INDEX

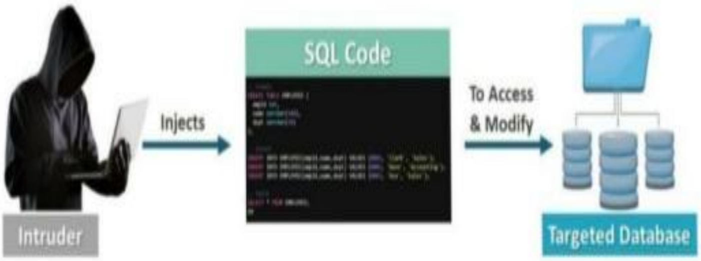
INTRODUCTION TO REAL-TIME SECURITY INTELLIGENCE

Security intelligence refers to the practice of collecting, standardizing and analysing data that is generated by networks, applications, and other IT infrastructure in real-time, and the use of that information to assess and improve an organization's security posture. Real-time security monitoring is continuously overseeing and analysing the data traffic and activities in an organization's network to detect, alert, and respond to potential security threats as they happen.

With Security Intelligence solutions, organizations can identify and mitigate those inside threats and many more, by detecting the following: Unauthorized application access or usage. Data loss such as sensitive data being transmitted to unauthorized destinations.

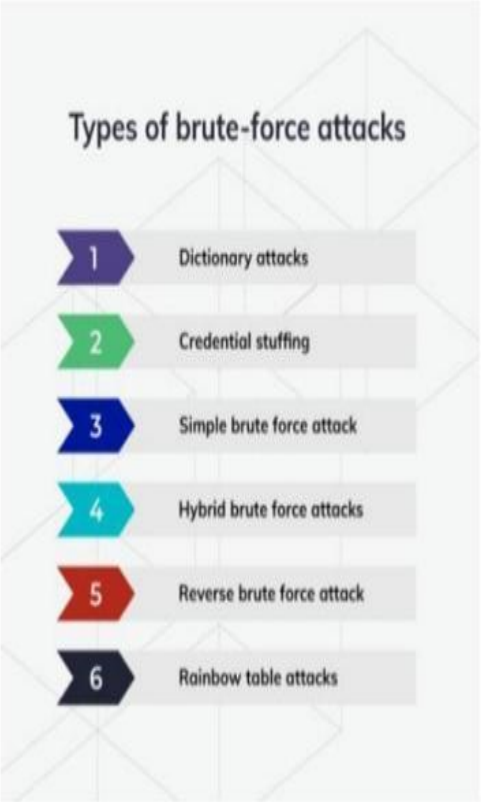
There are a few key principles that define security intelligence:

- Real-Time Analysis
- Pre-Exploit Analysis
- Collection, Normalization, And Analysis
- Actionable Insight
- Scalable
- Adjustable Size And Cost



information may include any number of items, including sensitive company data, user lists or private customer details.

- A brute force attack is a hacking method that uses trial and error to crack passwords, login credentials, and encryption keys. It is a simple yet reliable tactic for gaining unauthorized access to individual accounts and organizations' systems and networks.



Types of brute-force attacks

1 Dictionary attacks

2 Credential stuffing

3 Simple brute force attack

4 Hybrid brute force attacks

5 Reverse brute force attack

6 Rainbow table attacks

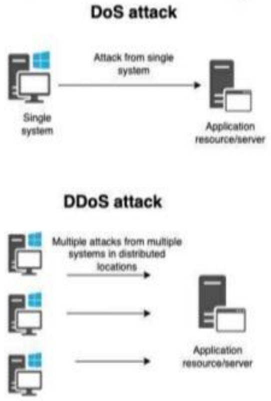
- A Trojan Horse Virus is a type of malware that downloads onto a computer disguised as a legitimate program. The delivery method

Real Time attacks

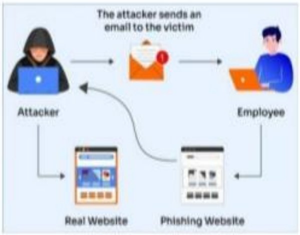
Email spoofing is a type of cyberattack that targets businesses by using emails with forged sender addresses. Because the recipient trusts the alleged sender, they are more likely to open the email and interact with its contents, such as a malicious link or attachment.

- DoS and DDoS attacks.
- Phishing attacks.
- Ransomware.
- SQL injection attacks.
- Brute force attacks.
- Trojan horses
- Spoofing
- Backdoor Trojan
- Password attacks.
- Malware.
- Man-in-the-middle.

- A DoS attack is characterized by using a single computer to launch the attack. A distributed denial-of-service (DDoS) attack is a type of DoS attack that comes from many distributed sources, such as a botnet DDoS attack.


DoS attack
Attack from single system
Single system
Application resource/server
DDoS attack
Multiple attacks from multiple systems in distributed locations
Application resource/server

- Phishing attacks are the practice of sending fraudulent communications that appear to come from a reputable source. It is usually done through email. The goal is to steal sensitive data like credit card and login information, or to install malware on the victim's machine.



- Ransomware is a type of malware which prevents you from accessing your device and the data stored on it, usually by encrypting your files. A criminal group will then demand a ransom in exchange for decryption. The computer itself may become locked, or the data on it might be encrypted, stolen or deleted.

- SQL injection, also known as SQLI, is a common attack vector that Quses malicious SQL code for backend database manipulation to access information that was not intended to be displayed. This

Abstract

Security Intelligence (SI) describes the practice of collecting, standardizing and analysing data generated by networks, applications and other IT infrastructure in real time and using this information to assess and improve the security status of an organization. Security Intelligence involves deploying software and personnel resources to discover practical and useful insights that impact risk mitigation and risk reduction for the organization. Security Intelligence may also be referred to as intelligent security analysis. The paper presents the analysis of current state-of-the-art in the use of Security Intelligence and its impact on the development of current software engineering methods and approaches together with the built solution monitoring the software security with the use of SI and ML.

