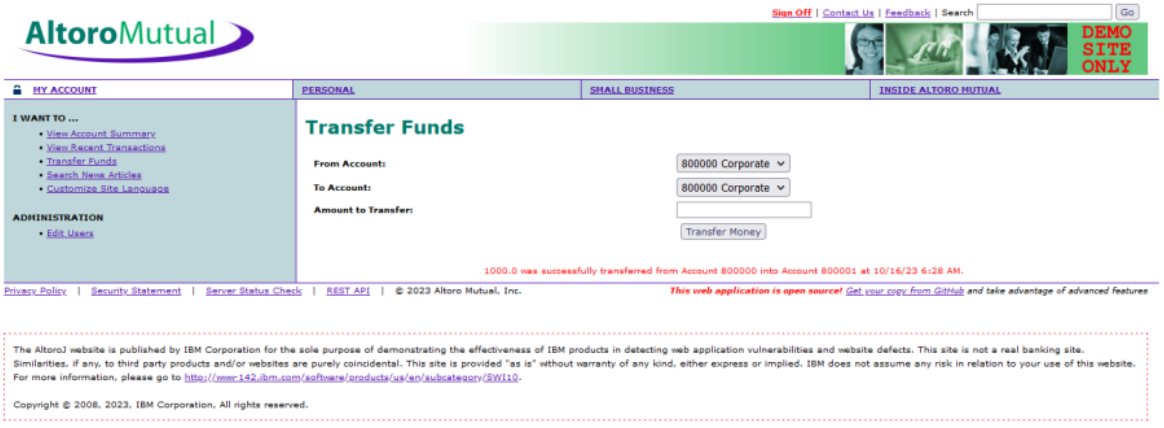
Open burp and notice the change



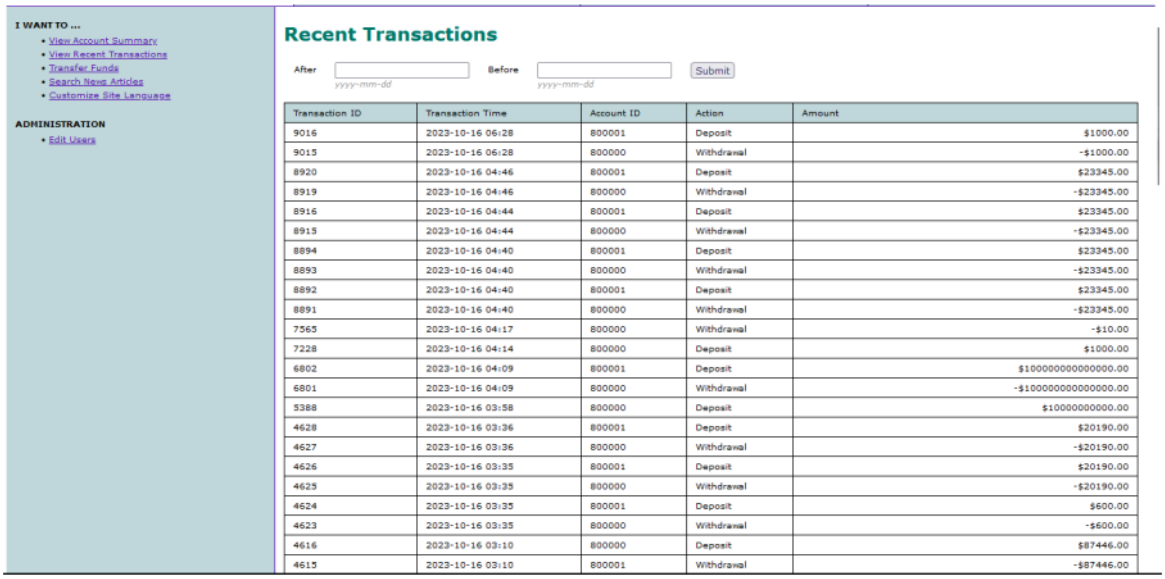
In the 15th line change the amount from 100 to 1000 and click forward



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



Off the Intercept and open “View Recent Transactions”.



Business Impact:

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

Website: www.vtop.vitbhopal.ac.in

IP Address 1: 182.73.197.23

List of Vulnerability Table -

S. No.	Vulnerability Name	CWE - No
1.	Nessus SYN scanner	NA
2.	Nessus Scan Information	NA
3.	OS Identification Failed	NA
4.	Open Port Re-check	NA
5.	Service Detection	NA
6.	Traceroute Information	NA
7.	Web Server No 404 Error Code Check	NA

REPORT

1. Nessus SYN scanner

CWE: N/A

OWASP Category: N/A

Description: Nessus SYN scanner is a plugin used for network scanning.

Business Impact: Informational plugin for network discovery.

Vulnerability Path: N/A

Vulnerability Parameter: N/A

2. Nessus Scan Information

CWE: N/A

OWASP Category: N/A

Description: Information about the Nessus scan itself.

Business Impact: Provides information about the scan process.

Vulnerability Path: N/A

Vulnerability Parameter: N/A

3. OS Identification Failed

CWE: N/A

OWASP Category: N/A

Description: Nessus failed to identify the operating system.

Business Impact: May affect vulnerability assessment.

Vulnerability Path: N/A

Vulnerability Parameter: N/A

4. Open Port Re-check

CWE: N/A

OWASP Category: N/A

Description: Nessus re-checks open ports.

Business Impact: Informational plugin for port status.

Vulnerability Path: N/A

Vulnerability Parameter: N/A

5. Service Detection

CWE: N/A

OWASP Category: N/A

Description: Plugin used to detect services running on open ports.

Business Impact: Provides information about running services.

Vulnerability Path: N/A

Vulnerability Parameter: N/A

6. Traceroute Information

CWE: N/A

OWASP Category: N/A

Description: Provides information about the traceroute.

Business Impact: Informational plugin for network mapping.

Vulnerability Path: N/A

Vulnerability Parameter: N/A

7. Web Server No 404 Error Code Check

CWE: N/A

OWASP Category: N/A

Description: Checks for the absence of 404 error codes on the web server.

Business Impact: Informational plugin for web server analysis.

Vulnerability Path: N/A

Vulnerability Parameter: N/A

Website: www.vtop.vitbhopal.ac.in
IP Address 2: 14.99.16.249

List of Vulnerability Table -

S. No.	Vulnerability Name	CWE - No
1.	Apache Tomcat 9.0.0-M1 < 9.0.68 Request Smuggling Vulnerability	444: Using Components with Known Vulnerabilities
2.	Apache Tomcat 9.0.0.M1 < 9.0.37 Multiple Vulnerabilities	444: Using Components with Known Vulnerabilities
3.	Apache Tomcat 9.0.0.M1 < 9.0.43 Multiple Vulnerabilities	444: Using Components with Known Vulnerabilities
4.	Apache Tomcat 9.0.0.M1 < 9.0.71	444: Using Components with Known Vulnerabilities
5.	Apache Tomcat 9.0.13 < 9.0.63 vulnerability	444: Using Components with Known Vulnerabilities

6.	Apache Tomcat 9.x < 9.0.40 Information Disclosure	200: Information Exposure
7.	Apache Tomcat 7.0.x <= 7.0.108 / 8.5.x <= 8.5.65 / 9.0.x <= 9.0.45 / 10.0.x <= 10.0.5 vulnerability	CWE-522: Insufficiently Protected Credentials
8.	Apache Tomcat 9.0.0.M1 < 9.0.80	444: Using Components with Known Vulnerabilities
9.	Apache Tomcat 9.0.30 < 9.0.65 vulnerability	444: Using Components with Known Vulnerabilities
10.	Apache Tomcat 9.0.0.M1 < 9.0.48 vulnerability	444: Using Components with Known Vulnerabilities
11.	Apache Tomcat 9.0.0.M1 < 9.0.81 multiple vulnerabilities	444: Using Components with Known Vulnerabilities
12.	Apache Tomcat 8.5.x < 8.5.58 / 9.0.x < 9.0.38 HTTP/2 Request Mix-Up	444: Using Components with Known Vulnerabilities
13.	Apache Tomcat 9.0.0.M1 < 9.0.72	444: Using Components with Known Vulnerabilities
14.	Apache Tomcat 9.0.0.M1 < 9.0.62 Spring4Shell (CVE-2022-22965) Mitigations	444: Using Components with Known Vulnerabilities
15.	Apache Tomcat Detection	NA
16.	Common Platform Enumeration (CPE)	NA
17.	Host Fully Qualified Domain Name (FQDN) Resolution	NA
18.	Inconsistent Hostname and IP Address	NA
19.	Nessus SYN scanner	NA
20.	Nessus Scan Information	NA
21.	OS Identification Failed	NA
22.	Open Port Re-check	NA
23.	Patch Report	NA
24.	Service Detection	NA
25.	Traceroute Information	NA
26.	Web Server No 404 Error Code Check	NA

REPORT

1. Apache Tomcat 9.0.0-M1 < 9.0.68 Request Smuggling Vulnerability

CWE: CWE-444

OWASP Category: A9:2017-Using Components with Known Vulnerabilities

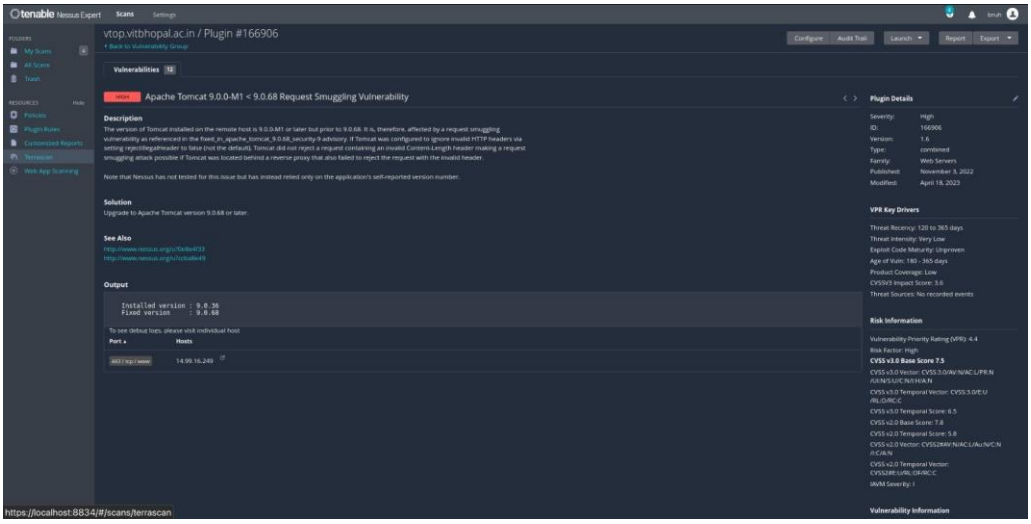
Description: Vulnerability in Apache Tomcat version 9.0.0-M1 to 9.0.68 allows an attacker to perform request smuggling attacks.

