Final Report

Smart Internz

Technology Stack: AI for Cybersecurity with IBM Qradar

Project Title: Malware Detection and Classification

Team ID: Team-593479

Team no.: 2.9

Team Members:

1. Ramar Priya Maha Lakshmi
2. Chevala Syam Sai
3. Panchada Varun
4. Mulumudi Prabhas

College: Vellore Institute of Technology, Amaravati

INDEX

INTRODUCTION

In the vast expanse of the digital world, the persistent threat of malware looms large, necessitating vigilant measures for identification and containment. Recognizing the pressing need for a proactive defense system, a pioneering project has emerged, introducing a dedicated online platform tailored for the detection and categorization of malicious software.

This innovative website offers a user-friendly interface where individuals can upload potentially suspicious files for a thorough examination. What sets this initiative apart is the integration of a state-of-the-art AI model specifically engineered for the intricate task of classifying diverse forms of malware. The AI engine serves as an intelligent guardian, employing advanced algorithms and machine learning techniques to dissect and interpret the behaviors and structures of uploaded files. Through the seamless amalgamation of technology and cybersecurity, this platform generates detailed reports, furnishing users with comprehensive insights into the nature of the submitted files, their potential risks, and identifying markers.

Powered by an advanced AI model, this project stands at the frontier of cybersecurity, providing a robust solution for the identification and comprehension of malicious entities.

The website's goal is to equip users with a thorough understanding of potential security threats lurking within their files, empowering them to take prompt and informed actions. By leveraging the prowess of artificial intelligence, this initiative aligns with the ongoing endeavor to combat cyber threats effectively.

Its unique approach signifies a leap forward in the realm of digital defense, harnessing cutting-edge technology to proactively safeguard users against an ever-evolving landscape of cyber vulnerabilities. Through the integration of an intelligent analysis system, this project doesn't just detect malware but significantly contributes to understanding and tackling the evolving face of digital threats.

ABSTRACT

The project "**Malware Detection and Classification**" addresses the pressing need for enhanced cybersecurity in our increasingly digital world. Leveraging state-of-the-art technologies and data-driven approaches, this project aims to identify, classify, and combat malware threats effectively.

In this project, we're embarking on a mission to fortify the digital world you interact with daily. Think of it as your computer's guardian, working tirelessly behind the scenes to keep it safe from unseen threats.

Our project involves creating a virtual detective with a keen sense of smell for digital danger. It examines files and programs to determine if they're friendly or up to no good. Our digital detective is like a bloodhound, always sniffing for clues to figure out if a file is safe or secretly plotting trouble. It looks at things like the file's size, where it came from, and what it's trying to do. If it smells something fishy, it alerts you.

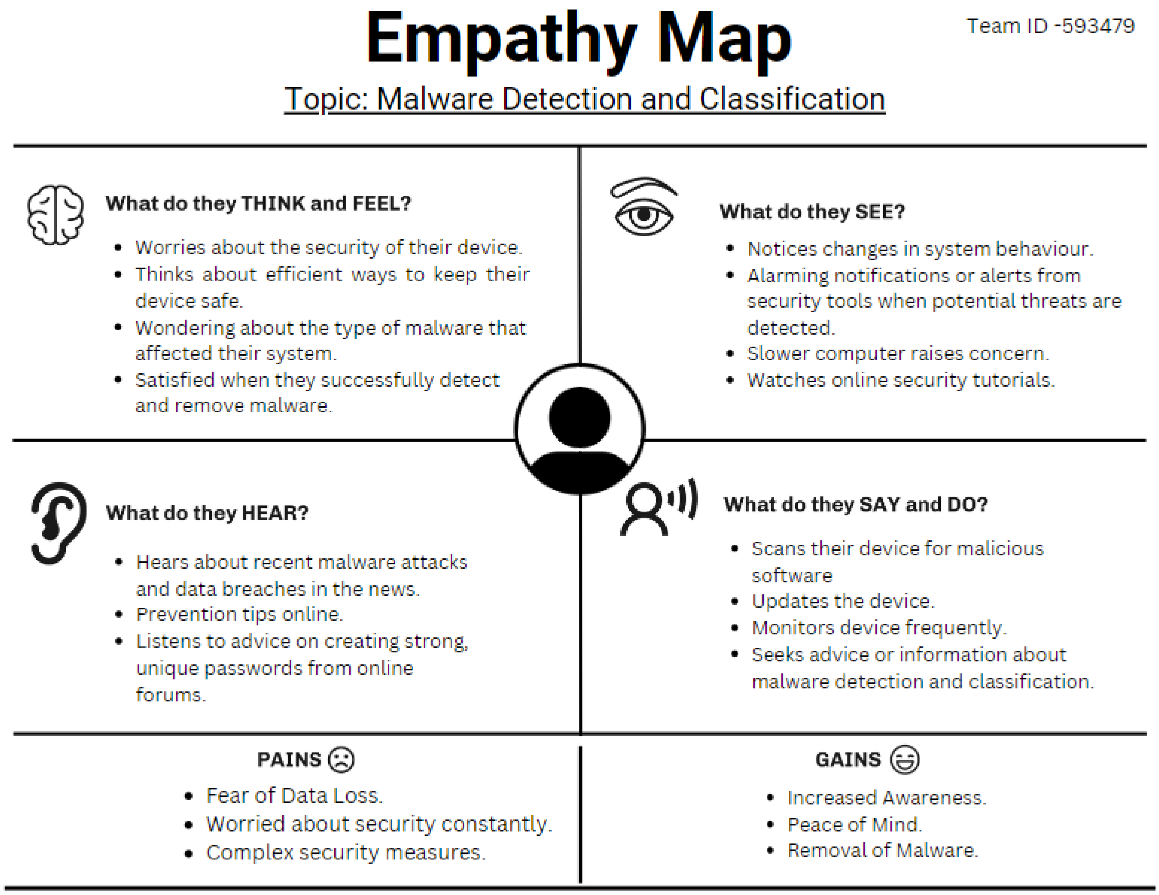
Through machine learning algorithms and pattern recognition, our system distinguishes malicious software from benign applications, thus safeguarding users and organizations from potential harm. For instance, it can detect and classify notorious malware strains like ransomware, trojans, and spyware, enhancing our collective resilience against evolving cyber threats. This project envisions a safer digital landscape, where the proactive detection and classification of malware contribute to a more secure and confident online experience for all stakeholders.

Vision Statement for Malware Detection and Classification: At the forefront of cybersecurity innovation, our vision is to create a resilient digital ecosystem where advanced and evolving malware threats are promptly detected, meticulously classified, and effectively neutralized. We envision a world where organizations, individuals, and communities can navigate the digital landscape with confidence, knowing that their systems and data are shielded from the ever-evolving malware landscape. Our commitment lies in leveraging cutting-edge technologies, continuous research, and global collaboration to pioneer solutions that not only

identify and classify malware but also anticipate and proactively defend against emerging threats. With this vision, we strive to build a safer, more secure digital future for all.

EMPATHY MAP CANVAS

The empathy map for **"Malware Detection and Classification"** illuminates the multifaceted user perspective in the realm of cybersecurity. Users often find themselves navigating a landscape filled with concerns and complexities. Users hear advice from peers and experts, seeking insights on protection. They engage in discussions about security and encounter visual cues from security software. This collective experience guides the development of user-centric solutions.



Empathy Map

Team ID -593479

Topic: Malware Detection and Classification

What do they THINK and FEEL?

- Worries about the security of their device.
- Thinks about efficient ways to keep their device safe.
- Wondering about the type of malware that affected their system.
- Satisfied when they successfully detect and remove malware.

What do they SEE?

- Notices changes in system behaviour.
- Alarming notifications or alerts from security tools when potential threats are detected.
- Slower computer raises concern.
- Watches online security tutorials.

What do they HEAR?

- Hears about recent malware attacks and data breaches in the news.
- Prevention tips online.
- Listens to advice on creating strong, unique passwords from online forums.

What do they SAY and DO?

- Scans their device for malicious software
- Updates the device.
- Monitors device frequently.
- Seeks advice or information about malware detection and classification.

PAINS ☹

- Fear of Data Loss.
- Worried about security constantly.
- Complex security measures.

GAINS 😄

- Increased Awareness.
- Peace of Mind.
- Removal of Malware.

They fear data loss, grapple with device security, and struggle with the intricacies of security measures. Uncertainty about the ever-evolving malware landscape adds an extra layer of stress. However, there are gains in the journey as well. Effective malware detection provides peace of mind, quick and accurate alerts empower proactive responses, and streamlined security measures simplify the process. Users also benefit from increased awareness, which enhances their knowledge of emerging threats and best practices. These pains and gains guide the design of user-centric cybersecurity solutions, aiming to alleviate concerns and empower users with confidence in their digital interactions.

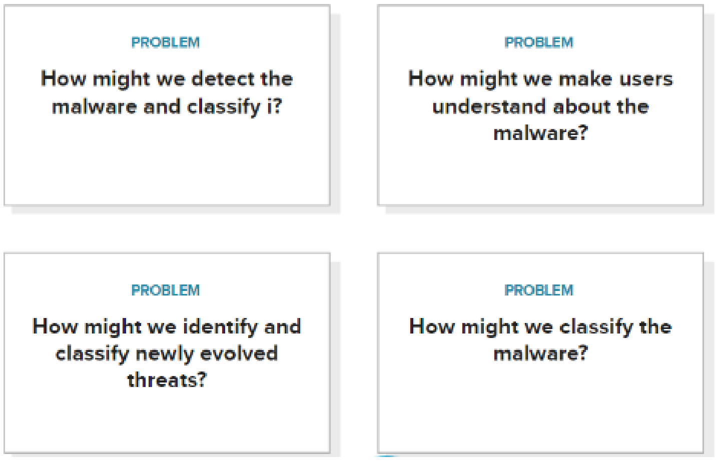
BRAINSTORMING AND IDEA PRIORITIZATION

Brainstorming for the topic of malware detection and classification is a dynamic exploration into the evolving world of cybersecurity threats. With the persistent growth in malware sophistication, our endeavour is to devise innovative strategies and technologies for recognizing and categorizing these threats. Our focus on robust detection methods and effective classification models seeks to enhance digital security for both individuals and organizations. By forging collaborative partnerships, staying abreast of industry standards, and adhering to ethical considerations, we aim to contribute to the collective arsenal against the ever-adaptive landscape of malicious software.

Step-1: Team Gathering, Collaboration and Select the Problem Statement

In this brainstorming phase, we have identified the possible problems that might be difficult to tackle.

We have ended up with the following problem statements



PROBLEM

How might we detect the malware and classify i?

PROBLEM

How might we make users understand about the malware?

PROBLEM

How might we identify and classify newly evolved threats?

PROBLEM

How might we classify the malware?

1.How might we detect the malware?

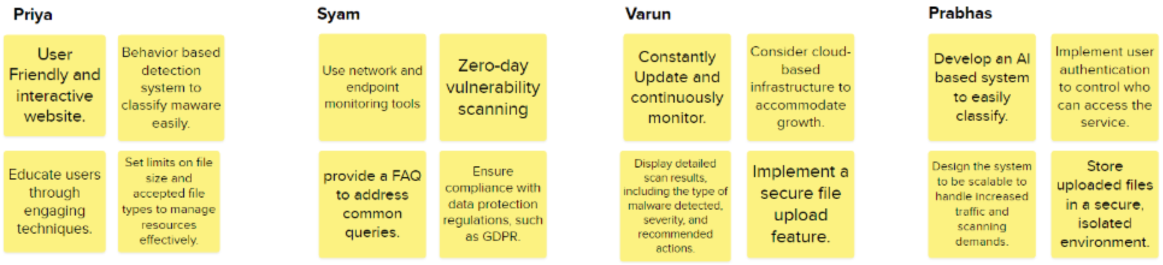
2.How might we make users understand about the malware?

3.How might we identify and classify newly evolved threats?

4.How might we classify the malware?

Step-2: Brainstorm, Idea Listing and Grouping

In this phase of brainstorming, each of us came up with best possible solutions to the above-mentioned problem statements. Listing these solutions will help us breakdown the problem statement and understand them in a better way.



Priya

User Friendly and interactive website.

Behavior based detection system to classify maware easily.

Educate users through engaging techniques.

Set limits on file size and accepted file types to manage resources effectively.

Syam

Use network and endpoint monitoring tools

Zero-day vulnerability scanning

provide a FAQ to address common queries.

Ensure compliance with data protection regulations, such as GDPR.

Varun

Constantly Update and continuously monitor.

Consider cloud-based infrastructure to accommodate growth.

Display detailed scan results, including the type of malware detected, severity, and recommended actions.

Implement a secure file upload feature.

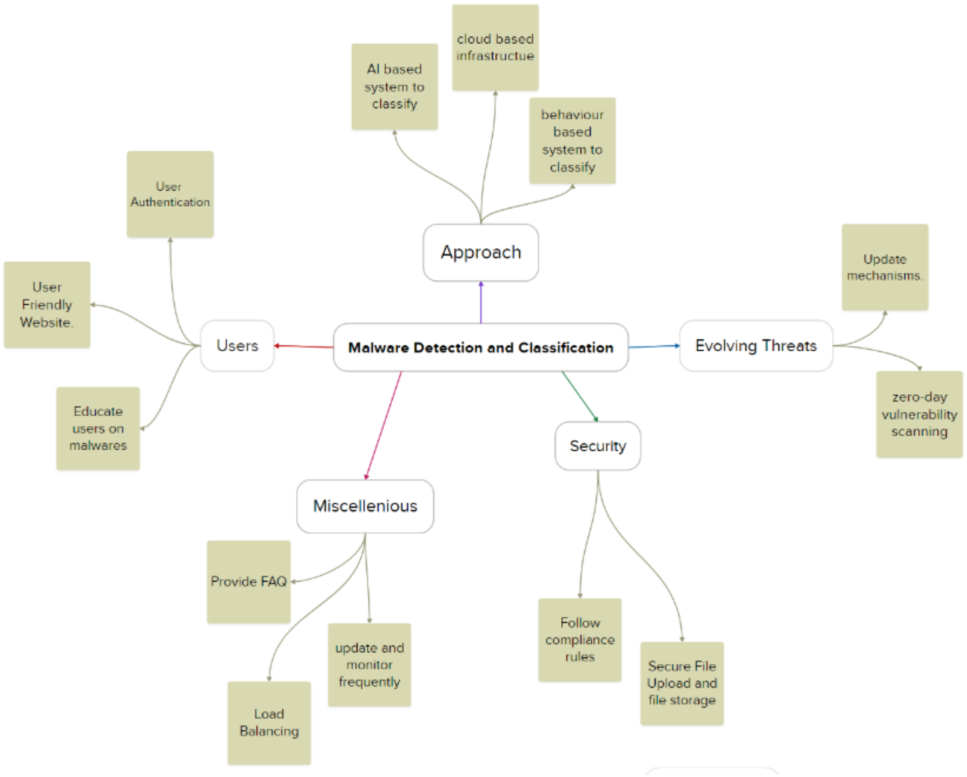
Prabhas

Develop an AI based system to easily classify.