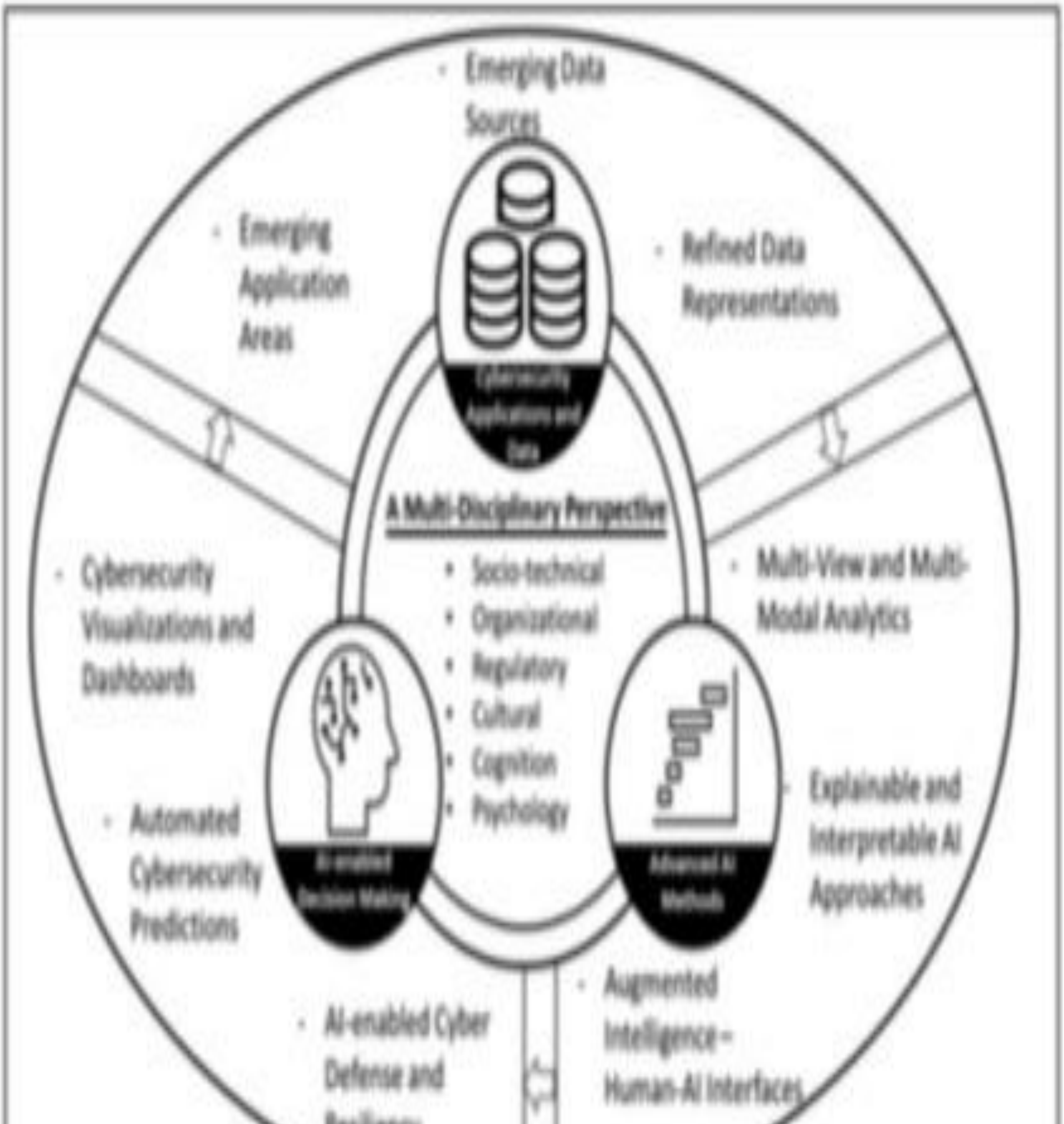
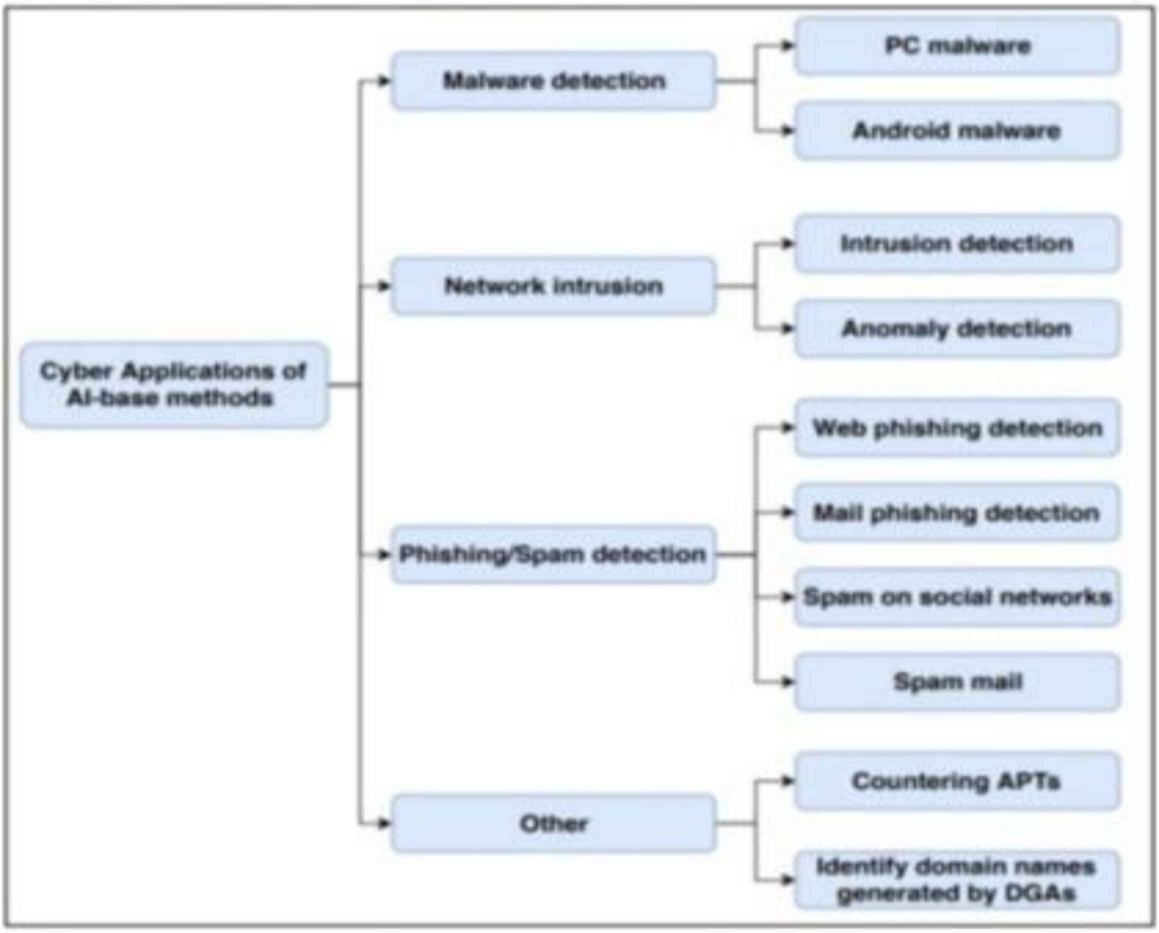
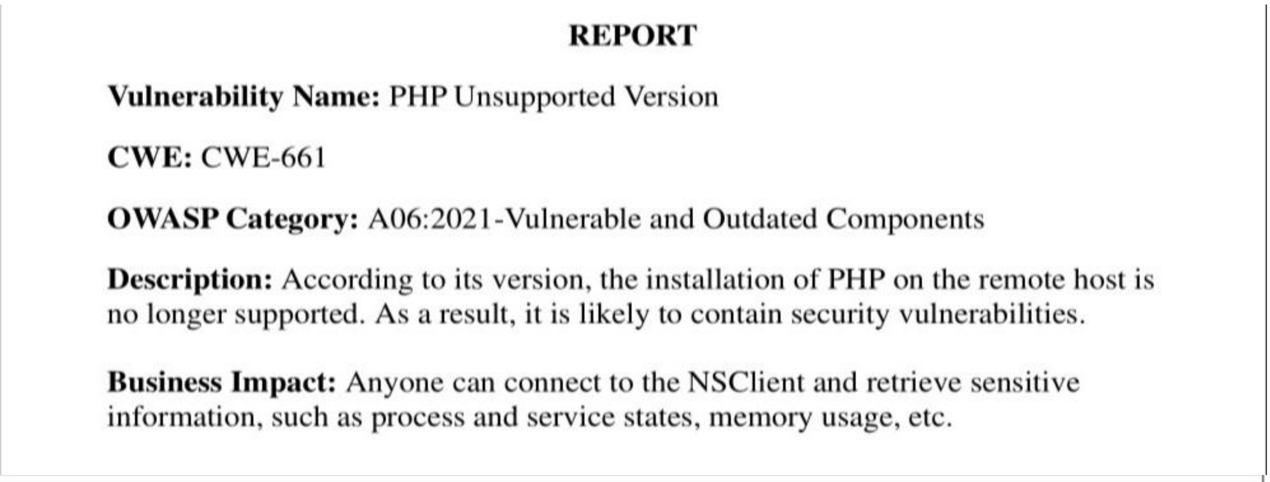

Emerging Data Sources
Emerging Application Areas
Refined Data Representations
Cybersecurity Applications and Data
A Multi-Disciplinary Perspective
Socio-technical
Organizational
Regulatory
Cultural
Cognition
Psychology
Cybersecurity Visualizations and Dashboards
Multi-View and Multi-Modal Analytics
AI-enabled Decision Making
Advanced AI Methods
Automated Cybersecurity Predictions
Explainable and Interpretable AI Approaches
AI-enabled Cyber Defense and Resiliency
Augmented Intelligence – Human-AI Interfaces

Figure 1: A Figure about Multi-Disciplinary AI for Cybersecurity Road Map Cybersecurity Application and Advanced AI-Enabled Decision-Making and Advanced AI Methods

The above image is showing about the multi-disciplinary perspective of AI technology in cybersecurity. It is consisted of three main phases. These phases include cybersecurity application and data, advanced AI methods, and AI-enabled decision making. In the cybersecurity application and data, it is dealing with emerging applications area, refined data representations, an emerging data source. The second phase is related to Advanced AI method to overcome cybersecurity issues. It includes multi-view and multi-modal analytics, Explainable and Interpretable AI approaches, and Augmented intelligences with Human AI interfaces for handling cyberattacks. Lastly, AI-enabled decision-making process. AI-enabled cyber defense and resiliency that shows relative information about AI, perform automated cybersecurity predictions for the system and cybersecurity visualization and dashboards. All these platforms are providing valuable insights about the data and AI can make efficient and real time decisions to get rid of cyber-security issues [1].





REPORT

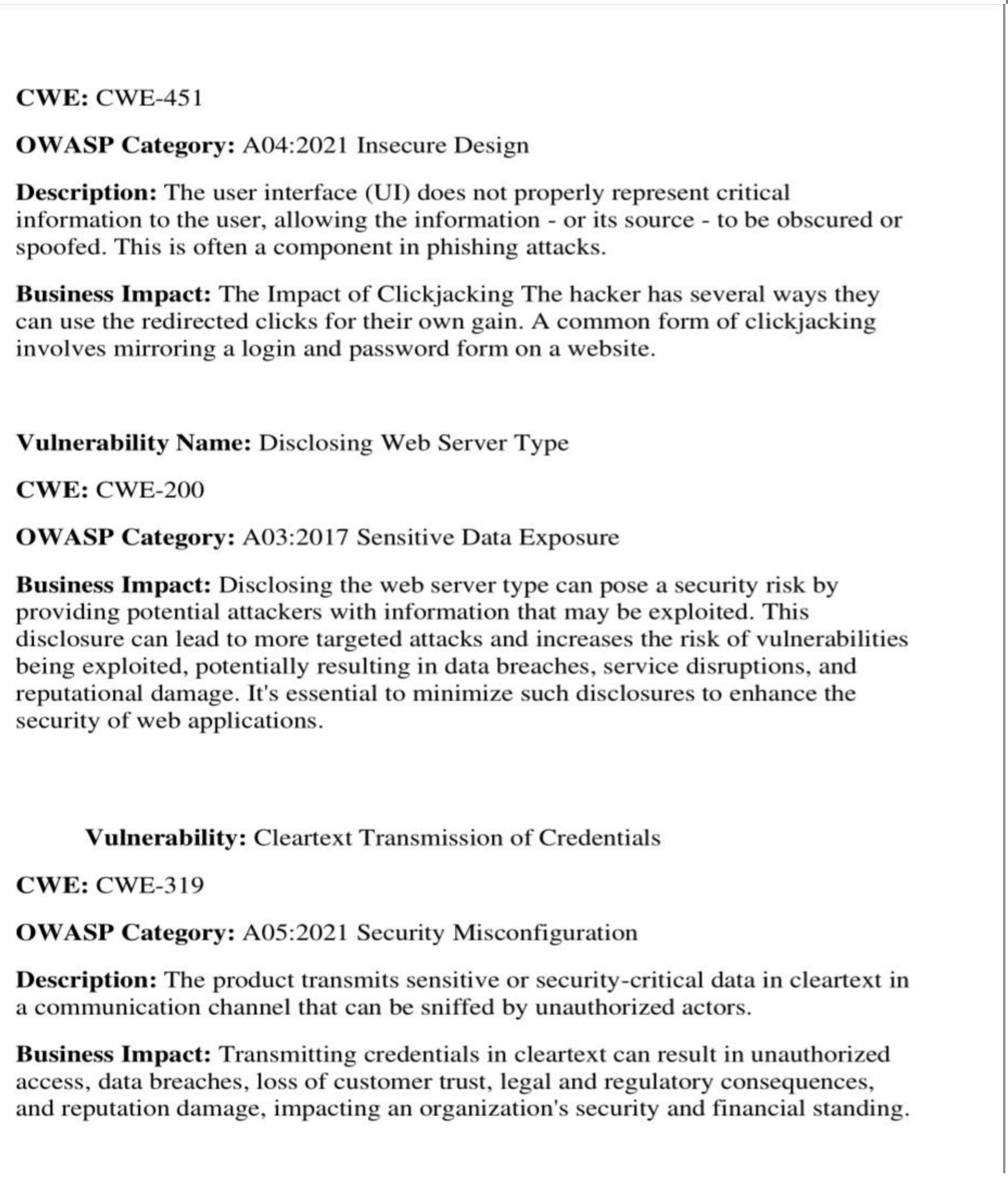
Vulnerability Name: PHP Unsupported Version

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.