Business Impact: Potential for HTTP request smuggling leading to unauthorized access or

information disclosure.

Vulnerability Path: https://vtop.vitbhopal.ac.in/

Vulnerability Parameter: view-source:https://vtop.vitbhopal.ac.in/



2. Apache Tomcat 9.0.0.M1 < 9.0.37 Multiple Vulnerabilities

CWE: CWE-444

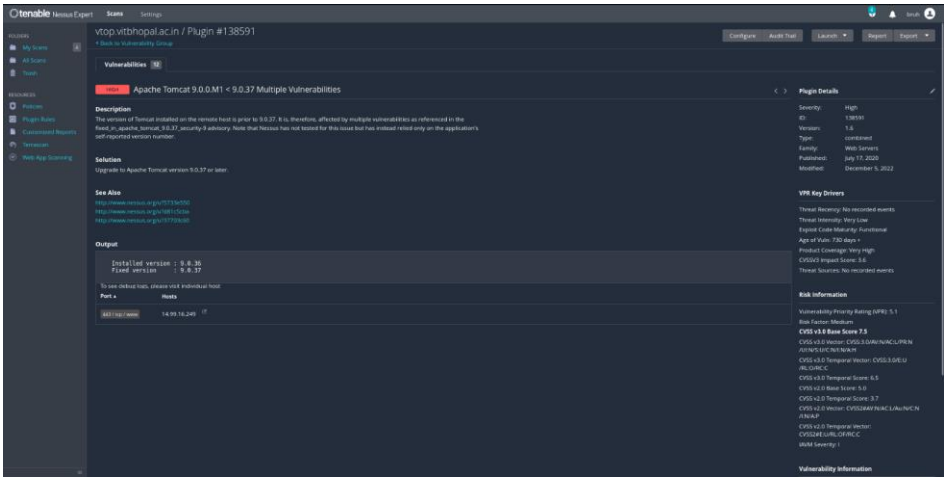
OWASP Category: A9:2017-Using Components with Known Vulnerabilities

Description: Multiple vulnerabilities in Apache Tomcat versions 9.0.0.M1 through 9.0.37 may allow attackers to gain unauthorized access or view sensitive information.

Business Impact: Potential for unauthorized access or information disclosure.

Vulnerability Path: https://vtop.vitbhopal.ac.in/

Vulnerability Parameter: view-source:https://vtop.vitbhopal.ac.in/



3. Apache Tomcat 9.0.0.M1 < 9.0.43 Multiple Vulnerabilities

CWE: CWE-444

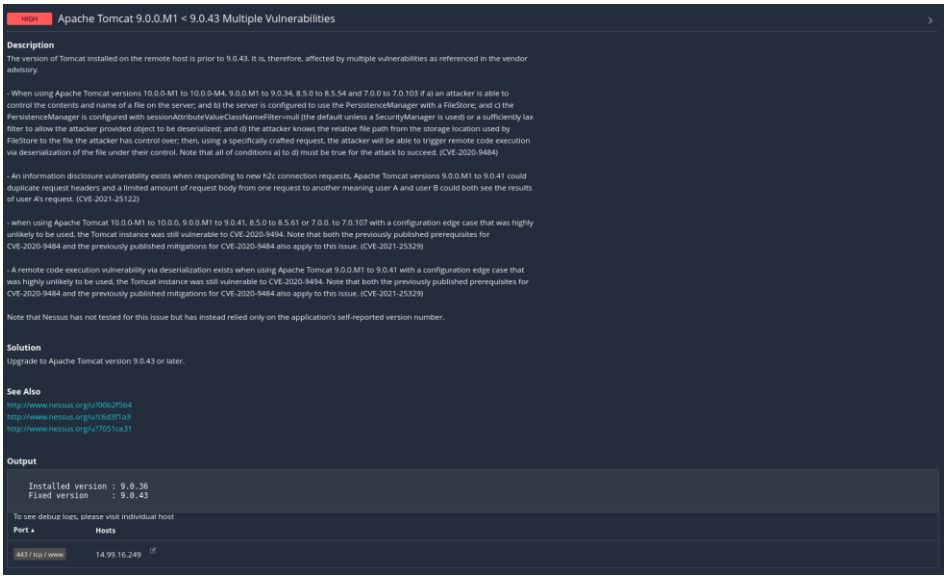
OWASP Category: A9:2017-Using Components with Known Vulnerabilities

Description: Multiple vulnerabilities in Apache Tomcat versions 9.0.0.M1 through 9.0.43 may allow attackers to gain unauthorized access or view sensitive information.

Business Impact: Potential for unauthorized access or information disclosure.

Vulnerability Path: https://vtop.vitbhopal.ac.in/

Vulnerability Parameter: view-source:https://vtop.vitbhopal.ac.in/



4. Apache Tomcat 9.0.0.M1 < 9.0.71

CWE: CWE-444

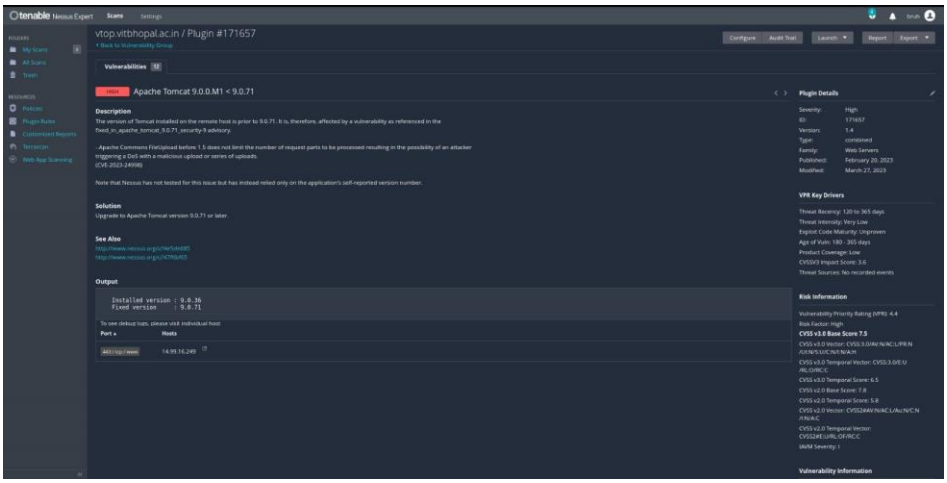
OWASP Category: A9:2017-Using Components with Known Vulnerabilities

Description: Vulnerability in Apache Tomcat versions 9.0.0.M1 through 9.0.71 may allow attackers to gain unauthorized access or view sensitive information.

Business Impact: Potential for unauthorized access or information disclosure.

Vulnerability Path: https://vtop.vitbhopal.ac.in/

Vulnerability Parameter: view-source:https://vtop.vitbhopal.ac.in/



5. Apache Tomcat 9.0.13 < 9.0.63 Vulnerability

CWE: CWE-444

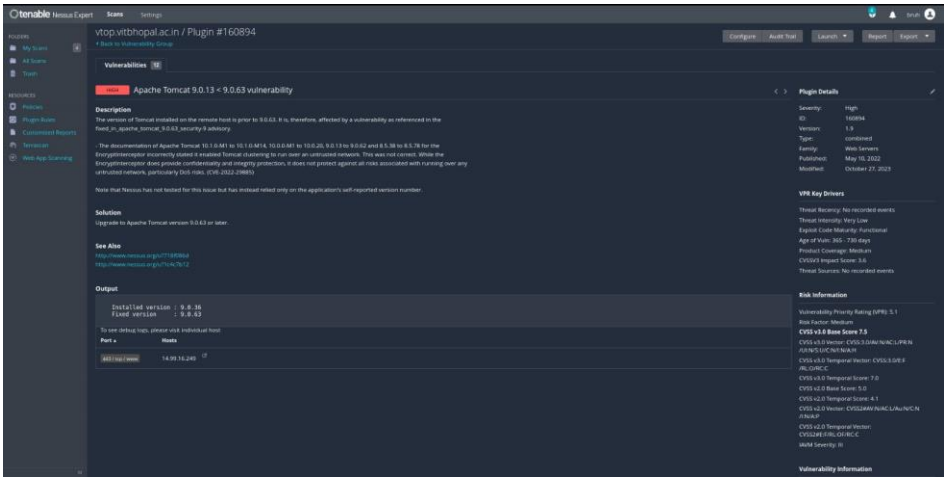
OWASP Category: A9:2017-Using Components with Known Vulnerabilities

Description: Vulnerability in Apache Tomcat versions 9.0.13 through 9.0.63 may allow attackers to gain unauthorized access or view sensitive information.

Business Impact: Potential for unauthorized access or information disclosure.

Vulnerability Path: https://vtop.vitbhopal.ac.in/

Vulnerability Parameter: view-source:https://vtop.vitbhopal.ac.in/



6. Apache Tomcat 9.0.0.M1 < 9.0.80

CWE: CWE-444

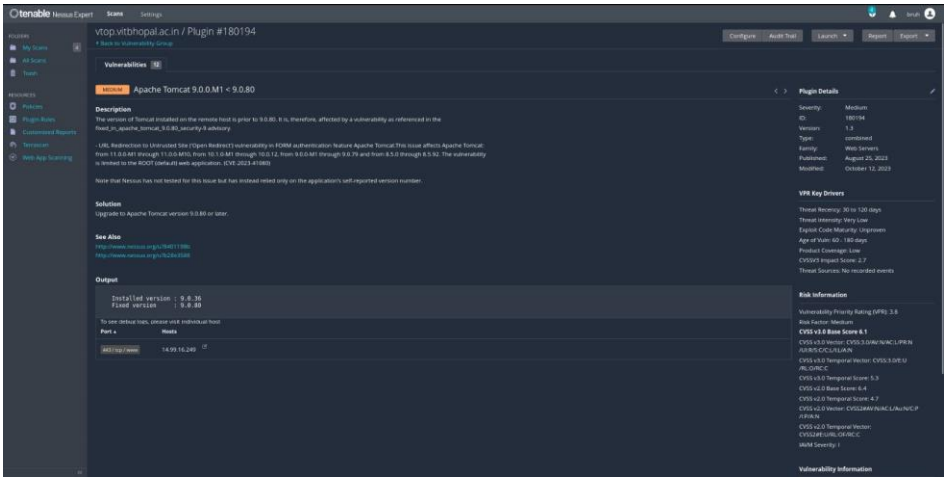
OWASP Category: A9:2017-Using Components with Known Vulnerabilities

Description: Vulnerability in Apache Tomcat versions 9.0.0.M1 through 9.0.80 may allow attackers to gain unauthorized access or view sensitive information.

Business Impact: Potential for unauthorized access or information disclosure.