Implement user authentication to control who can access the service.

Design the system to be scalable to handle increased traffic and scanning demands.

Store uploaded files in a secure, isolated environment.

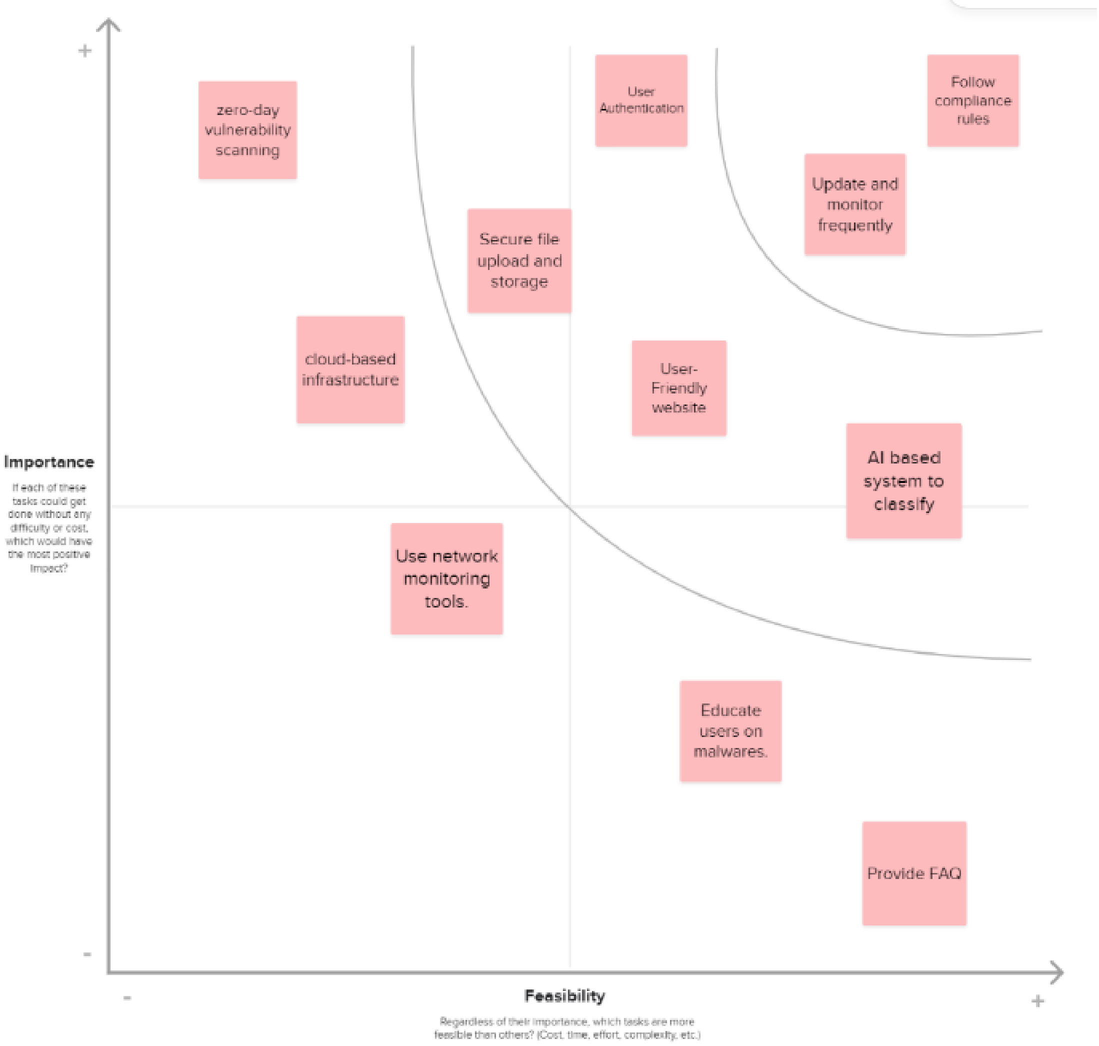

cloud based infrastructue
AI based system to classify
behaviour based system to classify
Approach
User Authentication
User Friendly Website.
Users
Malware Detection and Classification
Evolving Threats
Update mechanisms.
zero-day vulnerability scanning
Educate users on malwares
Security
Miscellenious
Provide FAQ
update and monitor frequently
Load Balancing
Follow compliance rules
Secure File Upload and file storage

A mind map helped us categorize the things that we need to work on and how to approach the problem statement in a better way.

Through this mind map our ideas got clear and paved a way to categorize related solutions.

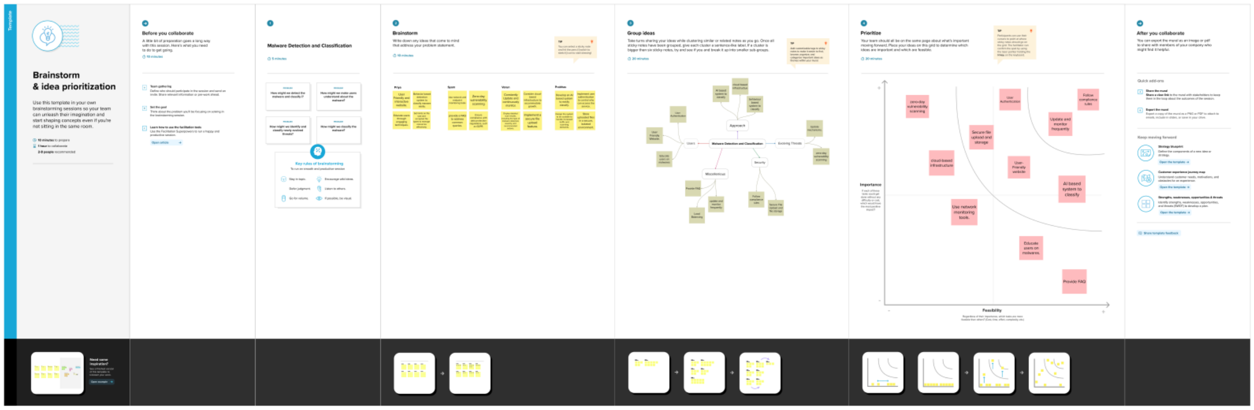
Step-3: Idea Prioritization

Prioritizing the attained solutions will help us work on the solutions according to their importance and feasibility. This helps us attain the goal and meet the importance of the solution at the same time.



If each of these tasks could get done without any difficulty or cost, which would have the most positive impact?

Regardless of their importance, which tasks are more feasible than others? (Cost, time, effort, complexity, etc.)



STAGE-1

Title of the Project:- Malware Detection and Classification

Overview:

In the contemporary digital landscape, the ever-present threat of malware necessitates a robust and dynamic defense mechanism. Recognizing this urgent need, an innovative project has emerged, aiming to create an online platform dedicated to the identification, analysis, and classification of potentially harmful software. This cutting-edge website offers a seamless and intuitive interface where users can effortlessly upload suspicious files for a comprehensive evaluation. What sets this initiative apart is the incorporation of an advanced AI model meticulously designed to classify a diverse spectrum of malicious software. This artificial intelligence acts as an astute sentinel, utilizing complex algorithms and machine learning to dissect and interpret the behavior, structure, and potential risks associated with the uploaded files.

At its core, this project serves not only as a detection tool but also as an educational resource, empowering users with valuable insights into the realm of cyber threats. The AI-driven analysis generates detailed reports that offer users a deeper understanding of the nature and potential risks associated with their submitted files. Through this enriched comprehension, users are equipped to make informed decisions and take proactive measures against cybersecurity vulnerabilities. The platform doesn't merely stop at identifying malware; rather, it stands as an ally in enhancing users' awareness and comprehension of the evolving nature of digital threats. This deeper insight into cyber threats and their characteristics contributes significantly to the ongoing endeavor to fortify digital security. The fusion of advanced technology and cybersecurity not only detects and categorizes malware but also educates and empowers users to navigate the complex landscape of cybersecurity with confidence.

By embracing this amalgamation of sophisticated technology and user-centric education, this project pioneers a new approach to fortifying digital defenses against an ever-evolving array of cyber vulnerabilities.

Sno	Vulnerability Name	CWE
1	PHP Unsupported Version	CWE-661
2	Missing Anti-clickjacking tokens	CWE-451
3	Disclosing Webserver Type	CWE-200
4	Cleartext Transmission of Credentials	CWE-319
5	Web Server Directory Enumeration	CWE-548

List of Teammates:

Sno	Name	College	Contact
1	Ramar Priya Maha Lakshmi	VIT-AP	priya.21bce7521@vitapstudent.ac.in
2	Chevala Syam Sai	VIT-AP	syam.21bce9088@vitapstudent.ac.in
3	Panchada Varun	VIT-AP	varun.21bec7262@vitapstudent.ac.in
4	Mulumudi Prabhas	VIT-AP	prabhas.21bce7249@vitapstudent.ac.in

List of Vulnerability Table:

REPORT

Vulnerability Name: PHP Unsupported Version

CWE: CWE-661

OWASP Category: A06:2021-Vulnerable and Outdated Components

Description: According to its version, the installation of PHP on the remote host is no longer supported. As a result, it is likely to contain security vulnerabilities.

Business Impact: Anyone can connect to the NSClient and retrieve sensitive information, such as process and service states, memory usage, etc.

Vulnerability Name: Missing anti-clicking tokens

CWE: CWE-451

OWASP Category: A04:2021 Insecure Design

Description: The user interface (UI) does not properly represent critical information to the user, allowing the information - or its source - to be obscured or spoofed. This is often a component in phishing attacks.

Business Impact: The Impact of Clickjacking The hacker has several ways they can use the redirected clicks for their own gain. A common form of clickjacking involves mirroring a login and password form on a website.

Vulnerability Name: Disclosing Web Server Type

CWE: CWE-200

OWASP Category: A03:2017 Sensitive Data Exposure

Business Impact: Disclosing the web server type can pose a security risk by providing potential attackers with information that may be exploited. This disclosure can lead to more targeted attacks and increases the risk of vulnerabilities being exploited, potentially resulting in data breaches, service disruptions, and reputational damage. It's essential to minimize such disclosures to enhance the security of web applications.

Vulnerability: Cleartext Transmission of Credentials

CWE: CWE-319

OWASP Category: A05:2021 Security Misconfiguration

Description: The product transmits sensitive or security-critical data in cleartext in a communication channel that can be sniffed by unauthorized actors.

Business Impact: Transmitting credentials in cleartext can result in unauthorized access, data breaches, loss of customer trust, legal and regulatory consequences, and reputation damage, impacting an organization's security and financial standing.

Vulnerability: Web Server Directory Enumeration

CWE: CWE-548

OWASP Category: A04: Insecure Design

Severity: low

Description: A directory listing is inappropriately exposed, yielding potentially sensitive information to attackers.

Business Impact: Webserver directory enumeration, often through techniques like directory listing, can have significant business impacts. By revealing the structure of a web server's directories and files, it provides potential attackers with insights into the system's architecture and potential vulnerabilities. This can lead to unauthorized access, data exposure, and even service disruptions. The business consequences include reputational damage, legal liabilities, financial losses, and the potential compromise of sensitive information. Mitigating directory enumeration is crucial to maintaining a secure online presence.

--

This is stage 1 where we understand web application testing. We take help from OWASP top 10 understand them.

--

REPORT ON PRACTICE WEBSITE

i. **Vulnerability:** SQL injection

CWE: CWE-89

OWASP Category: A03 2021-Injection

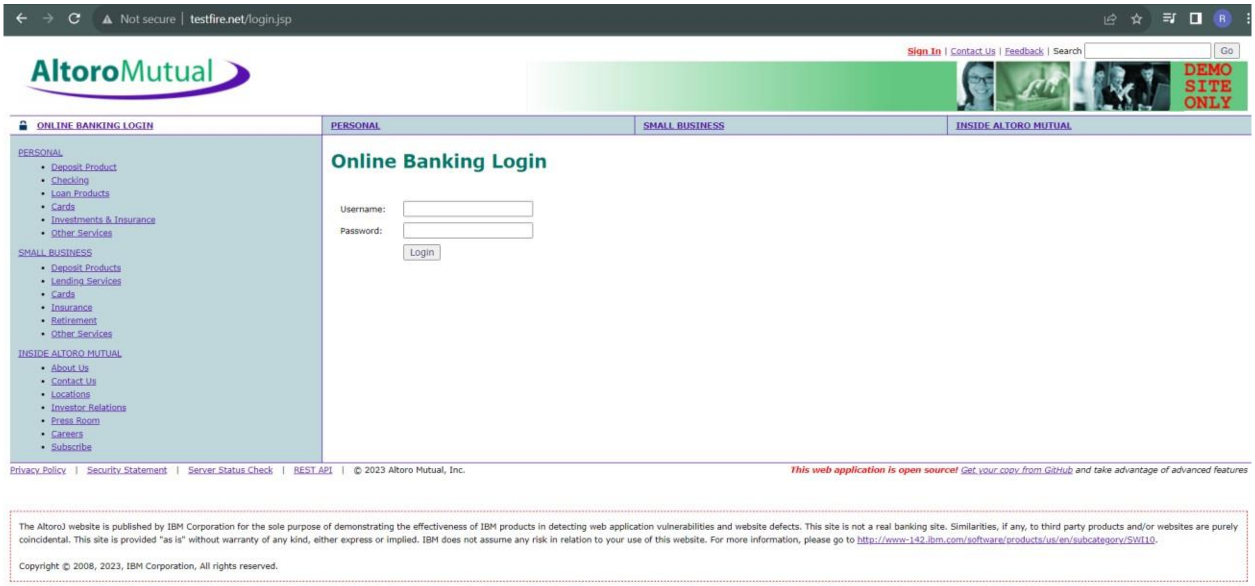
Description: The product constructs all or part of an SQL command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended SQL command when it is sent to a downstream component.

Business Impact: SQL injection can have severe consequences, including data breaches, financial losses, damaged reputation, and legal repercussions for businesses. Attackers exploit vulnerabilities to gain unauthorized access to databases, steal sensitive information, and disrupt operations. The fallout often includes financial liabilities, regulatory fines, loss of customer trust, and the cost of remediation efforts to fix the vulnerabilities and recover from the breach.