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.

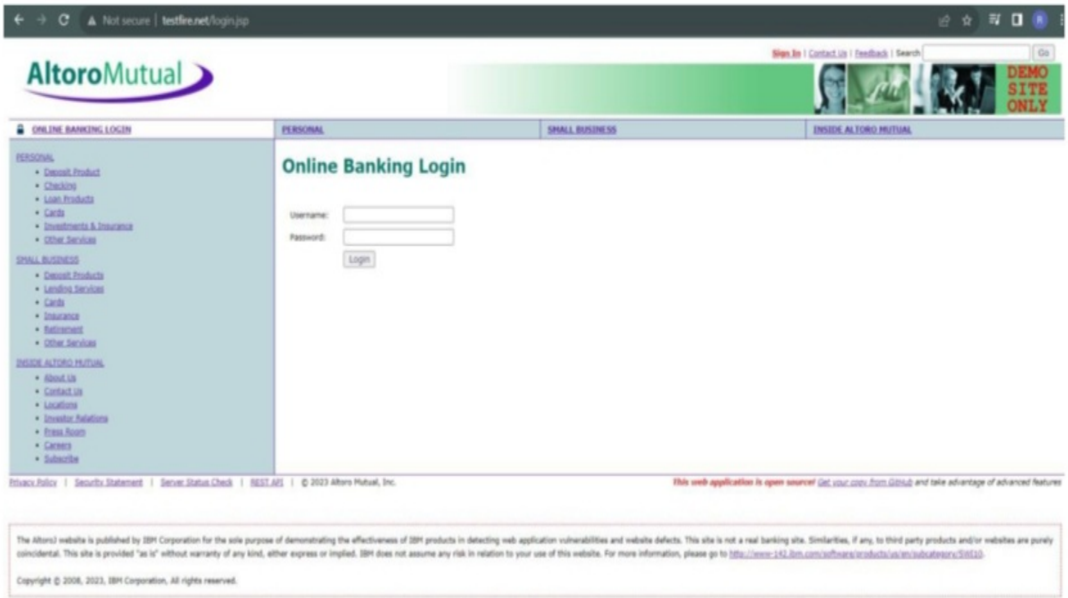
Business Impact: Transmitting credentials in cleartext can result in unauthorized access, data breaches, loss of customer trust, legal and regulatory consequences, and reputation damage, impacting an organization's security and financial standing.

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:

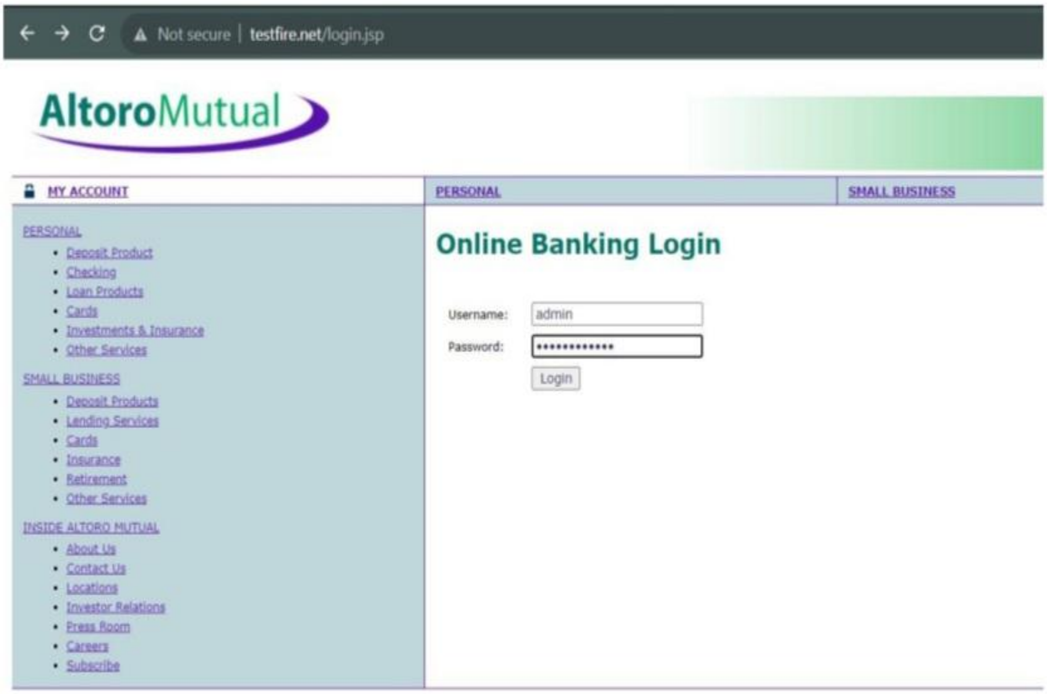
1. Access the URL.



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/SW010.

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

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



Online Banking Login

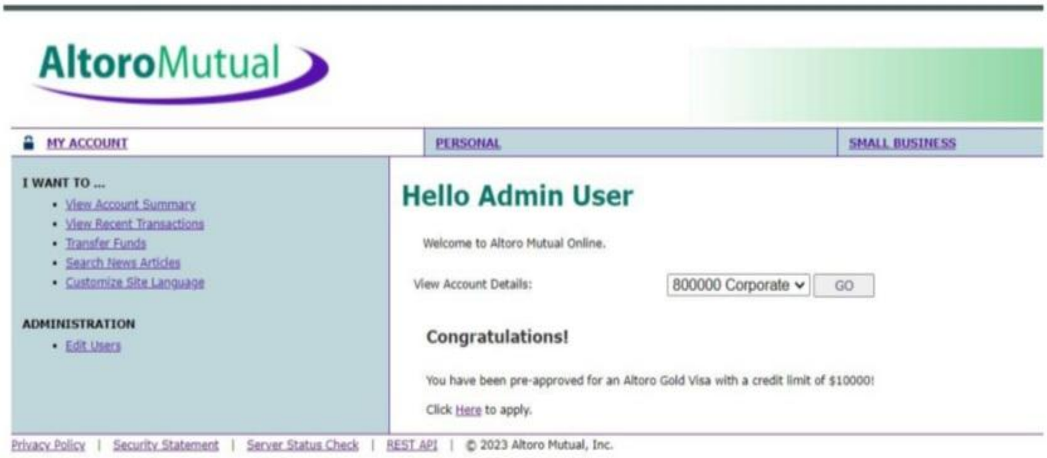
Username: admin

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

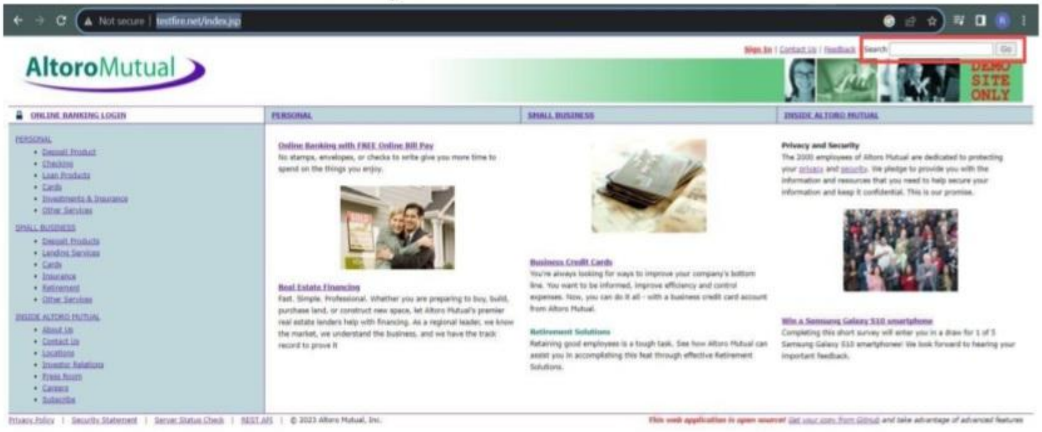
Description: The product does not neutralize or incorrectly neutralizes usercontrolled input for alternate script syntax.

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.