Vulnerability Path: https://vtop.vitbhopal.ac.in/

Vulnerability Parameter: view-source:https://vtop.vitbhopal.ac.in/



7. Apache Tomcat 9.0.30 < 9.0.65 Vulnerability

CWE: CWE-444

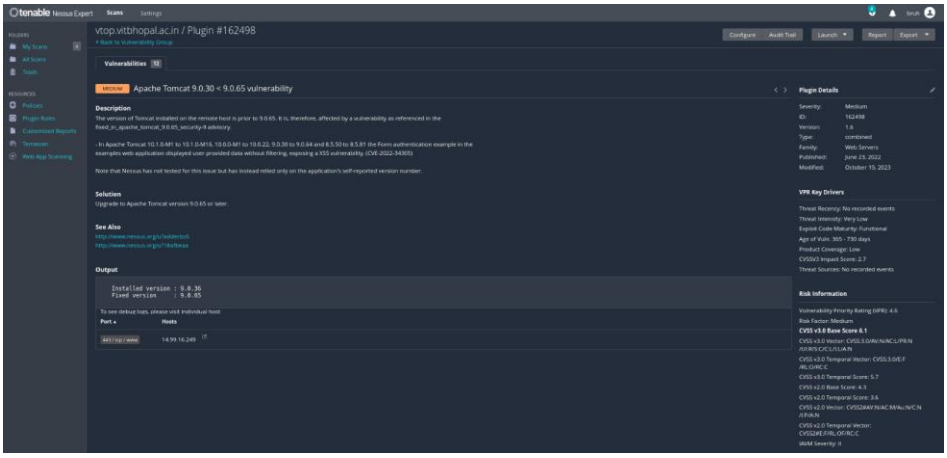
OWASP Category: A9:2017-Using Components with Known Vulnerabilities

Description: Vulnerability in Apache Tomcat versions 9.0.30 through 9.0.65 may allow attackers to gain unauthorized access or view sensitive information.

Business Impact: Potential for unauthorized access or information disclosure.

Vulnerability Path: https://vtop.vitbhopal.ac.in/

Vulnerability Parameter: view-source:https://vtop.vitbhopal.ac.in/



8. Apache Tomcat 9.0.0.M1 < 9.0.48 Vulnerability

CWE: CWE-444

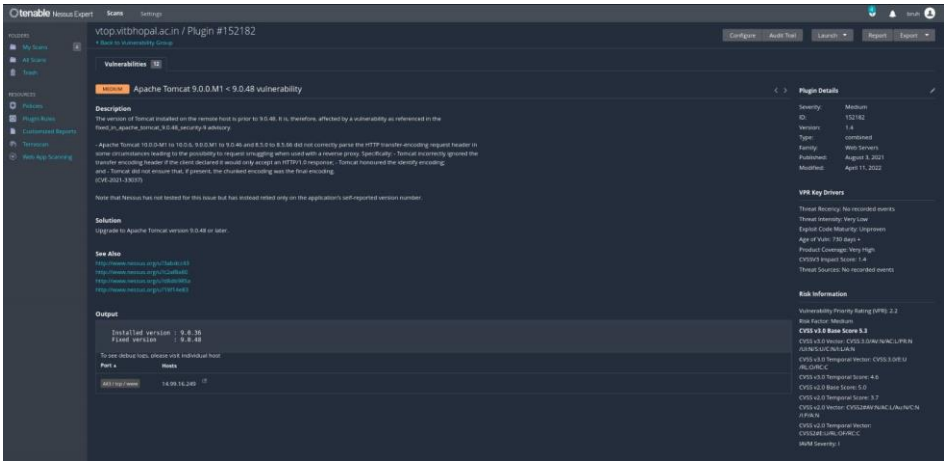
OWASP Category: A9:2017-Using Components with Known Vulnerabilities

Description: Vulnerability in Apache Tomcat versions 9.0.0.M1 through 9.0.48 may allow attackers to gain unauthorized access or view sensitive information.

Business Impact: Potential for unauthorized access or information disclosure.

Vulnerability Path: https://vtop.vitbhopal.ac.in/

Vulnerability Parameter: view-source:https://vtop.vitbhopal.ac.in/



9. Apache Tomcat 9.0.0.M1 < 9.0.81 Multiple Vulnerabilities

CWE: CWE-444

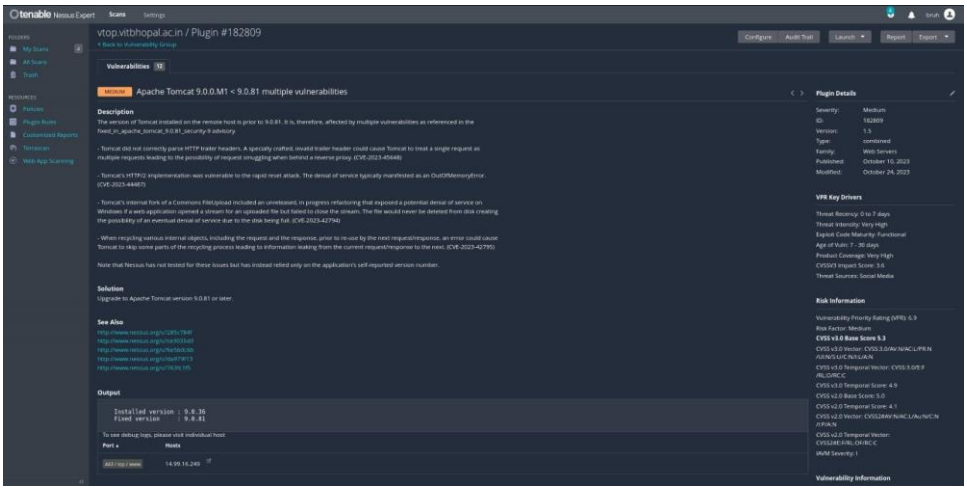
OWASP Category: A9:2017-Using Components with Known Vulnerabilities

Description: Multiple vulnerabilities in Apache Tomcat versions 9.0.0.M1 through 9.0.81 may allow attackers to gain unauthorized access or view sensitive information.

Business Impact: Potential for unauthorized access or information disclosure.

Vulnerability Path: https://vtop.vitbhopal.ac.in/

Vulnerability Parameter: view-source:https://vtop.vitbhopal.ac.in/



10. Apache Tomcat 9.0.0.M1 < 9.0.72

CWE: CWE-444

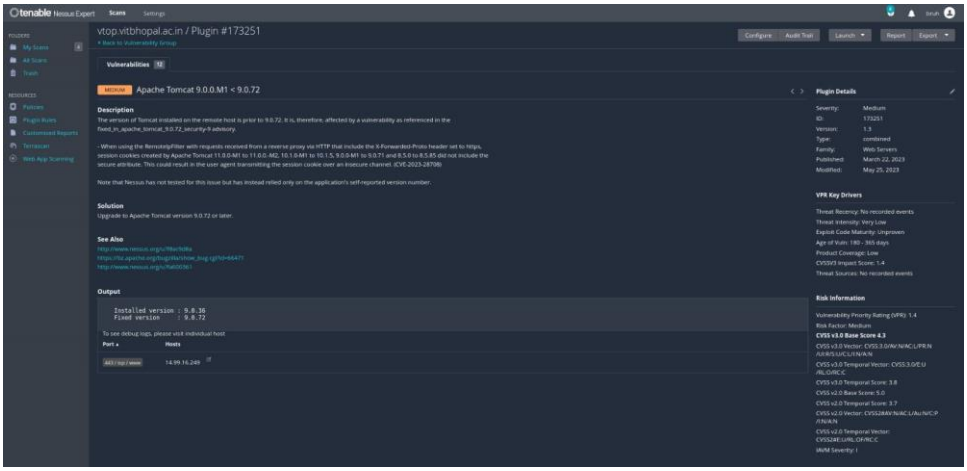
OWASP Category: A9:2017-Using Components with Known Vulnerabilities

Description: Vulnerability in Apache Tomcat versions 9.0.0.M1 through 9.0.72 may allow attackers to gain unauthorized access or view sensitive information.

Business Impact: Potential for unauthorized access or information disclosure.

Vulnerability Path: https://vtop.vitbhopal.ac.in/

Vulnerability Parameter: view-source:https://vtop.vitbhopal.ac.in/



11. Apache Tomcat 9.0.0.M1 < 9.0.62 Spring4Shell (CVE-2022-22965) Mitigations

CWE: CWE-444

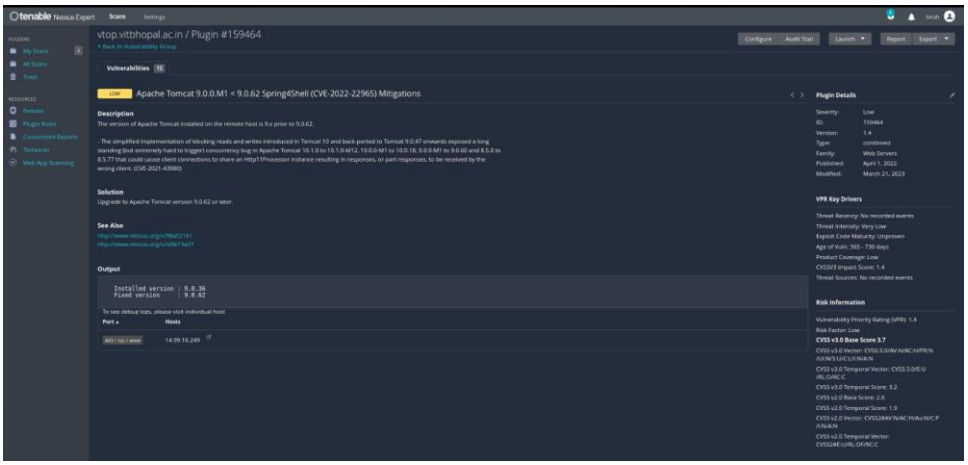
OWASP Category: A9:2017-Using Components with Known Vulnerabilities

Description: Mitigations for the Spring4Shell vulnerability (CVE-2022-22965) in Apache Tomcat versions 9.0.0.M1 through 9.0.62.

Business Impact: Provides mitigations for a critical vulnerability.

Vulnerability Path: https://vtop.vitbhopal.ac.in/

Vulnerability Parameter: view-source:https://vtop.vitbhopal.ac.