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

Steps to Reproduce:

1. Access the URL.



Online Banking Login

Username:

Password:

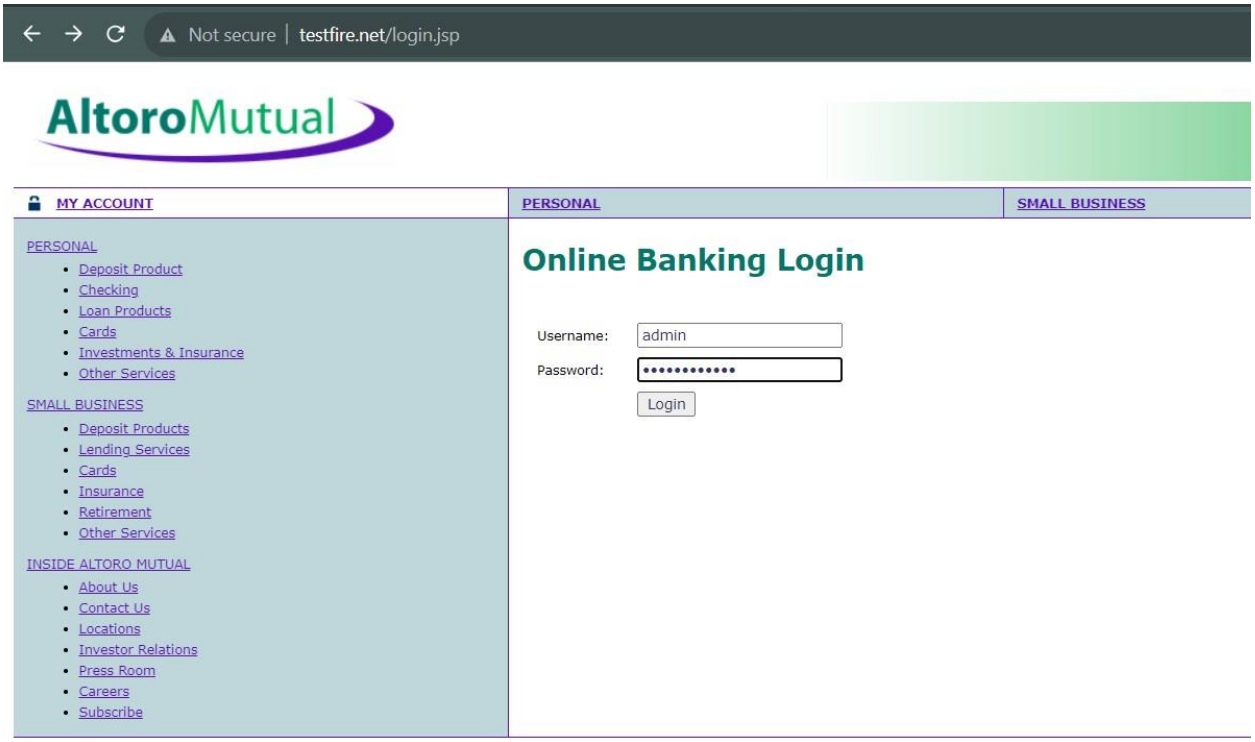
Privacy Policy | Security Statement | Server Status Check | REST API | © 2023 Altoro Mutual, Inc.

This web application is open source! Get your copy from GitHub and take advantage of advanced features

The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to http://www-142.ibm.com/software/products/us/en/subcategory/SWI10.

Copyright © 2008, 2023, IBM Corporation, All rights reserved.

2. Enter the Username with “admin” and Password with “ ‘or 1=1--+”.



Online Banking Login

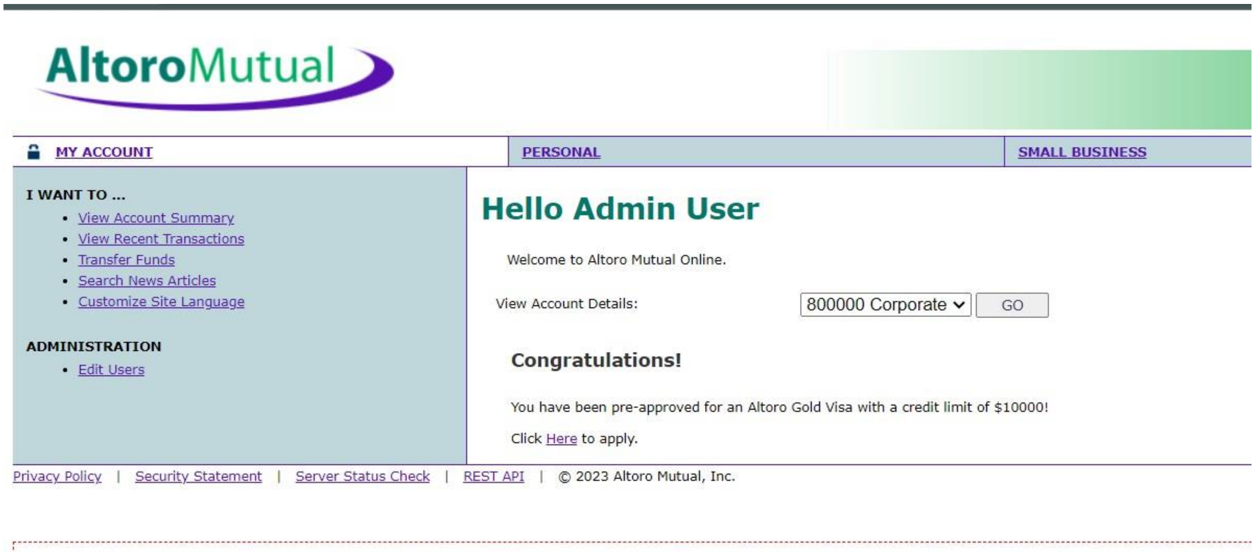
Username: admin

Password: ••••••••••••

In the above screenshot, when the user enters unanticipated input (i.e. payload) as **‘ or 1=1 --+** , the dynamically generated SQL query will be generated as below:

- Select * from Users where username= **admin** and password = **‘ or 1=1--+.**

i. Admin credentials are acquired.



Hello Admin User

Welcome to Altoro Mutual Online.

View Account Details: 800000 Corporate

Congratulations!

You have been pre-approved for an Altoro Gold Visa with a credit limit of $10000!

Click Here to apply.

Recommendation:

- Use Prepared Statements and Parameterized Queries.
- Input Validation and Whitelisting.

b. Vulnerability: Cross Site Scripting (XSS)

CWE: CWE-87

OWASP Category: A03 2021-Injection

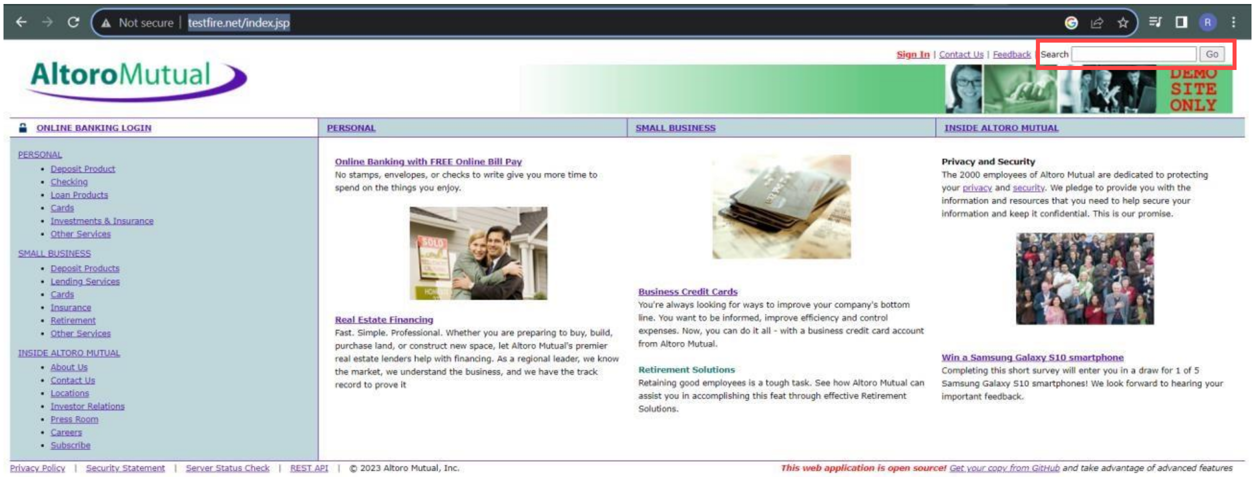
Description: The product does not neutralize or incorrectly neutralizes usercontrolled input for alternate script syntax.

Business Impact: Attackers can use XSS to execute malicious scripts on the users in this case victim browsers. Since the browser cannot know if the script is trusty or not, the script will be executed, and the attacker can hijack session cookies, deface websites, or redirect the user to an unwanted and malicious website.

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

Steps to Reproduce:

i. Go to the search bar of the given URL.



Online Banking with FREE Online Bill Pay
No stamps, envelopes, or checks to write give you more time to spend on the things you enjoy.

Real Estate Financing
Fast. Simple. Professional. Whether you are preparing to buy, build, purchase land, or construct new space, let Altoro Mutual's premier real estate lenders help with financing. As a regional leader, we know the market, we understand the business, and we have the track record to prove it

Business Credit Cards
You're always looking for ways to improve your company's bottom line. You want to be informed, improve efficiency and control expenses. Now, you can do it all - with a business credit card account from Altoro Mutual.

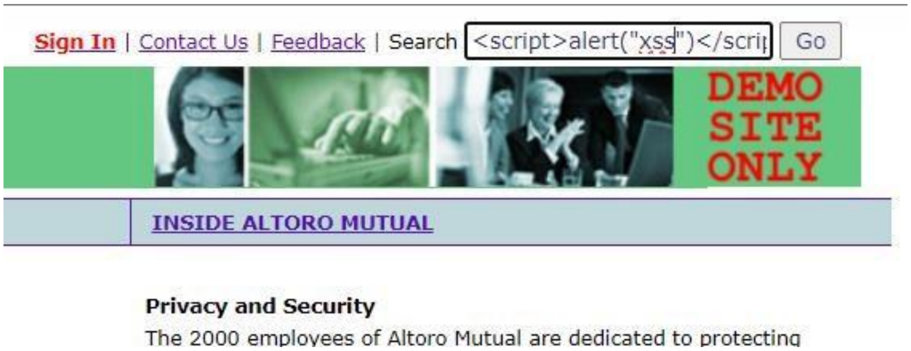
Retirement Solutions
Retaining good employees is a tough task. See how Altoro Mutual can assist you in accomplishing this feat through effective Retirement Solutions.

Privacy and Security
The 2000 employees of Altoro Mutual are dedicated to protecting your privacy and security. We pledge to provide you with the information and resources that you need to help secure your information and keep it confidential. This is our promise.

Win a Samsung Galaxy S10 smartphone
Completing this short survey will enter you in a draw for 1 of 5 Samsung Galaxy S10 smartphones! We look forward to hearing your important feedback.

This web application is open source! Get your copy from GitHub and take advantage of advanced features

2. Execute any javascript code.

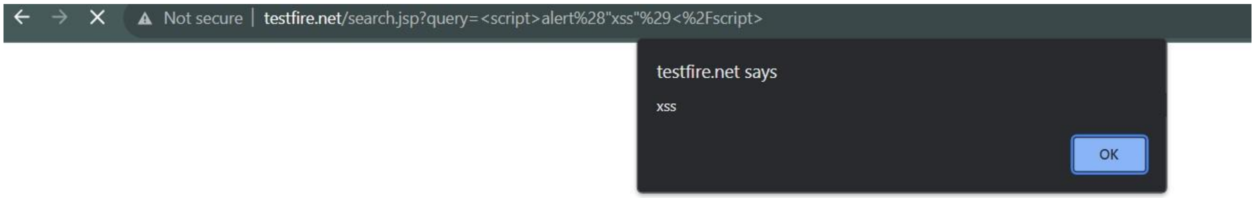


<script>alert("xss")</scri

Privacy and Security

The 2000 employees of Altoro Mutual are dedicated to protecting

i. Click on Go.



testfire.net/search.jsp?query=<script>alert%28"xss"%29<%2Fscript>

testfire.net says

xss

The entered code has been executed in the website.

Recommendations:

- Whitelisting input fields.
- Input Output encoding.

c. Vulnerability: Insecure Direct Object Reference (IDOR)

CWE: CWE-639

OWASP Category: A01 Broken Access Control

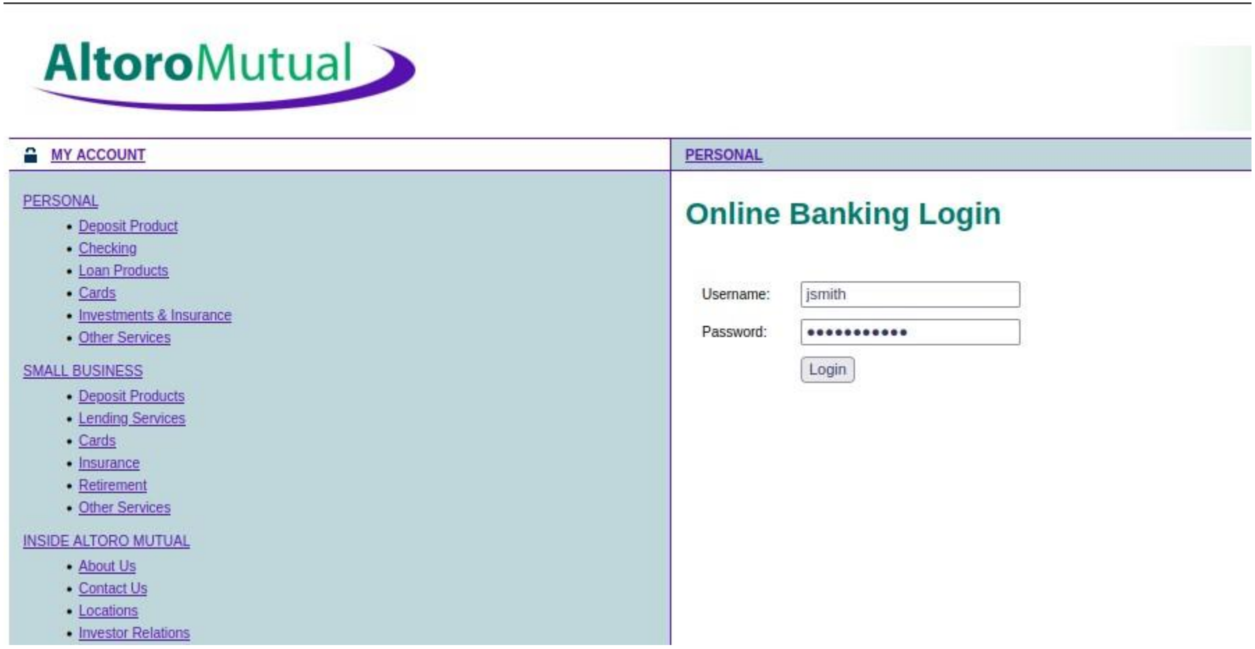
Description: The system’s authorization functionality does not prevent one user from gaining access to another user’s data or record by modifying the key value identifying the data.