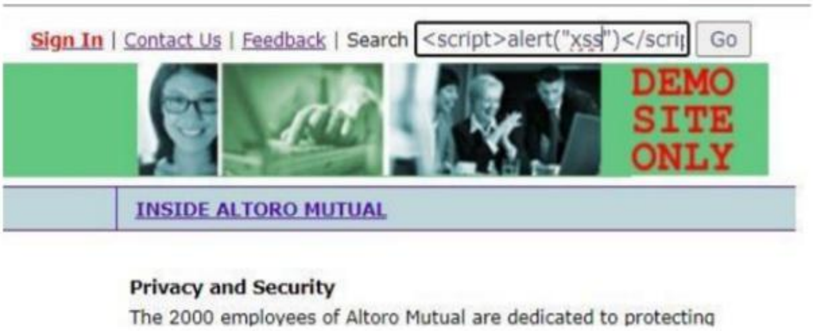
Privacy and Security
The 2000 employees of Altoro Mutual are dedicated to protecting your privacy and security. We pledge to provide you with the information and resources that you need to help secure your information and keep it confidential. This is our promise.

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.

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

2. Execute any javascript code.



Sign In | Contact Us | Feedback | Search <script>alert("xss")</scri Go

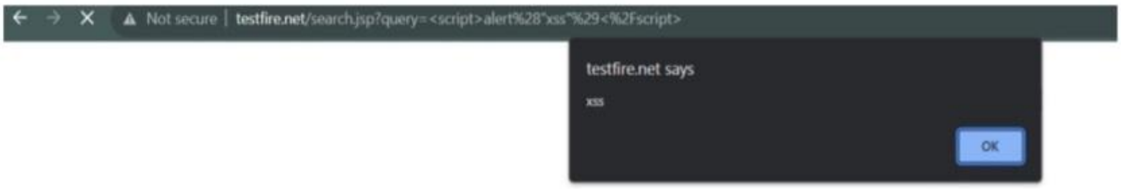
DEMO SITE ONLY

INSIDE ALTORO MUTUAL

Privacy and Security

The 2000 employees of Altoro Mutual are dedicated to protecting

i. Click on Go.



Not secure | testfire.net/search.jsp?query=<script>alert%28"xss"%29<%2Fscript>

testfire.net says

xss

OK

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

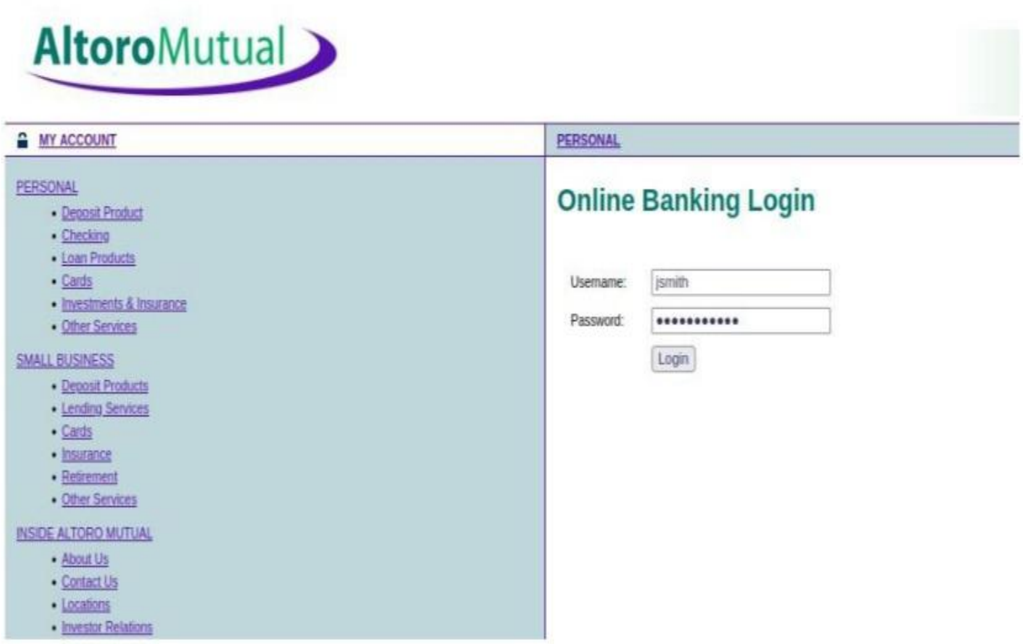
Description: The system's authorization functionality does not prevent one user from gaining access to another user's data or record by modifying the key value identifying the data.

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.

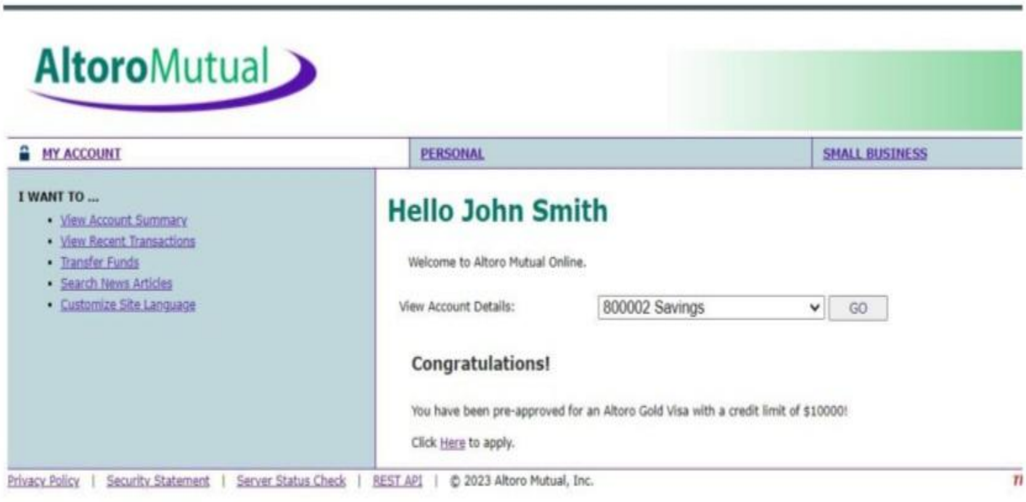


Online Banking Login

Username: jsmith

Password: ●●●●●●●●●●●●

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



Hello John Smith

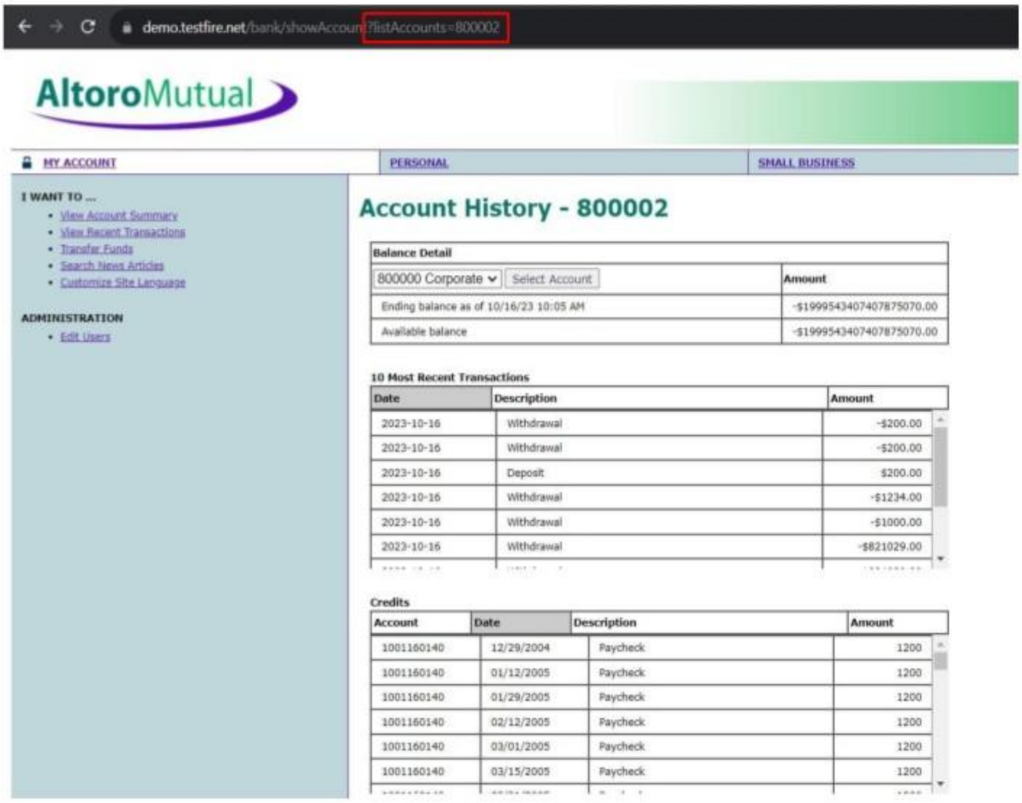
Welcome to Altoro Mutual Online.