12. Apache Tomcat 8.5.x < 8.5.58 / 9.0.x < 9.0.38 HTTP/2 Request Mix-Up

CWE: CWE-444

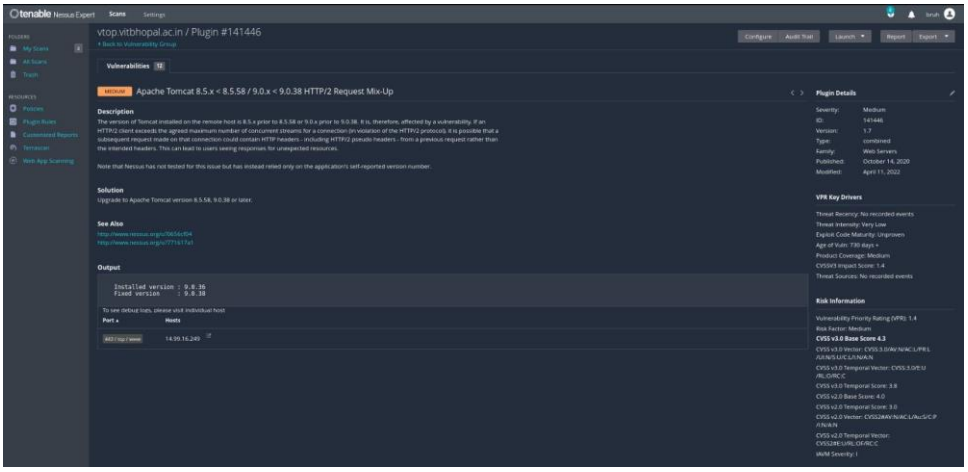
OWASP Category: A9:2017-Using Components with Known Vulnerabilities

Description: Vulnerability in Apache Tomcat versions 8.5.x through 8.5.58 and 9.0.x through 9.0.38 may allow attackers to conduct HTTP/2 request mix-up attacks.

Business Impact: Potential for unauthorized access or information disclosure.

Vulnerability Path: https://vtop.vitbhopal.ac.in/

Vulnerability Parameter: view-source:https://vtop.vitbhopal.ac.in/



STAGE 2

Overview:

Nessus scanning is a cybersecurity practice and a network vulnerability scanner that plays a crucial role in identifying and assessing vulnerabilities within computer systems, networks, and infrastructure. Nessus is developed by Tenable, Inc. and is widely used by security professionals and organizations to enhance their network security.

At its core, Nessus scanning is a systematic and automated process that involves the following key elements:

1. Vulnerability Detection: Nessus scanning actively seeks out vulnerabilities within a target system or network. These vulnerabilities can include software flaws, misconfigurations, weak passwords, and other security issues that could be exploited by malicious actors. The scanner relies on a comprehensive database of known vulnerabilities, continuously updated to include the latest threats.
2. Network Discovery: Before scanning for vulnerabilities, Nessus identifies and maps the target network or system. This initial discovery phase helps the scanner understand the topology of the network and determine what devices and services are present.
3. Scanning and Assessment: Once the network is discovered, Nessus conducts a series of tests and assessments. These include port scanning to identify open ports, services running on those ports, and attempts to identify vulnerabilities related to these services. The scanner may also test for weak or default passwords, misconfigured settings, and other common security issues.
4. Risk Assessment: After scanning, Nessus provides a detailed report that includes a list of identified vulnerabilities, their severity levels, potential impacts, and recommendations for remediation. Each vulnerability is typically assigned a Common Vulnerability Scoring System (CVSS) score to help organizations prioritize their response.
5. Customization and Reporting: Nessus is highly customizable, allowing users to define scan policies, specify targets, and tailor scans to their specific needs. It generates comprehensive reports, often with detailed information about the vulnerabilities found and suggested remediation steps.
6. Continuous Monitoring: Nessus can be configured to perform regular, automated scans, helping organizations to continuously monitor their network security posture. This proactive approach allows for the identification of new vulnerabilities as they emerge.
7. Compliance and Configuration Auditing: Beyond vulnerability scanning, Nessus can perform compliance checks and configuration audits to

ensure that systems and networks adhere to industry-specific standards and best practices.

The significance of Nessus scanning cannot be overstated in today's cybersecurity landscape. With a rapidly evolving threat landscape and ever-increasing network complexities, identifying and addressing vulnerabilities promptly is critical to safeguarding sensitive data and maintaining the integrity and availability of systems. Nessus not only provides valuable insights into existing weaknesses but also aids in compliance efforts, thereby helping organizations avoid potential breaches and data loss while remaining compliant with regulatory requirements.

Target Website: www.testfire.net
Target IP Address: 65.61.137.117
List of Vulnerabilities:

S. No.	Vulnerability	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
11.	HyperText Transfer Protocol (HTTP) Information	Info	24260
12.	Nessus SYN scanner	Info	11219
13.	Nessus Scan Information	Info	19506
14.	OS Identification	Info	11936
15.	SSL / TLS Versions Supported	Info	56984
16.	SSL Certificate Information	Info	10863
17.	SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)	Info	95631
18.	SSL Cipher Block Chaining Cipher Suites Supported	Info	70544
19.	SSL Cipher Suites Supported	Info	21643
20.	SSL Perfect Forward Secrecy Cipher Suites Supported	Info	57041

21.	SSL Root Certification Authority Certificate Information	Info	94761
22.	SSL/TLS Recommended Cipher Suites	Info	156899
23.	Service Detection	Info	22964
24.	TCP/IP Timestamps Supported	Info	25220
25.	TLS Version 1.1 Protocol Detection	Info	121010
26.	TLS Version 1.2 Protocol Detection	Info	136318
27.	Traceroute Information	Info	10287

REPORT

1. Vulnerability: TLS Version 1.0 Protocol Detection

Severity: Medium
Plugin: 104743
Port: HTTP 443
Description: This vulnerability indicates that the server supports the TLS 1.0 protocol, which is considered outdated and insecure due to known vulnerabilities.
Solution: Disable TLS 1.0 and upgrade to a more secure TLS version, such as TLS 1.2 or TLS 1.3.
Business Impact: Using TLS 1.0 poses a risk of data interception and exploitation, potentially leading to data breaches and loss of trust among users.

2. Vulnerability: TLS Version 1.1 Protocol Deprecated

Severity: Medium
Plugin: 157288
Port: 443
Description: TLS 1.1 is deprecated due to known vulnerabilities. This finding suggests that the server supports TLS 1.1.
Solution: Disable TLS 1.1 and upgrade to a more secure TLS version, such as TLS 1.2 or TLS 1.3.
Business Impact: Continuing to use TLS 1.1 increases the risk of security incidents and impacts the organization's reputation.

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

Severity: Low
Plugin: 83875
Port: 443
Description: The server employs weak Diffie-Hellman key exchange, making it vulnerable to the Logjam attack.
Solution: Generate a strong Diffie-Hellman key with a key length greater than 1024 bits.
Business Impact: Weak key exchange may lead to eavesdropping and the compromise of sensitive data.

4. Vulnerability: ICMP Timestamp Request Remote Date Disclosure

Severity: Info
Plugin: 10114
Port: NA
Description: This vulnerability allows remote attackers to determine the system's time and date.
Solution: Disable or filter ICMP timestamp requests.
Business Impact: Attackers can use this information to plan coordinated attacks, impacting the organization's security.

5. Vulnerability: Additional DNS Hostnames
Severity: Info
Plugin: 46180
Port: NA
Description: Multiple DNS hostnames are associated with the target, which may indicate misconfigurations or multiple entry points.
Solution: Review DNS configurations and consolidate hostnames if necessary.
Business Impact: Misconfigured DNS records can lead to routing and security issues.

6. Vulnerability: Apache Tomcat Detection
Severity: Info
Plugin: 39446
Port: 8080
Description: The scan detected the presence of an Apache Tomcat web server.
Solution: Ensure the Apache Tomcat server is up to date and securely configured.
Business Impact: Unsecured Apache Tomcat servers may be exploited, leading to data breaches or service disruptions.

7. Vulnerability: Common Platform Enumeration (CPE)
Severity: Info
Plugin: 45590
Port: NA
Description: This identifies the Common Platform Enumeration (CPE) entries associated with the target.
Solution: Ensure the CPE entries are accurate and up to date.
Business Impact: Inaccurate CPE entries can affect system management and software inventory.

8. Vulnerability: Device Type
Severity: Info
Plugin: 54615
Port: NA
Description: The scan detects and categorizes the type of devices present.
Solution: Review device categorization for accuracy.
Business Impact: Accurate device classification aids in network management and security.

9. Vulnerability: HSTS Missing from HTTPS Server
Severity: Info
Plugin: 84502
Port: 443
Description: HTTP Strict Transport Security (HSTS) is not implemented on the HTTPS server.
Solution: Enable HSTS to enhance security by ensuring secure connections.
Business Impact: Without HSTS, users may be vulnerable to man-in-the-middle attacks.
10. Vulnerability: HTTP Server Type and Version
Severity: Info
Plugin: 10107
Port: 80
Description: The scan identifies the type and version of the HTTP server.
Solution: Review the server type and version for security updates.
Business Impact: Server type and version disclosure can be exploited to target known vulnerabilities.
11. Vulnerability: HyperText Transfer Protocol (HTTP) Information
Severity: Info
Plugin: 24260
Port: 80
Description: HTTP information is provided, which may include headers, methods, and other details about the HTTP service.
Solution: Ensure that HTTP headers and configurations align with security best practices.
Business Impact: Incorrect or insecure HTTP configurations may lead to security vulnerabilities and data exposure.
12. Vulnerability: Nessus SYN scanner
Severity: Info
Plugin: 11219
Port: NA
Description: Nessus employs SYN scanning to discover open ports on the target.
Solution: Ensure that SYN scanning is conducted responsibly and with appropriate permissions.
Business Impact: SYN scanning helps identify potential entry points for attacks, making it a valuable security tool.
13. Vulnerability: Nessus Scan Information
Severity: Info
Plugin: 19506
Port: NA
Description: Nessus provides information about the scan configuration and settings.

Solution: Review and adjust scan configurations to meet security objectives.
Business Impact: Proper scan configurations ensure comprehensive and accurate vulnerability assessments.

14. Vulnerability: OS Identification
Severity: Info
Plugin: 11936
Port: NA
Description: The scan identifies the target's operating system.
Solution: Validate the accuracy of the OS identification and take necessary security measures.
Business Impact: Accurate OS identification aids in security policy enforcement and patch management.

15. Vulnerability: SSL / TLS Versions Supported
Severity: Info
Plugin: 56984
Port: 443
Description: The scan identifies the SSL/TLS versions supported by the server.
Solution: Disable outdated and insecure SSL/TLS versions.
Business Impact: Supporting insecure SSL/TLS versions can lead to data exposure and breaches.

16. Vulnerability: SSL Certificate Information
Severity: Info
Plugin: 10863
Port: 443
Description: SSL certificate details, including expiration date and issuer, are provided.
Solution: Regularly update SSL certificates to maintain secure connections.
Business Impact: Expired or misconfigured certificates can lead to security warnings and disruptions.

