Malware detection and classification platform

Team Id

2.3

Team Name

Virus Vigilantes

Team Members

Sanjaykrishnaa R S

Lakkireddy Tharuneswara Reddy

Raahul M

Stuti Maitra Sarkar

Abstract:

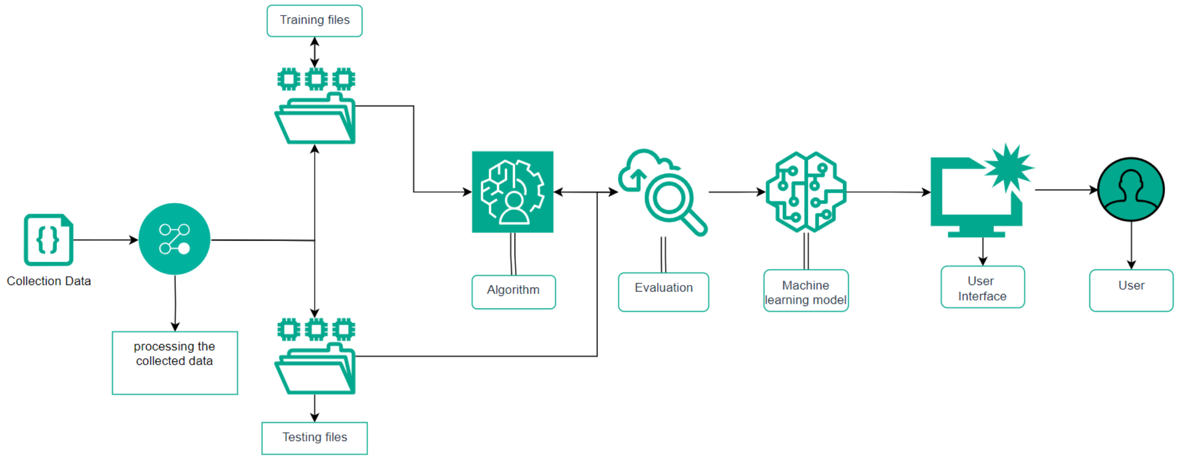
In today's dynamic digital landscape, safeguarding critical digital assets is of paramount importance for organizations. The escalating presence of malicious software necessitates the development of cutting-edge systems proficient in accurately identifying and categorizing these threats. This project proposes an advanced framework for "Malware Detection and Classification," leveraging the capabilities of artificial intelligence (AI).

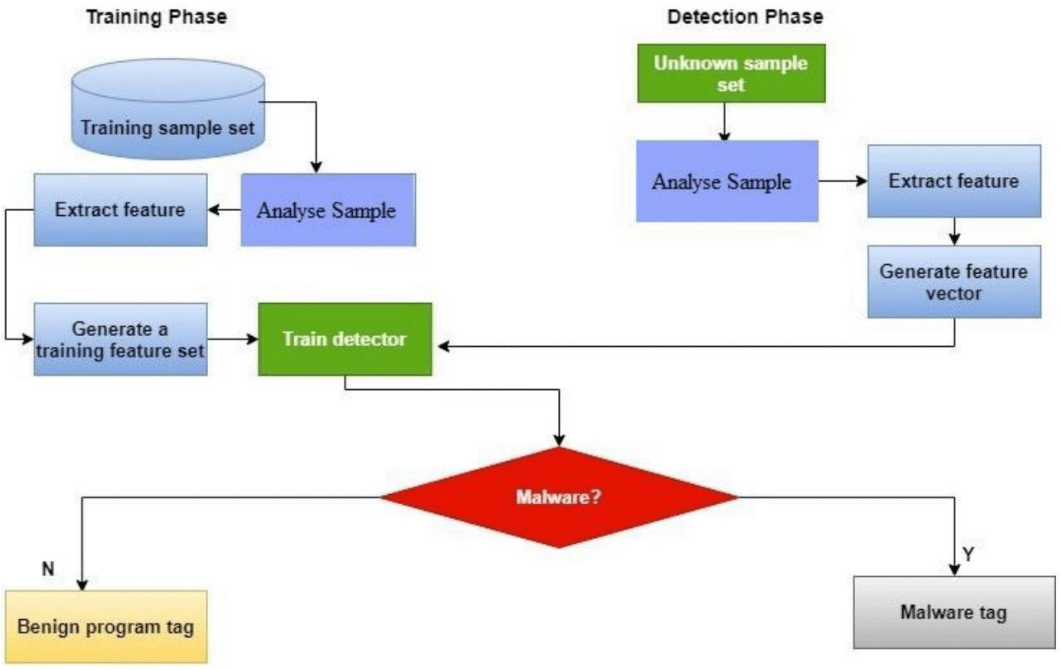
This comprehensive framework encompasses several key components:

1. **Data Collection and Preprocessing:**
    - Gather a diverse and extensive dataset comprising various malware samples, ensuring representation of different malware families and their characteristics.
    - Preprocess the data to extract relevant features, normalize the data, and prepare it for training AI models.
2. **Machine Learning and Deep Learning Models:**
    - Employ a variety of machine learning and deep learning models, such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Long Short-Term Memory (LSTM) networks.
    - Train these models on the pre-processed dataset to learn and generalize patterns associated with different types of malware.
3. **Feature Extraction and Selection:**
    - Extract meaningful features from the malware samples using techniques like static and dynamic analysis.
    - Select and prioritize the most informative features to enhance the accuracy and efficiency of the detection and classification models.
4. **Pattern Recognition and Behavioural Analysis:**
    - Develop algorithms that can identify patterns within malware samples to aid in their accurate categorization.
    - Analyse the behaviour of malware to identify deviations from normal behaviour, a crucial aspect in detecting sophisticated and evolving malware.
5. **Real-Time Monitoring and Incident Response:**
    - Implement real-time monitoring of network traffic and system behaviour to detect and respond promptly to potential malware threats.
    - Employ automated incident response mechanisms to mitigate the impact of identified threats and prevent their spread within the network.
6. **Adaptability and Continuous Learning:**

- Incorporate mechanisms for the AI models to continuously adapt and learn from new malware samples and emerging threat patterns.
- Utilize reinforcement learning and periodic model updates to ensure the system remains robust and effective against evolving malware.

By integrating these components into a unified and coherent framework, this project aims to provide organizations with a powerful tool to bolster their cybersecurity posture and effectively counter the evolving threat landscape. The application of AI in malware detection and classification holds the potential to significantly enhance the resilience and efficacy of organizations in safeguarding their digital assets against malicious adversaries.





Stage 1

Overview:

Vulnerability testing, often referred to as website vulnerability assessment or web application security testing, is a critical process for identifying and mitigating security weaknesses in a website. This process helps website owners and administrators ensure that their websites are protected against potential threats and vulnerabilities. Here's an overview of vulnerability testing for websites:

1. **Importance of Vulnerability Testing**: Websites are frequent targets for cyberattacks, and vulnerabilities in web applications can be exploited to steal sensitive data, deface the site, or compromise the security of users. Vulnerability testing is crucial for the following reasons:
   - **Risk Mitigation**: It helps mitigate the risk of security breaches and data theft.
   - **Compliance**: Many regulatory standards and industry best practices require regular vulnerability testing.
   - **Reputation Protection**: A breach can harm a website's reputation, so testing helps maintain user trust.
   - **Legal and Financial Consequences**: Failing to secure a website can lead to legal and financial consequences.
2. **Types of Vulnerability Testing**:
   - **Automated Scanning**: Automated vulnerability scanners like Nessus, OpenVAS, and OWASP ZAP can detect known vulnerabilities and common misconfigurations in web applications and servers.
   - **Manual Testing**: Security professionals perform manual testing to identify complex or less common vulnerabilities that automated tools may miss. This includes in-depth analysis, code review, and penetration testing.
   - **Dynamic Application Security Testing (DAST)**: DAST tools test running applications from the outside, simulating attacks and assessing their vulnerabilities. This approach is often used to find issues like SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF).
   - **Static Application Security Testing (SAST)**: SAST tools analyze the source code or binary code of an application to identify vulnerabilities at the code level, such as insecure coding practices, known vulnerabilities in libraries, and more.
   - **Interactive Application Security Testing (IAST)**: IAST tools combine elements of DAST and SAST, running tests during application runtime

but also analyzing code. This approach provides real-time feedback during testing.

  - **Manual Penetration Testing**: Ethical hackers perform controlled attacks on a website to discover vulnerabilities, often going beyond automated tools to find complex issues.

3. **Common Vulnerabilities Tested**: Vulnerability testing focuses on finding security issues like:
    - **SQL Injection**: Attackers can manipulate database queries to access or modify data.
    - **Cross-Site Scripting (XSS)**: Malicious scripts are injected into web pages, affecting users' browsers.
    - **Cross-Site Request Forgery (CSRF)**: Unauthorized actions are taken on behalf of an authenticated user.
    - **Broken Authentication and Session Management**: Flaws that allow unauthorized access to user accounts.
    - **Insecure Deserialization**: Attacker-controlled data is deserialized, leading to remote code execution.
    - **Security Misconfigurations**: Poorly configured servers, applications, or databases.
    - **Sensitive Data Exposure**: Inadequate protection of sensitive information.
4. **Testing Process**:
    - **Planning**: Define the scope, objectives, and testing methodology. Determine the tools and resources needed.
    - **Scanning**: Run automated and/or manual tests to identify vulnerabilities.
    - **Analysis**: Evaluate the test results to determine the severity and impact of each vulnerability.
    - **Reporting**: Generate comprehensive reports that detail the vulnerabilities found, their risk level, and recommendations for mitigation.
    - **Mitigation**: Implement fixes and improvements to address the identified vulnerabilities.
    - **Retesting**: Verify that the vulnerabilities have been successfully mitigated and the website is now secure.

5. **Regular Testing**: Vulnerability testing is not a one-time activity. It should be performed regularly, especially after updates or changes to the website, to ensure ongoing security.

Website vulnerability testing is an essential component of maintaining a secure online presence, and it should be part of any organization's security strategy. It helps protect both the website and the sensitive data it handles while ensuring the trust and confidence of users and customers.

Vulnerability report

Practice website chosen: testfire.net

S.no	**Vulnerability**	**CWE**
1.	Cross-Site Scripting (Stored)	CWE-79
2.	Html injection	CWE-80
3.	No Session Management	CWE-384
4.	Admin Login SQL Injection	CWE-284
5.	Default Credentials	CWE-1392
6.	Clickjacking (Improper Restriction of Rendered UI Layers or Frames)	CWE-1021
7.	Anti-CSRF Token missing	CWE-352
8.	Web Server Transmits Cleartext Credentials	CWE- 319
9.	Insecure Http flag	CWE-1004
10.	Password field autocomplete	CWE-522

1. Cross-Site Scripting (Stored)

CWE: CWE-79

OWASP Category: A03:2021 – Injection

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

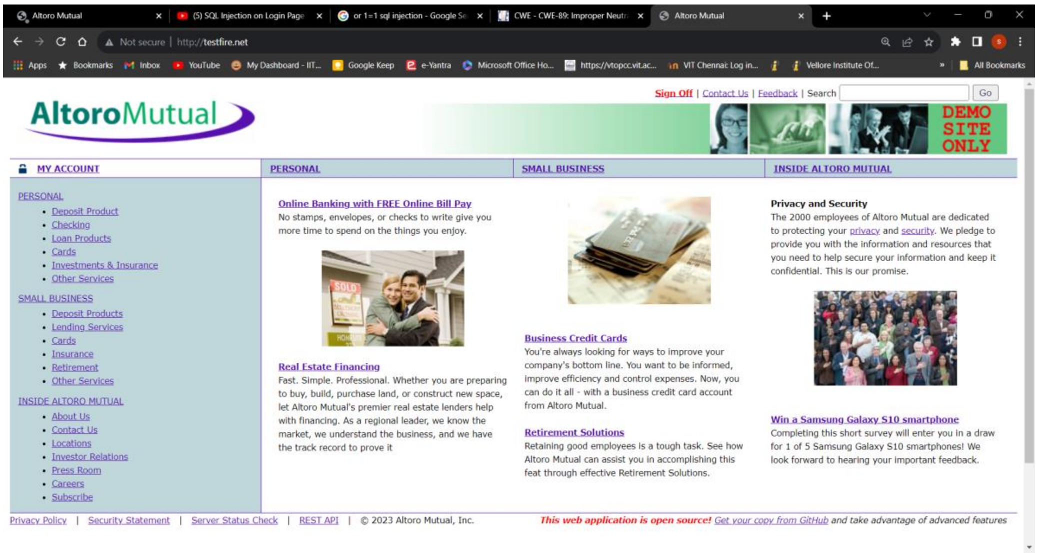
Business Impact: The most common attack performed with cross-site scripting involves the disclosure of information stored in user cookies. Typically, a malicious user will craft a client-side script, which -- when parsed by a web browser -- performs some activity (such as sending all site cookies to a given E-mail address). This script will be loaded and run by each user visiting the web site. Since the site requesting to run the script has access to the cookies in question, the malicious script does also.

Vulnerability Path : http://testfire.net

Vulnerability Parameter: http://testfire.net/search.jsp?query=

Steps to Reproduce :

Step 1. Access the 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.

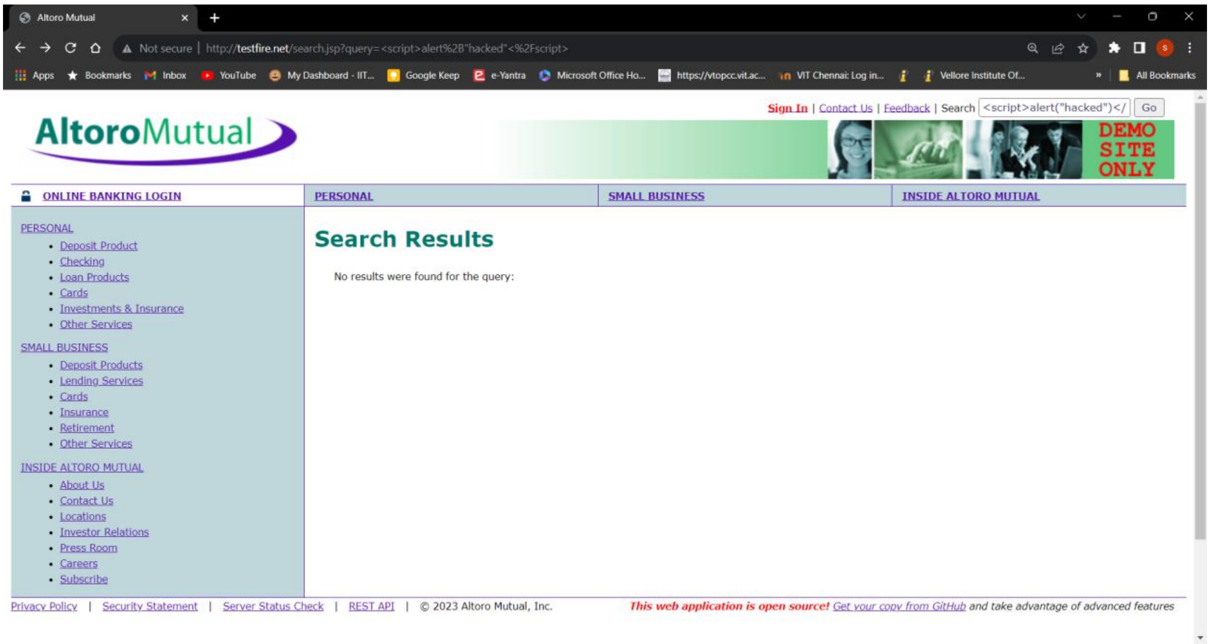
Retirement Solutions
Retaining good employees is a tough task. See how Altoro Mutual can assist you in accomplishing this feat through effective Retirement Solutions.

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.