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.



demo.testfire.net/bank/showAccount?listAccounts=800002

Account History - 800002

Balance Detail	
800000 Corporate	Amount
Ending balance as of 10/16/23 10:05 AM	-$19995434074078750 70.00
Available balance	-$1999543407407875070.00

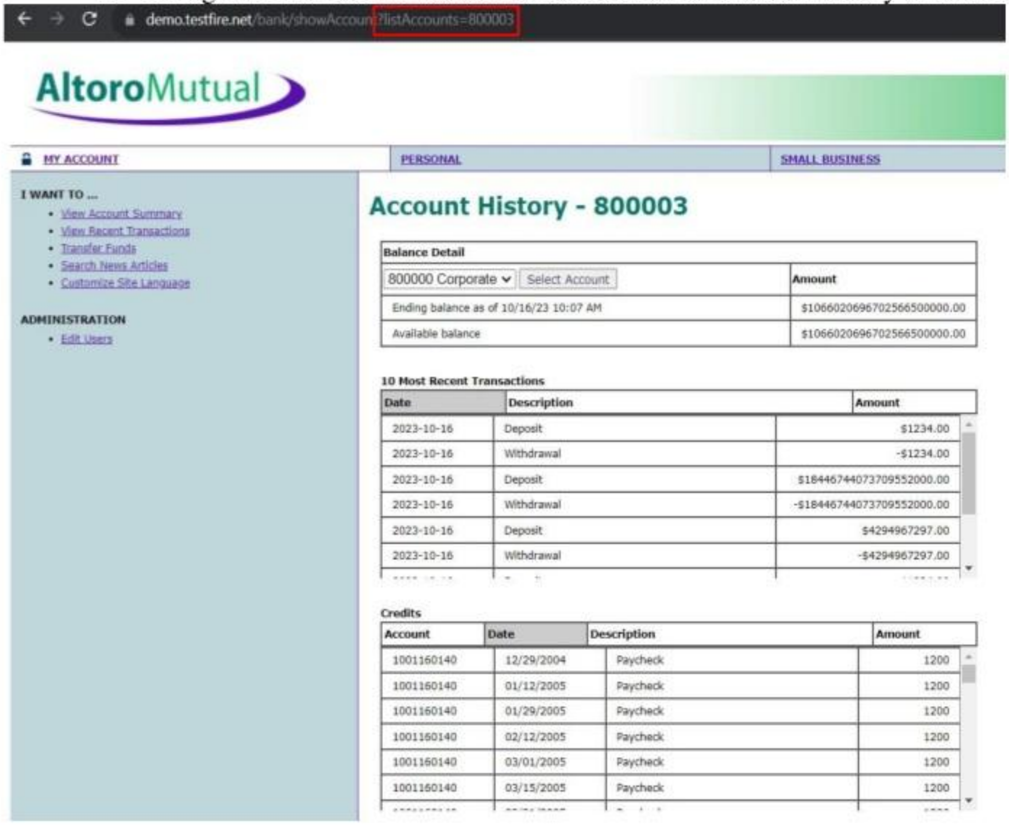
10 Most Recent Transactions

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.



demo.testfire.net/bank/showAccount?listAccounts=800003

Account History - 800003

Balance Detail	
800000 Corporate	Amount
Ending balance as of 10/16/23 10:07 AM	$1066020696702566500000.00
Available balance	$1066020696702566500000.00

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

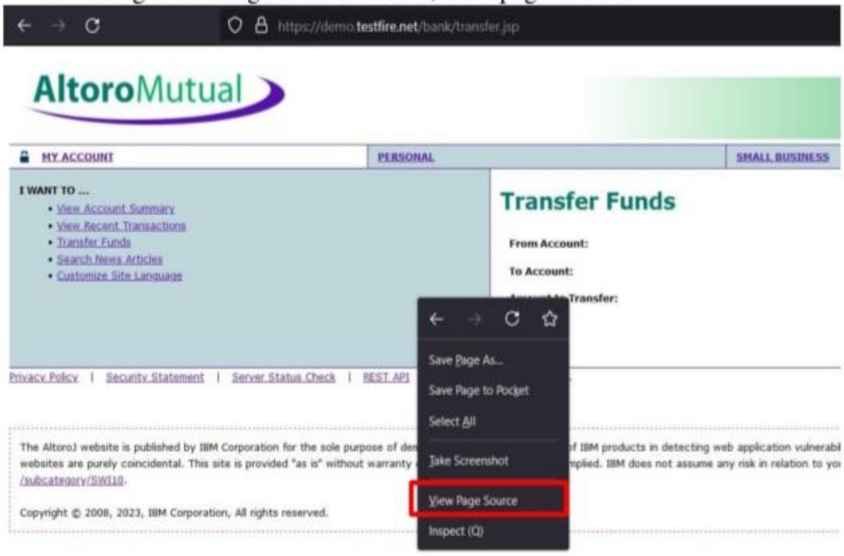
Description: The product transmits sensitive or security-critical data in cleartext in a communication channel that can be sniffed by unauthorized actors.

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:

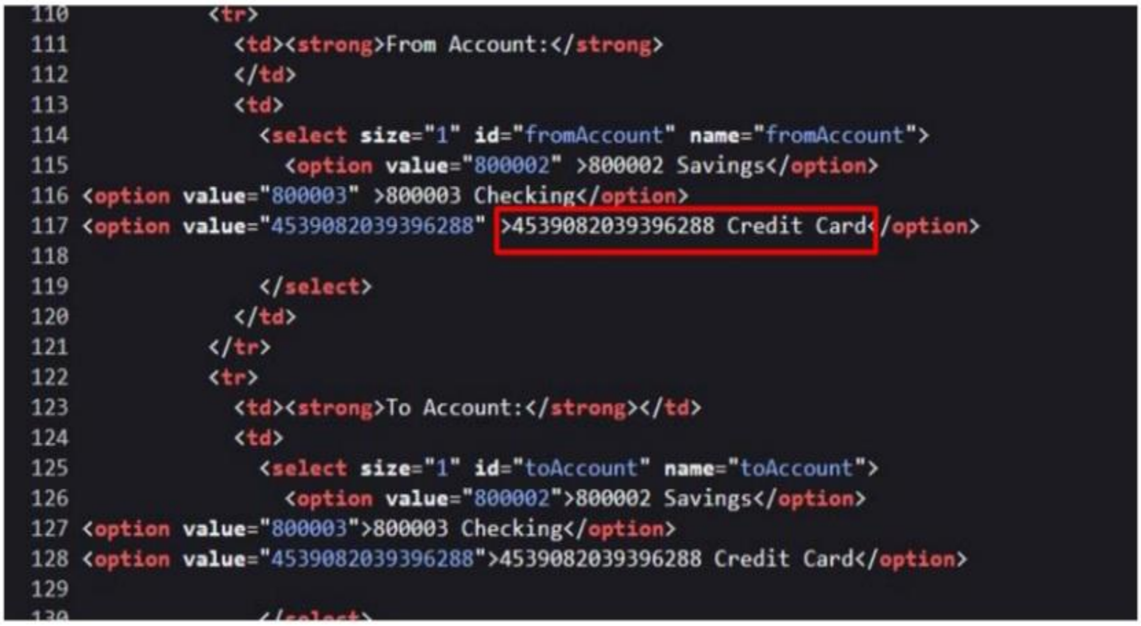
1. Navigate to the given URL. Then, view page source.



The AltoroJ website is published by IBM Corporation for the sole purpose of de f IBM products in detecting web application vulnerabi websites are purely coincidental. This site is provided "as is" without warranty plied. IBM does not assume any risk in relation to yo /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

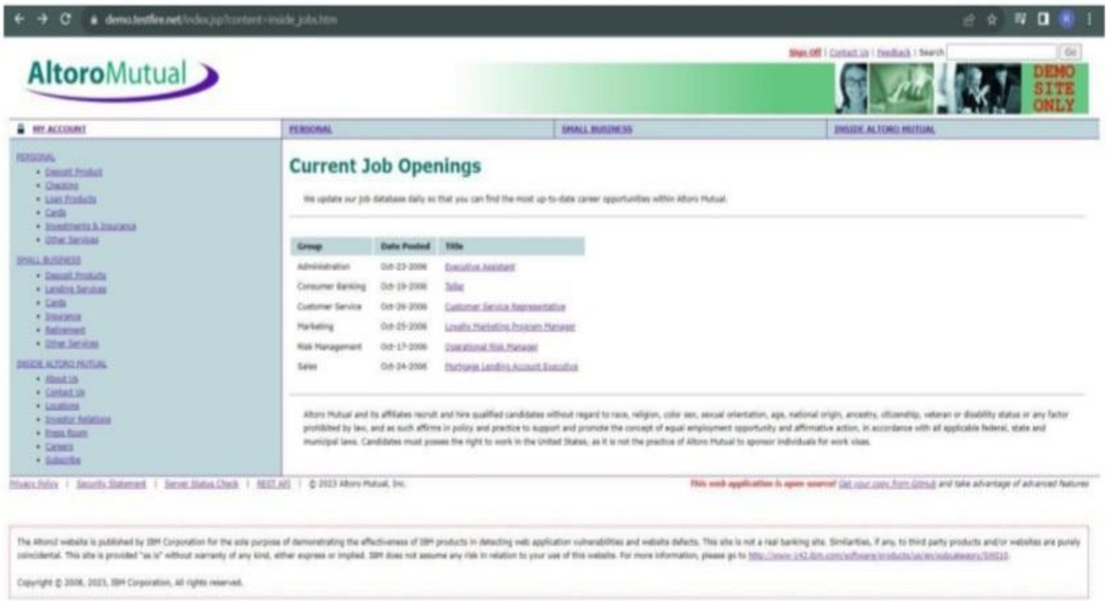
OWASP Category: A03:2017 Sensitive Data Exposure.

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.

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 Altoro 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/SW110.