17. Vulnerability: SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)
Severity: Info
Plugin: 95631
Port: 443
Description: The SSL certificate is signed using a weak hashing algorithm from a known certificate authority.
Solution: Obtain a new certificate signed with a stronger hashing algorithm.
Business Impact: Weakly signed certificates can be exploited, impacting the trustworthiness of secure connections.

18. Vulnerability: SSL Cipher Block Chaining Cipher Suites Supported
Severity: Info
Plugin: 70544
Port: 443

Description: The scan identifies SSL cipher suites that use Cipher Block Chaining (CBC).
Solution: Disable insecure CBC cipher suites and prioritize secure options.
Business Impact: Insecure cipher suites can lead to attacks like "Padding Oracle" and data leaks.

19. Vulnerability: SSL Cipher Suites Supported
Severity: Info
Plugin: 21643
Port: 443
Description: The scan lists the supported SSL cipher suites.
Solution: Disable insecure cipher suites and prioritize strong encryption.
Business Impact: Weak cipher suites can lead to data exposure and attacks.

20. Vulnerability: SSL Perfect Forward Secrecy Cipher Suites Supported
Severity: Info
Plugin: 57041
Port: 443
Description: The scan identifies SSL cipher suites that support Perfect Forward Secrecy (PFS).
Solution: Enable PFS cipher suites to enhance security.
Business Impact: PFS ensures that past communications remain secure even if encryption keys are compromised.

21. Vulnerability: SSL Root Certification Authority Certificate Information
Severity: Info
Plugin: 94761
Port: 443
Description: Information about the SSL root certification authority certificate is provided.
Solution: Ensure the root certificate is trusted and up to date.
Business Impact: Expired or untrusted root certificates can lead to security warnings.

22. Vulnerability: SSL/TLS Recommended Cipher Suites
Severity: Info
Plugin: 156899
Port: 443
Description: The scan provides information about recommended SSL/TLS cipher suites.
Solution: Configure the server to use recommended and secure cipher suites.
Business Impact: Properly configured cipher suites enhance data security.

23. Vulnerability: Service Detection
Severity: Info
Plugin: 22964
Port: NA
Description: The scan identifies the services and ports exposed by the target.

Solution: Review and secure exposed services and ports.
Business Impact: Accurate service detection is essential for security policy enforcement.

24. Vulnerability: TCP/IP Timestamps Supported
Severity: Info
Plugin: 25220
Port: NA
Description: The server supports TCP/IP timestamps.
Solution: Evaluate the necessity of TCP/IP timestamps and disable if not needed.
Business Impact: Enabling unnecessary timestamps can expose the system to certain attacks.

25. Vulnerability: TLS Version 1.1 Protocol Detection
Severity: Info
Plugin: 121010
Port: 443
Description: The scan detects the support for TLS 1.1 protocol.
Solution: Disable TLS 1.1 and upgrade to a more secure TLS version.
Business Impact: Continuing to support TLS 1.1 increases security risks and vulnerabilities.

26. Vulnerability: TLS Version 1.2 Protocol Detection
Severity: Info
Plugin: 136318
Port: NA
Description: The scan detects the support for TLS 1.2 protocol.
Solution: Maintain support for TLS 1.2, which is a secure protocol.
Business Impact: Supporting TLS 1.2 is a best practice for secure communication.

27. Vulnerability: Traceroute Information
Severity: Info
Plugin: 10287
Port: NA
Description: Traceroute information is provided, revealing the network path between the scanner and the target.
Solution: Ensure that sensitive network path information is not disclosed.
Business Impact: Disclosing network paths may expose infrastructure details, aiding potential attackers.

Target Website: www.vtop.vitbhopal.ac.in
Target IP Address 1: 182.73.197.23
List of Vulnerabilities:

S. No.	Vulnerability	Severity	Plugins
1.	Nessus SYN scanner	Info	11219

2.	Nessus Scan Information	Info	19506
3.	OS Identification Failed	Info	50350
4.	Open Port Re-check	Info	10919
5.	Service Detection	Info	22964
6.	Traceroute Information	Info	10287
7.	Web Server No 404 Error Code Check	Info	10386

REPORT

1. Vulnerability: Nessus SYN Scanner

Severity: Info
Plugin: 11219
Port: NA
Description: Detection of the use of the Nessus SYN scanner tool. This indicates that the scan is being conducted using Nessus's SYN scanning methodology.
Solution: No specific action is required for this detection as it is an indication of the scanning tool being used.
Business Impact: The Nessus SYN scanner is an essential tool for conducting network and vulnerability assessments. It is not a vulnerability, but a tool used for improving security.

2. Vulnerability: Nessus Scan Information

Severity: Info
Plugin: 19506
Port: NA
Description: Detection of general information related to the Nessus scan, such as scan settings, policy, and timestamps. This information is part of the scan report.
Solution: No specific action is required for this detection as it is a report of the scan information.
Business Impact: Nessus scan information is crucial for assessing the security posture of a network and identifying vulnerabilities.

3. Vulnerability: OS Identification Failed

Severity: Info
Plugin: 50350
Port: NA
Description: Detection that the scan failed to identify the target's operating system. This may indicate difficulty in accurately determining the OS.
Solution: Review and validate the OS identification results and consider alternative methods if OS identification is essential.
Business Impact: Accurate OS identification is important for maintaining and securing the target's infrastructure.

4. Vulnerability: Open Port Re-check

Severity: Info
Plugin: 10919
Port: NA
Description: Detection of a re-check for open ports. This indicates a secondary check for previously identified open ports to confirm their status.
Solution: No specific action is required for this detection as it is a part of the scan process.
Business Impact: Open port re-checks are a part of ensuring the accuracy of open port identification.

5. Vulnerability: Service Detection
Severity: Info
Plugin: 22964
Port: NA
Description: Detection of services running on the target system. This information helps identify the services available on the target.
Solution: No specific action is required for this detection as it is a part of the scan process.
Business Impact: Accurate service detection aids in network management and security.

6. Vulnerability: Traceroute Information
Severity: Info
Plugin: 10287
Port: NA
Description: Detection of traceroute information, which is used to identify the network path to the target. Traceroute helps understand the route that packets take between the source and destination.
Solution: No specific action is required for this detection as it is a part of the scan process.
Business Impact: Accurate traceroute information aids in network troubleshooting and management.

7. Vulnerability: Web Server No 404 Error Code Check
Severity: Info
Plugin: 10386
Port: 80
Description: Detection of a check for 404 error codes from the web server. This indicates that the scanner is assessing how the web server handles missing or nonexistent pages (404 errors).
Solution: Review and validate the handling of 404 errors on the web server. Ensure that sensitive information is not disclosed in error messages.
Business Impact: Proper handling of 404 errors is important for user experience and security, as it can prevent the disclosure of sensitive information.

Target Website: www.vtop.vitbhopal.ac.in
Target IP Address 2: 14.99.16.249
List of Vulnerabilities:

S. No.	Vulnerabilities	Severity	Plugins
1.	Apache Tomcat 9.0.0-M1 < 9.0.68 Request Smuggling Vulnerability	High	166906
2.	Apache Tomcat 9.0.0.M1 < 9.0.37 Multiple Vulnerabilities	High	138591
3.	Apache Tomcat 9.0.0.M1 < 9.0.43 Multiple Vulnerabilities	High	147164
4.	Apache Tomcat 9.0.0.M1 < 9.0.71	High	171657
5.	Apache Tomcat 9.0.13 < 9.0.63 vulnerability	High	160894
6.	Apache Tomcat 9.x < 9.0.40 Information Disclosure	High	144050
7.	Apache Tomcat 7.0.x <= 7.0.108 / 8.5.x <= 8.5.65 / 9.0.x <= 9.0.45 / 10.0.x <= 10.0.5 vulnerability	Medium	151502
8.	Apache Tomcat 9.0.0.M1 < 9.0.80	Medium	180194
9.	Apache Tomcat 9.0.30 < 9.0.65 vulnerability	Medium	162498
10.	Apache Tomcat 9.0.0.M1 < 9.0.48 vulnerability	Medium	152182
11.	Apache Tomcat 9.0.0.M1 < 9.0.81 multiple vulnerabilities	Medium	182809
12.	Apache Tomcat 8.5.x < 8.5.58 / 9.0.x < 9.0.38 HTTP/2 Request Mix-Up	Medium	141446
13.	Apache Tomcat 9.0.0.M1 < 9.0.72	Medium	173251
14.	Apache Tomcat 9.0.0.M1 < 9.0.62 Spring4Shell (CVE-2022-22965) Mitigations	Low	159464
15.	Apache Tomcat Detection	Info	39446
16.	Common Platform Enumeration (CPE)	Info	45590
17.	Host Fully Qualified Domain Name (FQDN) Resolution	Info	12053
18.	Inconsistent Hostname and IP Address	Info	46215
19.	Nessus SYN scanner	Info	11219
20.	Nessus Scan Information	Info	19506
21.	OS Identification Failed	Info	50350
22.	Open Port Re-check	Info	10919

23.	Patch Report	Info	66334
24.	Service Detection	Info	22964
25.	Traceroute Information	Info	10287
26.	Web Server No 404 Error Code Check	Info	10386

REPORT

1. Vulnerability: Apache Tomcat 9.0.0-M1 < 9.0.68 Request Smuggling Vulnerability

Severity: High

Plugin: 166906

Port: 8080

Description: Vulnerability in Apache Tomcat versions that can allow request smuggling attacks.

Solution: Update Apache Tomcat to a version that is not affected by this vulnerability.

Business Impact: Failure to address this vulnerability could lead to request smuggling attacks, potentially causing data manipulation or security breaches.

2. Vulnerability: Apache Tomcat 9.0.0.M1 < 9.0.37 Multiple Vulnerabilities

Port: 8080

Severity: High

Plugin: 138591

Description: Detection of multiple vulnerabilities in the specified Apache Tomcat version range.

Solution: Upgrade Apache Tomcat to a version that addresses these vulnerabilities.

Business Impact: Failure to address these vulnerabilities can lead to various security risks, including potential data breaches.

3. Vulnerability: Apache Tomcat 9.0.0.M1 < 9.0.43 Multiple Vulnerabilities

Severity: High

Plugin: 147164

Port: 8080

Description: Detection of multiple vulnerabilities in the specified Apache Tomcat version range.

Solution: Upgrade Apache Tomcat to a version that fixes these vulnerabilities.

Business Impact: Ignoring these vulnerabilities can expose the system to various security threats.

4. Vulnerability: Apache Tomcat 9.0.0.M1 < 9.0.71

Severity: High

Plugin: 171657

Port: 8080

Description: Detection of the use of an Apache Tomcat version within the specified range.

Solution: Consider upgrading to a more recent, secure version of Apache Tomcat.

Business Impact: Using older versions of Apache Tomcat can expose systems to known vulnerabilities and security issues.