© 2023 Altoro Mutual, Inc.   *This web application is open source! Get your copy from GitHub and take advantage of advanced features*

Step 2: enter the script in the search box <script>alert"hacked"</script>

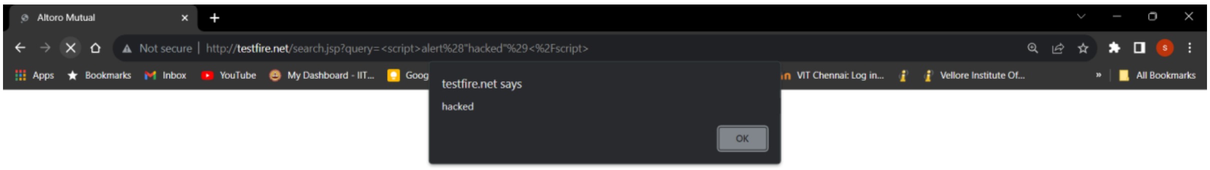


Search Results

No results were found for the query:

© 2023 Altoro Mutual, Inc.   *This web application is open source! Get your copy from GitHub and take advantage of advanced features*

Step 3:-after entering the script content like” hacked” u will find the dialogue box as shown below.



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

testfire.net says

hacked

Recommendation:

Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.

Examples of libraries and frameworks that make it easier to generate properly encoded output include Microsoft's Anti-XSS library, the OWASP ESAPI Encoding module, and Apache Wicket.

2. Html injection

CWE: CWE-80

OWASP Category: A03:2021 – Injection

Description: The product receives input from an upstream component, but it does not neutralize or incorrectly neutralizes special characters such as "<", ">", and "&" that could be interpreted as web-scripting elements when they are sent to a downstream component that processes web pages.

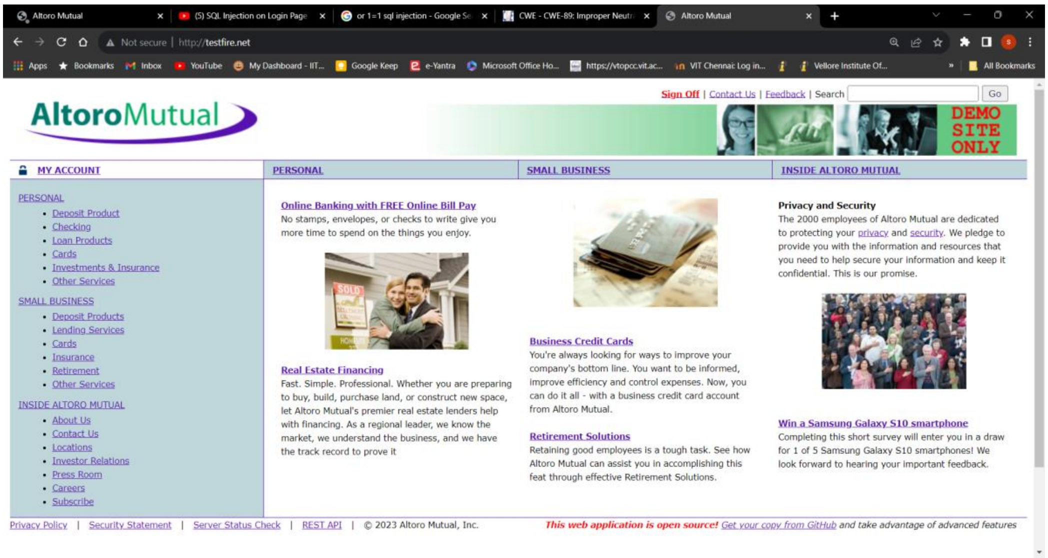
Business Impact: In some circumstances it may be possible to run arbitrary code on a victim's computer when cross-site scripting is combined with other flaws.

Vulnerability Path : http://testfire.net

Vulnerability Parameter: http://testfire.net/search.jsp?query=

Steps to Reproduce :

Step 1. Access the URL



Not secure | http://testfire.net

Sign Off | Contact Us | Feedback | Search

AltoroMutual

MY ACCOUNT | PERSONAL | SMALL BUSINESS | INSIDE ALTORO MUTUAL

PERSONAL
- Deposit Product
- Checking
- Loan Products
- Cards
- Investments & Insurance
- Other Services

SMALL BUSINESS
- Deposit Products
- Lending Services
- Cards
- Insurance
- Retirement
- Other Services

INSIDE ALTORO MUTUAL
- About Us
- Contact Us
- Locations
- Investor Relations
- Press Room
- Careers
- Subscribe

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.

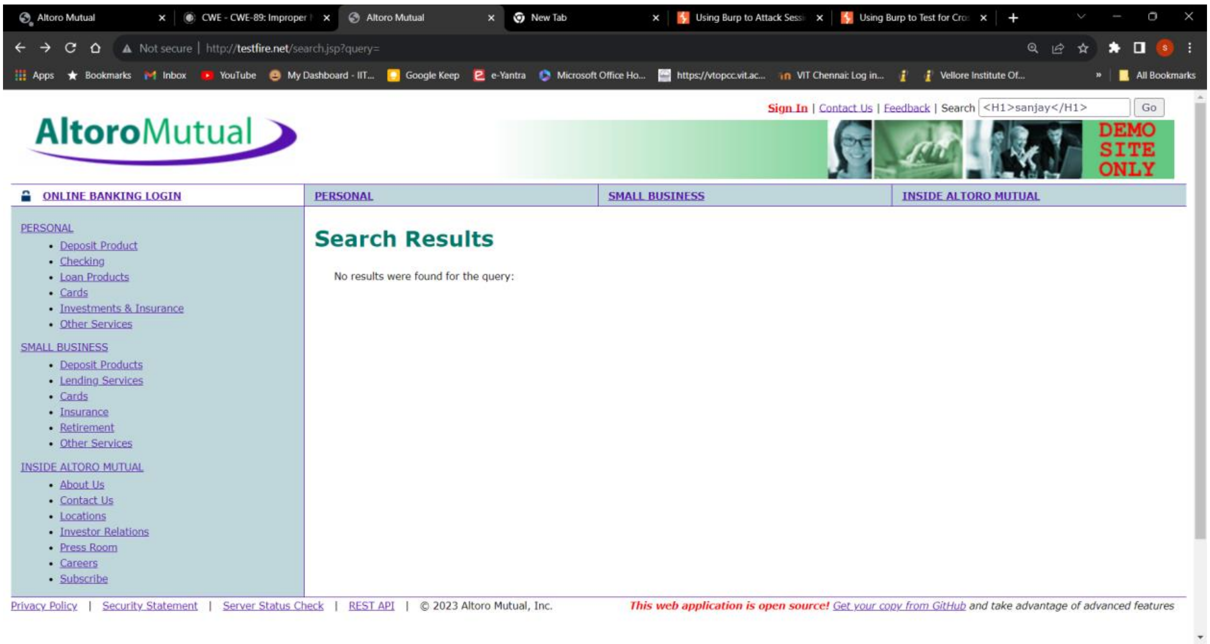
Privacy and Security
The 2000 employees of Altoro Mutual are dedicated to protecting your privacy and security. We pledge to provide you with the information and resources that you need to help secure your information and keep it confidential. This is our promise.

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

Step 2: type the html script in the search box



Not secure | http://testfire.net/search.jsp?query=

Sign In | Contact Us | Feedback | Search <H1>sanjay</H1>

AltoroMutual

ONLINE BANKING LOGIN | PERSONAL | SMALL BUSINESS | INSIDE ALTORO MUTUAL

PERSONAL
- Deposit Product
- Checking
- Loan Products
- Cards
- Investments & Insurance
- Other Services

SMALL BUSINESS
- Deposit Products
- Lending Services
- Cards
- Insurance
- Retirement
- Other Services

INSIDE ALTORO MUTUAL
- About Us
- Contact Us
- Locations
- Investor Relations
- Press Room
- Careers
- Subscribe

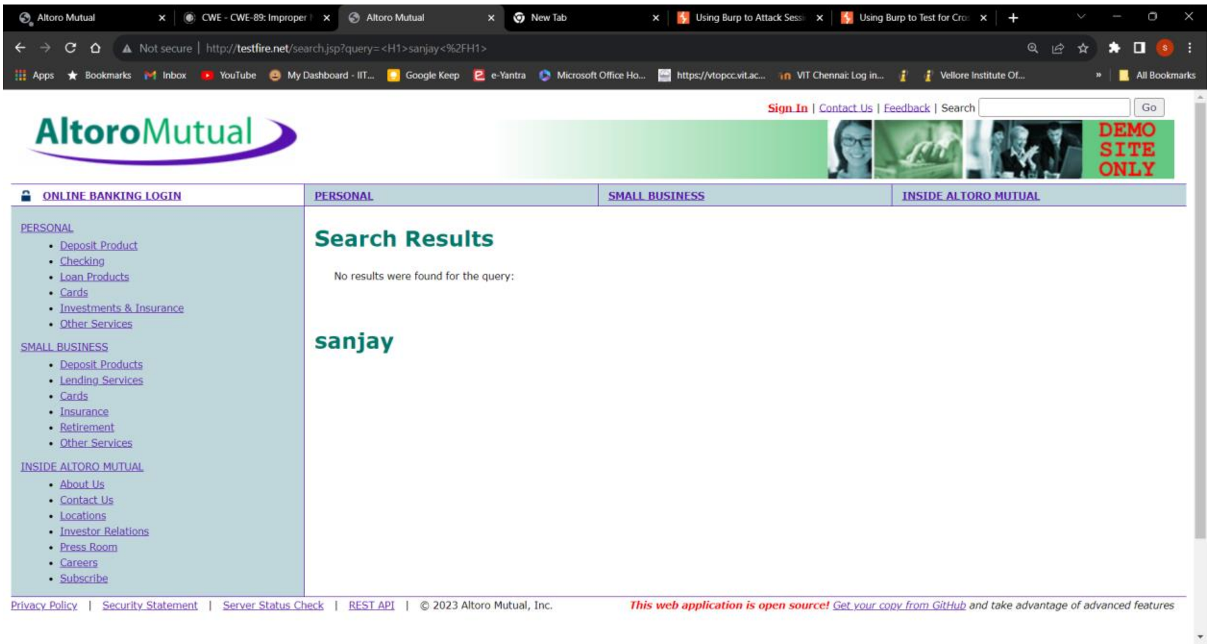
Search Results

No results were found for the query:

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

Step 3: The script affects the webpage



Search Results

No results were found for the query:

sanjay

3. No Session Management

CWE: CWE-384

OWASP Category: A07:2021 –Identification and Authentication Failures

Description: An attacker is able to force a known session identifier on a user so that, once the user authenticates, the attacker has access to the authenticated session.

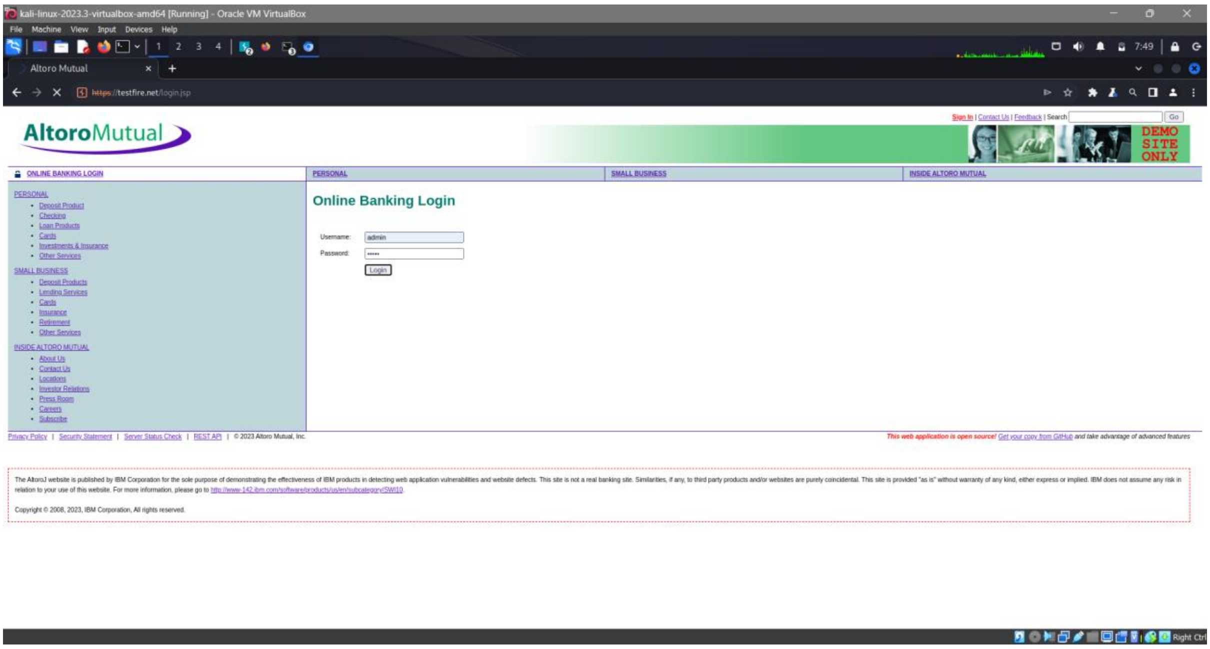
Business Impact: Without appropriate session management, you can run into several security problems, putting your users at risk. Common vulnerabilities caused by a lack of or poorly implemented session management include: Session hijacking

Vulnerability Path : http://testfire.net

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

Steps to Reproduce :

Step 1. Access the URL



Online Banking Login

Username: admin

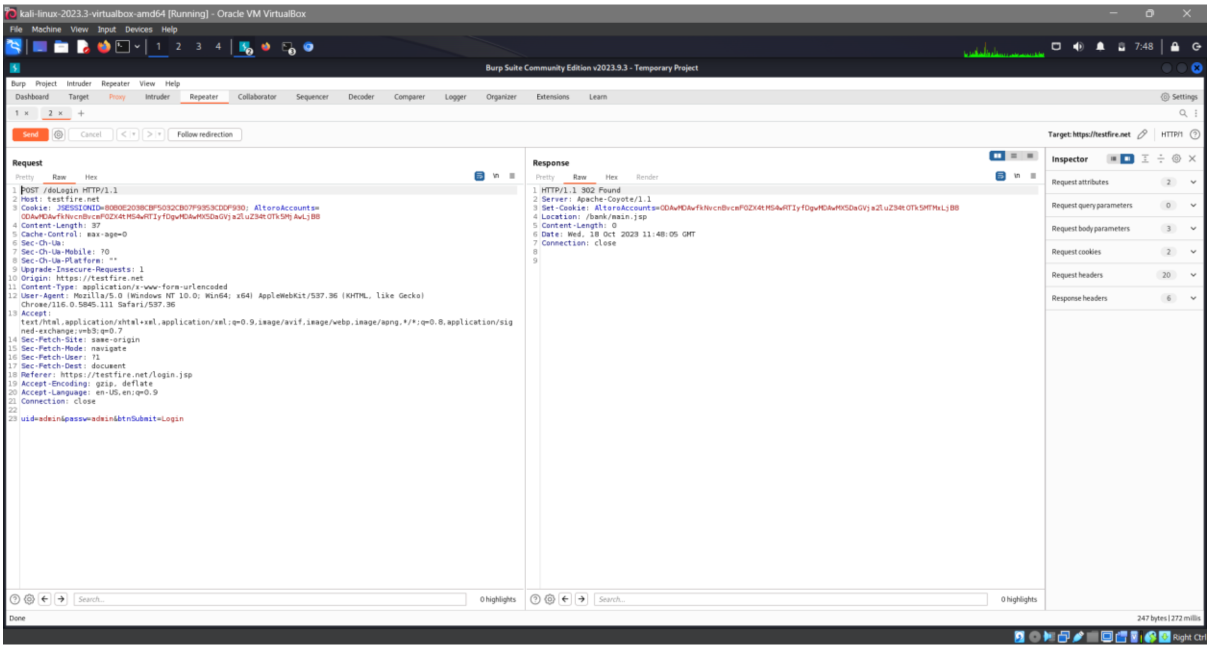
Password: •••••

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.