Business Impact: IDOR can lead to unauthorized access to sensitive data or resources, potentially resulting in data breaches, privacy violations, financial losses, and damage to an organization’s reputation. It can also lead to legal and regulatory consequences, impacting the overall trust and confidence in the business.

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

Steps to Reproduce:

1. Navigate into the given URL and login using john smith credentials.

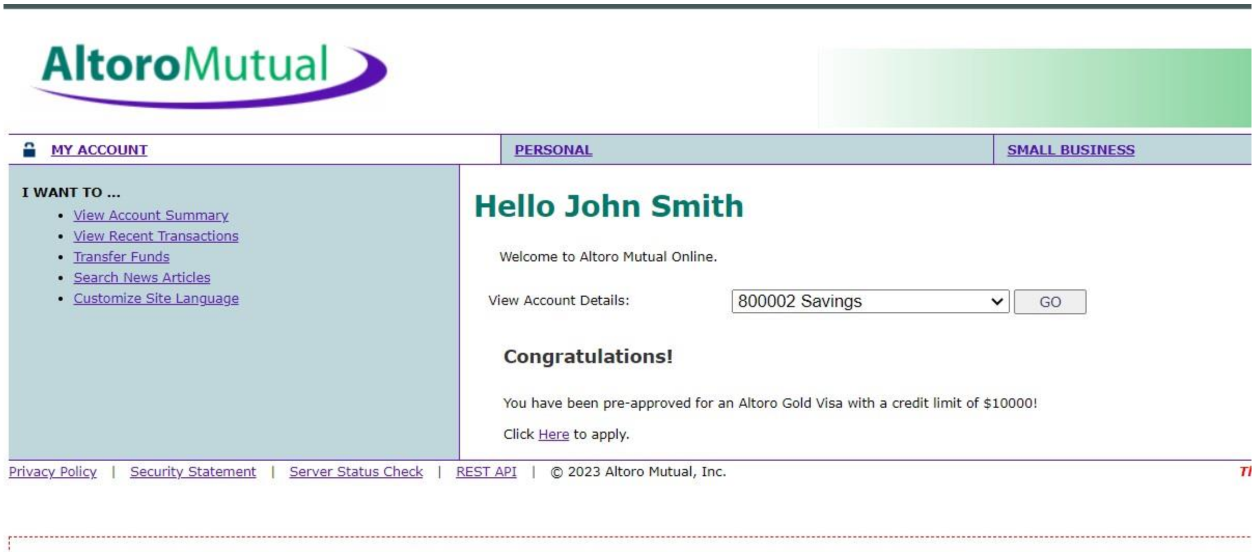


Online Banking Login

Username: jsmith

Password: ●●●●●●●●●●●

2. Click on “Go” to view John Smith’s savings.



Hello John Smith

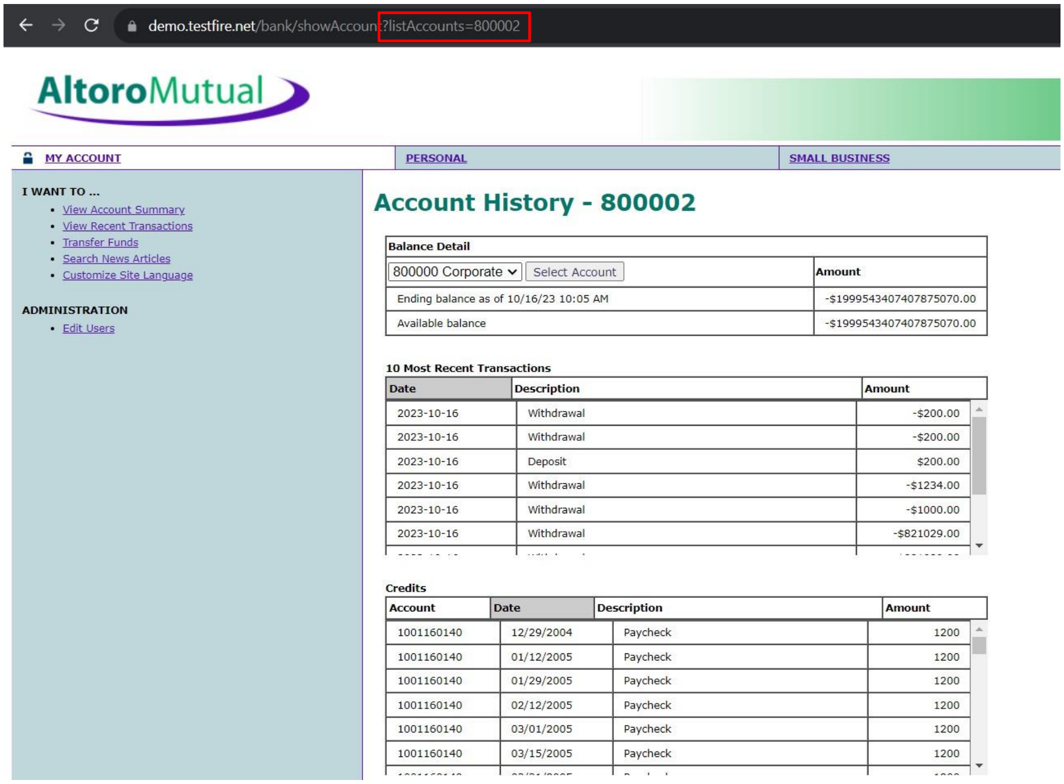
Welcome to Altoro Mutual Online.

View Account Details: 800002 Savings

Congratulations!

You have been pre-approved for an Altoro Gold Visa with a credit limit of $10000!

Click Here to apply.



Account History - 800002

Balance Detail	
800000 Corporate	Amount
Ending balance as of 10/16/23 10:05 AM	-$1999543407407875070.00
Available balance	-$1999543407407875070.00

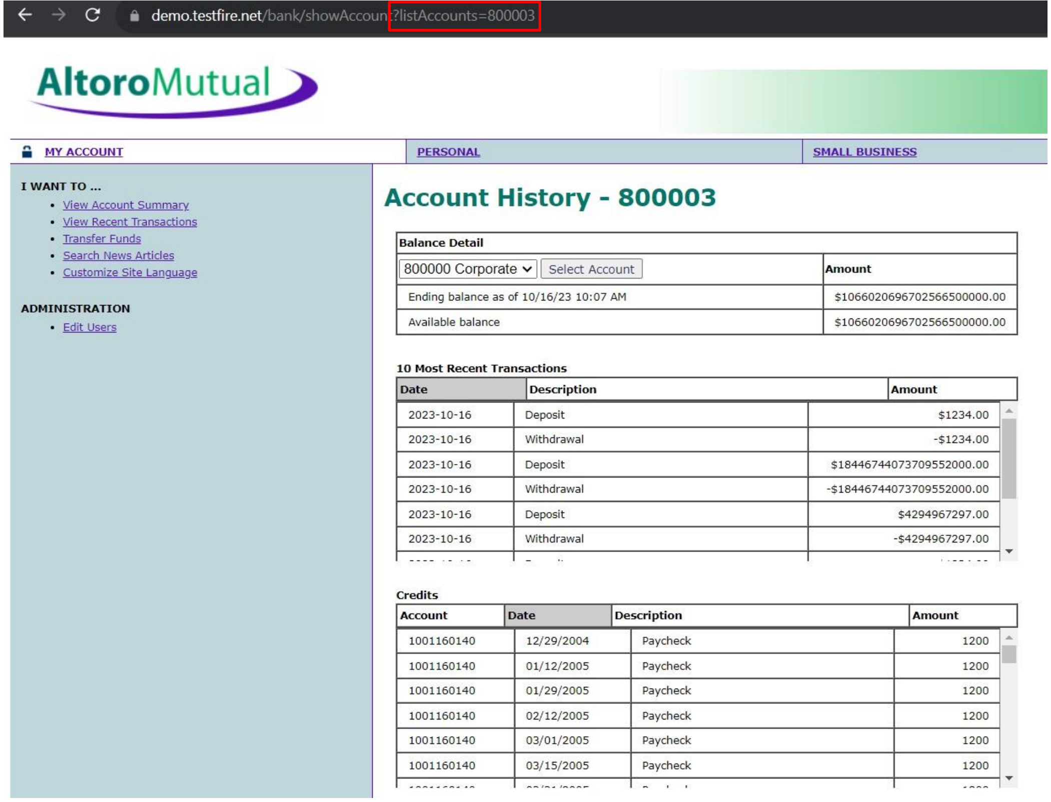
10 Most Recent Transactions

Date	Description	Amount
2023-10-16	Withdrawal	-$200.00
2023-10-16	Withdrawal	-$200.00
2023-10-16	Deposit	$200.00
2023-10-16	Withdrawal	-$1234.00
2023-10-16	Withdrawal	-$1000.00
2023-10-16	Withdrawal	-$821029.00

Credits

Account	Date	Description	Amount
1001160140	12/29/2004	Paycheck	1200
1001160140	01/12/2005	Paycheck	1200
1001160140	01/29/2005	Paycheck	1200
1001160140	02/12/2005	Paycheck	1200
1001160140	03/01/2005	Paycheck	1200
1001160140	03/15/2005	Paycheck	1200

3. Change the listAccount=800002 to 800003 to view account history of other customers.



Account History - 800003

Balance Detail	
800000 Corporate	Amount
Ending balance as of 10/16/23 10:07 AM	$10660206967025665000000.00
Available balance	$10660206967025665000000.00

10 Most Recent Transactions

Date	Description	Amount
2023-10-16	Deposit	$1234.00
2023-10-16	Withdrawal	-$1234.00
2023-10-16	Deposit	$18446744073709552000.00
2023-10-16	Withdrawal	-$18446744073709552000.00
2023-10-16	Deposit	$4294967297.00
2023-10-16	Withdrawal	-$4294967297.00

Credits

Account	Date	Description	Amount
1001160140	12/29/2004	Paycheck	1200
1001160140	01/12/2005	Paycheck	1200
1001160140	01/29/2005	Paycheck	1200
1001160140	02/12/2005	Paycheck	1200
1001160140	03/01/2005	Paycheck	1200
1001160140	03/15/2005	Paycheck	1200

Recommendations:

- Implement Proper Access Controls.
- Employ Session Management and Authentication.

d. Vulnerability: Personal Identifiable Information (PII)

CWE: CWE-319

OWASP Category: A02:2021 Cryptographic Failures

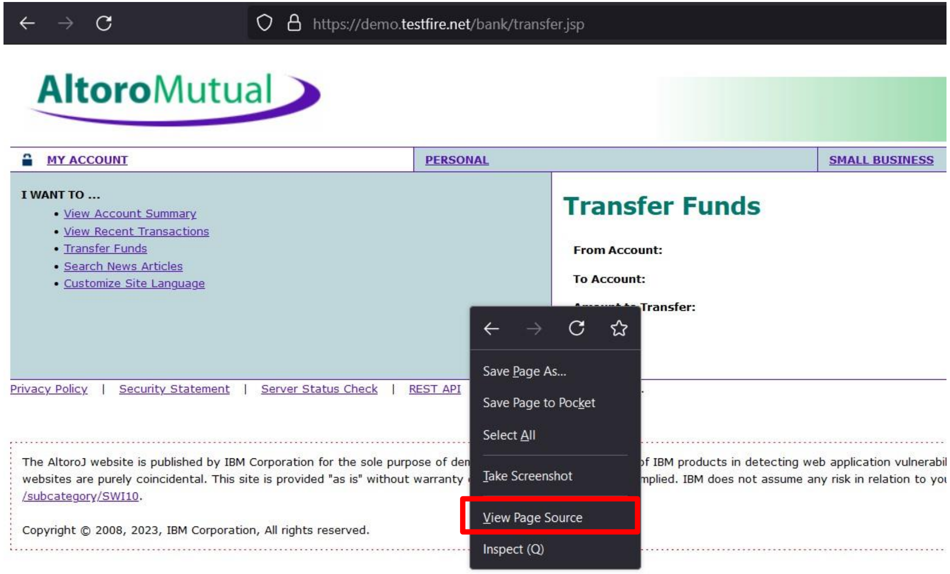
Description: The product transmits sensitive or security-critical data in cleartext in a communication channel that can be sniffed by unauthorized actors.

Business Impact: Exposure of Personal Identifiable Information (PII) can lead to legal fines, reputation damage, financial losses, operational disruption, customer churn, cybersecurity costs, competitive disadvantage, and long-term legal liability, underscoring the importance of robust data protection.

Vulnerability Path: https://testfire.net/bank/transfer.jsp

Steps to Reproduce:

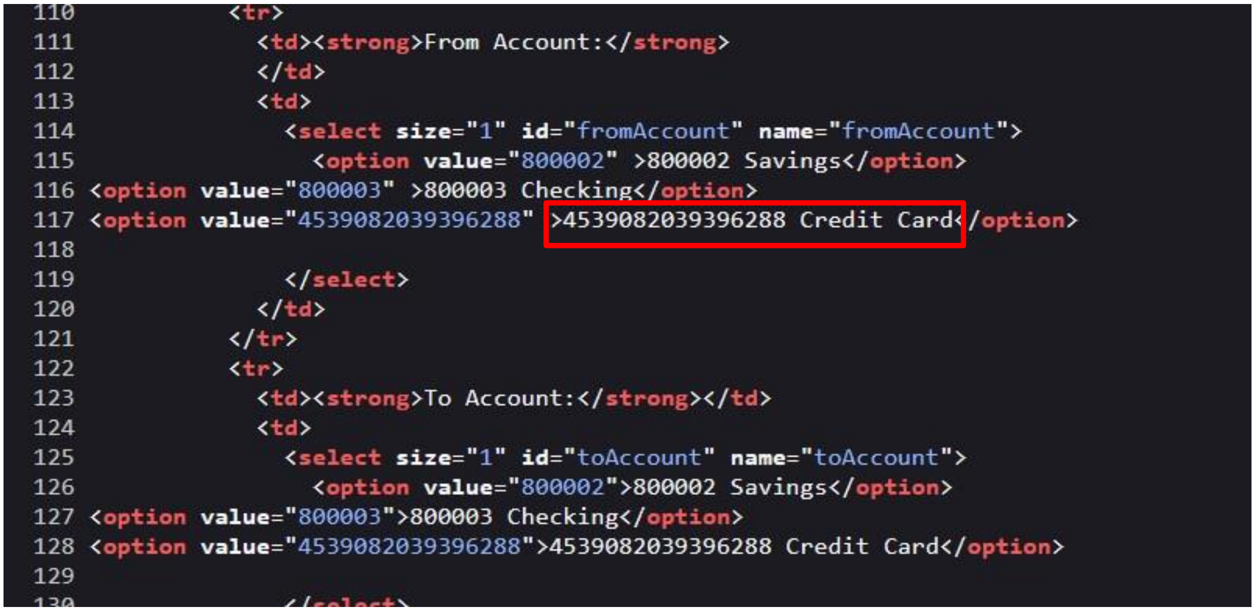
1. Navigate to the given URL. Then, view page source.