5. Vulnerability: Apache Tomcat 9.0.13 < 9.0.63 Vulnerability

Severity: High

Plugin: 160894

Port: 8080

Description: Detection of a vulnerability within the specified Apache Tomcat version range.

Solution: Update Apache Tomcat to a version that addresses this vulnerability.

Business Impact: Neglecting this vulnerability can result in potential security breaches and system compromise.

6. Vulnerability: Apache Tomcat 9.x < 9.0.40 Information Disclosure

Severity: High

Plugin: 144050

Port: 8080

Description: Detection of an information disclosure vulnerability in Apache Tomcat.

Solution: Update Apache Tomcat to a version that patches this vulnerability.

Business Impact: Exploiting this vulnerability can lead to unauthorized access to sensitive information, potentially causing data leaks.

7. Vulnerability: Apache Tomcat 7.0.x <= 7.0.108 / 8.5.x <= 8.5.65 / 9.0.x <= 9.0.45 Vulnerability

Severity: Medium

Plugin: 151502

Port: 8080

Description: Detection of vulnerabilities in specific versions of Apache Tomcat.

Solution: Upgrade Apache Tomcat to a version that addresses these vulnerabilities.

Business Impact: Neglecting these vulnerabilities can lead to security risks, including potential data breaches.

8. Vulnerability: Apache Tomcat 9.0.0.M1 < 9.0.80

Severity: Medium

Plugin: 180194

Port: 8080

Description: Detection of the use of an Apache Tomcat version within the specified range.

Solution: Consider upgrading to a more recent, secure version of Apache Tomcat.

Business Impact: Using older versions of Apache Tomcat can expose systems to known vulnerabilities and security issues.

9. Vulnerability: Apache Tomcat 9.0.30 < 9.0.65 Vulnerability

Severity: Medium

Plugin: 162498

Port: 8080

Description: Detection of a vulnerability within the specified Apache Tomcat version range.

Solution: Update Apache Tomcat to a version that addresses this vulnerability.

Business Impact: Neglecting this vulnerability can result in potential security breaches and system compromise.

10. Vulnerability: Apache Tomcat 9.0.0.M1 < 9.0.48 Vulnerability

Severity: Medium

Plugin: 152182

Port: 8080

Description: Detection of a vulnerability within the specified Apache Tomcat version range.

Solution: Update Apache Tomcat to a version that patches this vulnerability.

Business Impact: Exploiting this vulnerability can lead to unauthorized access to the system and potential data leaks.

11. Vulnerability: Apache Tomcat 9.0.0.M1 < 9.0.81 Multiple Vulnerabilities

Severity: Medium

Plugin: 182809

Port: 8080

Description: Detection of multiple vulnerabilities in the specified Apache Tomcat version range.

Solution: Upgrade Apache Tomcat to a version that fixes these vulnerabilities.

Business Impact: Ignoring these vulnerabilities can expose the system to various security threats, including potential data breaches.

12. Vulnerability: Apache Tomcat 8.5.x < 8.5.58 / 9.0.x < 9.0.38 HTTP/2 Request Mix-Up

Severity: Medium

Plugin: 141446

Port: 8080

Description: Detection of a vulnerability related to HTTP/2 request mix-up in specific Apache Tomcat versions.

Solution: Update Apache Tomcat to a version that addresses this vulnerability.

Business Impact: Exploiting this vulnerability can lead to unauthorized access and potential data manipulation.

13. Vulnerability: Apache Tomcat 9.0.0.M1 < 9.0.72

Severity: Medium

Plugin: 173251

Port: 8080

Description: Detection of the use of an Apache Tomcat version within the specified range.

Solution: Consider upgrading to a more recent, secure version of Apache Tomcat.

Business Impact: Using older versions of Apache Tomcat can expose systems to known vulnerabilities and security issues.

14. Vulnerability: Apache Tomcat 9.0.0.M1 < 9.0.62 Spring4Shell (CVE-2022-22965) Mitigations

Severity: Low

Plugin: 159464

Port: 8080

Description: Detection of mitigations related to the Spring4Shell vulnerability (CVE-2022-22965) in specified Apache Tomcat versions.

Solution: Implement the necessary mitigations as recommended to protect against the Spring4Shell vulnerability.

Business Impact: Neglecting these mitigations can expose the system to the Spring4Shell vulnerability, potentially leading to unauthorized access and data breaches.

15. Vulnerability: Apache Tomcat Detection

Severity: Info

Plugin: 39446

Port: 8080

Description: Detection of an Apache Tomcat server, an open-source web application server.

Solution: Keep the Apache Tomcat server and its components updated to mitigate known vulnerabilities.

Business Impact: Running outdated Apache Tomcat versions can expose the

system to security vulnerabilities and potential attacks.

16. Vulnerability: Common Platform Enumeration (CPE)

Severity: Info

Plugin: 45590

Port: NA

Description: Detection of Common Platform Enumeration (CPE) information related to the target.

Solution: Review and validate the CPE information for accuracy and relevance.

Business Impact: Accurate CPE information is essential for managing and securing the components of a system.

17. Vulnerability: Host Fully Qualified Domain Name (FQDN) Resolution

Severity: Info

Plugin: 12053

Port: NA

Description: Detection of the fully qualified domain name (FQDN) resolution for the target.

Solution: Review and validate the FQDN resolution for correctness.

Business Impact: Accurate FQDN resolution is crucial for system identification and security management.

18. Vulnerability: Inconsistent Hostname and IP Address

Severity: Info

Plugin: 46215

Port: NA

Description: Detection of inconsistencies between hostnames and IP addresses associated with the target.

Solution: Resolve inconsistencies to ensure accurate DNS configurations.

Business Impact: Inconsistent hostname and IP address configurations can lead to network and security issues.

19. Vulnerability: Nessus SYN Scanner

Severity: Info

Plugin: 11219

Port: NA

Description: Detection of the Nessus SYN scanner tool's use, indicating that the scanner is being used for the assessment.

Solution: No specific action is required for this detection as it is an indication of the scanning tool.

Business Impact: The Nessus SYN scanner is an important tool for network and vulnerability assessments, helping organizations identify and address security issues.

20. Vulnerability: Nessus Scan Information

Severity: Info

Plugin: 19506

Port: NA

Description: Detection of general information related to the Nessus scan, such as scan settings, policy, and timestamps.

Solution: No specific action is required for this detection as it is a reporting of the scan information.

Business Impact: Nessus scan information is important for assessing the security posture of a network and identifying vulnerabilities.

21. Vulnerability: OS Identification Failed

Severity: Info

Plugin: 50350

Port: NA

Description: Detection that the scan failed to identify the target's operating system. This may indicate difficulty in accurately determining the OS.

Solution: Review and validate the OS identification results and consider alternative methods if OS identification is essential.

Business Impact: Accurate OS identification is important for maintaining and securing the target's infrastructure.

22. Vulnerability: Open Port Re-check

Severity: Info

Plugin: 10919

Port: NA

Description: Detection of a re-check for open ports. This indicates a secondary check for previously identified open ports to confirm their status.

Solution: No specific action is required for this detection as it is a part of the scan process.

Business Impact: Open port re-checks are a part of ensuring the accuracy of open port identification.

23. Vulnerability: Patch Report

Severity: Info

Plugin: 66334

Port: NA

Description: Detection of patch report information, which may relate to the status of applied security patches.

Solution: Review the patch report information and take necessary actions to address any missing or critical patches.

Business Impact: Ensuring that systems have up-to-date patches is essential for mitigating known vulnerabilities and enhancing security.

24. Vulnerability: Service Detection

Severity: Info

Plugin: 22964

Port: NA

Description: Detection of services running on the target system. This information helps identify the services available on the target.

Solution: No specific action is required for this detection as it is a part of the scan process.

Business Impact: Accurate service detection aids in network management and security.

25. Vulnerability: Traceroute Information

Severity: Info

Plugin: 10287

Port: NA

Description: Detection of traceroute information, which is used to identify the network path to the target. Traceroute helps understand the route that packets take between the source and destination.

Solution: No specific action is required for this detection as it is a part of the scan process.

Business Impact: Accurate traceroute information aids in network troubleshooting and management.

26. Vulnerability: Web Server No 404 Error Code Check

Severity: Info

Plugin: 10386

Port: 80

Description: Detection of a check for 404 error codes from the web server. This indicates that the scanner is assessing how the web server handles missing or nonexistent pages (404 errors).

Solution: Review and validate the handling of 404 errors on the web server. Ensure that sensitive information is not disclosed in error messages.

Business Impact: Proper handling of 404 errors is important for user experience and security, as it can prevent the disclosure of sensitive information.

STAGE 3

Achieving Proactive Cybersecurity with SOC and SIEM Integration

- **Soc**

  A security operations center (SOC) – sometimes called an information security operations center, or ISOC – is an in-house or outsourced team of IT security professionals that monitors an organization's entire IT infrastructure, 24/7, to detect cybersecurity events in real time and address them as quickly and effectively as possible. It also continually analyzes threat data to find ways to improve the organization's security posture. SOC is a critical
component of a robust cybersecurity strategy

- **SOC – cycle**

  The SOC (Security Operations Center) cycle, also known as the SOC lifecycle or SOC workflow, is a continuous process that outlines the key steps involved in managing an organization's cybersecurity. It encompasses

  activities from threat detection to incident response and recovery. The SOC

  cycle typically consists of the following stages:

  - **Threat Detection and Monitoring:**

  Continuous monitoring of the organization's network, systems, and applications to identify potential security threats and anomalies. Leveraging various security tools, such as intrusion detection systems (IDS), intrusion prevention systems (IPS), firewalls, SIEM (Security Information and Event Management) solutions, and threat intelligence feeds.

  - **Alert Triage and Analysis:**

  Analyzing and prioritizing security alerts generated by the monitoring tools based on their severity and potential impact.
  Determining if an alert indicates a genuine security incident or a false positive.

  - **Incident Investigation and Response:**

  If an alert is confirmed as a legitimate security incident, the SOC

team conducts a thorough investigation to understand the nature and extent of the attack.
Gathering evidence, analyzing log data, and performing digital forensics to determine the source and impact of the incident.
Initiating the incident response process, which may involve isolating affected systems, containing the threat, and preventing further damage.

- **Incident Containment and Eradication:**

Taking immediate actions to contain the incident and prevent it from spreading further within the organization's network.
Removing the malicious elements and eradicating the threat to restore the affected systems to a secure state.

- **Recovery and Remediation:**

After the threat is eradicated, the SOC team focuses on restoring affected systems and services to normal operation.
Implementing remediation measures to address the root cause of the incident and prevent similar attacks in the future.

- **Post-Incident Analysis and Lessons Learned:**

Conducting a thorough post-mortem analysis of the incident to understand how it happened, what was the impact, and what steps were taken to respond.
Identifying areas of improvement in the organization's security posture and incident response procedures.
Updating security policies and procedures based on the lessons learned from the incident.