Step 2.without the proper session management the burp can still access the request of session as shown.



kali-linux-2023.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
Burp Suite Community Edition v2023.9.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Send
Cancel
Follow redirection
Target: https://testfire.net
HTTP/1
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 3
Request cookies 2
Request headers 20
Response headers 6
0 highlights
0 highlights
Done
247 bytes | 272 millis

Request

```
POST /doLogin HTTP/1.1
Host: testfire.net
Cookie: JSESSIONID=80B0E2038CBF5032CB07F9353CDDF930; AltoroAccounts=
ODAwMDAwfkNvcnBvcmF0ZX4tMS4wRTIyfDgwMDAwMX5DaGVja2luZ34tOTk5MjAwLjB8
Content-Length: 37
Cache-Control: max-age=0
Sec-Ch-Ua:
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: ""
Upgrade-Insecure-Requests: 1
Origin: https://testfire.net
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/116.0.5845.111 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sig
ned-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://testfire.net/login.jsp
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

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

Response

```
HTTP/1.1 302 Found
Server: Apache-Coyote/1.1
Set-Cookie: AltoroAccounts=ODAwMDAwfkNvcnBvcmF0ZX4tMS4wRTIyfDgwMDAwMX5DaGVja2luZ34tOTk5MTMxLjB8
Location: /bank/main.jsp
Content-Length: 0
Date: Wed, 18 Oct 2023 11:48:05 GMT
Connection: close
```

Recommendation:

- Invalidate any existing session identifiers prior to authorizing a new user session.

4. Admin Login SQL Injection

CWE: CWE-284

OWASP Category: A03:2021-Injections

Description: Without sufficient removal or quoting of SQL syntax in user-controllable inputs, the generated SQL query can cause those inputs to be interpreted as SQL instead of ordinary user data. This can be used to alter query logic to bypass security checks, or to insert additional statements that modify the back-end database, possibly including execution of system commands.

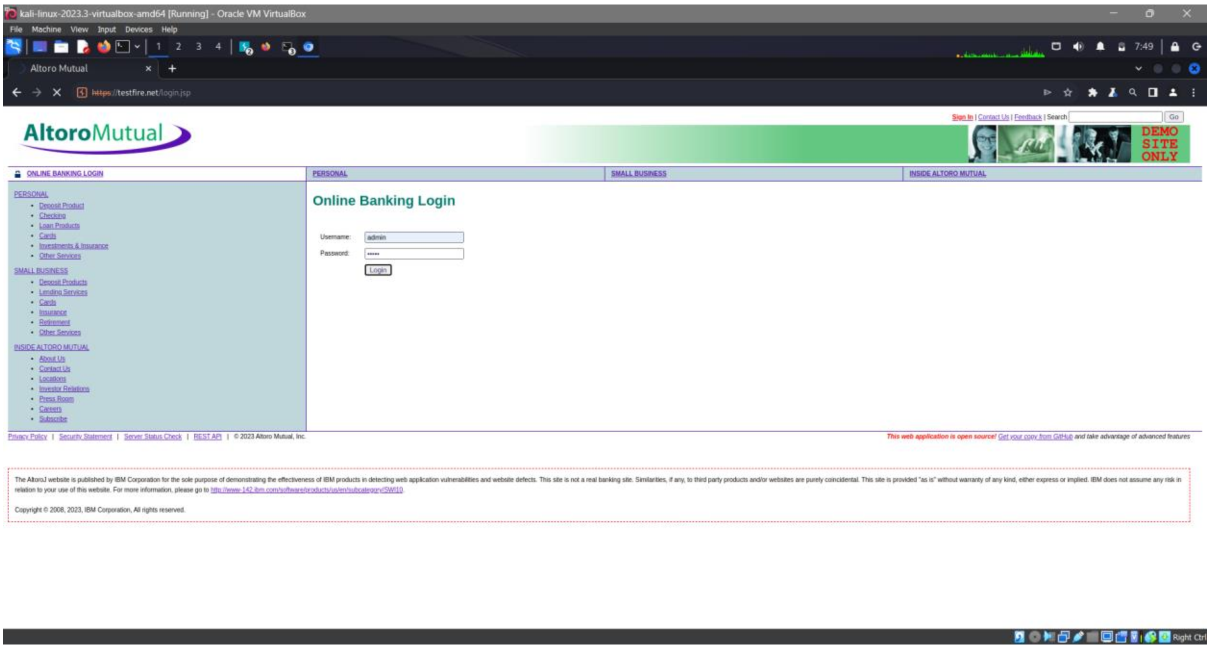
Business Impact: If authorization information is held in a SQL database, it may be possible to change this information through the successful exploitation of a SQL injection vulnerability

Vulnerability Path: http://testfire.net

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

Steps to Reproduce:

Step 1. Access the URL


kali-linux-2023.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Altoro Mutual
https://testfire.net/login.jsp
AltoroMutual
Sign In | Contact Us | Feedback | Search Go
DEMO SITE ONLY
ONLINE BANKING LOGIN
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL
PERSONAL
Deposit Product
Checking
Loan Products
Cards
Investments & Insurance
Other Services
SMALL BUSINESS
Deposit Products
Lending Services
Cards
Insurance
Retirement
Other Services
INSIDE ALTORO MUTUAL
About Us
Contact Us
Locations
Investor Relations
Press Room
Careers
Subscribe
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
Right Ctrl

Online Banking Login

Username: admin

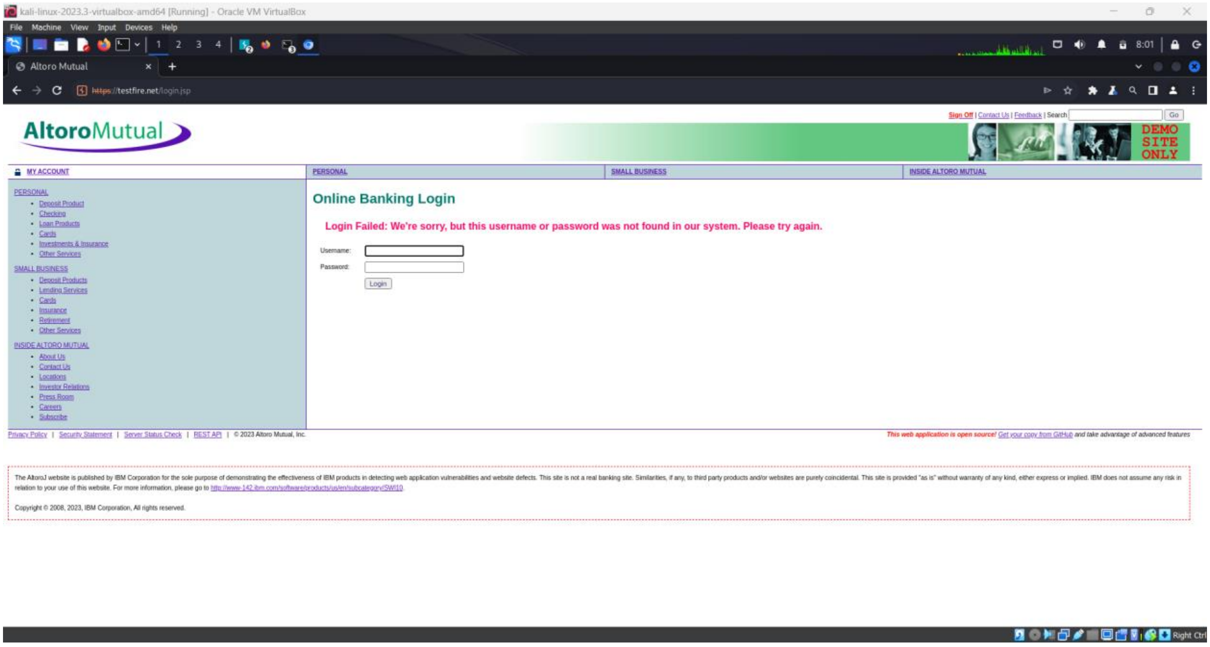
Password: •••••

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.

Step 2:- Enter the login credentials in and try to validate as shown below.



Online Banking Login

Login Failed: We're sorry, but this username or password was not found in our system. Please try again.

Username:

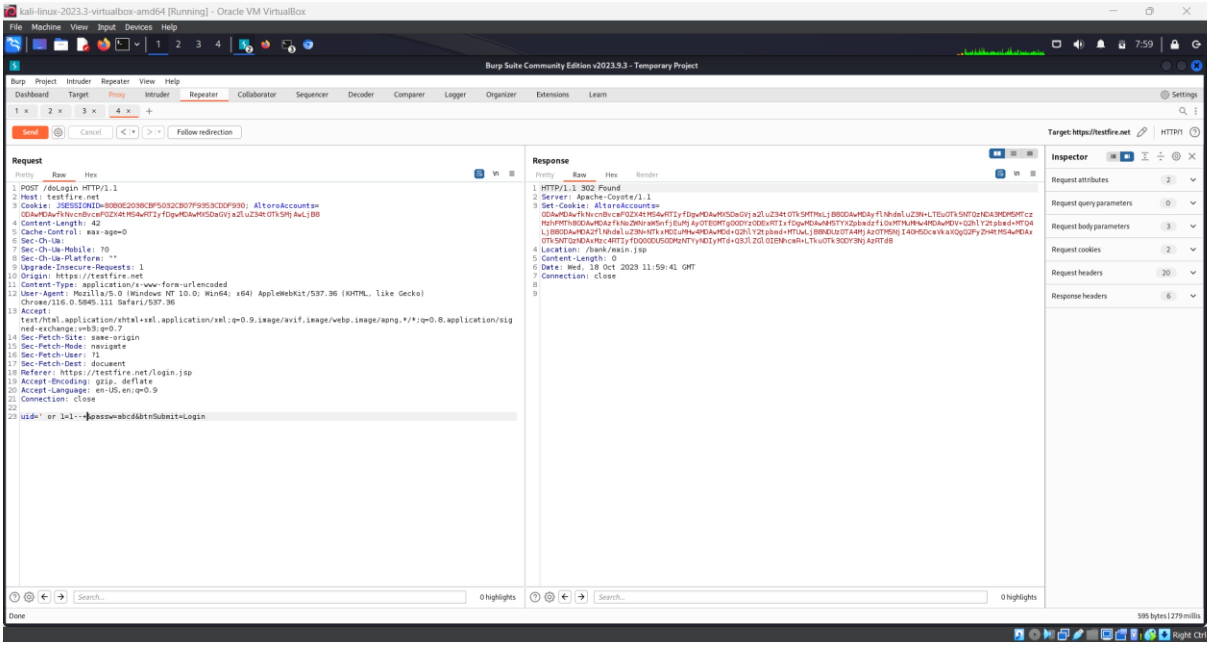
Password:

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.

Step 3:- in the backend we need to use the burp to configure the user with sql injection.



Request

```
POST /doLogin HTTP/1.1
Host: testfire.net
Cookie: JSESSIONID=8080E2038CBF5032CB07F9353CDDF930; AltoroAccounts=
ODAwMDAwfkNvcnBvcmF0ZX4tMS4wRTIyfDgwMDAwMX5DaGVja2luZ34tOTk5MjAwLjB8
Content-Length: 42
Cache-Control: max-age=0
Sec-Ch-Ua:
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: ""
Upgrade-Insecure-Requests: 1
Origin: https://testfire.net
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/116.0.5845.111 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sig
ned-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://testfire.net/login.jsp
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