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

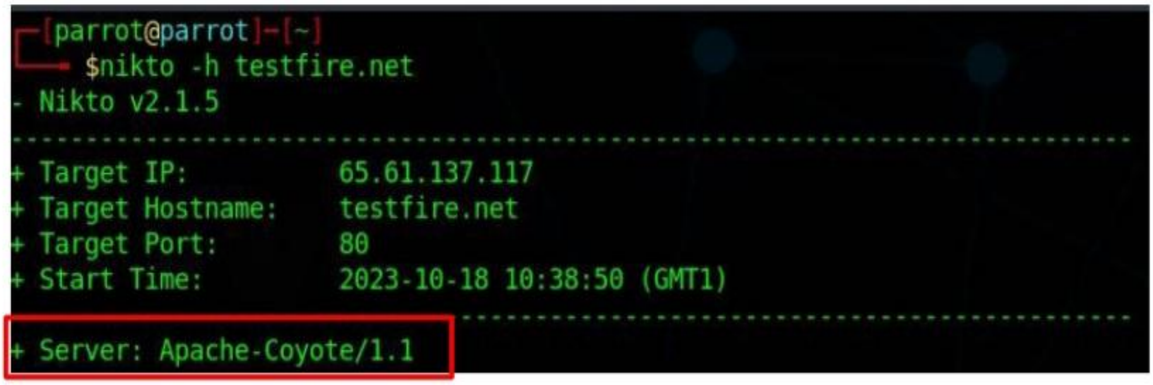
OWASP Category: A06:2021 Vulnerable and Outdated Components

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

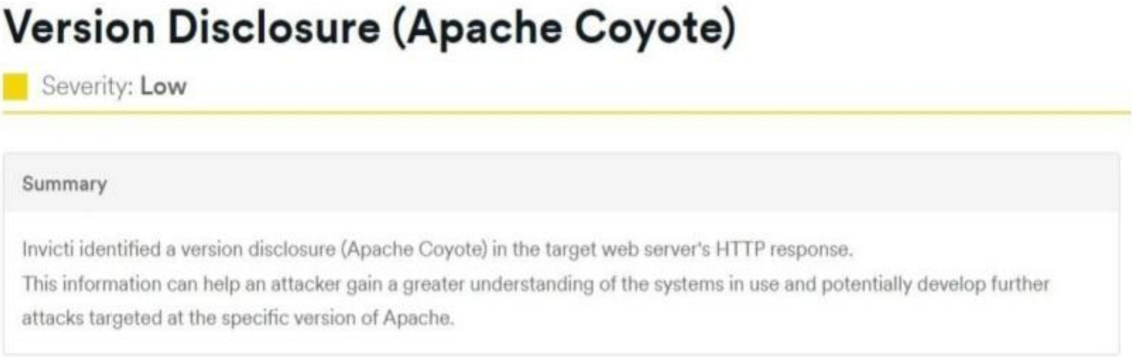
Vulnerability Path: https://testfire.net/bank/transfer.jsp **Steps to Reproduce:**

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

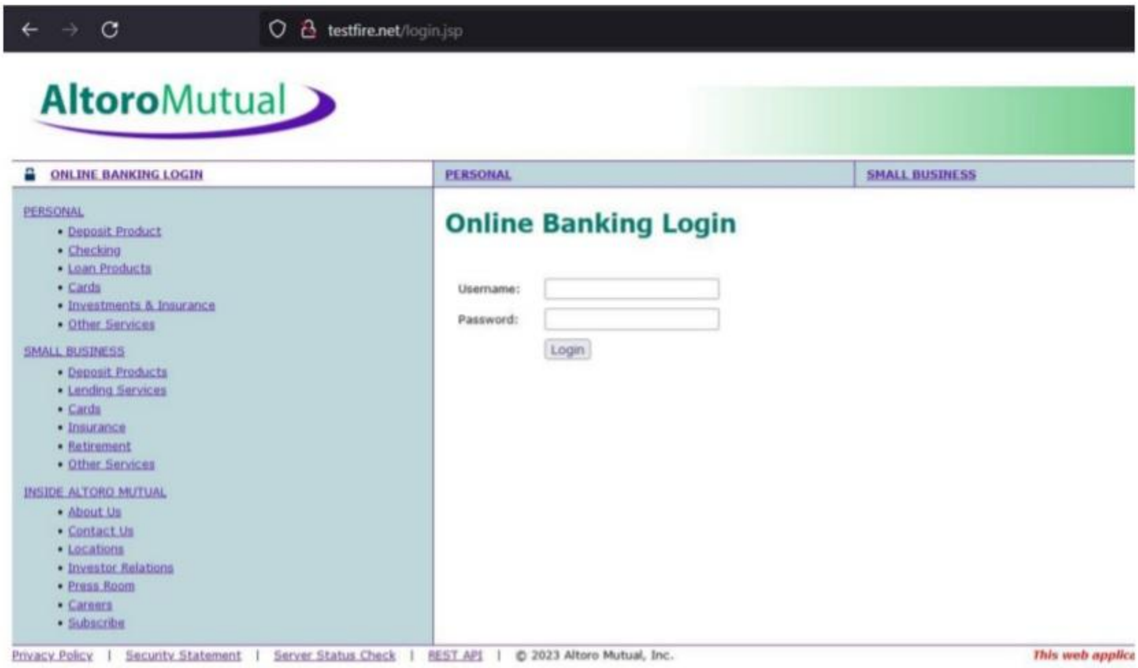
Description: The product transmits sensitive or security-critical data in cleartext in a communication channel that can be sniffed by unauthorized actors.

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.

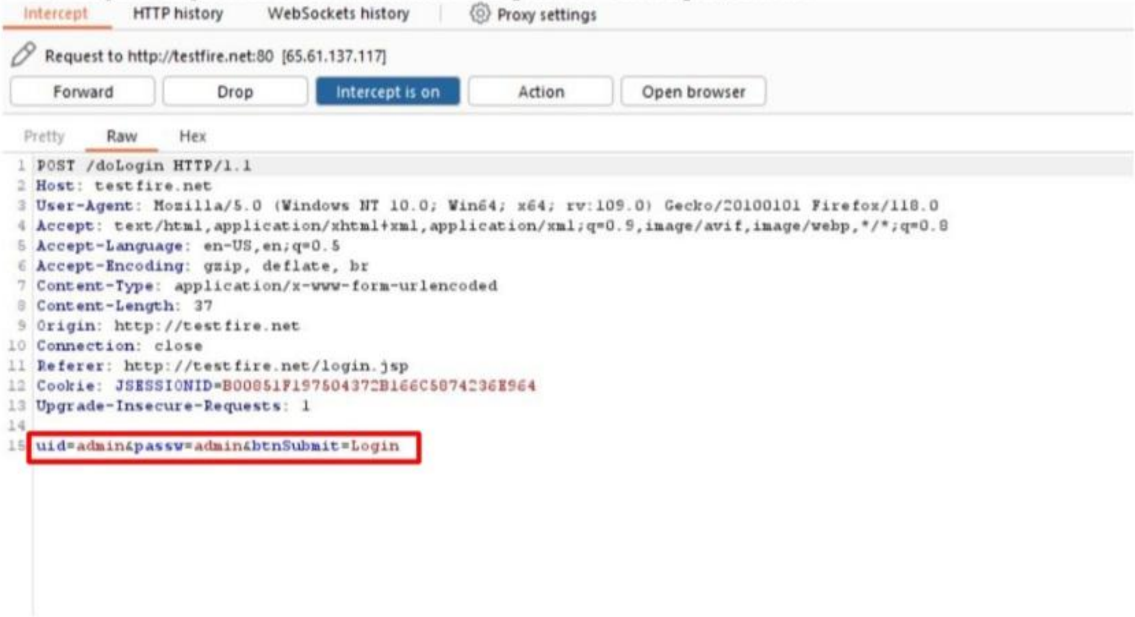
Vulnerability Path: http://testfire.net/login.jsp

Steps to Reproduce:

1. Navigate to the above mentioned URL.



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

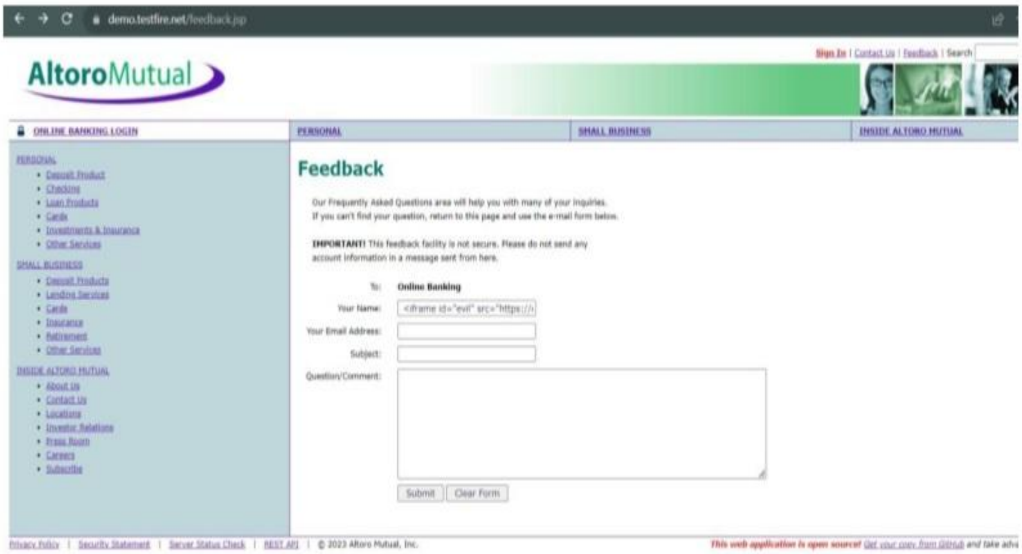
Description: The user interface (UI) does not properly represent critical information to the user, allowing the information – or its source – to be obscured or spoofed. This is often a component in phishing attacks.