- **Threat Intelligence and Proactive Measures:**

Integrating threat intelligence into the SOC workflow to stay ahead of emerging threats and known attack patterns.
Proactively hunting for signs of potential threats and vulnerabilities before they lead to full-fledged security incidents.

- **Continuous Monitoring and Improvement:**

The SOC cycle is a continuous process, with ongoing monitoring, analysis, and improvement of security measures to adapt to the evolving threat landscape.
By following this cycle, the SOC team can effectively detect, respond

to, and recover from security incidents, minimizing the impact of cyber threats on the organization's assets and data.

- **Siem**

  Security information and event management, or SIEM, is a security solution that helps organizations recognize and address potential security threats and vulnerabilities before they have a chance to disrupt business operations. SIEM systems help enterprise security teams detect user behaviour anomalies and use artificial intelligence (AI) to automate many of the manual processes associated with threat detection and incident response.
  SIEM is an important part of an organization’s cybersecurity ecosystem. SIEM gives security teams a central place to collect, aggregate, and analyze volumes of data across an enterprise, effectively streamlining security workflows. It also delivers operational capabilities such as compliance reporting, incident management, and dashboards that prioritize threat activity.

- **Siem Cycle**

  The lifecycle of a Security Information and Event Management (SIEM) system involves several interconnected stages that ensure the effective implementation, operation, and maintenance of the SIEM solution. The SIEM life cycle typically includes the following phases:

  - **Planning and Assessment:**

    Define the objectives and scope of the SIEM implementation, considering the organization's security requirements and compliance goals.

    Conduct a thorough assessment of the existing security infrastructure, data sources, and log management practices to identify gaps and necessary improvements.

    Develop a detailed plan for deploying the SIEM solution, including resource allocation, timeline, and responsibilities.

  - **Design and Architecture:**

    Design the SIEM architecture based on the organization's requirements and data sources, considering factors like scalability, redundancy, and performance.

Determine the best deployment model (on-premises, cloud-based, hybrid) that aligns with the organization's needs and resources.

Plan the integration of data sources into the SIEM, ensuring that relevant security events are collected and centralized for analysis.

- **Data Collection and Integration:**

Implement data collectors and agents to gather logs and events from various sources, such as firewalls, network devices, servers, applications,
and endpoints.

Normalize and enrich the collected data to facilitate efficient analysis and correlation.

Configure connectors and parsers to integrate data feeds from security devices and other sources into the SIEM platform.

- **Event Correlation and Analysis:**

Develop and fine-tune correlation rules and use cases to identify patterns of malicious activity and security threats.

Conduct real-time event correlation and analysis to generate actionable alerts for potential security incidents.

Utilize threat intelligence feeds to enhance the SIEM's ability to detect emerging threats and known attack vectors.

- **Incident Detection and Response:**

Respond to generated alerts by investigating potential security incidents.

Perform detailed analysis to determine the scope and impact of identified security events.

Initiate incident response activities, including containment, eradication, and recovery.

- **Forensics and Investigation:**

Conduct in-depth forensics analysis to understand the root cause of incidents and the methods used by attackers.

Preserve and document evidence for potential legal or regulatory purposes.

- **Reporting and Compliance:**

Generate and present security reports and dashboards for various stakeholders, including IT management, executives, auditors, and regulatory authorities.

Ensure compliance with relevant industry standards and regulations by monitoring and reporting on security events and incidents.

- **Continuous Monitoring and Maintenance:**

Continuously monitor the SIEM infrastructure and adjust the configuration as needed to maintain optimal performance.

Regularly update correlation rules, threat intelligence feeds, and other components to keep the SIEM effective against evolving threats.

Conduct periodic reviews and assessments of the SIEM's performance and effectiveness to identify areas for improvement.

- **Training and Knowledge Transfer:**

Train SOC personnel and IT staff on the effective use of the SIEM solution.

Foster knowledge sharing and best practices from incident investigations and analysis within the organization.

The SIEM lifecycle is a continuous and iterative process, with each phase building upon the insights and experiences gained from previous stages. This approach ensures that the SIEM solution remains relevant, efficient, and effective in helping organizations detect and respond to security threats.

As a syslog server incessantly pings with every security notification, security teams can feel as though they are drowning in a sea of security warnings. Without a SIEM, it's difficult to know which events are truly critical and which can be ignored. However, when a SIEM has been implemented, security teams get a much clearer picture of their environment's security. There could truly be no threats, or multiple incidents may be occurring that simply have not yet affected performance.

- **MISP**

MISP Threat Sharing (MISP) is an open source threat intelligence platform.

An efficient IOC and indicators database, allowing to store technical and non-technical information about malware samples, incidents, attackers

and intelligence.

Features of MISP: -

- An efficient IoC and indicators database allowing to store technical and non-technical information about malware samples, incidents, attackers and intelligence.
- Automatic correlation finding relationships between attributes and indicators from malware, attacks campaigns or analysis. Correlation engine includes correlation between attributes and more advanced correlations like Fuzzy hashing correlation (e.g. ssdeep) or CIDR block matching. Correlation can be also enabled or event disabled per attribute.
- A flexible data model where complex objects can be expressed and linked together to express threat intelligence, incidents or connected elements.
- Built-in sharing functionality to ease data sharing using different model of distributions. MISP can synchronize automatically events and attributes among different MISP. Advanced filtering functionalities can be used to meet each organization sharing policy including a flexible sharing group capacity and an attribute level distribution mechanisms.
- An intuitive user-interface for end-users to create, update and collaborate on events and attributes/indicators. A graphical interface to navigate seamlessly between events and their correlations. An event graph functionality to create and view relationships between objects and attributes. Advanced filtering functionalities and warning list to help the analysts to contribute events and attributes.
- storing data in a structured format (allowing automated use of the database for various purposes) with an extensive support of cyber security indicators along fraud indicators as in the financial sector.
- export: generating IDS (Suricata, Snort and Bro are supported by default), OpenIOC, plain text, CSV, MISP XML or JSON output to integrate with other systems (network IDS, host IDS, custom tools

- import: bulk-import, batch-import, free-text import, import from OpenIOC, GFI sandbox, ThreatConnect CSV or MISP format.
- Flexible free text import tool to ease the integration of unstructured reports into MISP.
- A gentle system to collaborate on events and attributes allowing MISP users to propose changes or updates to attributes/indicators.
- data-sharing: automatically exchange and synchronization with other parties and trust-groups using MISP.

- feed import: flexible tool to import and integrate MISP feed and any threatintel or OSINT feed from third parties. Many default feeds are included in standard MISP installation.
- delegating of sharing: allows a simple pseudo-anonymous mechanism to delegate publication of event/indicators to another organization.
- Flexible API to integrate MISP with your own solutions. MISP is bundled with PyMISP which is a flexible Python Library to fetch, add or update events attributes, handle malware samples or search for attributes.
- adjustable taxonomy to classify and tag events following your own classification schemes or existing taxonomies. The taxonomy can be local to your MISP but also shareable among MISP instances. MISP comes with a default set of well-known taxonomies and classification schemes to support standard classification as used by ENISA, Europol, DHS, CSIRTs or many other organisations.
- intelligence vocabularies called MISP galaxy and bundled with existing threat actors, malware, RAT, ransomware or MITRE ATT&CK which can be easily linked with events in MISP.
- expansion modules in Python to expand MISP with your own services or activate already available misp-modules.
- sighting support to get observations from organizations concerning shared indicators and attributes. Sighting can be contributed via MISP user-interface, API as MISP document or STIX sighting documents. Starting with MISP 2.4.66, Sighting has been extended to support false-negative sighting or expiration sighting.
- STIX support: export data in the STIX format (XML and JSON) including export/import in STIX 2.0 format.
- integrated encryption and signing of the notifications via PGP and/or S/MIME depending of the user preferences.

- Real-time publish-subscribe channel within MISP to automatically get all changes (e.g. new events, indicators, sightings or tagging) in ZMQ (e.g. misp-dashboard) or Kafka.

- **How you think you deploy soc in your college – VIT Bhopal**

  Establishing a Security Operations Center (SOC) within an organization involves a systematic approach, careful planning, and allocation of resources. Below are the fundamental steps for deploying a SOC:

  1. Evaluation and Needs Assessment:

  - Conduct a comprehensive evaluation of the organization's current cybersecurity status, including existing security measures, tools, and processes.

  - Identify specific security risks, challenges, and compliance requirements that the SOC will tackle.

  - Define clear goals and objectives for the SOC deployment to align with the organization's overall security strategy.

  2. Budget and Resource Planning:

  - Determine the budget and resource requirements for setting up and maintaining the SOC.

  - Allocate personnel, hardware, software, and other essential resources to support SOC operations.

  3. Assemble a Skilled Team:

  - Recruit or assign proficient security experts to build the SOC team.

- This team should encompass security analysts, incident responders, threat hunters, and SOC management personnel.

4. Infrastructure and Technology Setup:

- Establish the physical or virtual infrastructure for the SOC, encompassing servers, network equipment, and storage.
- Deploy necessary security technologies like SIEM, intrusion detection and prevention systems (IDS/IPS), firewalls, endpoint protection, and threat intelligence feeds.

5. Integration and Data Gathering:

- Integrate security tools and systems with the SIEM to centralize log and event data collection.
- Ensure that crucial data sources such as firewalls, servers, network devices, and applications send logs to the SIEM.

6. Procedure Development:

- Develop standard operating procedures (SOPs) for various SOC tasks, including incident management, response protocols, escalation procedures, and communication guidelines.
- Implement incident categorization and prioritization mechanisms.

7. Monitoring and Alerting Implementation:

- Configure the SIEM to generate real-time alerts based on predefined correlation rules and security use cases.
- Fine-tune alerting thresholds to reduce false positives and focus on critical alerts.

8. Incident Response and Escalation Planning:

- Create a formal incident response plan outlining the steps to be taken in case of a security incident.

- Define roles and responsibilities for incident handling and establish a clear escalation path for severe incidents.

9. Training and Skill Enhancement:

- Provide comprehensive training to the SOC team on using security tools, incident analysis, threat hunting, and best practices for incident response.
- Keep the team updated on the latest cybersecurity trends, attack techniques, and relevant certifications.

10. Testing and Continuous Enhancement:

- Conduct regular tabletop exercises and simulated cyberattack scenarios to assess the SOC team's response capabilities.
- Use insights from testing to improve and refine the SOC's processes and procedures.

11. Monitoring and Reporting:

- Continuously monitor the SOC's performance in detecting and responding to security incidents.
- Generate regular reports and metrics to measure the SOC's effectiveness and communicate its value to stakeholders.

12. Integration with IT and Business Functions:

- Foster collaboration between the SOC and other IT and business units to ensure a coordinated approach to security.
- Engage with executive management and board members to secure support for SOC initiatives.