uid=' or 1=1--+&passw=abcd&btnSubmit=Login
```

Response

```
HTTP/1.1 302 Found
Server: Apache-Coyote/1.1
Set-Cookie: AltoroAccounts=
ODAwMDAwfkNvcnBvcmF0ZX4tMS4wRTIyfDgwMDAwMX5DaGVja2luZ34tOTk5MTMxLjB8ODAwMDAyflNhdmluZ3N+LTEuOTk5NTQzNDA3MDM5MTcz
MzhFMTh8ODAwMDAzfkNoZWNraW5nfjEuMjAyOTE0MTg0ODYzODExRTIxfDgwMDAwNH5TYXZpbmdzfi0xMTMuMHw4MDAwMDV+Q2hlY2tpbmd+MTQ4
LjB8ODAwMDA2flNhdmluZ3N+NTkxMDIuMHw4MDAwMDd+Q2hlY2tpbmd+MTUwLjB8NDUzOTA4MjAzOTM5NjI4OH5DcmVkaXQgQ2FyZH4tMS4wMDAx
OTk5NTQzNDAxMzc4RTIyfDQ0ODU5ODMzNTYyNDIyMTd+Q3JlZGl0IENhcmR+LTkuOTk3ODY3NjAzRTd8
Location: /bank/main.jsp
Content-Length: 0
Date: Wed, 18 Oct 2023 11:59:41 GMT
Connection: close
```

Recommendation:

Employ a layered approach to security that includes utilizing parameterized queries when accepting user input, ensuring that only expected data (white listing) is accepted by an application, and harden the database server to prevent data from being accessed inappropriately.

5. Default Credentials

CWE : CWE-1392

OWASP Category:A07:2021-Identification and Authentication Failures

Description:It is common practice for products to be designed to use default keys, passwords, or other mechanisms for authentication. The rationale is to simplify the manufacturing process or the system administrator's task of installation and deployment into an enterprise. However, if admins do not change the defaults, it is easier for attackers to bypass authentication quickly across multiple organizations.

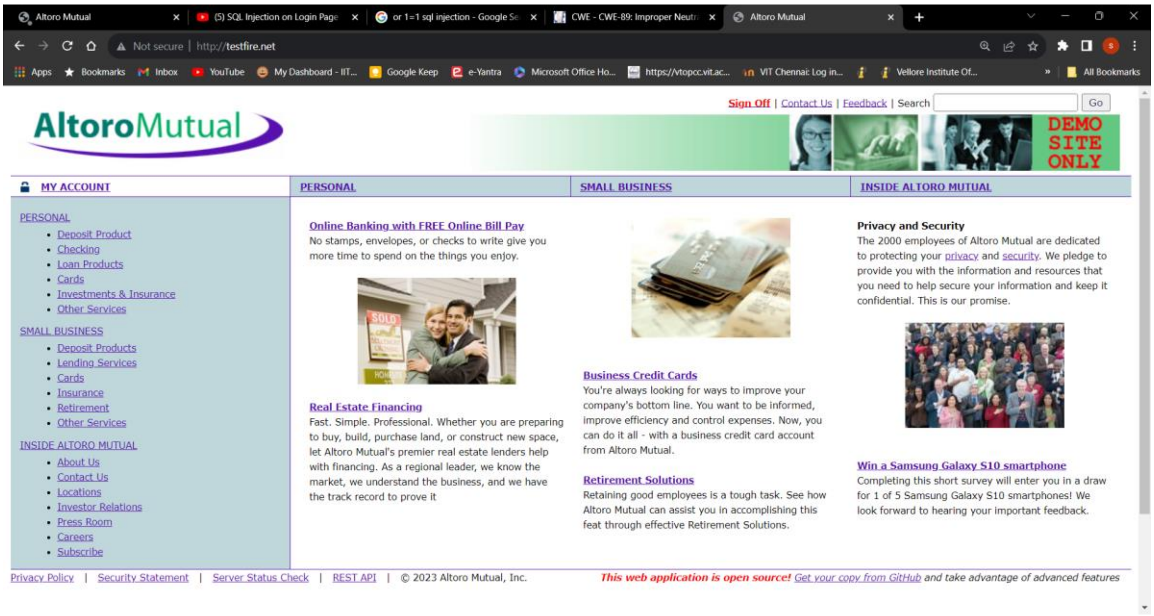
Business Impact:Attackers can easily obtain default passwords and identify internet-connected target systems. Passwords can be found in product documentation and compiled lists available on the internet.

Vulnerability Path : http://testfire.net

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

Steps to Reproduce :

Step 1. Access the 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.

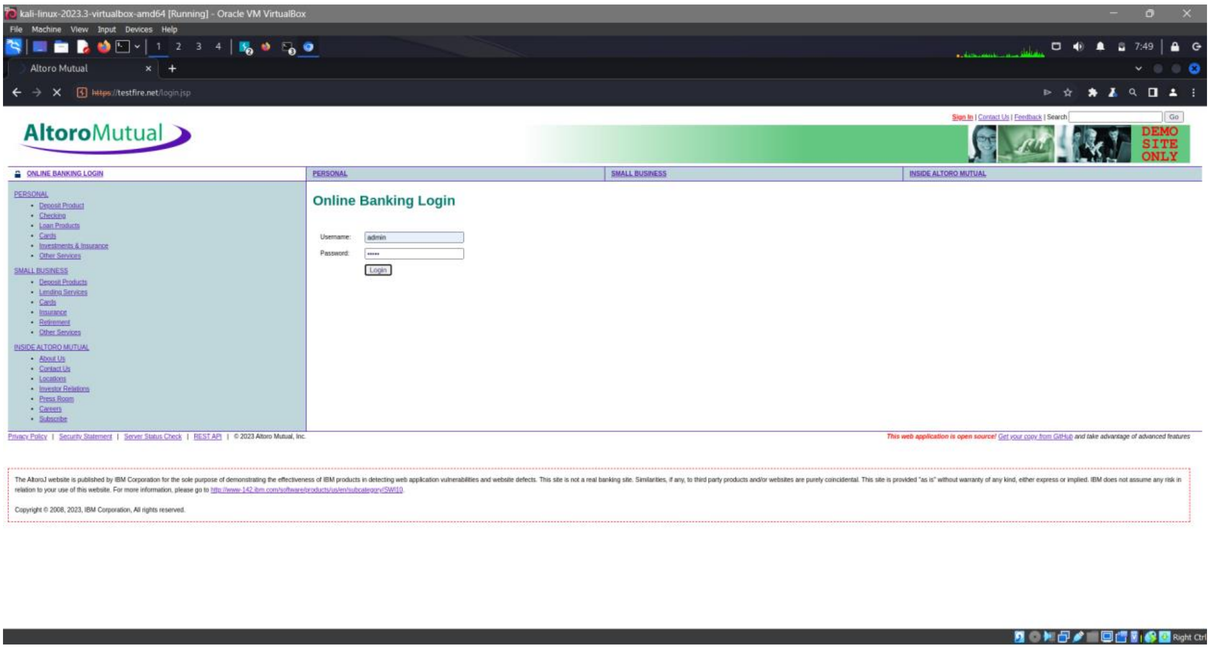
Retirement Solutions
Retaining good employees is a tough task. See how Altoro Mutual can assist you in accomplishing this feat through effective Retirement Solutions.

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

Step 2: The website is based on apache tomcat server so we are able to login using a default user and password .



Online Banking Login

Username: admin

Password: *****

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.

Recommendation:

- Prohibit use of default, hard-coded, or other values that do not vary for each installation of the product - especially for separate organizations.

6. Clickjacking (Improper Restriction of Rendered UI Layers or Frames)

CWE :CWE-1021

OWASP Category: A04-2021- insecure design

Description:it occurs whenever a web application is fetching a remote resource without validating the user-supplied URL. It allows an attacker to coerce the application to send a crafted request to an unexpected destination, even when protected by a firewall, VPN, or another type of network access control list (ACL).

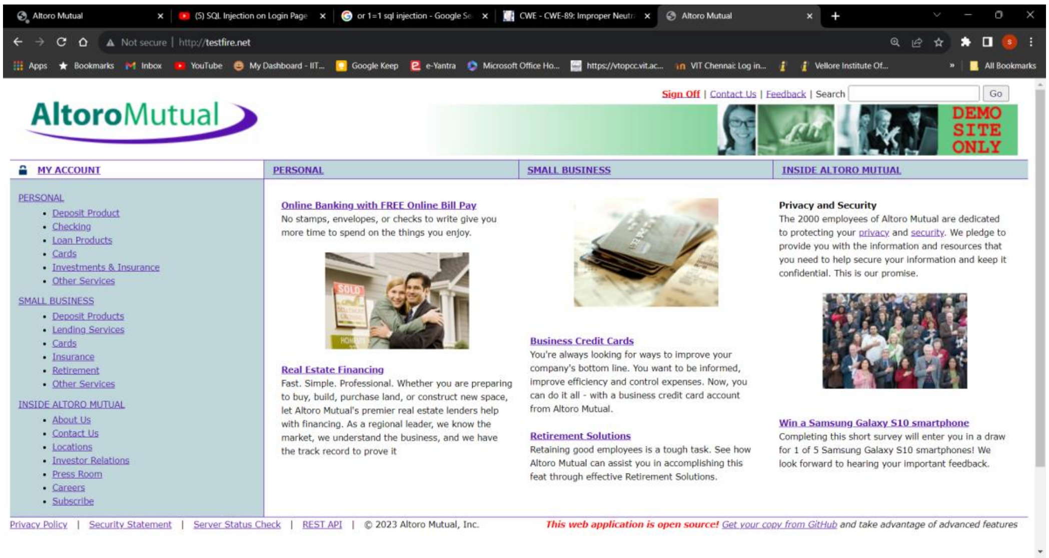
Business Impact: The common consequences of clickjacking include unauthorized actions, data theft, phishing, cookie theft, social engineering, reputation damage, legal and regulatory consequences, and user frustration. To prevent these, organizations should implement security headers, frame-busting techniques, user education, and regular security testing.

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

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

Steps to Reproduce :

Step 1:- Access the URl



Sign Off | Contact Us | Feedback | Search [ ] Go

MY ACCOUNT | PERSONAL | SMALL BUSINESS | INSIDE ALTORO MUTUAL

PERSONAL
- Deposit Product
- Checking
- Loan Products
- Cards
- Investments & Insurance
- Other Services

SMALL BUSINESS
- Deposit Products
- Lending Services
- Cards
- Insurance
- Retirement
- Other Services

INSIDE ALTORO MUTUAL
- About Us
- Contact Us
- Locations
- Investor Relations
- Press Room
- Careers
- Subscribe

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.

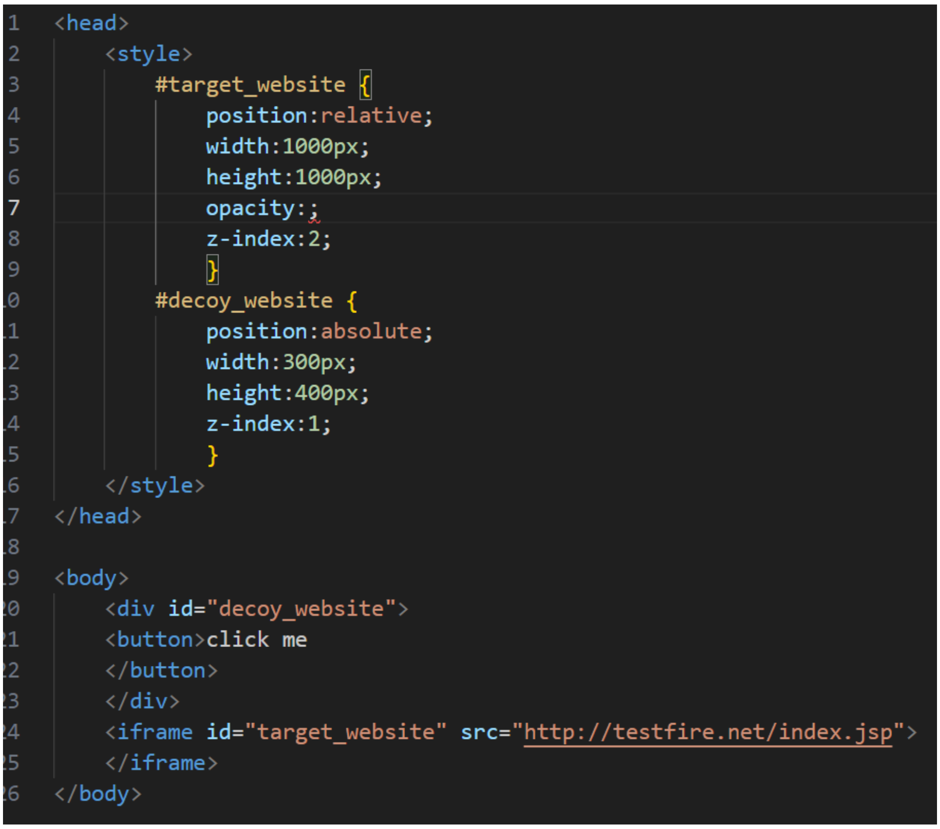
Privacy and Security
The 2000 employees of Altoro Mutual are dedicated to protecting your privacy and security. We pledge to provide you with the information and resources that you need to help secure your information and keep it confidential. This is our promise.

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

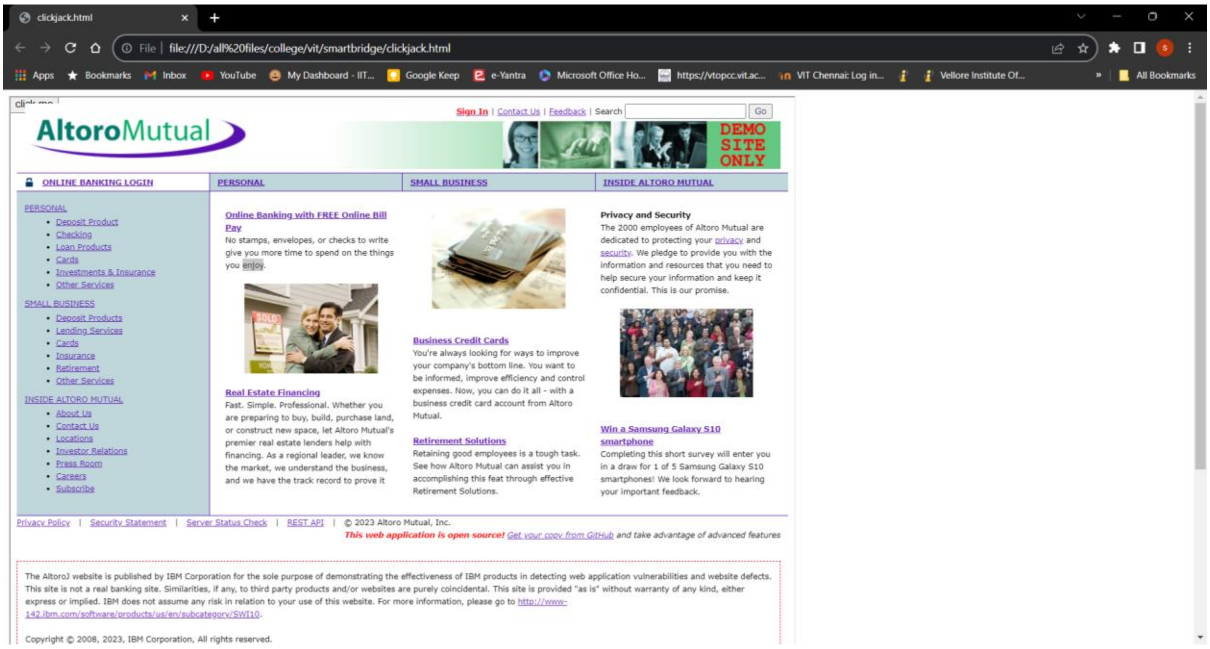
Step 2:- we write a html code as shown below when we run with the web address .



```
<head>
    <style>
        #target_website {
            position:relative;
            width:1000px;
            height:1000px;
            opacity:;
            z-index:2;
            }
        #decoy_website {
            position:absolute;
            width:300px;
            height:400px;
            z-index:1;
            }
    </style>
</head>

<body>
    <div id="decoy_website">
    <button>click me
    </button>
    </div>
    <iframe id="target_website" src="http://testfire.net/index.jsp">
    </iframe>
</body>
```

Step 3:- this will be the output of clickjacking the website with html code .



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.

© 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.

Recommendation:

- Segment remote resource access functionality in separate networks to reduce the impact of SSRF
- Enforce “deny by default” firewall policies or network access control rules to block all but essential intranet traffic.
- Enforce the URL schema, port, and destination with a positive allow list
- Do not send raw responses to clients
- Disable HTTP redirection

7. Anti-CSRF Token missing

CWE : CWE-352

OWASP Category:A05:2021 – Security Misconfiguration

Description:The web application does not, or cannot, sufficiently verify whether a well-formed, valid, consistent request was intentionally provided by the user who submitted the request.

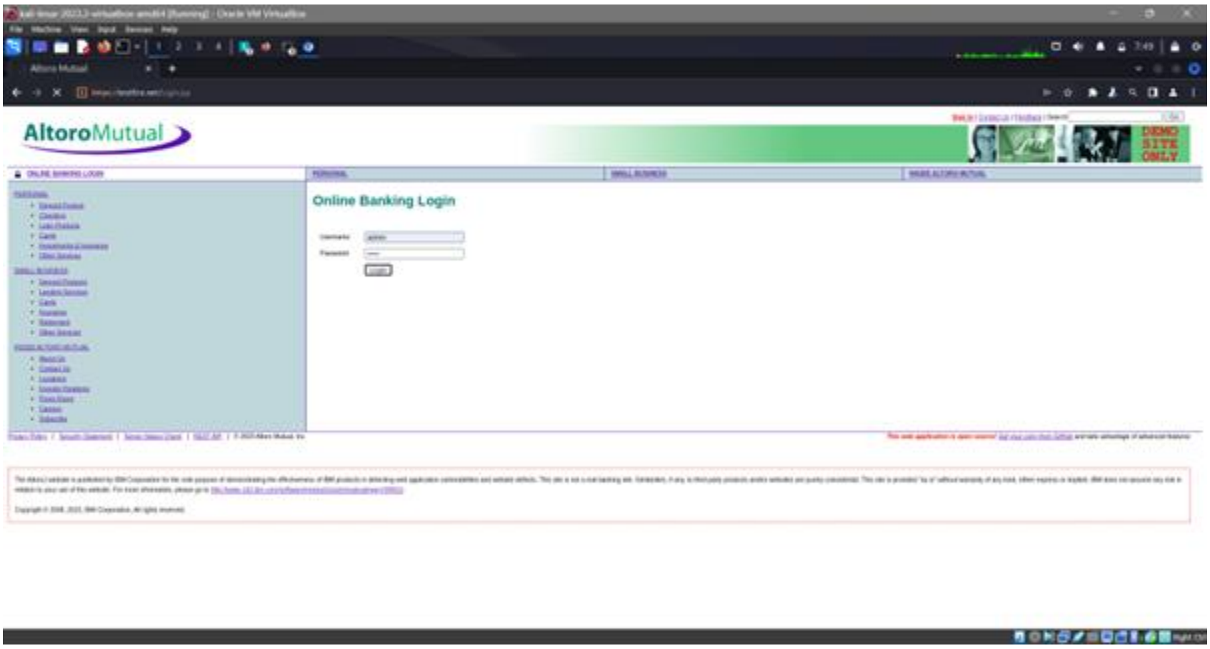
Business Impact:It can result in damaged client relationships, unauthorized fund transfers, changed passwords and data theft—including stolen session cookies.

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

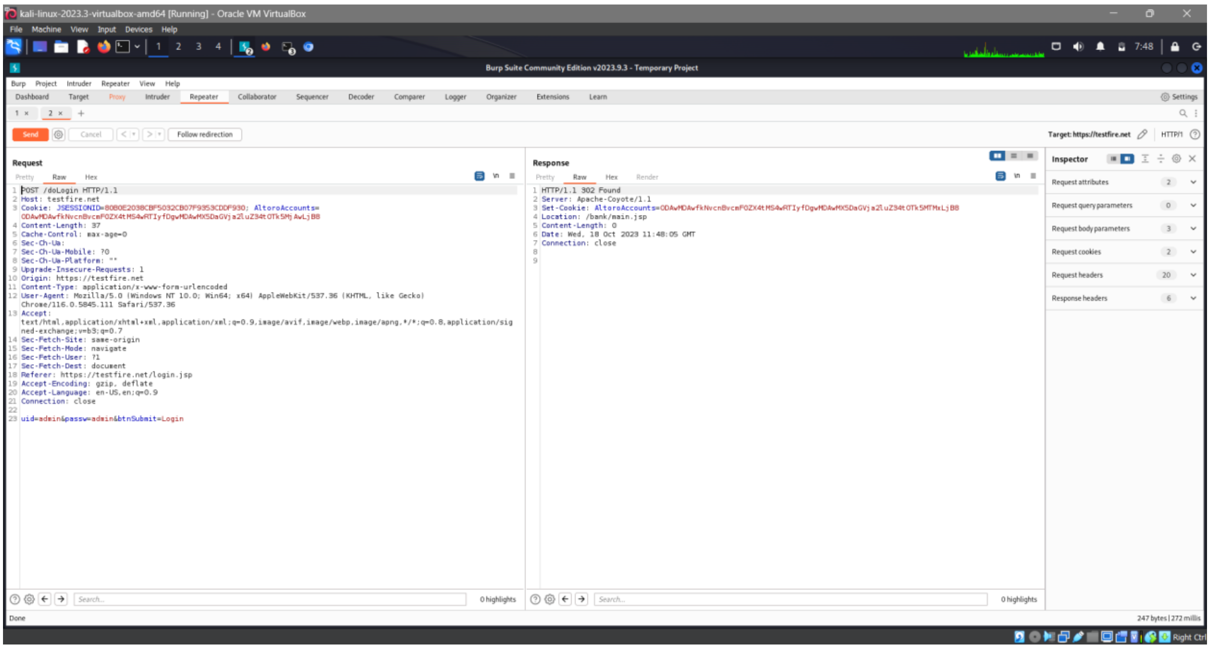
Vulnerability Parameter: http://testfire.net/login.jsp

Steps to Reproduce :

Step 1. Access the URL



Step 2: Now intercept with the burp proxy and send request in the repeater