The AltoroJ website is published by IBM Corporation for the sole purpose of den… of IBM products in detecting web application vulnerabil… websites are purely coincidental. This site is provided "as is" without warranty … mplied. IBM does not assume any risk in relation to you… /subcategory/SWI10.

Copyright © 2008, 2023, IBM Corporation, All rights reserved.

2. Scroll down. Credit card details are shown explicitly.



```
            <tr>
              <td><strong>From Account:</strong>
              </td>
              <td>
                <select size="1" id="fromAccount" name="fromAccount">
                  <option value="800002" >800002 Savings</option>
<option value="800003" >800003 Checking</option>
<option value="4539082039396288" >4539082039396288 Credit Card</option>

                </select>
              </td>
            </tr>
            <tr>
              <td><strong>To Account:</strong></td>
              <td>
                <select size="1" id="toAccount" name="toAccount">
                  <option value="800002">800002 Savings</option>
<option value="800003">800003 Checking</option>
<option value="4539082039396288">4539082039396288 Credit Card</option>

                </select>
```

Recommendations:

- Data Encryption.
- Data Minimization.
- Limit access to authorized people.

e. Vulnerability: Information Disclosure

CWE: CWE-200

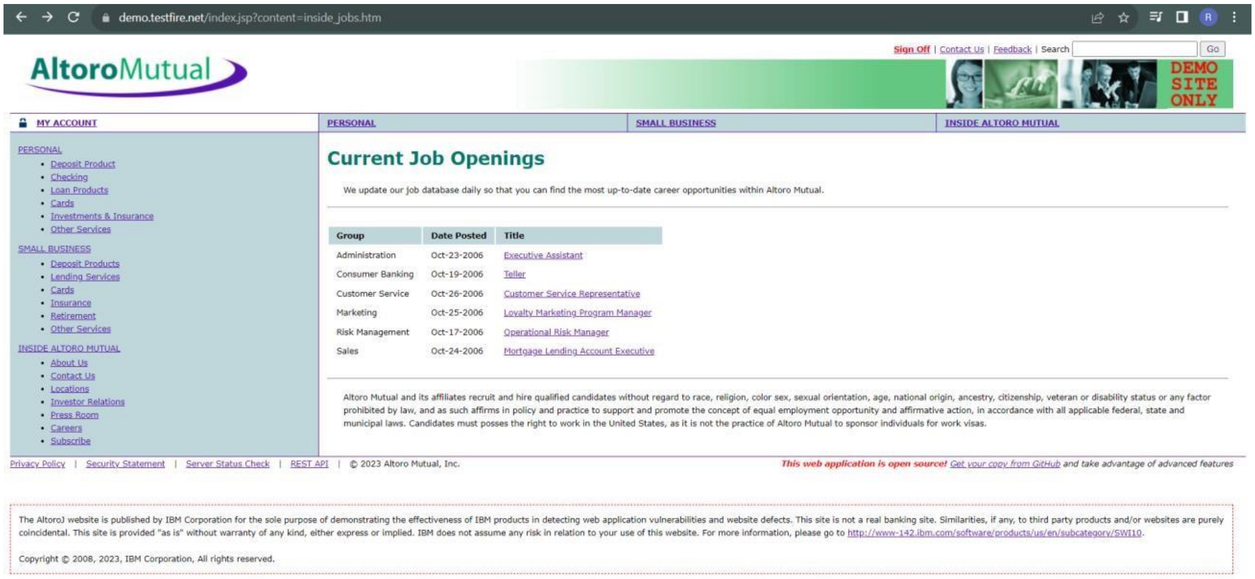
OWASP Category: A03:2017 Sensitive Data Exposure.

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

Business Impact: Information disclosure jeopardizes privacy, competitive standing, and trust, potentially resulting in legal actions, financial losses, and reputational harm, undermining an organization’s security, prosperity, and image.

Vulnerability Path: https://demo.testfire.net/index.jsp?content=inside_jobs.htm **Steps to Reproduce:**

i. Navigate to the given URL.



Current Job Openings

We update our job database daily so that you can find the most up-to-date career opportunities within Altoro Mutual.

Group	Date Posted	Title
Administration	Oct-23-2006	Executive Assistant
Consumer Banking	Oct-19-2006	Teller
Customer Service	Oct-26-2006	Customer Service Representative
Marketing	Oct-25-2006	Loyalty Marketing Program Manager
Risk Management	Oct-17-2006	Operational Risk Manager
Sales	Oct-24-2006	Mortgage Lending Account Executive

Altoro Mutual and its affiliates recruit and hire qualified candidates without regard to race, religion, color sex, sexual orientation, age, national origin, ancestry, citizenship, veteran or disability status or any factor prohibited by law, and as such affirms in policy and practice to support and promote the concept of equal employment opportunity and affirmative action, in accordance with all applicable federal, state and municipal laws. Candidates must posses the right to work in the United States, as it is not the practice of Altoro Mutual to sponsor individuals for work visas.

This web application is open source! Get your copy from GitHub and take advantage of advanced features

The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to http://www-142.ibm.com/software/products/us/en/subcategory/SWI10.

Copyright © 2008, 2023, IBM Corporation, All rights reserved.

The details of the company are clearly visible.

Recommendations:

- The information must not be in clear text.
- Classify the data into “sensitive” and “non-sensitive”.

f. Vulnerability: Outdated Server

CWE: CWE-1352

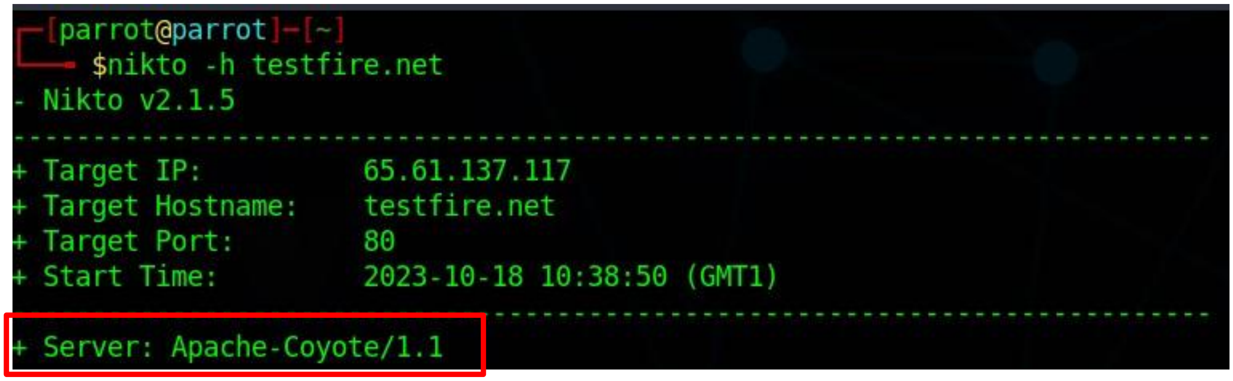
OWASP Category: A06:2021 Vulnerable and Outdated Components

Description: The product relies on third-party components that are not actively supported or maintained by the original developer or a trusted proxy for the original developer.

Business Impact: Using outdated or vulnerable components may result in non-compliance with data protection and security regulations, leading to fines and legal penalties. Security incidents and breaches can disrupt day-today operations, leading to downtime, increased support costs, and decreased productivity. Exploitable vulnerabilities in components can lead to data breaches, potentially resulting in loss of sensitive information, legal consequences, and damage

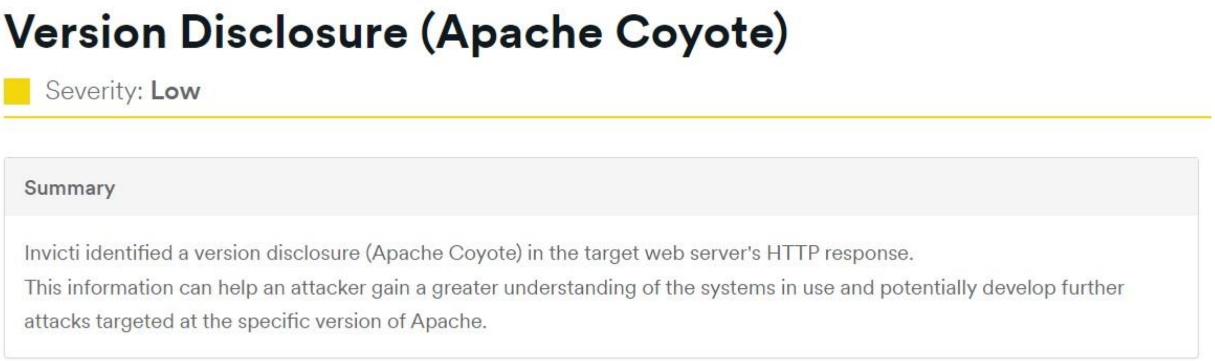
Vulnerability Path: https://testfire.net/bank/transfer.jsp **Steps to Reproduce:**

i. Tool Used: **Nikto.** Type the following Command.



```
┌─[parrot@parrot]─[~]
└──╼ $nikto -h testfire.net
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          65.61.137.117
+ Target Hostname:    testfire.net
+ Target Port:        80
+ Start Time:         2023-10-18 10:38:50 (GMT1)
---------------------------------------------------------------------------
+ Server: Apache-Coyote/1.1
```

2. Search vulnerabilities in web.



Version Disclosure (Apache Coyote)

🟨 Severity: **Low**

Summary

Invicti identified a version disclosure (Apache Coyote) in the target web server's HTTP response.
This information can help an attacker gain a greater understanding of the systems in use and potentially develop further attacks targeted at the specific version of Apache.

Recommendations:

- Configure your web server to prevent information leakage from the SERVER header of its HTTP response.
- Conduct frequent vulnerable scans.

g. Vulnerability: Transmission of Cleartext Credentials

CWE: CWE-319

OWASP Category: A05:2021 Security Misconfiguration

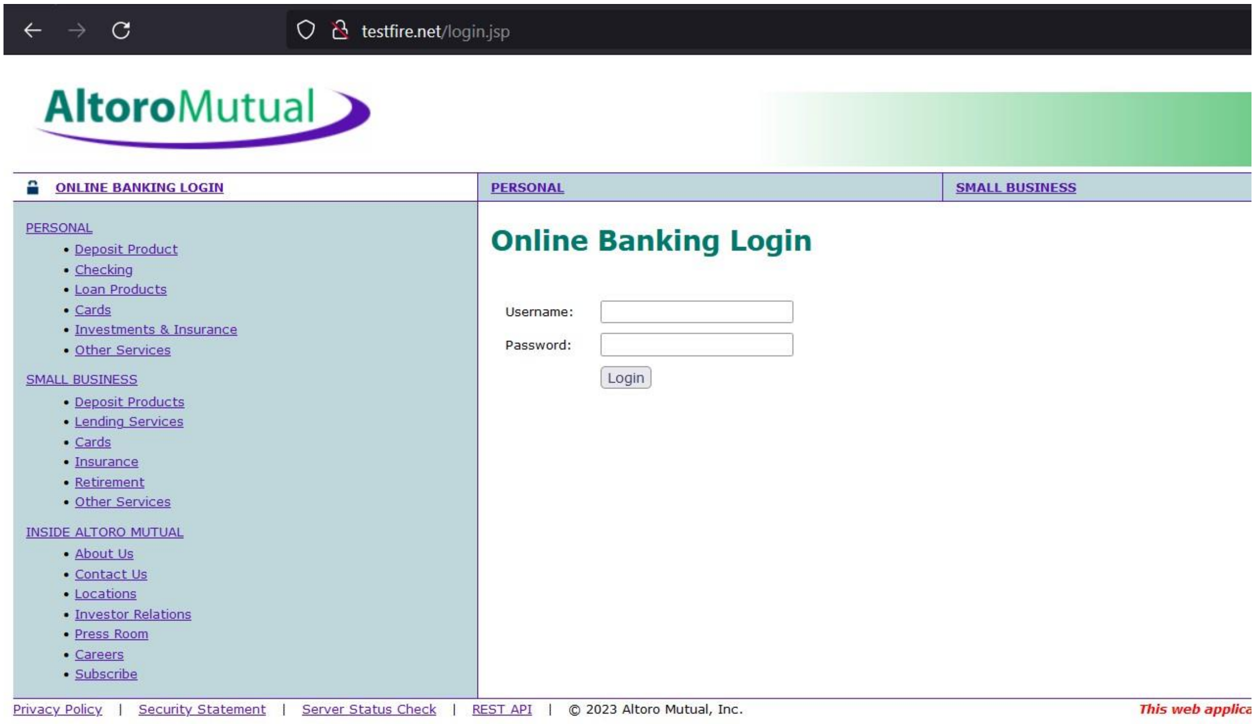
Description: The product transmits sensitive or security-critical data in cleartext in a communication channel that can be sniffed by unauthorized actors.

Business Impact: Transmitting credentials in cleartext can result in unauthorized access, data breaches, loss of customer trust, legal and regulatory consequences, and reputation damage, impacting an organization’s security and financial standing.