Deploying a SOC is an ongoing process that demands adaptability and continuous improvement. Regular assessments, training, and updates are critical to ensure the SOC remains effective in addressing the organization's evolving security challenges.

- **Threat intelligence**

Threat intelligence, often referred to as "cyber threat intelligence" (CTI) or simply "threat intel," consists of comprehensive data containing intricate insights into cybersecurity threats that pose a risk to an organization. This valuable resource empowers security teams to proactively anticipate and counteract potential cyberattacks, leveraging data-driven strategies. Moreover, it enhances an organization's ability to identify and respond to ongoing attacks more effectively.

To generate threat intelligence, security analysts compile raw threat data and security-related information from diverse sources. They then process this information by cross-referencing and analyzing it to reveal underlying trends, patterns, and connections. This process yields a profound understanding of existing or potential threats.

The threat intelligence lifecycle

- Step 1: Planning
    a. Security analysts work with organizational stakeholders—executive leaders, department heads, IT and security team members, and others involved in cybersecurity decision-making—to set intelligence requirements. These typically include cybersecurity questions that stakeholders want or need to have answered. For example, the CISO may want to know whether a new, headline-making strain of ransomware is likely to affect the organization.
- Step 2: Threat Data Collection
    b. The security team collects any raw threat data that may hold—or contribute to—the answers stakeholders are looking for. Continuing the example above, if a security team is investigating a new ransomware strain, the team might gather information on the ransomware gang behind the attacks, the types of organizations they've targeted in the past, and the attack vectors they've exploited to infect previous victims.

- Step 3: Processing

    At this stage, security analysts aggregate, standardize, and correlate the raw data they've gathered to make it easier to analyze the data for insights. This might include filtering out false positives, or applying a threat intelligence framework, such as

MITRE ATT&CK, to data surrounding a previous security incident, to better

Many threat intelligence tools automate this processing, using artificial intelligence (AI) and machine learning to correlate threat information from multiple sources and identify initial trends or patterns in the data.

- Step 4: Analysis

  Analysis is the point at which raw threat data becomes true threat intelligence. At this stage, security analysts test and verify trends, patterns, and other insights they can use to answer stakeholders' security requirements and make recommendations.

  For example, if security analysts find that the gang connected with a new ransomware strain has targeted other businesses in the organizations industry, the team may identify specific vulnerabilities in the organization's IT infrastructure that the gang is likely to exploit, as well as security controls or patches that might mitigate or eliminate those vulnerabilities.

- Step 5. Dissemination

  The security team shares its insights and recommendations with the appropriate stakeholders. Action may be taken based on these recommendations, such as establishing new SIEM detection rules to target newly identified IoCs or updating firewall blacklists to block traffic from newly identified suspicious IP addresses. Many threat intelligence tools integrate and share data with security tools such as SOARs or XDRs, to automatically generate alerts for active attacks, assign risk scores for threat prioritization, or trigger other actions.

- Step 6. Feedback

  At this stage, stakeholders and analysts reflect on the most recent threat intelligence cycle to determine if the requirements were met. Any new questions that arise or new intelligence gaps identified may inform the next round of the lifecycle.

Conclusion :-

- **Stage 1 :- Web Application Testing**

Web application testing is the process of evaluating a web-based software application to identify and rectify issues related to its functionality, security, performance, and user experience. This testing is essential to ensure that the web application functions as intended and provides a secure and reliable experience for users. Here are some key aspects of web application testing:

- Functionality Testing:
  This type of testing assesses whether the web application performs its intended functions correctly. Testers check for issues like broken links, form validation, navigation, and overall usability.
- Security Testing:
  Security testing focuses on identifying vulnerabilities and weaknesses in the web application that could be exploited by attackers. It includes tests for vulnerabilities such as SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF).
- Performance Testing:
  Performance testing evaluates the web application's responsiveness, scalability, and speed. It includes tests like load testing, stress testing, and capacity testing to determine how the application performs under different conditions.
- Compatibility Testing:
  This testing ensures that the web application functions correctly across various browsers, operating systems, and devices. It aims to deliver a consistent user experience regardless of the user's choice of technology.
- Usability Testing:
  Usability testing assesses the user-friendliness of the application. Testers evaluate the design, layout, and overall user experience to identify areas for improvement.
- Regression Testing:
  Regression testing confirms that new updates or changes to the web application do not introduce new issues or break existing functionality.

- Load Testing:
  Load testing examines how the application performs under expected and peak loads. It helps determine if the application can handle high user traffic without degrading performance.
- Accessibility Testing:
  Accessibility testing checks whether the web application is accessible to users with disabilities, ensuring compliance with accessibility standards such as WCAG (Web Content Accessibility Guidelines).
- API Testing:
  API testing focuses on the application's backend by evaluating the functionality of its APIs (Application Programming Interfaces). It ensures that data can be exchanged correctly between the application and external services.
- Database Testing:
  Database testing verifies the integrity, accuracy, and efficiency of the application's database operations, including data retrieval, storage, and manipulation.
- Scalability Testing:
  Scalability testing assesses the application's ability to grow and accommodate an increasing number of users, data, or transactions without performance degradation.
- Cross-Site Request Forgery (CSRF) Testing:
  CSRF testing looks for vulnerabilities that could lead to unauthorized actions being performed on behalf of an authenticated user without their consent.

- **Stage 2 :- What do you understand from the nessus report .**
  Nessus is a vulnerability scanning tool used to identify and report security issues in computer systems and networks.
  The outcome of a Nessus report will depend on the specific target scanned and the vulnerabilities found. Typically, a Nessus report will list the identified vulnerabilities along with their severity levels, detailed descriptions, and recommendations for remediation. The severity levels are usually categorized as critical, high, medium, and low, depending on the potential impact and

exploitability of the vulnerability

- **Stage 3 :- What do you understand from SOC / SEIM / Qradar Dashboard** .

  SOC

  A SOC is a dedicated facility or team responsible for monitoring an organization's IT infrastructure, networks, and systems for cybersecurity threats and incidents. It focuses on identifying, assessing, and responding to security events in real-time, often using advanced technologies and skilled personnel.

  SIEM

  SIEM is a comprehensive technology that combines security information management (SIM) and security event management (SEM). It collects data from various sources, including logs and alerts, and correlates these data points to provide insights into security-related events and incidents. SIEM systems help organizations manage and analyze security information in a centralized manner, enabling proactive threat detection and incident response.

  QRadar Dashboard

  A QRadar dashboard is a user-friendly interface within IBM QRadar, a leading SIEM solution. It offers security analysts a visual and customizable display of key security metrics, alerts, and events. QRadar dashboards provide an at-a-glance view of an organization's security posture, facilitating rapid incident detection, investigation, and response. These dashboards can be tailored to specific roles and responsibilities within a security team, enhancing overall operational efficiency.

Future Scopes :

- **Stage 1 :- Future scope of web application testing**

  Increased Complexity of Web Applications:
  Web applications are becoming more complex with the integration of technologies like single-page applications (SPAs), progressive web apps

(PWAs), and microservices. Testing these intricate applications requires advanced testing techniques and tools.

AI and Automation:
The future of web application testing is closely tied to artificial intelligence (AI) and automation. AI can be used for test case generation, intelligent test data management, and predictive analytics to identify potential issues proactively.

Shift-Left Testing:
There is a growing trend in shifting testing activities to earlier stages of the development lifecycle. This includes incorporating testing into the DevOps pipeline to catch and address issues more rapidly.

Security Testing Emphasis:
With the increasing frequency and sophistication of cyber threats, security testing, including penetration testing and vulnerability assessments, will be a vital aspect of web application testing.

IoT and Mobile Testing:
As the Internet of Things (IoT) and mobile applications become more prevalent, testing web services that interact with IoT devices and mobile apps will be a significant focus.

Performance Testing for the Cloud:
Cloud-based applications are common, and performance testing in cloud environments will be essential to ensure scalability and reliability.

Microservices Testing:
With the adoption of microservices architectures, testing the interactions between microservices and the overall system's behavior becomes critical.

Cross-Browser and Cross-Device Testing:
Testing web applications across various browsers, operating systems, and devices remains important as users access applications from diverse platforms.

Compliance and Accessibility Testing:
Regulatory requirements and the need for accessible web applications will continue to drive compliance and accessibility testing.

Blockchain Integration Testing:

Web applications that utilize blockchain technology require specialized testing to ensure the security and integrity of transactions.

Continuous Learning and Training:
Testers and QA professionals will need to continuously update their skills and knowledge to keep pace with evolving technologies and testing methodologies.

User Experience Testing:
Focus on user experience (UX) testing will intensify to ensure web applications are not only functional but also provide an exceptional user experience.

Ethical Hacking and Bug Bounty Programs:
Organizations may invest in ethical hacking practices and bug bounty programs to identify and address security vulnerabilities.

The future of web application testing is dynamic and involves adapting to emerging technologies, ensuring security, and delivering high-quality user experiences. Testers and quality assurance professionals will need to be flexible, embrace automation and AI, and stay informed about the latest industry trends to remain effective in their roles

- **Stage 2 :- Future scope of testing process**

  The future scope of the testing process will see increased automation, integration with emerging technologies, and a focus on ensuring quality, security, and performance in the ever-evolving software landscape. Testing professionals will need to adapt to these changes and continuously upgrade their skills to stay relevant in the dynamic field of software testing

- **Stage 3 :- Future scope of SOC / SEIM**

  The future scope of SOC (Security Operations Center) and SIEM (Security Information and Event Management) is expected to expand and evolve in response to the changing cybersecurity landscape and technological advancements. The future scope of SOC and SIEM will involve increased automation, advanced threat detection, integration with emerging technologies, and a proactive approach to cybersecurity. Organizations will need to invest in the latest tools and technologies while continuously developing the expertise of their cybersecurity teams to stay ahead of evolving threats.

Topics explored :-

Introduction to cybersecurity, Growth of cybersecurity, Data sanity, Cloud service and cloud security, Data breach, Firewall, Malware, Digital ecosystem, Data protection, Types of cyber attacks, Testing and scanning tools, Introduction to networking, Web APIs, web hooks, Web shell concepts, Vulnerability stack, OWASP top 10 applications, QRadar, SOC, SIEM

Tools explored :-

Nessus, thehackersone.com, chaptgpt, wepik.com (AI image editor), Gamma (AI based PPT), OWASP top 10 vulnerabilities(2023), thehackersnews.com, CWE, exploitDB, virtual box, live websites- bugcrowd, nslookup.io, OSINT framework, Burpsuite, IBM fix central, QRadar Installation, Nmap, sqlmap, Identify fixes - wincollect agent, metasploitable, malware bytes, Linux cheatsheet, QRadar for SOC dashboard presentation, Kali linux.