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**

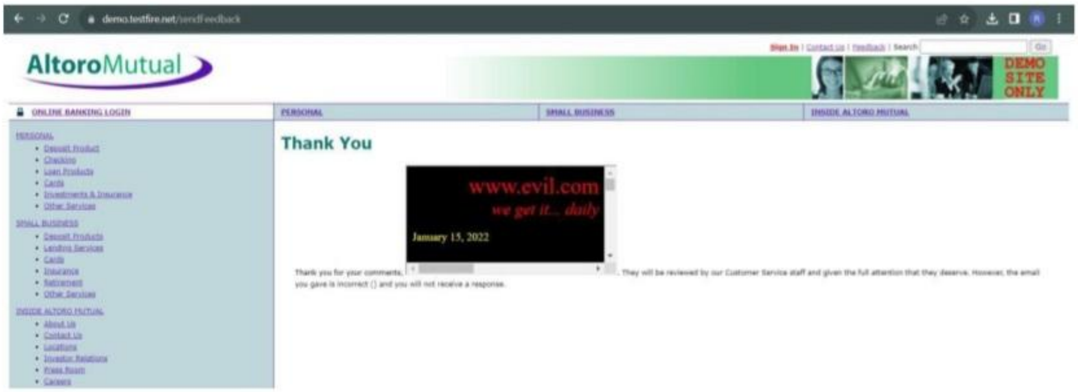
Your Name: <iframe id="evil" src="https://

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

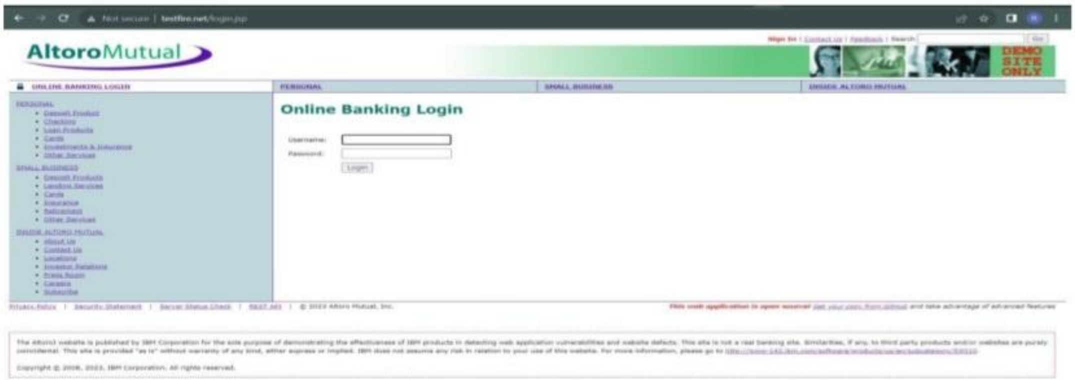
OWASP Category: A01:2021 Broken Access Control

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:

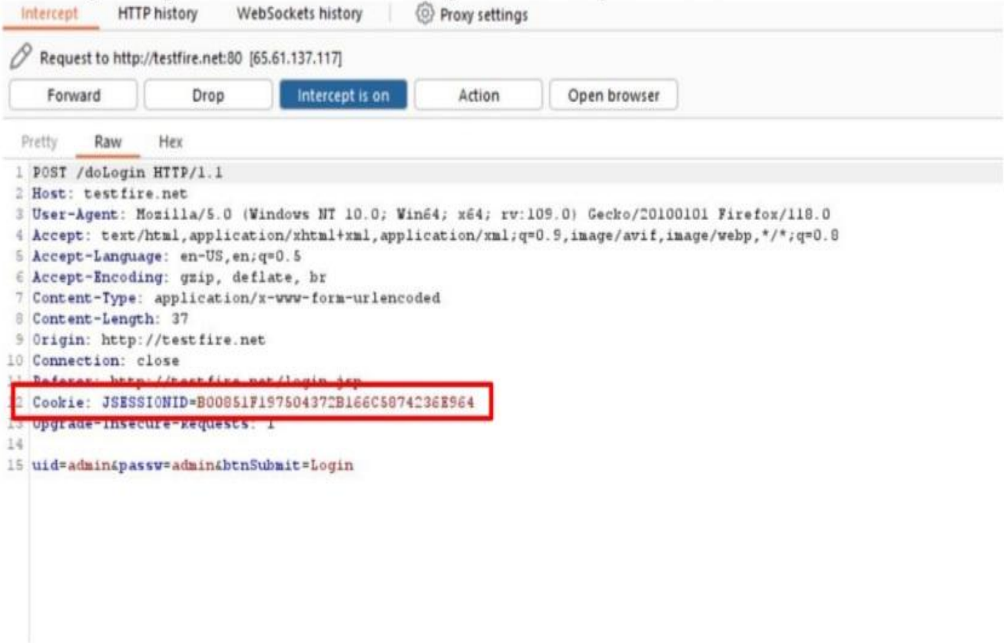
Password:

Login

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

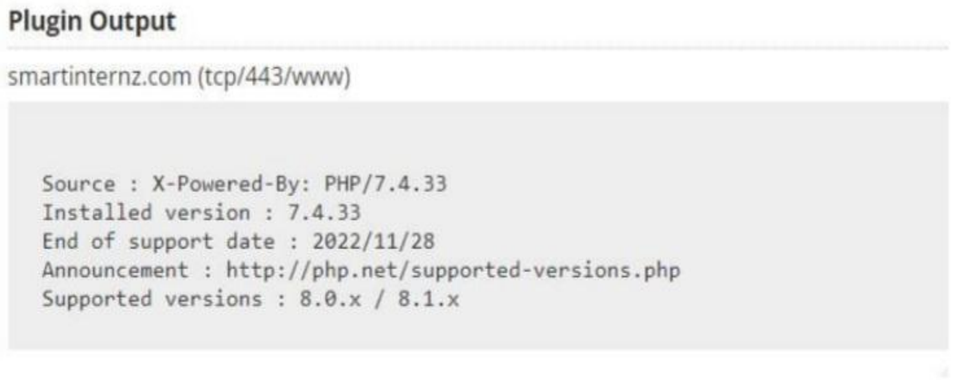
Description: According to its version, the installation of PHP on the remote host is no longer supported. As a result, it is likely to contain security vulnerabilities.

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

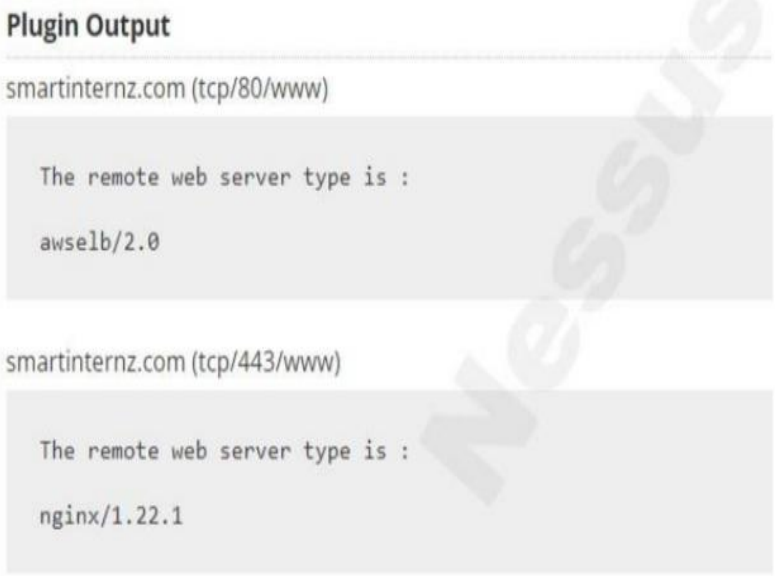
OWASP Category: A04:2021 Insecure Design

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



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

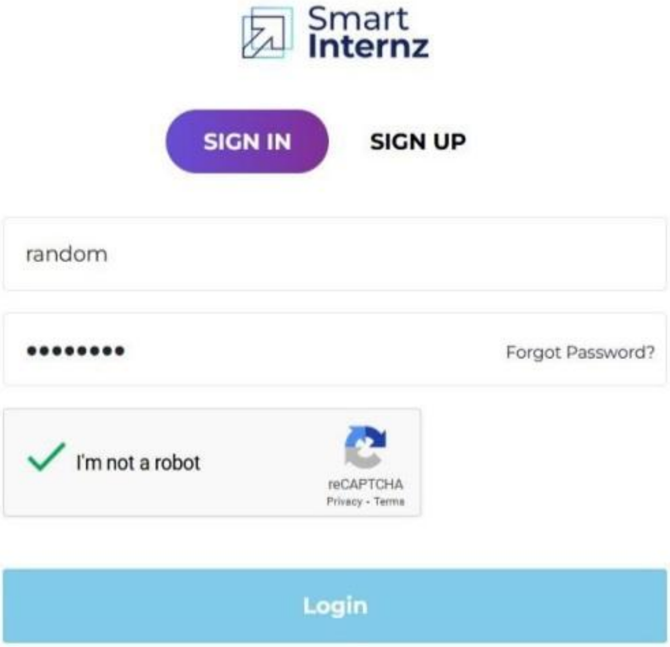
Description: The product transmits sensitive or security-critical data in cleartext in a communication channel that can be sniffed by unauthorized actors.

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:

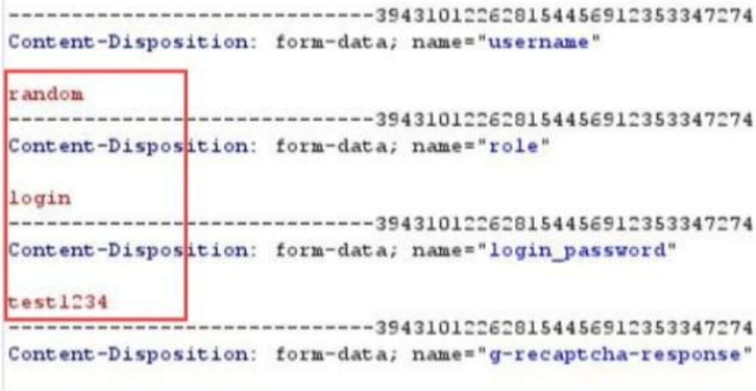
1. Navigate to the above-mentioned URL and login.