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

Steps to Reproduce:

1. Navigate to the above mentioned URL.

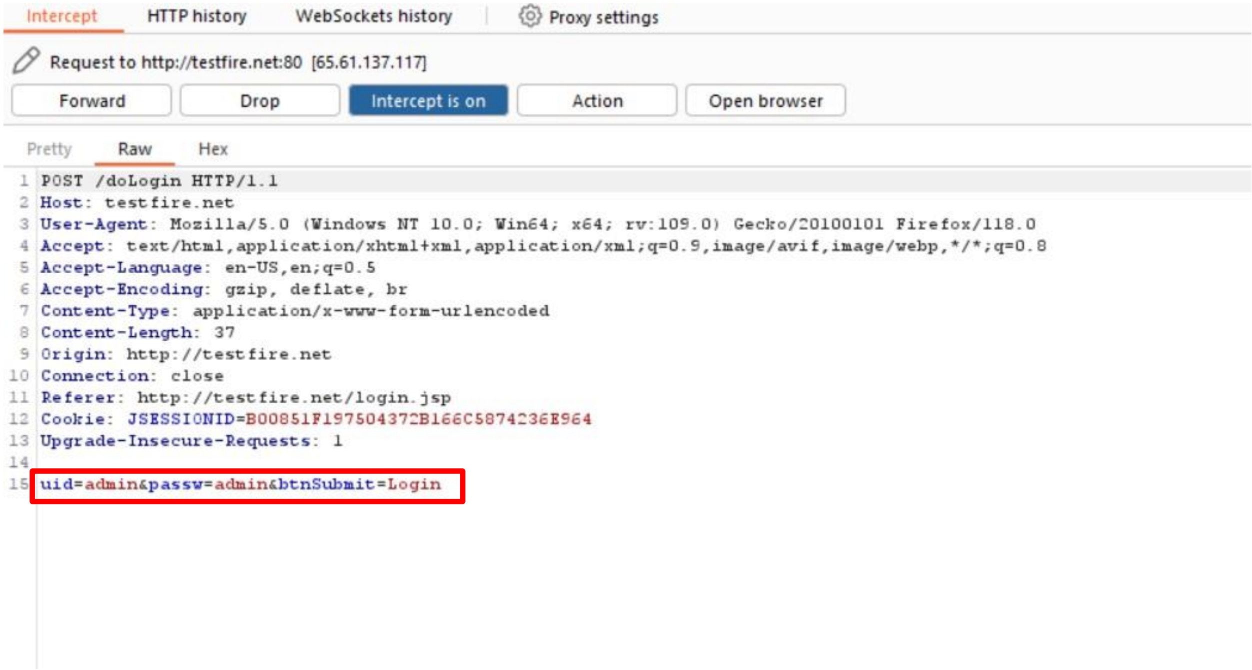


Online Banking Login

Username:

Password:

2. Login using admin credentials with "**Burp Suite**" intercept turned on.



Request to http://testfire.net:80 [65.61.137.117]

```
POST /doLogin HTTP/1.1
Host: testfire.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/118.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 37
Origin: http://testfire.net
Connection: close
Referer: http://testfire.net/login.jsp
Cookie: JSESSIONID=B00851F197504372B166C5874236E964
Upgrade-Insecure-Requests: 1

uid=admin&passw=admin&btnSubmit=Login
```

It is clearly visible that the credentials are transmitted in cleartext.

Recommendations:

- Hash and Salt credentials.
- Implement Secure Protocols.

h. Vulnerability: Clickjacking

CWE: CWE-451

OWASP Category: A04:2021 Insecure Design

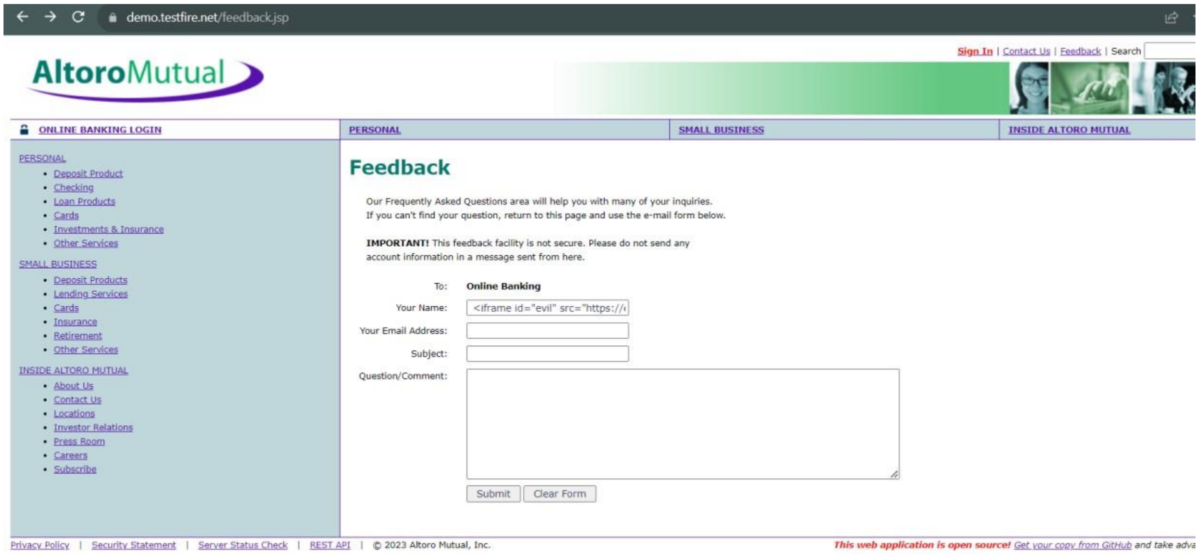
Description: The user interface (UI) does not properly represent critical information to the user, allowing the information – or its source – to be obscured or spoofed. This is often a component in phishing attacks.

Business Impact: The Impact of Clickjacking The hacker has several ways they can use the redirected clicks for their own gain. A common form of clickjacking involves mirroring a login and password form on a website.

Vulnerability Path: https://demo.testfire.net/feedback.jsp

Steps to reproduce:

1. Navigate to the above-mentioned URL. Enter the payload “<iframe id=”evil” src=https://evil.com sandbox=”allow-forms”></iframe>



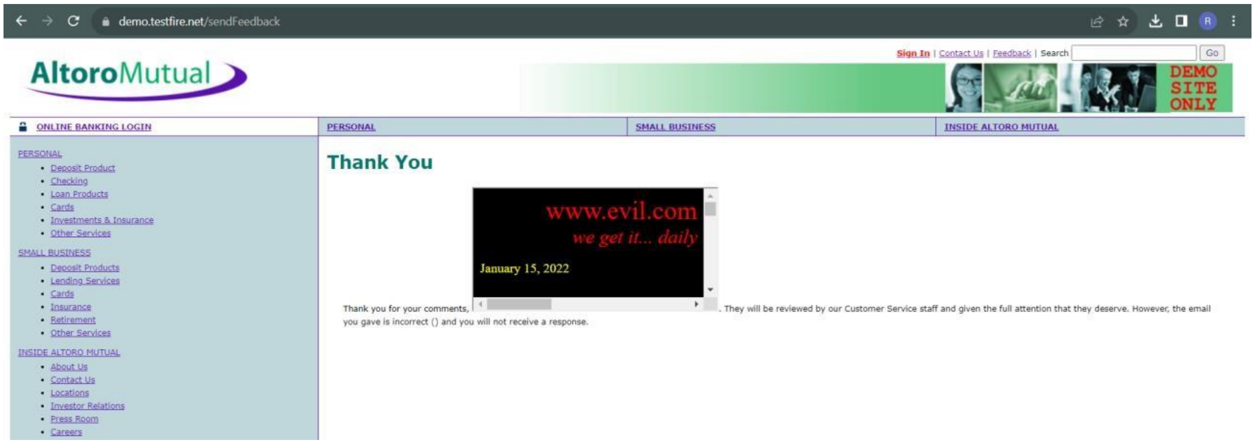
Feedback

Our Frequently Asked Questions area will help you with many of your inquiries.
If you can't find your question, return to this page and use the e-mail form below.

IMPORTANT! This feedback facility is not secure. Please do not send any account information in a message sent from here.

To: **Online Banking**
Your Name: <iframe id="evil" src="https://
Your Email Address:
Subject:
Question/Comment:

2. Click on submit.



Thank You

Thank you for your comments, . They will be reviewed by our Customer Service staff and given the full attention that they deserve. However, the email you gave is incorrect () and you will not receive a response.

Recommendations:

- Implement X-Frame Options Header.
- Utilize Content Security Policy.
- Employ frame-busting JavaScript code.

i. **Vulnerability:** Cookie with Insecure or Improper or Missing SameSite attribute

CWE: CWE-1275

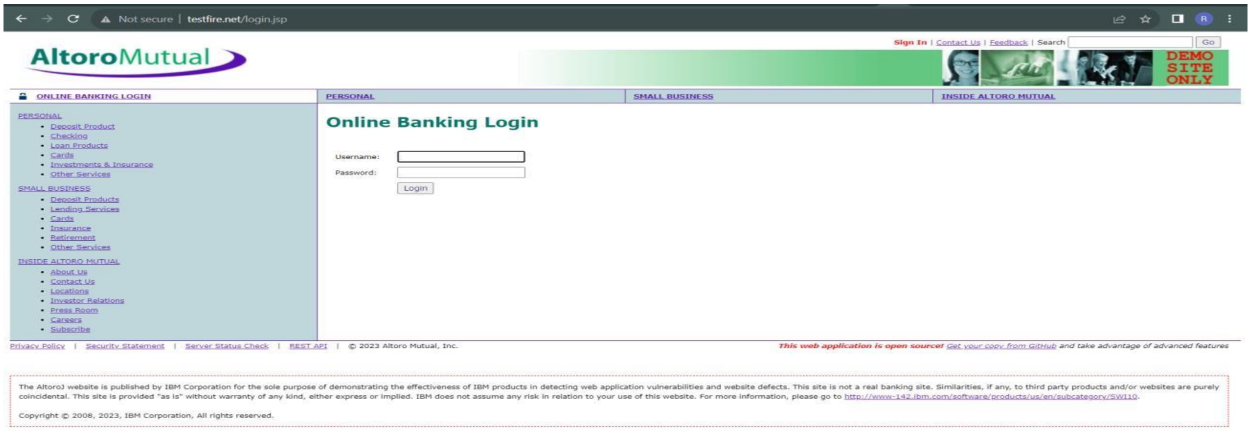
OWASP Category: A01:2021 Broken Access Control

Description: The SameSite attribute for sensitive cookies is not set, or an insecure value is used.

Business Impact: Inadequate SameSite attribute settings on cookies can lead to security vulnerabilities, enabling Cross-Site Request Forgery (CSRF) and Cross-Site Scripting (XSS) attacks, potentially resulting in data breaches, loss of customer trust, legal consequences, and financial damage.

Vulnerability Path: http://testfire.net/login.jsp **Steps to Reproduce:**

1. Navigate to the above-mentioned URL.



Online Banking Login

Username:

Password:

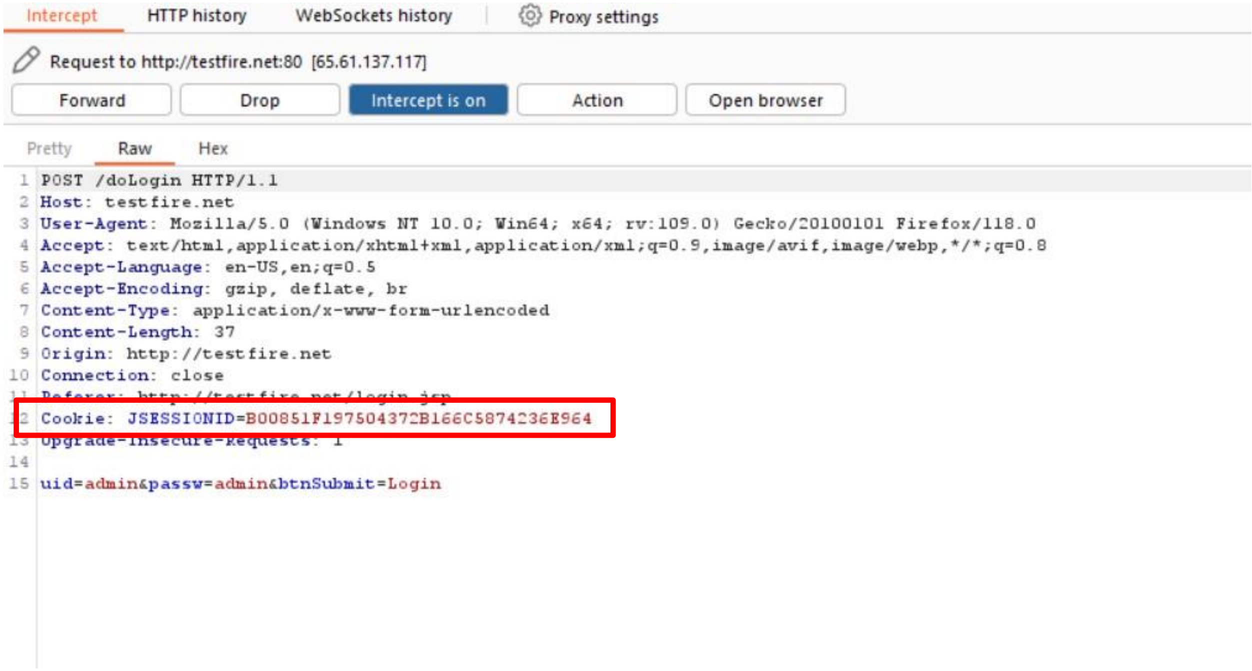
© 2023 Altoro Mutual, Inc.

This web application is open source! Get your copy from GitHub and take advantage of advanced features

The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to http://www-142.ibm.com/software/products/us/en/subcategory/SWI10.

Copyright © 2008, 2023, IBM Corporation, All rights reserved.

2. Login using admin credentials with “**Burp Suite”** intercept turned on.



Request to http://testfire.net:80 [65.61.137.117]

```
POST /doLogin HTTP/1.1
Host: testfire.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/118.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 37
Origin: http://testfire.net
Connection: close
Referer: http://testfire.net/login.jsp
Cookie: JSESSIONID=B00851F197504372B166C5874236E964
Upgrade-Insecure-Requests: 1

uid=admin&passw=admin&btnSubmit=Login
```

Recommendations:

- Implement proper SameSite settings.
- Regular Security Audits.

REPORT ON MAIN WEBSITE

Chosen Website: https://smartinternz.com

a. Vulnerability: PHP Unsupported Version Detection

CWE: CWE-661

OWASP Category: A06:2021-Vulnerable and Outdated Components

Severity: High

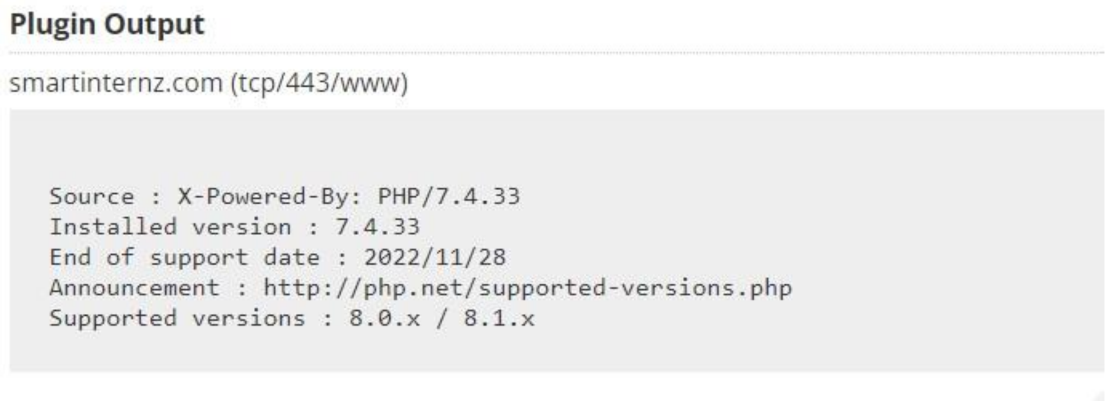
Description: According to its version, the installation of PHP on the remote host is no longer supported. As a result, it is likely to contain security vulnerabilities.