```
POST /doLogin HTTP/1.1
Host: testfire.net
Cookie: JSESSIONID=80B0E2038CBF5032CB07F9353CDDF930; AltoroAccounts=
ODAwMDAwfkNvcnBvcmF0ZX4tMS4wRTIyfDgwMDAwMX5DaGVja2luZ34tOTk5MjAwLjB8
Content-Length: 37
Cache-Control: max-age=0
Sec-Ch-Ua:
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: ""
Upgrade-Insecure-Requests: 1
Origin: https://testfire.net
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/116.0.5845.111 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sig
ned-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://testfire.net/login.jsp
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

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

```
HTTP/1.1 302 Found
Server: Apache-Coyote/1.1
Set-Cookie: AltoroAccounts=ODAwMDAwfkNvcnBvcmF0ZX4tMS4wRTIyfDgwMDAwMX5DaGVja2luZ34tOTk5MTMxLjB8
Location: /bank/main.jsp
Content-Length: 0
Date: Wed, 18 Oct 2023 11:48:05 GMT
Connection: close
```

Recommendation:

- The most effective way to protect against CSRF vulnerabilities is to include within relevant requests an additional token that is not transmitted in a cookie.

- validate that Host and Refer headers in relevant requests are both present and contain the same domain name

8. Web Server Transmits Cleartext Credentials

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.

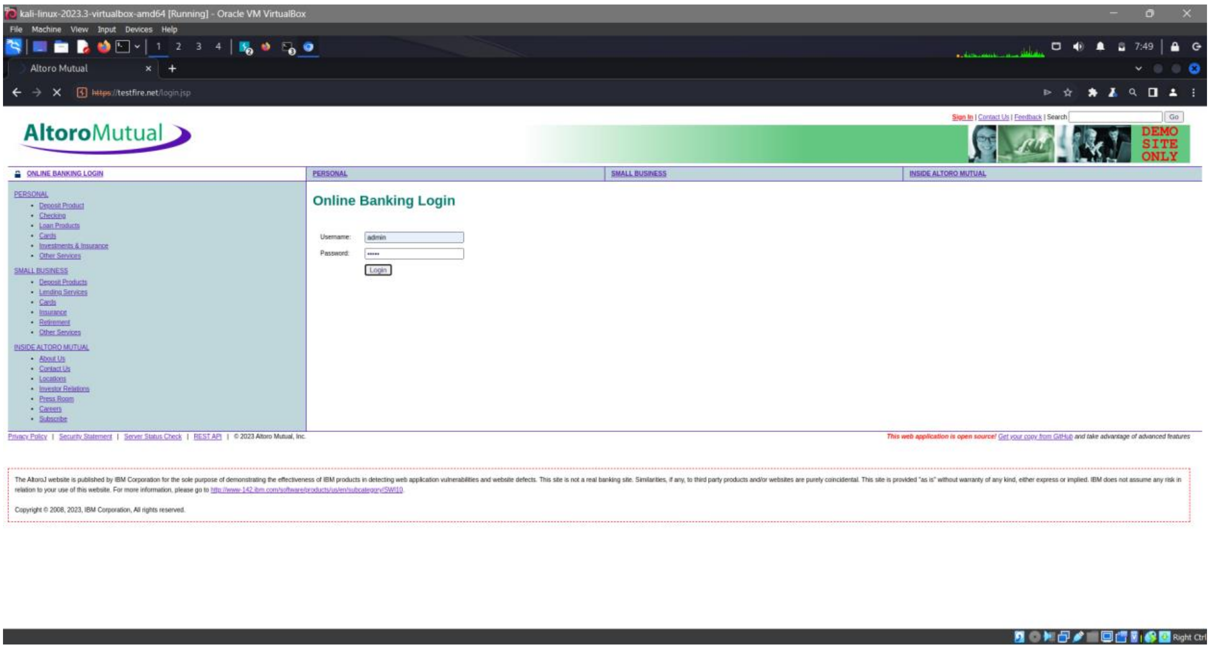
Business Impact: The technical impact of CWE-319 is that anyone can read the information by gaining access to the channel being used for communication. This can expose sensitive or confidential information to unauthorized parties, such as Passwords, Credit card numbers, Personal data.

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

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

Steps to Reproduce :

Step 1: Access url :



kali-linux-2023.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox

~~https~~://testfire.net/login.jsp

Online Banking Login

Username: admin

Password: •••••

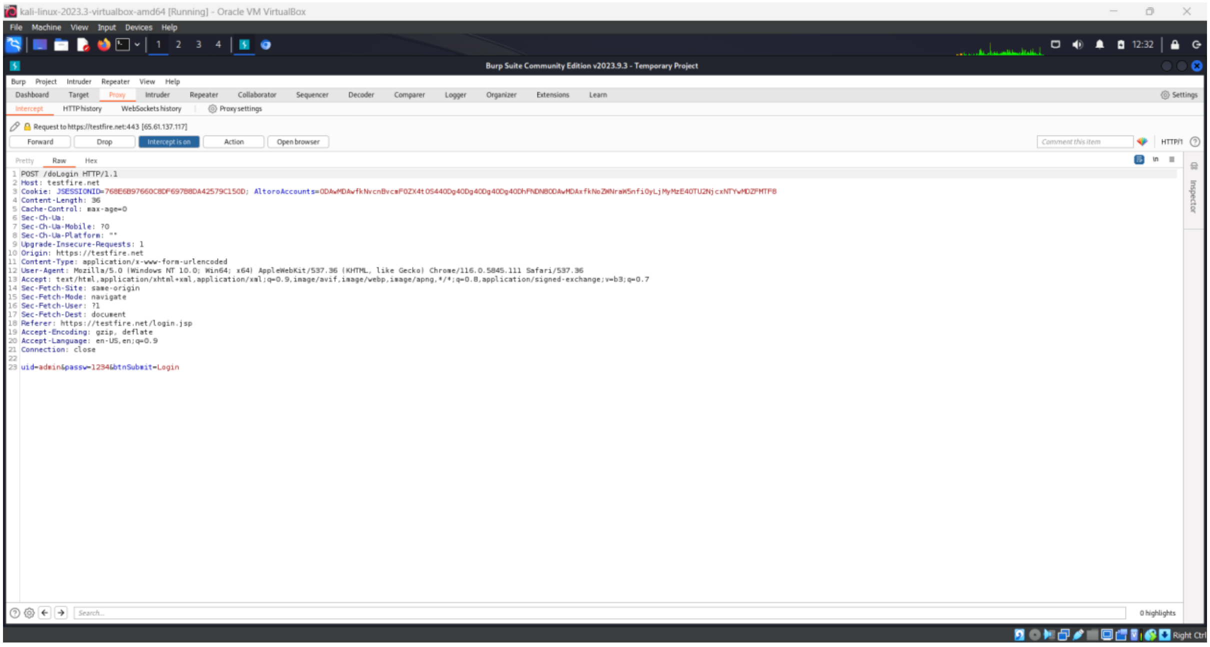
Privacy Policy | Security Statement | Server Status Check | REST API | © 2023 Altoro Mutual, Inc.

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.

Step 2: Intercept the login with burp and you can view the credentials


kali-linux-2023.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Burp Suite Community Edition v2023.9.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is on Action Open browser
Comment this item
HTTP/1
Pretty Raw Hex
Inspector
Search...
0 highlights
Right Ctrl

Request to https://testfire.net:443 [65.61.137.117]

```
POST /doLogin HTTP/1.1
Host: testfire.net
Cookie: JSESSIONID=768E6B97660C8DF69788DA42579C150D; AltoroAccounts=0DAwMDAwfkNvcnBvcmF0ZX4tOS440Dg40Dg40Dg40Dg40DhFNDN80DAwMDAxfkNoZWNraW5nfi0yLjMyMzE40TU2NjcxNTYwMDZFMTF8
Content-Length: 36
Cache-Control: max-age=0
Sec-Ch-Ua:
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: ""
Upgrade-Insecure-Requests: 1
Origin: https://testfire.net
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.111 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://testfire.net/login.jsp
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

uid=admin&passw=1234&btnSubmit=Login
```

Recommendation:

Before transmitting, encrypt the data using reliable, confidentiality-protecting cryptographic protocols.

9. Secure Http flag

CWE : CWE-1004

OWASP Category: A05:2021 – Security Misconfiguration

Description:The software uses a cookie to store sensitive information, but the cookie is not marked with the HttpOnly flag.

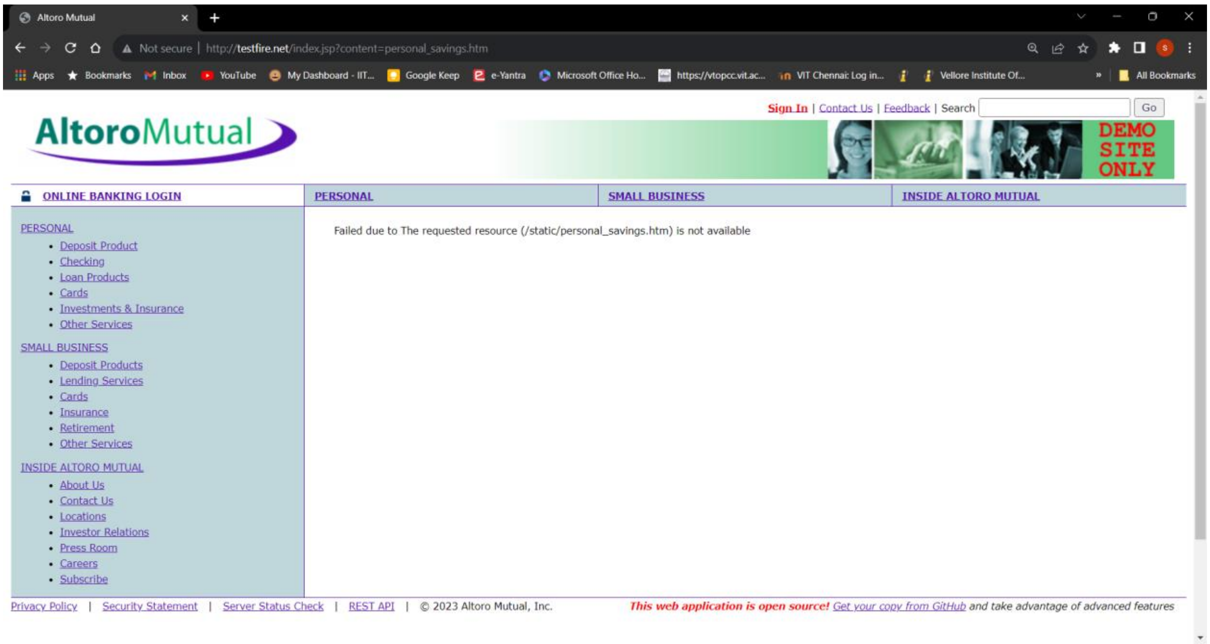
Business Impact: This measure makes certain client-side attacks, such as cross-site scripting, slightly harder to exploit by preventing them from trivially capturing the cookie's value via an injected script.

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

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

Steps to Reproduce :

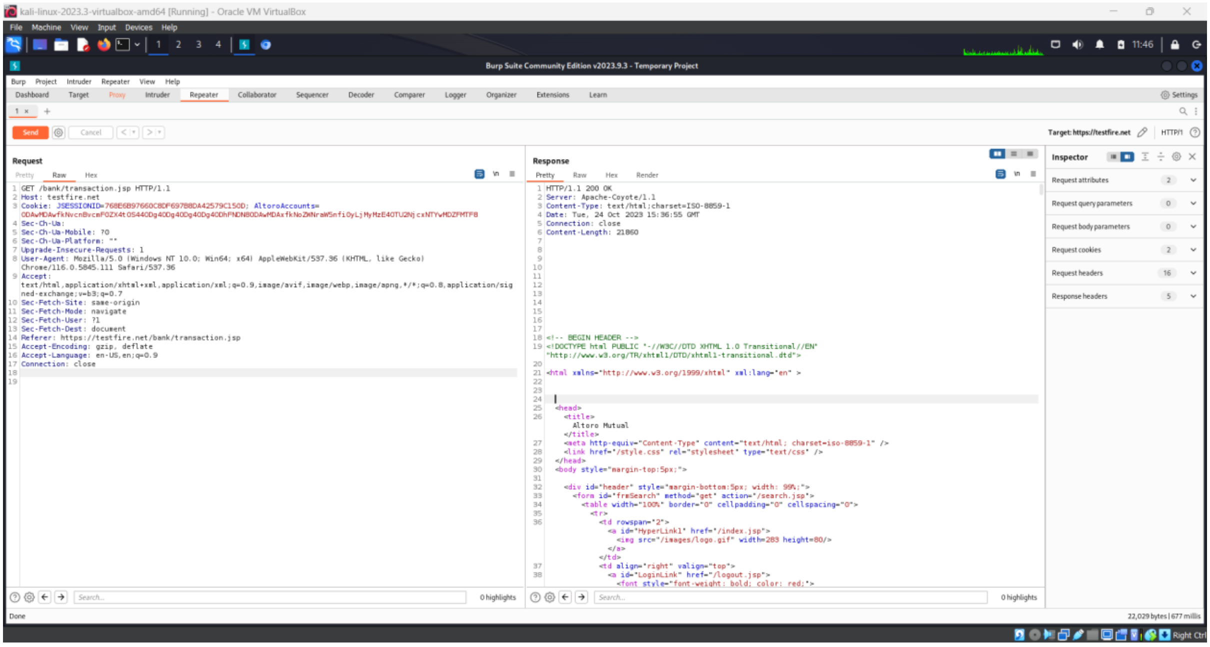
Step 1. Access the URL



Not secure | http://testfire.net/index.jsp?content=personal_savings.htm

Failed due to The requested resource (/static/personal_savings.htm) is not available

Step 2: Now intercept with burp proxy and run the request in the repeater.


kali-linux-2023.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
Burp Suite Community Edition v2023.9.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Send
Cancel
Target: https://testfire.net
HTTP/1
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 2
Request headers 16
Response headers 5
0 highlights
Done
22,029 bytes | 677 millis

```
GET /bank/transaction.jsp HTTP/1.1
Host: testfire.net
Cookie: JSESSIONID=768E6B97660C8DF69788DA42579C150D; AltoroAccounts=
ODAwMDAwfkNvcnBvcmF0ZX4tOS440Dg40Dg40Dg40Dg40DhFNDN8ODAwMDAxfkNoZWNraW5nfi0yLjMyMzE4OTU2NjcxNTYwMDZFMTF8
Sec-Ch-Ua:
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: ""
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/116.0.5845.111 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sig
ned-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://testfire.net/bank/transaction.jsp
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Date: Tue, 24 Oct 2023 15:36:55 GMT
Connection: close
Content-Length: 21860











<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



  <head>
    <title>
      Altoro Mutual
    </title>
    <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
    <link href="/style.css" rel="stylesheet" type="text/css" />
  </head>
  <body style="margin-top:5px;">

    <div id="header" style="margin-bottom:5px; width: 99%;">
      <form id="frmSearch" method="get" action="/search.jsp">
        <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
            <td rowspan="2">
              <a id="HyperLink1" href="/index.jsp">
                <img src="/images/logo.gif" width=283 height=80/>
              </a>
            </td>
            <td align="right" valign="top">
              <a id="LoginLink" href="/logout.jsp">
                <font style="font-weight: bold; color: red;">
```

Recommendation:

- You specifically require legitimate client-side scripts within your application to read or set a cookie's value, you should set the HttpOnly flag by including this attribute within the relevant Set-cookie directive

10. Password field autocomplete

CWE :CWE-522

OWASP Category: A04:2021 – Insecure Design

Description: The product transmits or stores authentication credentials, but it uses an insecure method that is susceptible to unauthorized interception and/or retrieval.