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

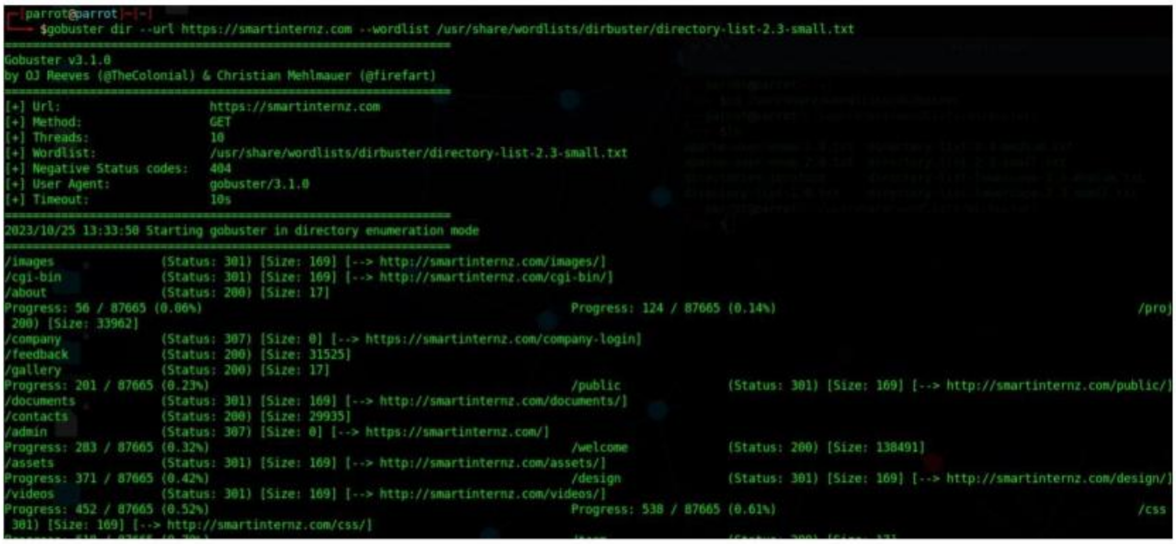
Severity: low

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.

The above image is showing relative information about the main important branches of cyber application of AI-based methods. All these branches are related to solving cybersecurity issues present in the system. From this, the first branch is malware detection, the second one is network intrusion, the third one is phishing spam detection, and others. All these branches contain their own sub branches. These sub-branches are necessary to solve relative cybersecurity problems. By using AI-based methods the cybersecurity issues can be solved easily. The malware detection is divided into two important types. These types include PC malware and Android malware. Both these malware are strong and based on the required software because PC and mobile contains two different types of operating systems. However, the network intrusion is divided into two main types include intrusion detection with AI-based technology and Anomaly detection with AI-based technology. On the other hand, there are four main types of phishing/span detection. It includes web phishing detection, spam on social networks, mail phishing detection and spam mail. All these detections were operated through AI-based applications and mainly applied for the internet services [2].

Automating Routine Tasks

It is simple through machine learning and artificial intelligence technologies to automate routine cybersecurity tasks. It can be done through leveraging their ability to process and analyze the large volume of data efficiently. Its working is given below

Log Analysis

Some security logs taken from different sources like firewalls, antivirus software, and intrusion detection systems that will generate vast amount of data. Therefore, the ML and AI algorithms will be applied because they can parse and analyze these logs in real-time, identifying anomalies, and patterns. With such automation, the need of manual log review will be eliminated and it will save time and minimize risk of human errors [5].

User Authentication

With the AI-driven systems, the organizations can automate user authentication processes by analyzing user behavior and device characteristics. It means, if the user behavior is deviating significantly from the typical patterns, the system will trigger multi-factor authentication or flag the activity for further investigation process [8].

Patch Management

ML and AI is also assisting in automating patch management by prioritizing various vulnerabilities based on its potential impact and severity level on the organization. These vulnerability scanners are powered by AI and they can identify unpatched systems, and provide recommendations about most critical patches for immediate deployment [6].

Phishing Detection

The ML models can detect automatically all phishing emails by analyzing sender behavior, email content, and user interaction patterns. Some suspicious email can be flagged or quarantined for review by reducing the likelihood of successful phishing attacks [9].

Improving Threat Detection

AI and ML can easily enhance the threat detection capabilities through applying these techniques

Pattern Recognition

It is simple for ML patterns to identify known attack patterns that are present in large and complex datasets. Through training on the historical data, it is simple for the algorithms to recognize the signatures of different malware strains and attack vectors [3]. Behavioral Analysis: Due to advancement in AI-Driven technologies, they can easily identify known attack patterns even in complex dataset. Secondly, through deviations from established baselines will trigger alerts, enabling detection and minimize threats from attackers.

Enabling Predictive Analysis

The Predictive Analysis in cybersecurity leverages ML and AI to antedate and prepare for any security breaches in the system.

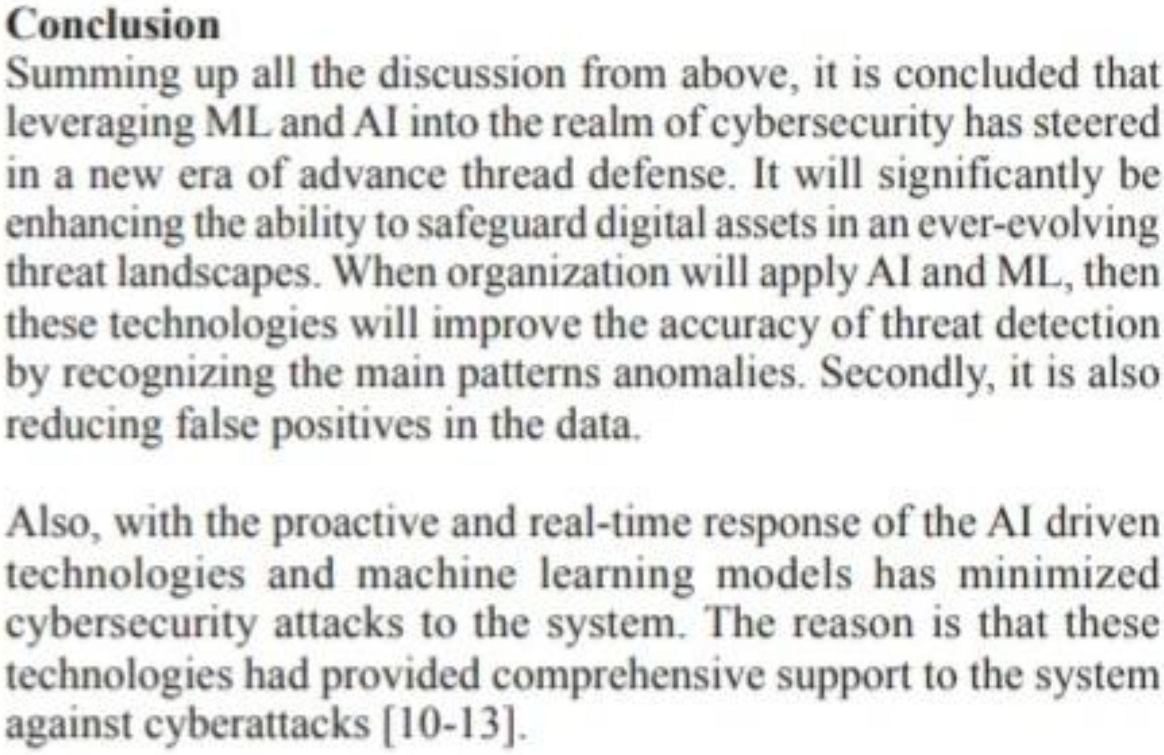
Historical Data Analysis

It is possible for machine learning models to analyze the historical security incident data by identifying trends and patterns linked with past attacks. Through recognizing organizations, and commonalities, the system can predict potential future trends [1].

Behavioral Predictions

Moreover, the AI-driven systems can provide prediction regarding the system behavior and give prediction based on the historical data.

Vulnerability Assessment: AI can predict all vulnerabilities easily based on known software weakness and historical exploration patterns. Through understanding where vulnerabilities are likely to emerge, the organizations can emerge them proactively [7].



Conclusion

Summing up all the discussion from above, it is concluded that leveraging ML and AI into the realm of cybersecurity has steered in a new era of advance thread defense. It will significantly be enhancing the ability to safeguard digital assets in an ever-evolving threat landscapes. When organization will apply AI and ML, then these technologies will improve the accuracy of threat detection by recognizing the main patterns anomalies. Secondly, it is also reducing false positives in the data.

Also, with the proactive and real-time response of the AI driven technologies and machine learning models has minimized cybersecurity attacks to the system. The reason is that these technologies had provided comprehensive support to the system against cyberattacks [10-13].

Real-time intelligence is a rapidly growing field with significant potential for various industries and applications. Organizations can analyze vast amounts of data in real-time and make informed decisions by leveraging technologies such as machine learning, AI, IoT, edge computing, and predictive analytics.Cyber security is one of the most important aspects of the fast-paced growing digital world. The threats of it are hard to deny, so it is crucial to learn how to defend from them and teach others how to do it too.

VS Code:

- Download: https://code.visualstudio.com/download
- Installation guide: https://code.visualstudio.com/docs/setup/setup-overview

Python :

- Download link: https://python.org/downloads/

Kali Linux :

- Download link :https://www.kali.org/get-kali/#kali-platforms

Virtual Box :

- Download link: https://www.virtualbox.org/wiki/Downloads

THE END