Business Impact: Anyone can connect to the NSClient and retrieve sensitive information, such as process and service states, memory usage, etc.

Vulnerability Path: https://smartinternz.com

Steps to Reproduce:

1. Nessus Scan reveals the PHP version supporting the website.



Plugin Output

smartinternz.com (tcp/443/www)

```
Source : X-Powered-By: PHP/7.4.33
Installed version : 7.4.33
End of support date : 2022/11/28
Announcement : http://php.net/supported-versions.php
Supported versions : 8.0.x / 8.1.x
```

Recommendations:

- Upgrade to a version of PHP that is currently supported.
- Find it on your network and fix it as soon as possible.

b. Vulnerability: Missing Anti-clickjacking tokens

CWE: CWE-451

OWASP Category: A04:2021 Insecure Design

Severity: High

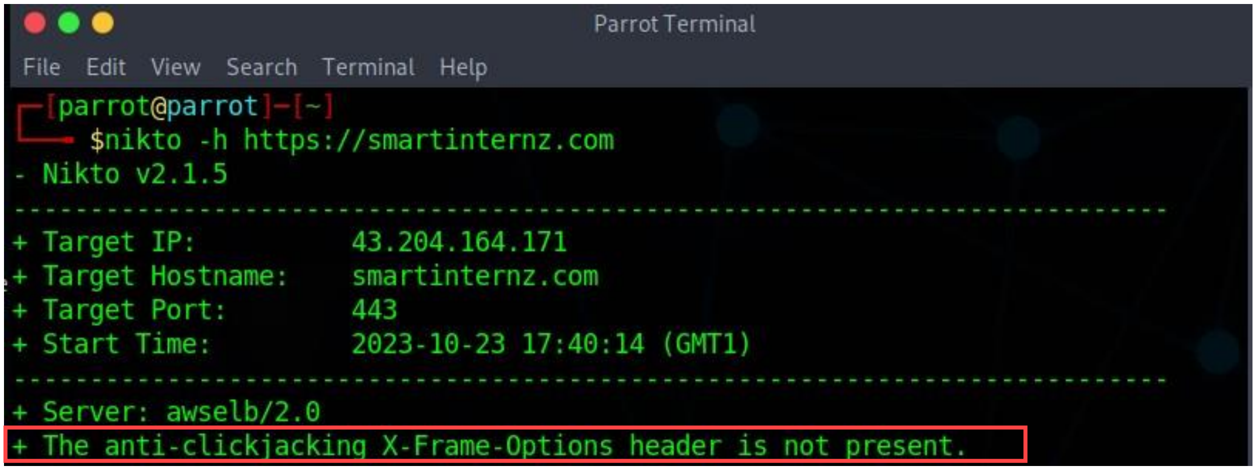
Description: The user interface (UI) does not properly represent critical information to the user, allowing the information - or its source - to be obscured or spoofed. This is often a component in phishing attacks.

Business Impact: The Impact of Clickjacking The hacker has several ways they can use the redirected clicks for their own gain. A common form of clickjacking involves mirroring a login and password form on a website.

Vulnerability Path: https://smartinternz.com

Steps to Reproduce:

1. Tool Used: **Nikto.** Type the following Command.



```
┌─[parrot@parrot]─[~]
└──╼ $nikto -h https://smartinternz.com
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          43.204.164.171
+ Target Hostname:    smartinternz.com
+ Target Port:        443
+ Start Time:         2023-10-23 17:40:14 (GMT1)
---------------------------------------------------------------------------
+ Server: awselb/2.0
+ The anti-clickjacking X-Frame-Options header is not present.
```

Recommendations:

- Implement X-Frame Options Header.
- Utilize Content Security Policy.
- Employ frame-busting JavaScript code.

c. Vulnerability: Disclosing webserver type

CWE: CWE-200

OWASP Category: A03:2017 Sensitive Data Exposure

Severity: low

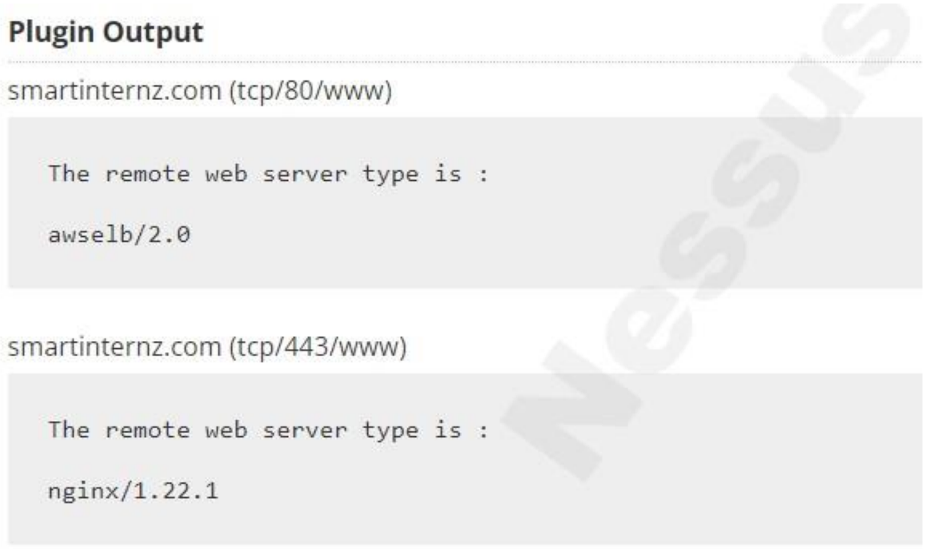
Description: The product exposes sensitive information to an actor that is not explicitly authorized to have access to that information.

Business Impact: Disclosing the web server type can pose a security risk by providing potential attackers with information that may be exploited. This disclosure can lead to more targeted attacks and increases the risk of vulnerabilities being exploited, potentially resulting in data breaches, service disruptions, and reputational damage. It's essential to minimize such disclosures to enhance the security of web applications.

Vulnerability Path: https://smartinternz.com

Steps to Reproduce:

1. Nessus Scan reveals the webserver version supporting the website.



Plugin Output

smartinternz.com (tcp/80/www)

```
The remote web server type is :

awselb/2.0
```

smartinternz.com (tcp/443/www)

```
The remote web server type is :

nginx/1.22.1
```

Recommendations:

- You can limit the information that nginx presents by creating/editing the following directive in *nginx.conf*.
- Replace it with false information.

d. Vulnerability: Cleartext Transmission of Credentials

CWE: CWE-319

OWASP Category: A05:2021 Security Misconfiguration

Severity: Medium

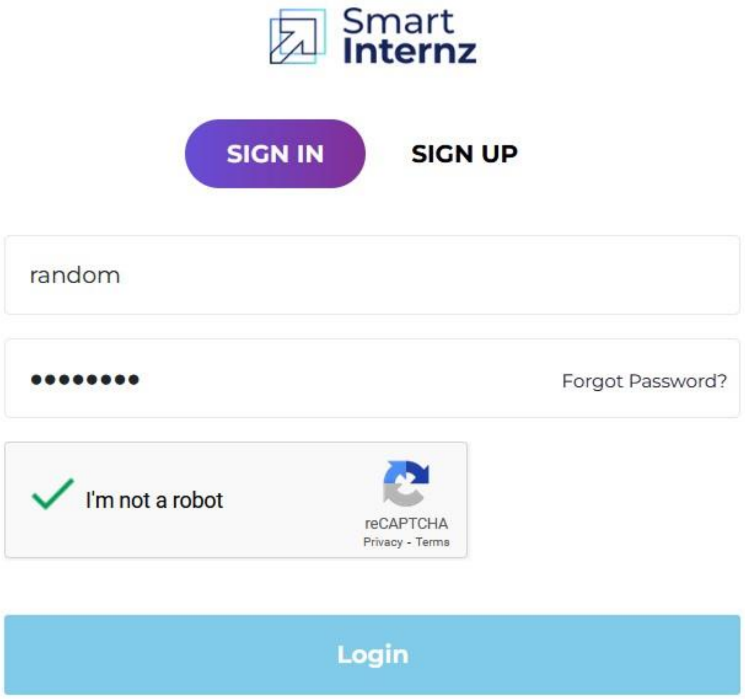
Description: The product transmits sensitive or security-critical data in cleartext in a communication channel that can be sniffed by unauthorized actors.

Business Impact: Transmitting credentials in cleartext can result in unauthorized access, data breaches, loss of customer trust, legal and regulatory consequences, and reputation damage, impacting an organization's security and financial standing.

Vulnerability Path: https://smartinternz.com/student-login

Steps to Reproduce:

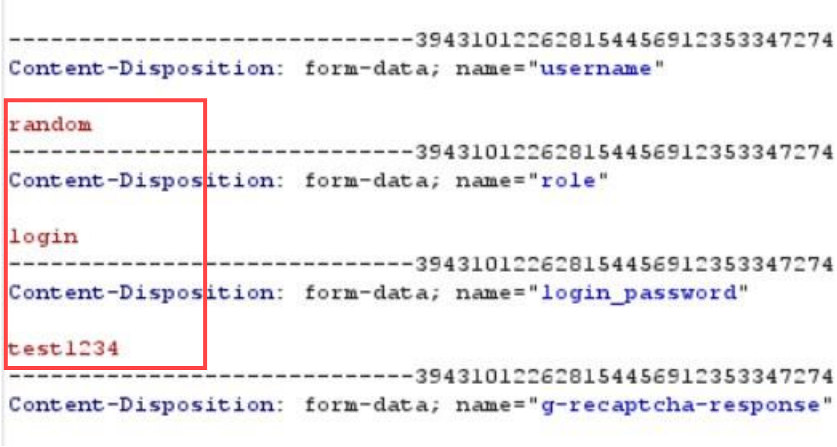
1. Navigate to the above-mentioned URL and login.



random

•••••••••

2. Tool Used: **Burp Suite.** Capture the traffic.



```
----------------------------394310122628154456912353347274
Content-Disposition: form-data; name="username"

random
----------------------------394310122628154456912353347274
Content-Disposition: form-data; name="role"

login
----------------------------394310122628154456912353347274
Content-Disposition: form-data; name="login_password"

test1234
----------------------------394310122628154456912353347274
Content-Disposition: form-data; name="g-recaptcha-response"
```

Recommendations:

- Hash and Salt credentials.
- Implement Secure Protocols.

e. Vulnerability: Web Server Directory Enumeration

CWE: CWE-548

OWASP Category: A04: Insecure Design

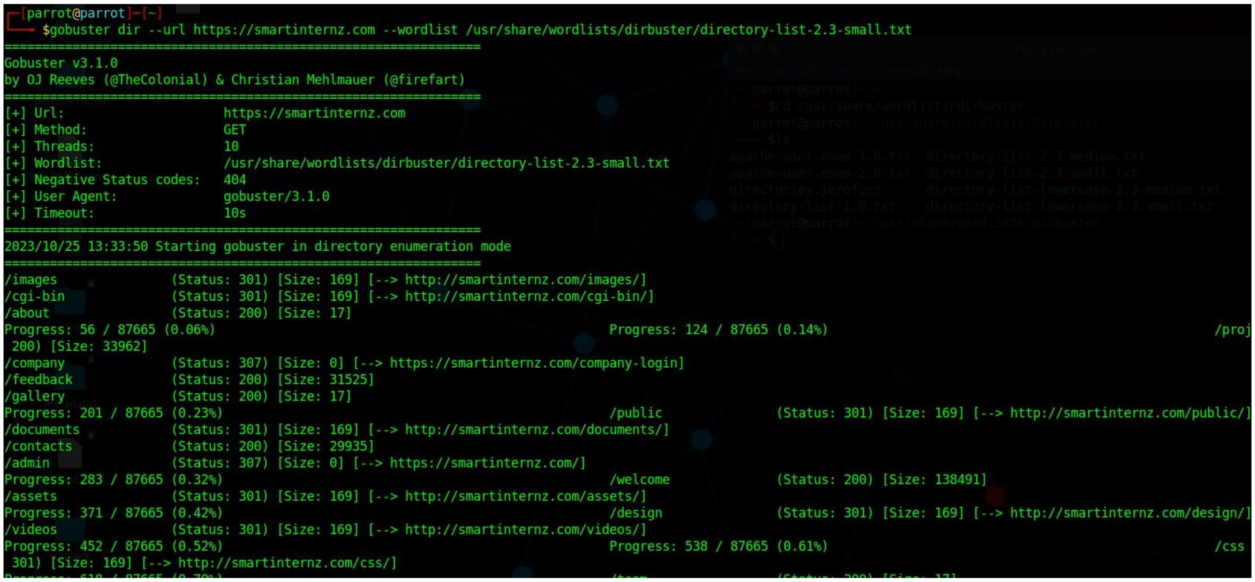
Severity: low

Description: A directory listing is inappropriately exposed, yielding potentially sensitive information to attackers.

Business Impact: Webserver directory enumeration, often through techniques like directory listing, can have significant business impacts. By revealing the structure of a web server's directories and files, it provides potential attackers with insights into the system's architecture and potential vulnerabilities. This can lead to unauthorized access, data exposure, and even service disruptions. The business consequences include reputational damage, legal liabilities, financial losses, and the potential compromise of sensitive information. Mitigating directory enumeration is crucial to maintaining a secure online presence. **Vulnerability Path:** https://smartinternz.com

Steps to Reproduce:

1. Tool Used: **Gobuster.** Type the following command.



```
┌─[parrot@parrot]─[~]
└──╼ $gobuster dir --url https://smartinternz.com --wordlist /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://smartinternz.com
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2023/10/25 13:33:50 Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 169] [--> http://smartinternz.com/images/]
/cgi-bin              (Status: 301) [Size: 169] [--> http://smartinternz.com/cgi-bin/]
/about                (Status: 200) [Size: 17]
Progress: 56 / 87665 (0.06%)                                          Progress: 124 / 87665 (0.14%)                                            /proj
 200) [Size: 33962]
/company              (Status: 307) [Size: 0] [--> https://smartinternz.com/company-login]
/feedback             (Status: 200) [Size: 31525]
/gallery              (Status: 200) [Size: 17]
Progress: 201 / 87665 (0.23%)                                         /public              (Status: 301) [Size: 169] [--> http://smartinternz.com/public/]
/documents            (Status: 301) [Size: 169] [--> http://smartinternz.com/documents/]
/contacts             (Status: 200) [Size: 29935]
/admin                (Status: 307) [Size: 0] [--> https://smartinternz.com/]
Progress: 283 / 87665 (0.32%)                                         /welcome             (Status: 200) [Size: 138491]
/assets               (Status: 301) [Size: 169] [--> http://smartinternz.com/assets/]
Progress: 371 / 87665 (0.42%)                                         /design              (Status: 301) [Size: 169] [--> http://smartinternz.com/design/]
/videos               (Status: 301) [Size: 169] [--> http://smartinternz.com/videos/]
Progress: 452 / 87665 (0.52%)                                         Progress: 538 / 87665 (0.61%)                                            /css
 301) [Size: 169] [--> http://smartinternz.com/css/]
```

Recommendations:

- Disable directory listing.
- Restrict access to sensitive files and directories.
- Use Strong Authentication mechanisms to control access.