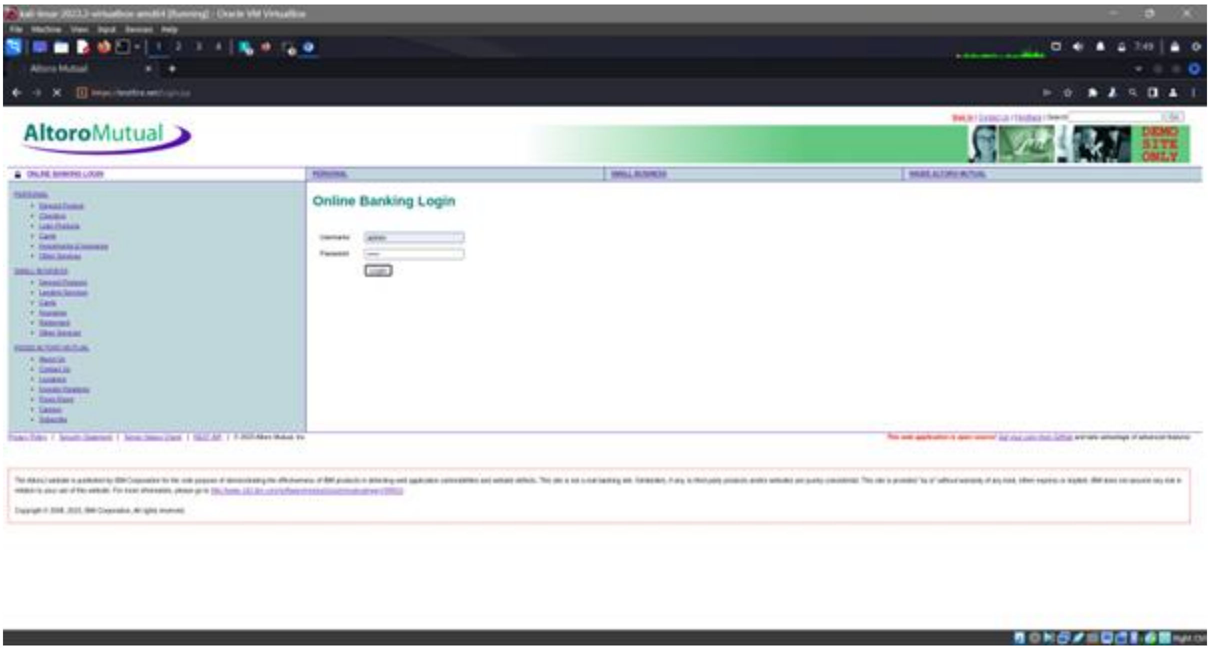
Business Impact: An attacker could gain access to user accounts and access sensitive data used by the user accounts.

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

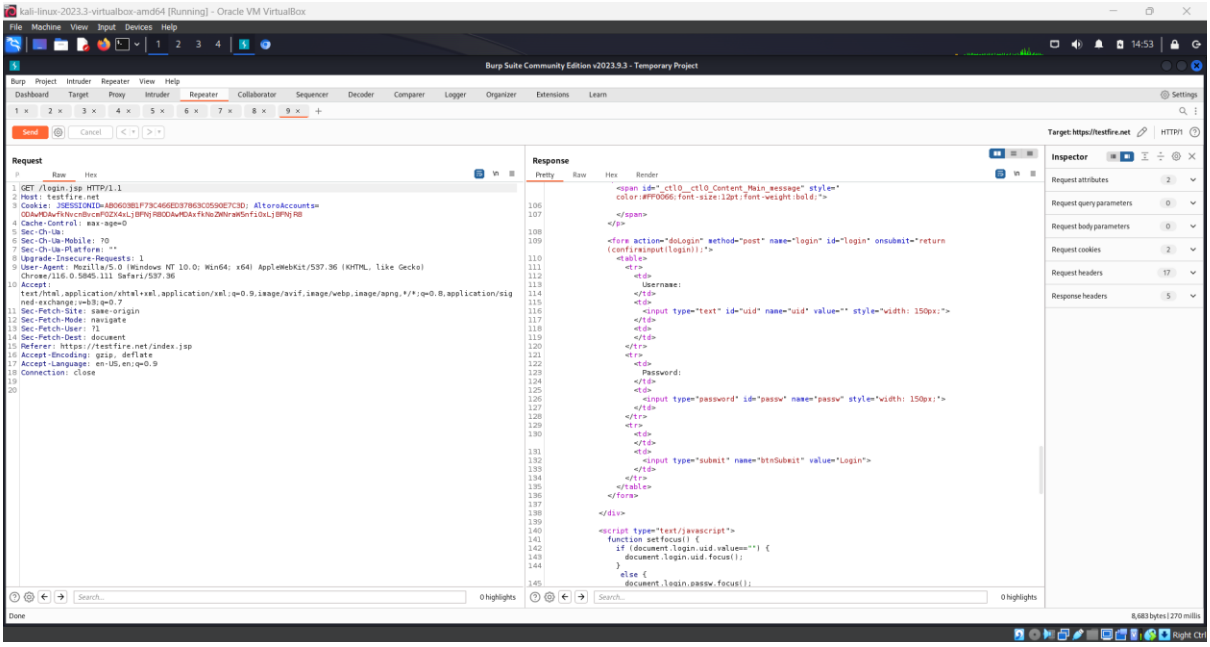
Vulnerability Parameter: http://testfire.net/login.jsp

Steps to Reproduce :

Step 1. Access the URL



Step 2: intercept with burp and check the html script.



kali-linux-2023.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
Burp Suite Community Edition v2023.9.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Send
Cancel
Target: https://testfire.net
Request
Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 2
Request headers 17
Response headers 5
0 highlights
Done
8,683 bytes | 270 millis

```
GET /login.jsp HTTP/1.1
Host: testfire.net
Cookie: JSESSIONID=AB0603B1F73C466ED37863C0590E7C3D; AltoroAccounts=
ODAwMDAwfkNvcnBvcmF0ZX4xLjBFNjR8ODAwMDAxfkNoZWNraW5nfi0xLjBFNjR8
Cache-Control: max-age=0
Sec-Ch-Ua:
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: ""
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/116.0.5845.111 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sig
ned-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://testfire.net/index.jsp
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

```
      <span id="_ctl0__ctl0_Content_Main_message" style="
      color:#FF0066;font-size:12pt;font-weight:bold;">

      </span>
    </p>

    <form action="doLogin" method="post" name="login" id="login" onsubmit="return
    (confirminput(login));">
      <table>
        <tr>
          <td>
            Username:
          </td>
          <td>
            <input type="text" id="uid" name="uid" value="" style="width: 150px;">
          </td>
          <td>
          </td>
        </tr>
        <tr>
          <td>
            Password:
          </td>
          <td>
            <input type="password" id="passw" name="passw" style="width: 150px;">
          </td>
        </tr>
        <tr>
          <td>
          </td>
          <td>
            <input type="submit" name="btnSubmit" value="Login">
          </td>
        </tr>
      </table>
    </form>