STAGE-2

Overview:

Nessus is a widely-used vulnerability assessment tool that helps in the identification of security issues. Typically, a Nessus scan report provides comprehensive insights into vulnerabilities present within a system or network. If one were to conduct a Nessus scan on a platform like YouTube, it would potentially highlight various security vulnerabilities or issues that might exist within the YouTube infrastructure. These could include, but are not limited to, issues with outdated software, misconfigurations, potential weaknesses in server protocols, or known vulnerabilities in the systems used by YouTube.

The specifics of such a report generated by a Nessus scan would typically include a list of vulnerabilities, their severity level, potential impact if exploited, and recommendations for mitigation or remediation.

Target Website: https://youtube.com

Target IP Address: 142.250.191.78

List of Vulnerabilities:

Sno	Vulnerability Name	Severity	Plugins
1.	HTTP Server Type and Version	None	ID-43111
2.	Web Server no 404 Error Code Check	None	ID-10386
3.	Hyper Text Transfer Protocol Information (HTTP)	None	ID-24260
4.	HTTP Methods Allowed	None	ID-43111
5.	HTTP Redirect Information	None	ID-91634

REPORT

Vulnerability Name: HTTP Server Type and Version

Severity: None

Plugin: ID-43111

Port: 80 & 443

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

Solution: n/A

Business Impact: n/A

Vulnerability Name: Web Server no 404 Error Code Check

Severity: None

Plugin: ID-10386

Port: 80

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

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

Solution: n/A

Business Impact: n/A

Vulnerability Name: Hyper Text Transfer Protocol Information (HTTP)

Severity: None

Plugin: ID-24260

Port: 80 & 443

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

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

Solution: n/A

Business Impact: n/A

Vulnerability Name: HTTP Methods Allowed

Severity: None

Plugin: ID-43111

Port: 443 & 80

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

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

Solution: n/a

Business Impact: n/a

Vulnerability Name: HTTP Redirect Information

Severity: None

Plugin: ID-91634

Port: 80 & 443

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

The following HTTP methods are considered insecure:
PUT, DELETE, CONNECT, TRACE, HEAD

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

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'
in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

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

Solution: n/a

Business Impact: n/a

STAGE - 3

ABILITY OF SOC/SIEM

1. Security Operations Center (SOC): The Security Operations Center (SOC) serves as a central unit in cybersecurity, responsible for monitoring, detecting, analyzing, and responding to security incidents. Its primary function is to ensure the security posture of an organization by constantly monitoring and analyzing security events occurring in real-time. The SOC team uses various tools, technologies, and methodologies to safeguard against threats and vulnerabilities.

2. SOC Cycle: The SOC operates on a cyclical process, often referred to as the SOC cycle. This cycle includes key stages such as threat detection, investigation, and response. The SOC continuously detects potential threats, investigates any suspicious activities or events, and responds promptly to mitigate and resolve security incidents. This iterative cycle allows for a proactive and continuous improvement in an organization's security posture.

3. Security Information and Event Management (SIEM): SIEM is a crucial tool within a SOC. It's a software solution that aggregates and correlates data from multiple sources across an organization's network infrastructure. The SIEM system collects security event data and log information from different devices, applications, and systems, providing a comprehensive overview of an organization's security status. The SIEM system helps in real-time monitoring, threat detection, incident response, and compliance management.

4. SIEM Cycle: The SIEM cycle involves the collection, normalization, correlation, and analysis of security event data. This data is obtained from various sources such as firewalls, antivirus software, servers, and more. The SIEM platform correlates this data to identify patterns, detect anomalies, and produce actionable insights for the SOC team. Through this cyclical process, the SIEM system provides a continuous flow of information, enabling rapid threat detection and response.

5. Malware Information Sharing Platform (MISP): MISP is a collaborative platform utilized by cybersecurity professionals and analysts to share, store, and correlate indicators of compromise (IoCs) and threat intelligence. It allows organizations to securely share and discuss cybersecurity information, improving their collective ability to detect, prevent, and respond to cyber threats. MISP facilitates the aggregation and dissemination of threat intelligence, contributing significantly to the overall security posture and defense against evolving cyber threats.

6. VIT-AP Network Information: Vellore Institute of Technology, Andhra Pradesh (VIT-AP) houses a sophisticated network infrastructure that forms the backbone of its technological ecosystem. The network at VIT-AP is a robust amalgamation of interconnected systems, servers, and devices that facilitate seamless communication, data exchange, and access to digital resources across the campus. This extensive network supports various academic, administrative, and research-related activities, enabling a comprehensive and efficient flow of information. With an emphasis on security and reliability, VIT-AP's network is equipped with robust firewalls, intrusion detection systems, and stringent access controls to safeguard against potential cyber threats. Through a combination of advanced hardware, software, and stringent security measures, VIT-AP ensures the uninterrupted functionality and protection of its network, fostering an environment conducive to academic excellence, research advancements, and administrative efficiency.

7. How do you think you can deploy SOC at VIT-AP: Implementing a Security Operations Center (SOC) at Vellore Institute of Technology (VIT-AP) would involve strategically setting up a dedicated team of security professionals, along with advanced tools and systems. This team would monitor, detect, and respond to potential security threats in VIT-AP's network infrastructure. Establishing an incident response framework, deploying sophisticated security tools such as SIEM, and ensuring continuous monitoring and improvement would be crucial. Collaboration with internal stakeholders and information sharing for threat intelligence would also be prioritized to fortify VIT-AP's cybersecurity posture. This multifaceted approach would enable VIT-AP to proactively safeguard its network against potential cyber threats and ensure compliance with evolving security standards.

8. Threat Intelligence: Threat intelligence involves the collection, analysis, and distribution of information regarding potential cybersecurity threats. This data provides valuable insights into the tactics, techniques, and procedures of malicious actors, enabling organizations to anticipate and mitigate potential risks. It encompasses information about emerging vulnerabilities, malware, and attack patterns, assisting in strengthening an organization's security posture.

9. Incident Response: Incident response refers to the organized approach taken to manage and address the aftermath of a security breach or cyber incident. It involves a series of defined procedures aimed at swiftly identifying, mitigating, and recovering from security breaches. The goal of incident response is to minimize the impact of a security incident, restore normal operations, and prevent future occurrences. This process typically includes detection, analysis, containment, eradication, recovery, and lessons learned for future prevention.

10. QRadar: QRadar is an IBM Security product and a robust Security Information and Event Management (SIEM) solution. It serves as a centralized platform for collecting, analyzing, and correlating log data from various sources across an organization's network infrastructure. QRadar utilizes this data to detect and prioritize potential security threats in real-time, offering a comprehensive view of an organization's security posture. Through advanced analytics and threat intelligence integration, QRadar assists security teams in proactively identifying and responding to security incidents, thereby enhancing the overall security readiness and incident response capabilities of an organization.

What do you understand from web application testing?

Web application testing is a critical process designed to assess the functionality, security, and performance of online applications. It involves evaluating various components of web applications such as usability, accessibility, and compatibility across different browsers and devices. Security testing aims to identify vulnerabilities and potential threats to ensure robust protection against cyberattacks. Functional testing checks if the application behaves as expected, while performance testing assesses the application's responsiveness under various conditions. This comprehensive testing approach is crucial to ensure that web applications are secure, reliable, and user-friendly, delivering a positive experience to users while maintaining a high level of security.

What do you understand form nessus report?

A Nessus report is a comprehensive documentation summarizing the findings from a vulnerability scan conducted by the Nessus vulnerability assessment tool. It outlines identified security weaknesses, potential threats, and vulnerabilities within a network or system. The report provides detailed insights into specific issues such as outdated software, misconfigurations, potential entry points for cyber threats, and more, categorizing them based on severity levels. Additionally, it often includes recommendations for remediation or mitigation strategies to address the identified vulnerabilities. This report serves as a valuable resource for IT professionals and security teams, guiding them in fortifying systems and networks against potential cyber risks.

What do you understand from SOC/ SIEM/ QRadar Dashboard?

A Security Operations Center (SOC) leverages the Security Information and Event Management (SIEM) platform, such as QRadar, to monitor and manage an organization's security posture. The SOC/SIEM/QRadar dashboard provides a centralized and visual interface displaying real-time security insights, including alerts, incidents, and overall network health. It offers at-a-glance visibility into potential threats, anomalies, and ongoing security events within the organization's network. The dashboard compiles and presents critical information, enabling security analysts to swiftly identify, investigate, and respond to security incidents, ensuring a proactive and effective approach to safeguarding the organization's digital infrastructure.

Future scope of web application testing

The future of web application testing holds immense potential as technological advancements continue to reshape digital landscapes. With the rapid evolution of web applications and the increasing complexity of cyber threats, the scope of testing is set to expand. AI and machine learning will play pivotal roles in automating testing processes, optimizing test coverage, and enhancing predictive analysis for potential vulnerabilities. The focus will shift towards more comprehensive security testing, including penetration testing, and a stronger emphasis on identifying and remedying complex security flaws. Additionally, the integration of DevSecOps practices will become more prominent, enabling security measures to be incorporated earlier in the software development lifecycle. As web applications become more intricate and integrated into various devices and IoT, testing will evolve to address these diverse environments, emphasizing compatibility, usability, and performance across multiple platforms and devices.

Future scope of testing Process

The future of software testing holds significant promise as technology and development methodologies evolve. Automation will continue to play a pivotal role, with AI and machine learning making testing processes more intelligent, efficient, and adaptive. Shift-left testing, where testing occurs earlier in the software development lifecycle, will become the norm, reducing defects and saving costs. Continuous testing will seamlessly integrate into DevOps and Agile workflows, allowing for quicker and more robust testing cycles. With the rise of IoT and mobile applications, there will be a greater emphasis on compatibility, performance, and security testing across various devices and platforms. Furthermore, ethical hacking and security testing will gain prominence as cybersecurity threats become more sophisticated. Overall, the future of testing is marked by increased automation, faster feedback loops, and a holistic approach to ensure software quality and security in an ever-changing technological landscape.

Future scope of SOC/SIEM

The future of Security Operations Centers (SOC) and Security Information and Event Management (SIEM) systems lies in advanced automation, integration of AI and machine learning, and enhanced anomaly detection. These technologies will drive predictive analysis and behavioral analytics, reducing false positives and streamlining incident response. Cloud-based solutions will offer scalability, and compliance management will be a key focus to meet evolving global standards in cybersecurity. The evolution of SOC and SIEM will pivot towards proactive and adaptive approaches to tackle sophisticated cyber threats.

Topics Explored: Web Application Testing, Nessus Report, SOC, SIEM, QRadar Dashboard, Future Scope of Web Application Testing, Future Scope of Testing Process, Future Scope of SOC/SIEM

Tools Explored: Nessus, SIEM, QRadar, tools for web application testing

CONCLUSION

The development of a sophisticated malware detection and classification project represents a significant leap in the perpetual endeavor to fortify cybersecurity measures. By harnessing the power of cutting-edge artificial intelligence, this project aims to provide users with an advanced platform for uploading and analyzing potentially malicious files. The integration of AI models within the system enables swift and accurate classification of diverse forms of malware, equipping users with in-depth reports detailing the nature and potential risks associated with the uploaded files.

As technology continues to evolve, the ongoing progression of this initiative remains integral in bolstering defenses against the ever-evolving landscape of cyber threats. The primary goal of this project is to proactively identify and comprehend potential security risks, ultimately contributing to the collective efforts to establish a more secure digital environment.

The utilization of artificial intelligence in the realm of cybersecurity holds the key to empowering users by enhancing their understanding of potential threats and vulnerabilities. The project's emphasis on leveraging AI models for the identification and classification of malware underscores the commitment to delivering a robust, user-friendly platform. It aims not only to detect potential security risks but also to educate and inform users about the nature of these threats. Through this continuous pursuit of innovation, the project seeks to serve as a proactive defense against emerging cyber threats, supporting the broader mission of creating a safer digital space for users.

In a dynamic digital landscape fraught with ever-evolving cybersecurity risks, the amalgamation of AI-powered malware detection and classification represents a pivotal step towards a more resilient security infrastructure. As this project advances, its dedication to leveraging sophisticated technology for threat identification and providing users with comprehensive insights remains integral to the ongoing fight against cyber threats. Through a combination of proactive detection, education, and response, this initiative stands at the forefront of cybersecurity measures, contributing significantly to the collective mission of ensuring a more secure digital future.

FUTURE SCOPE

The future scope of the malware detection and classification project is poised for further advancements in leveraging cutting-edge technologies and methodologies. With continuous developments in artificial intelligence and machine learning, the project is set to witness enhanced capabilities in swiftly identifying and categorizing emerging and complex forms of malware. The integration of more sophisticated algorithms and AI models is expected to refine the system's accuracy and efficiency in classifying diverse threats, thereby empowering users with more detailed and precise reports about potential risks associated with uploaded files and also keenly categorize the detected malware.

Furthermore, the project's evolution will likely include collaborations with threat intelligence platforms and global cybersecurity networks, fostering a collective effort to share and update threat data. This collaborative approach will significantly enrich the project's database, enabling a broader spectrum of threat identification and response. The adoption of advanced automation and predictive analysis tools is also anticipated, streamlining the identification and immediate response to potential threats.

Moreover, the project's future scope encompasses expanding its user base and functionalities, potentially reaching a wider audience and serving diverse sectors. By integrating the system into various industries, such as finance, healthcare, and government, it can provide tailored solutions to address specific cybersecurity challenges unique to each sector. Overall, the continuous development and refinement of this project are geared towards establishing a more robust, proactive, and user-centric defense system against the ever-evolving landscape of cyber threats.

REFERENCES

1. https://ieeexplore.ieee.org/document/9117547
2. https://www.researchgate.net/publication/349613618_Malware_Detection_Classification_using_Machine_Learning
3. https://medium.com/@rushiil.deshmukh/malware-classification-using-machine-learning-and-deep-learning-4de22e194dbe
4. Aijaz, U.N., Patra, A., Siddiq, A.S., Chatterjee, B., Ghiyas Khan, M., 2018. Malware Detection on Server using Distributed Machine Learning. Proceedings of Knowledge Discovery in Information Technology and Communication Engineering (KITE-2018) 2, 172–175. URL: http://www.pices-journal.com/downloads/V2I7-PICES0046.pdf
5. https://aws.amazon.com/blogs/machine-learning/malware-detection-and-classification-with-amazon-rekognition/