  </div>

  <script type="text/javascript">
    function setfocus() {
      if (document.login.uid.value=="") {
        document.login.uid.focus();
      }
       else {
        document.login.passw.focus();
```

Recommendation:

Use an appropriate security mechanism to protect the credentials. Make appropriate use of cryptography to protect the credentials.

The scan for the main website has shown there are only info level vulnerabilities therefore for proper penetration testing we use another website.

Original website: https://vtopcc.vit.ac.in

Alternate website: http://testphp.vulnweb.com/

S.no	**Vulnerability**	**CWE**
1.	Cross-Site Scripting (Stored)	CWE-79
2.	Html injection	CWE-80
3.	No Session Management	CWE-384
4.	Admin Login SQL Injection	CWE-284
5.	Default Credentials	CWE-1392

1. Cross-Site Scripting (Stored)

CWE: CWE-79

OWASP Category: A03:2021 – Injection

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

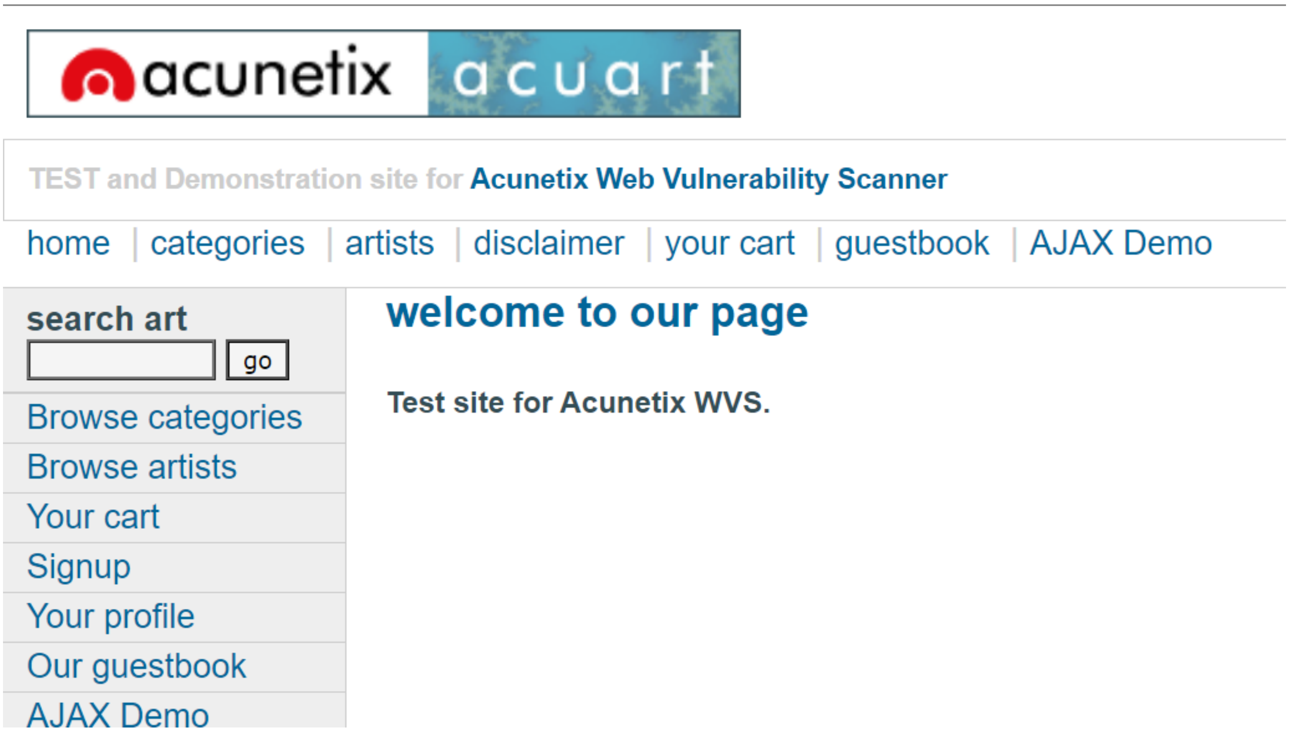
Business Impact: The most common attack performed with cross-site scripting involves the disclosure of information stored in user cookies. Typically, a malicious user will craft a client-side script, which -- when parsed by a web browser -- performs some activity (such as sending all site cookies to a given E-mail address). This script will be loaded and run by each user visiting the web site. Since the site requesting to run the script has access to the cookies in question, the malicious script does also.

Vulnerability Path : http://testphp.vulnweb.com

Vulnerability Parameter: http://testphp.vulnweb.com/search.php?test=query

Steps to Reproduce :

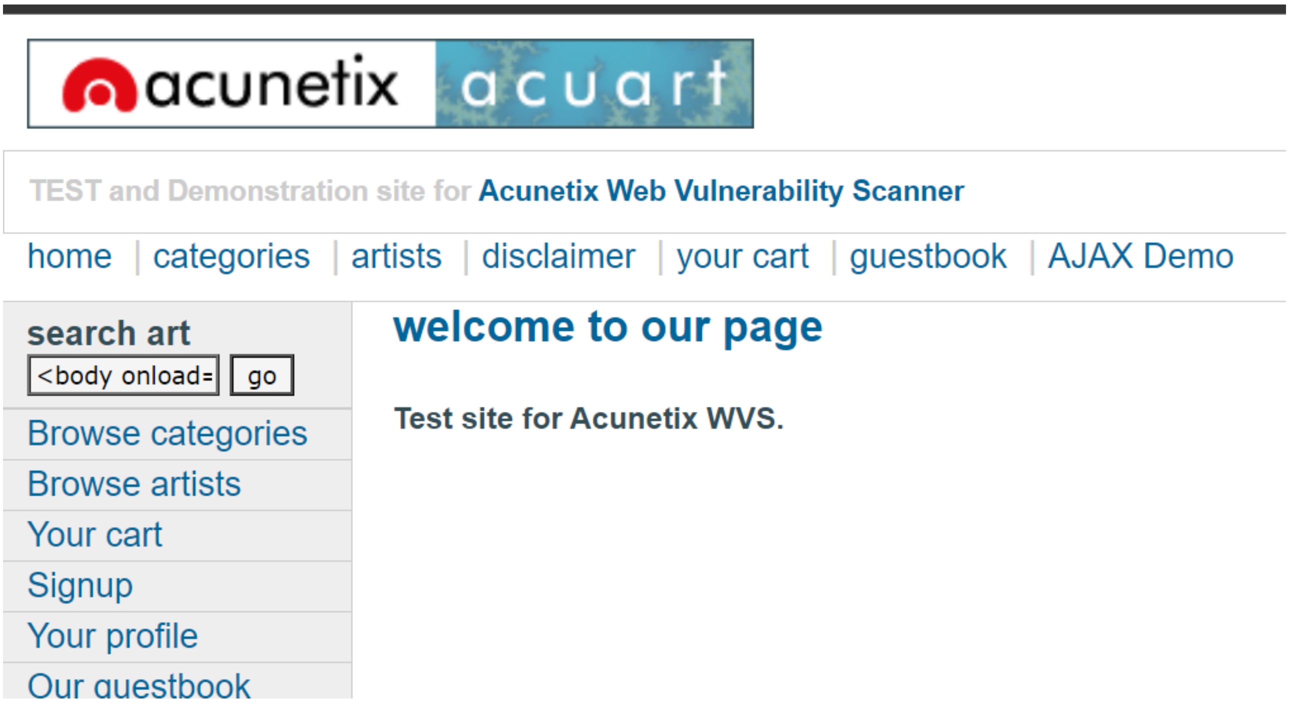
Step 1. Access the URL


acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

welcome to our page

Test site for Acunetix WVS.

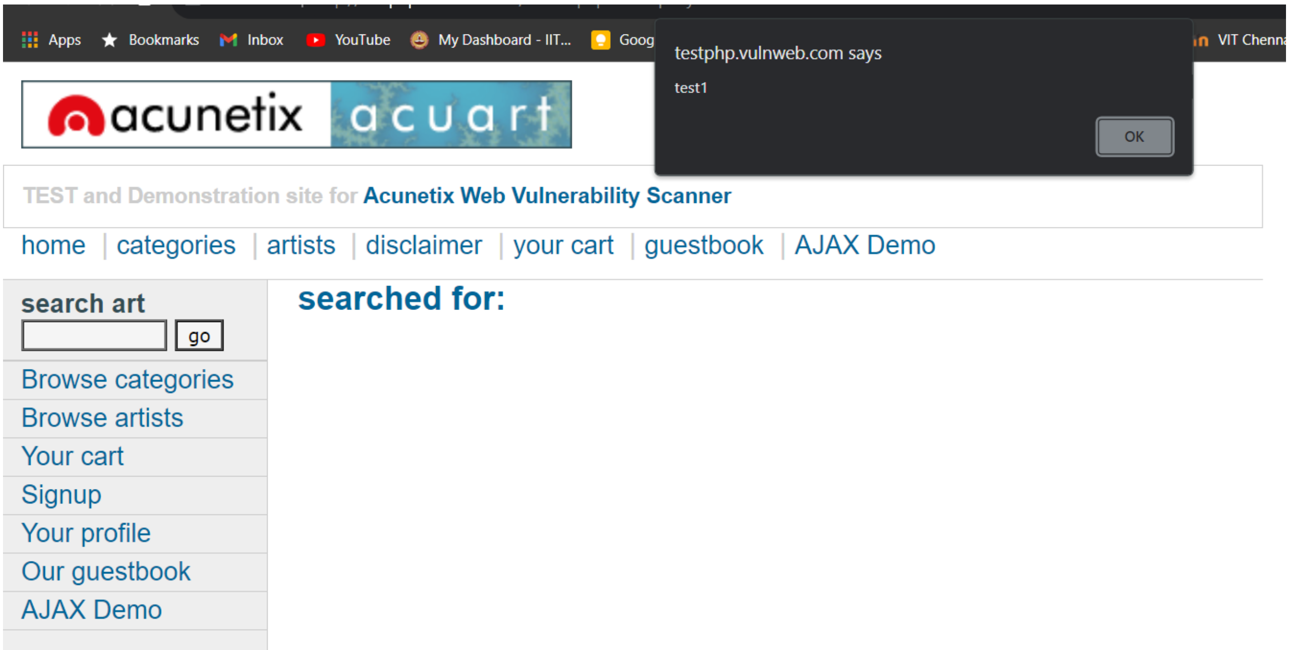
Step 2: enter the script in the search box <body onload=alert('test1')>


acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
<body onload=
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook

welcome to our page

Test site for Acunetix WVS.

Step 3:-after entering the script content like” hacked” u will find the dialogue box as shown below.



testphp.vulnweb.com says

test1

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

searched for:

Recommendation:

Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.

2. Html injection

CWE: CWE-80

OWASP Category: A03:2021 – Injection

Description: The product receives input from an upstream component, but it does not neutralize or incorrectly neutralizes special characters such as "<", ">", and "&" that could be interpreted as web-scripting elements when they are sent to a downstream component that processes web pages.

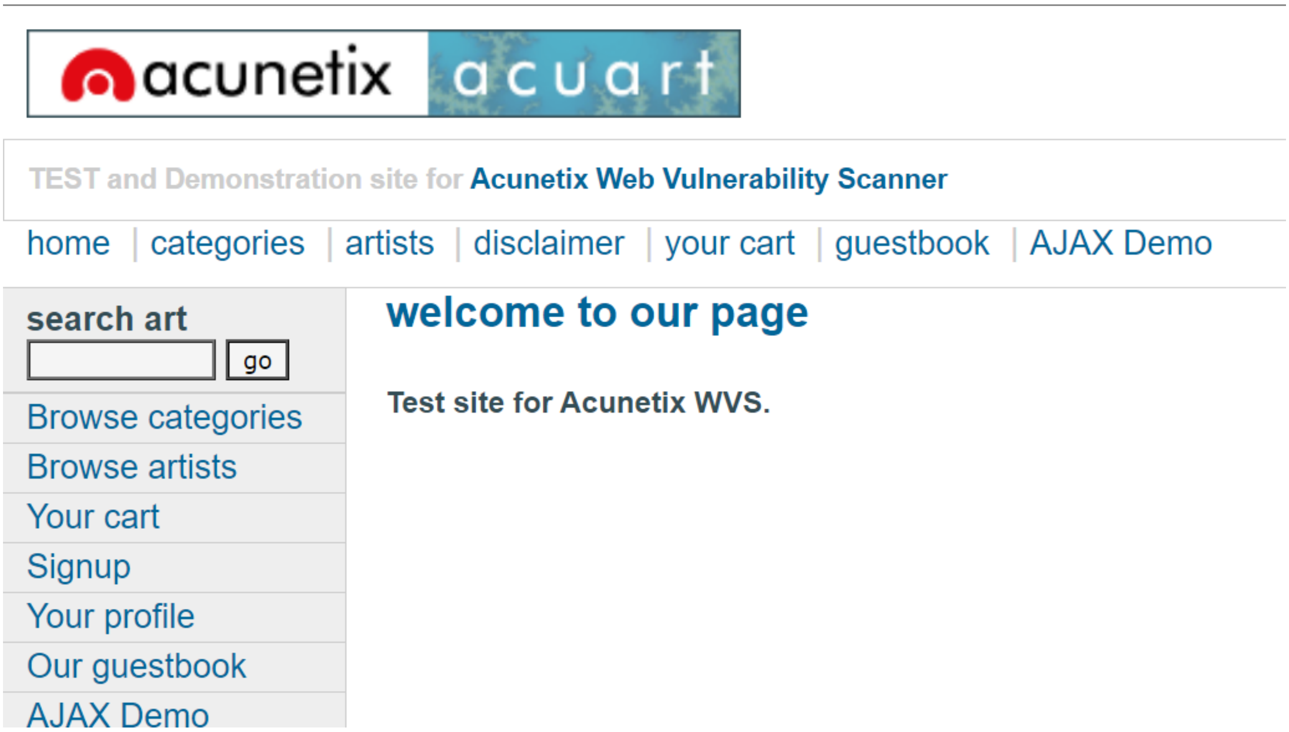
Business Impact: In some circumstances it may be possible to run arbitrary code on a victim's computer when cross-site scripting is combined with other flaws.

Vulnerability Path : http://testphp.vulnweb.com

Vulnerability Parameter: http://testphp.vulnweb.com/search.php?test=query

Steps to Reproduce :

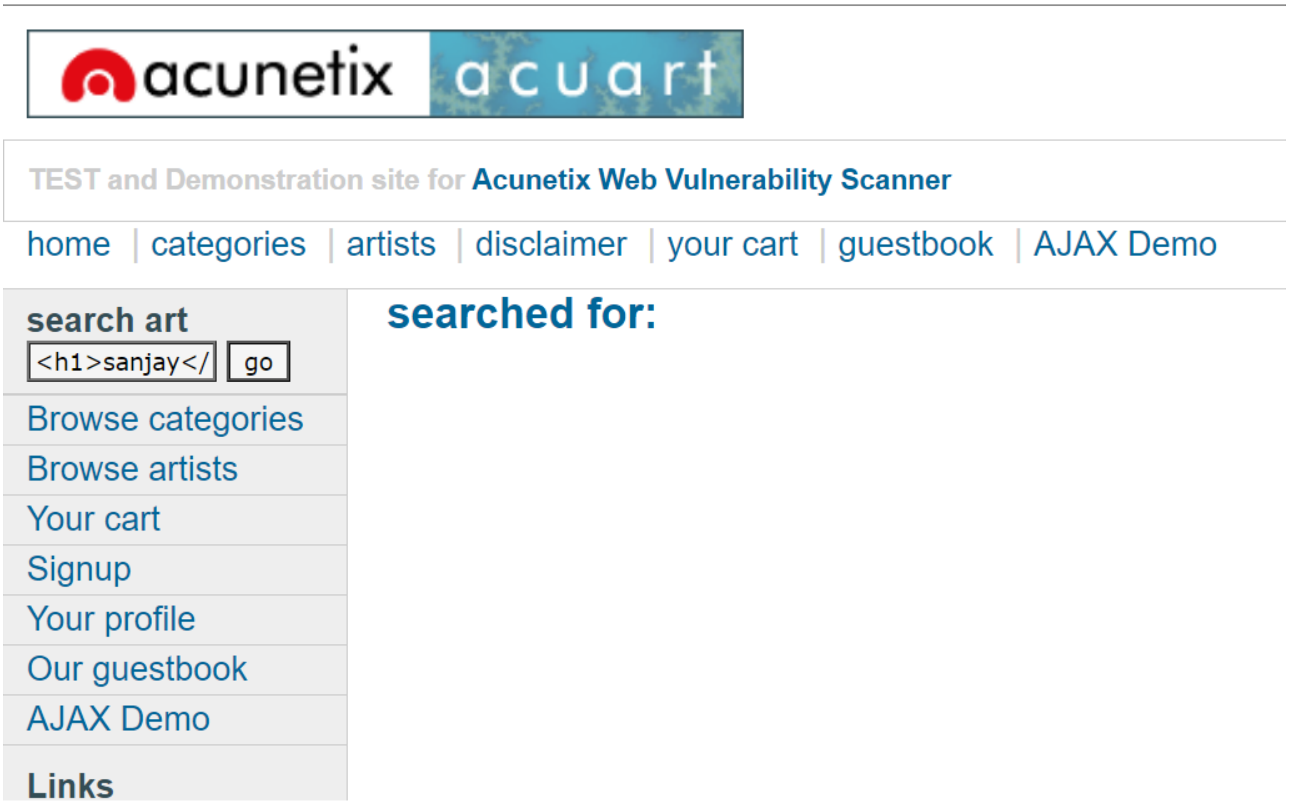
Step 1. Access the URL


acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

welcome to our page

Test site for Acunetix WVS.

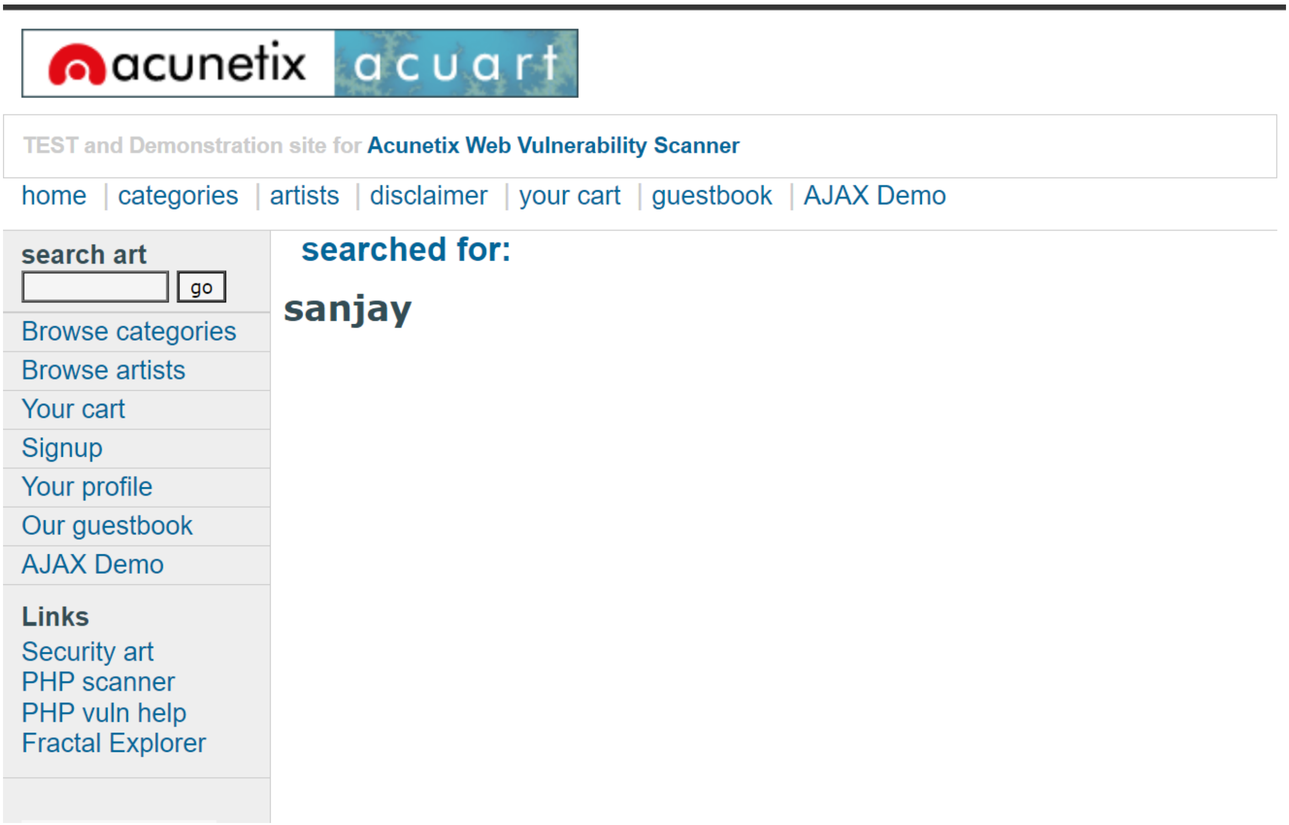
Step 2: type the html script in the search box


acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Links

<h1>sanjay</

searched for:

Step 3: The script affects the webpage



searched for:

sanjay

3. No Session Management

CWE: CWE-384

OWASP Category: A07:2021 –Identification and Authentication Failures

Description: An attacker is able to force a known session identifier on a user so that, once the user authenticates, the attacker has access to the authenticated session.

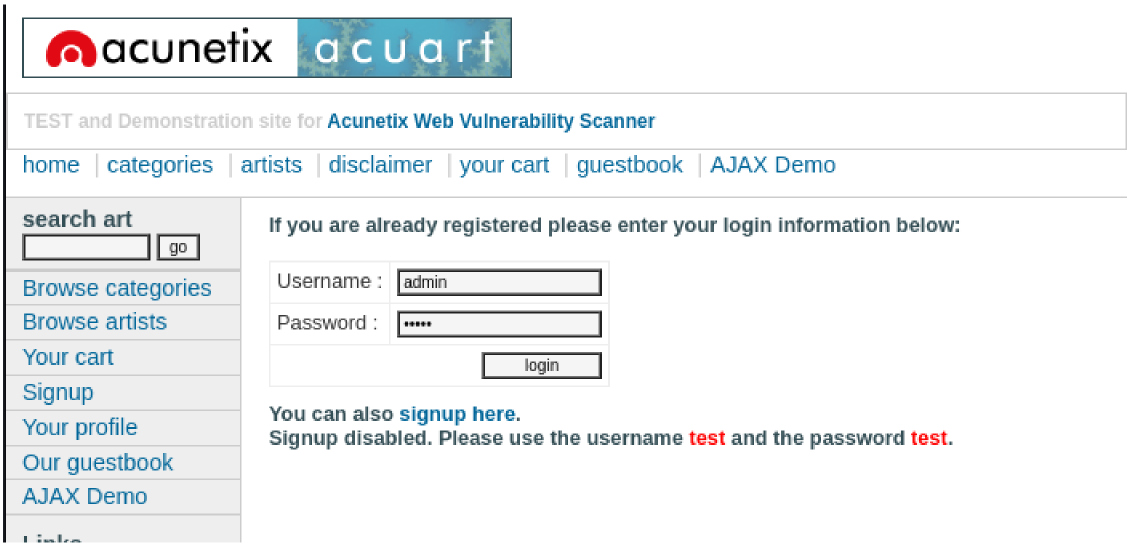
Business Impact: Without appropriate session management, you can run into several security problems, putting your users at risk. Common vulnerabilities caused by a lack of or poorly implemented session management include: Session hijacking

Vulnerability Path : http://testphp.vulnweb.com/logon.jsp

Vulnerability Parameter: http://testphp.vulnweb.com/login.jsp

Steps to Reproduce :

Step 1. Access the URL



TEST and Demonstration site for Acunetix Web Vulnerability Scanner

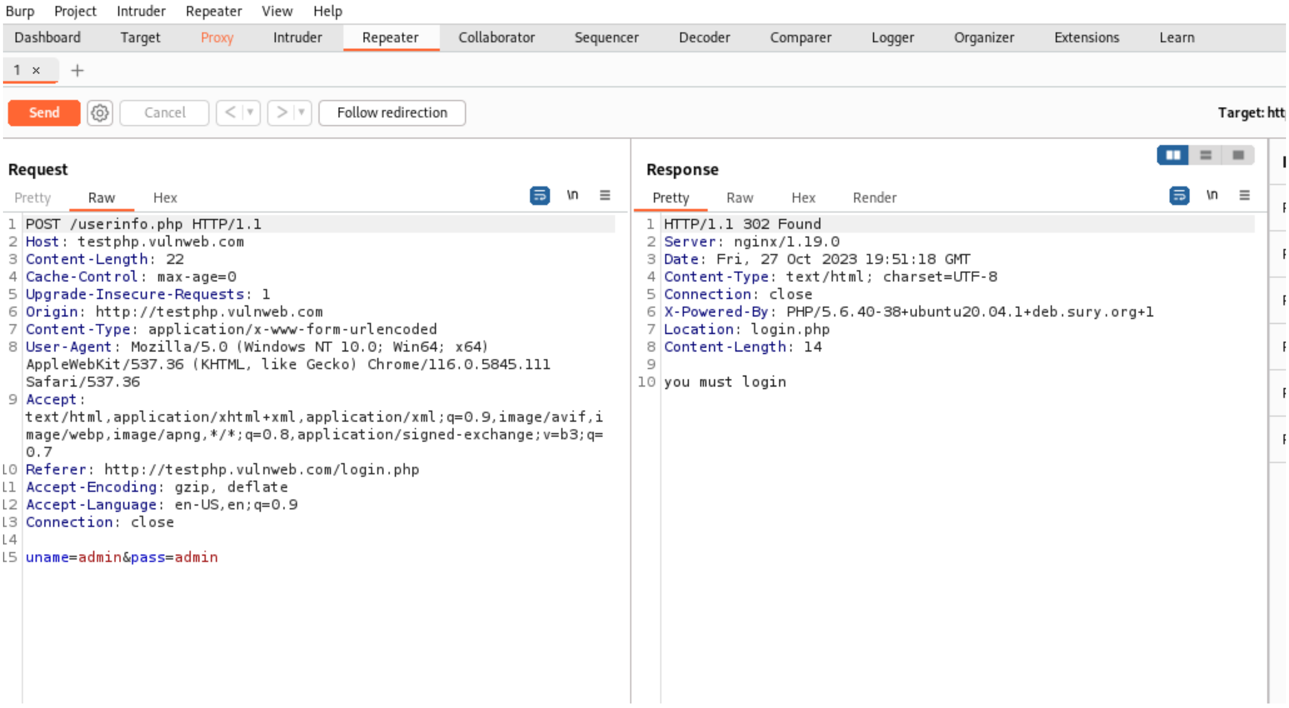
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

If you are already registered please enter your login information below:

Username :	admin
Password :	•••••
	login

You can also signup here.
Signup disabled. Please use the username test and the password test.

Step 2.without the proper session management the burp can still access the request of session as shown.



Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
1 ×
Send
Cancel
Follow redirection
Target: htt
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render

Request

```
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
Content-Length: 22
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://testphp.vulnweb.com
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.111
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
mage/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=
0.7
Referer: http://testphp.vulnweb.com/login.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

uname=admin&pass=admin
```

Response

```
HTTP/1.1 302 Found
Server: nginx/1.19.0
Date: Fri, 27 Oct 2023 19:51:18 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Location: login.php
Content-Length: 14

you must login
```

Recommendation:

- Invalidate any existing session identifiers prior to authorizing a new user session.

4. Default Credentials

CWE : CWE-1392

OWASP Category:A07:2021-Identification and Authentication Failures

Description:It is common practice for products to be designed to use default keys, passwords, or other mechanisms for authentication. The rationale is to simplify the manufacturing process or the system administrator's task of installation and deployment into an enterprise. However, if admins do not change the defaults, it is easier for attackers to bypass authentication quickly across multiple organizations.

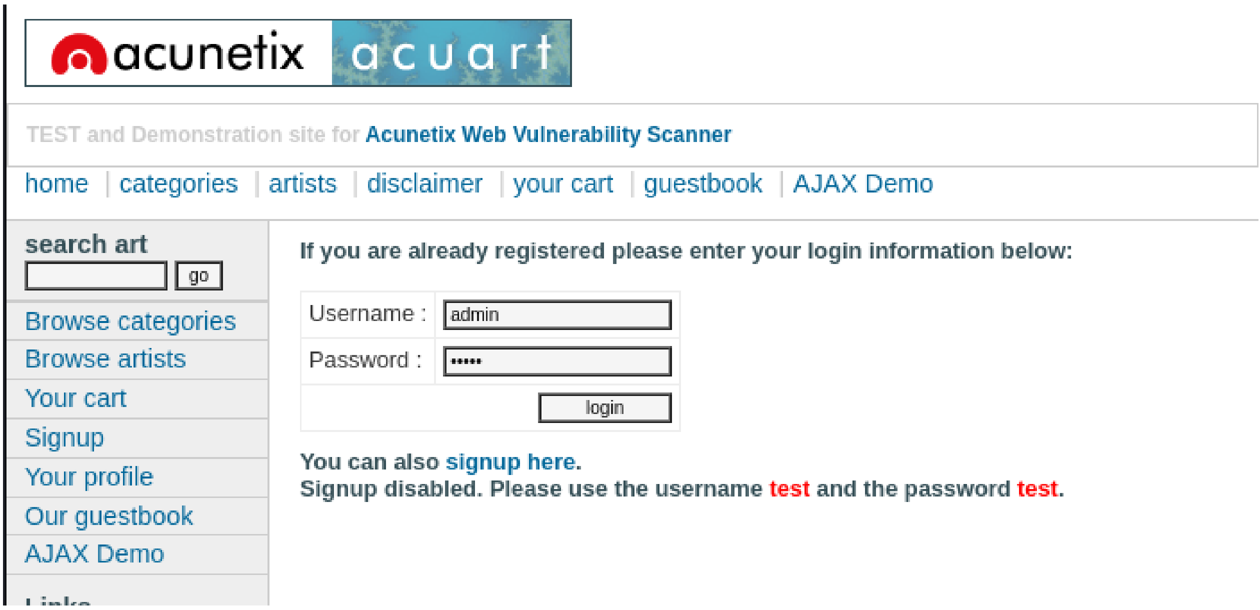
Business Impact:Attackers can easily obtain default passwords and identify internet-connected target systems. Passwords can be found in product documentation and compiled lists available on the internet.

Vulnerability Path : http://testphp.vulnweb.com/login.jsp

Vulnerability Parameter: http://testphp.vulnweb.com/login.jsp

Steps to Reproduce :

Step 1. Access the URL



TEST and Demonstration site for Acunetix Web Vulnerability Scanner

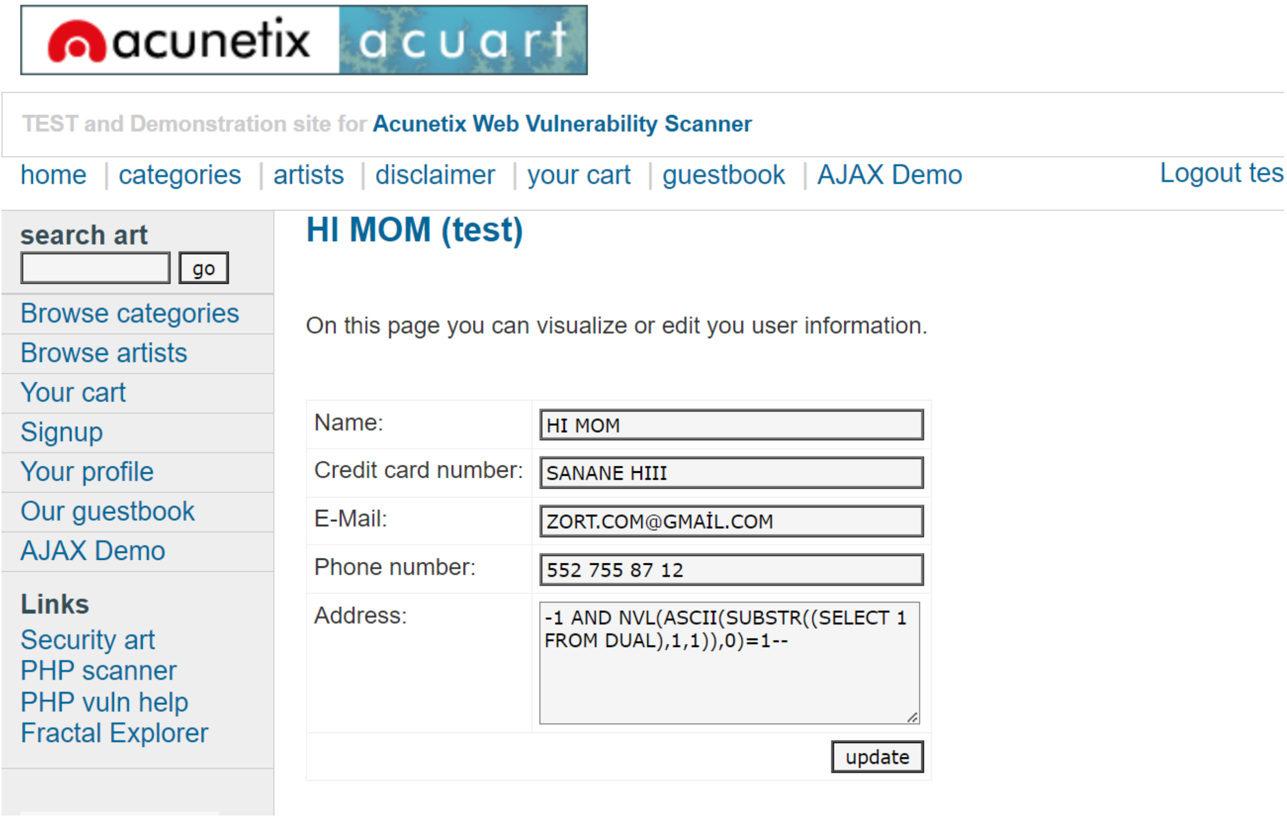
If you are already registered please enter your login information below:

Username : admin

Password : •••••

You can also signup here.
Signup disabled. Please use the username test and the password test.

Step 2: The website is based on apache tomcat server so we are able to login using a default user and password .



HI MOM (test)

On this page you can visualize or edit you user information.

Name:	HI MOM
Credit card number:	SANANE HIII
E-Mail:	ZORT.COM@GMAİL.COM
Phone number:	552 755 87 12
Address:	-1 AND NVL(ASCII(SUBSTR((SELECT 1 FROM DUAL),1,1)),0)=1--

Recommendation:

- Prohibit use of default, hard-coded, or other values that do not vary for each installation of the product - especially for separate organizations.

5. Clickjacking (Improper Restriction of Rendered UI Layers or Frames)

CWE :CWE-1021

OWASP Category: A04-2021- insecure design

Description:it occurs whenever a web application is fetching a remote resource without validating the user-supplied URL. It allows an attacker to coerce the application to send a crafted request to an unexpected destination, even when protected by a firewall, VPN, or another type of network access control list (ACL).

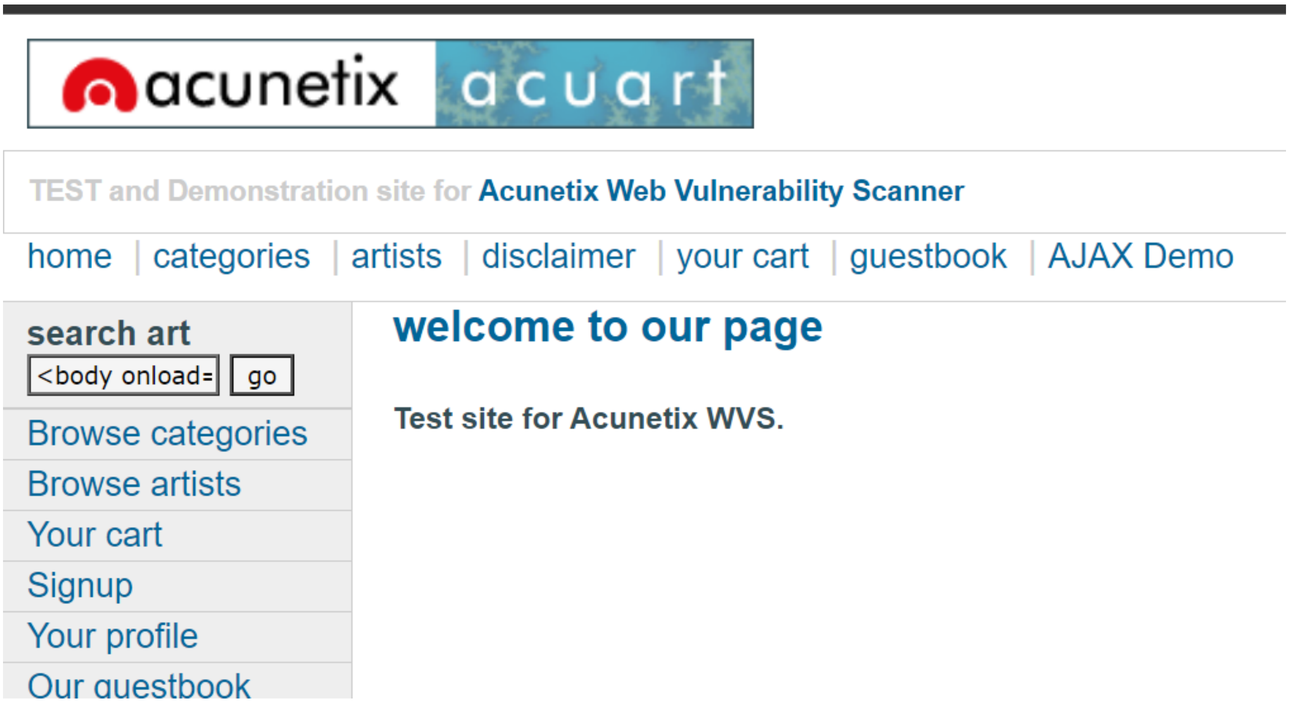
Business Impact: The common consequences of clickjacking include unauthorized actions, data theft, phishing, cookie theft, social engineering, reputation damage, legal and regulatory consequences, and user frustration. To prevent these, organizations should implement security headers, frame-busting techniques, user education, and regular security testing.

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

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

Steps to Reproduce :

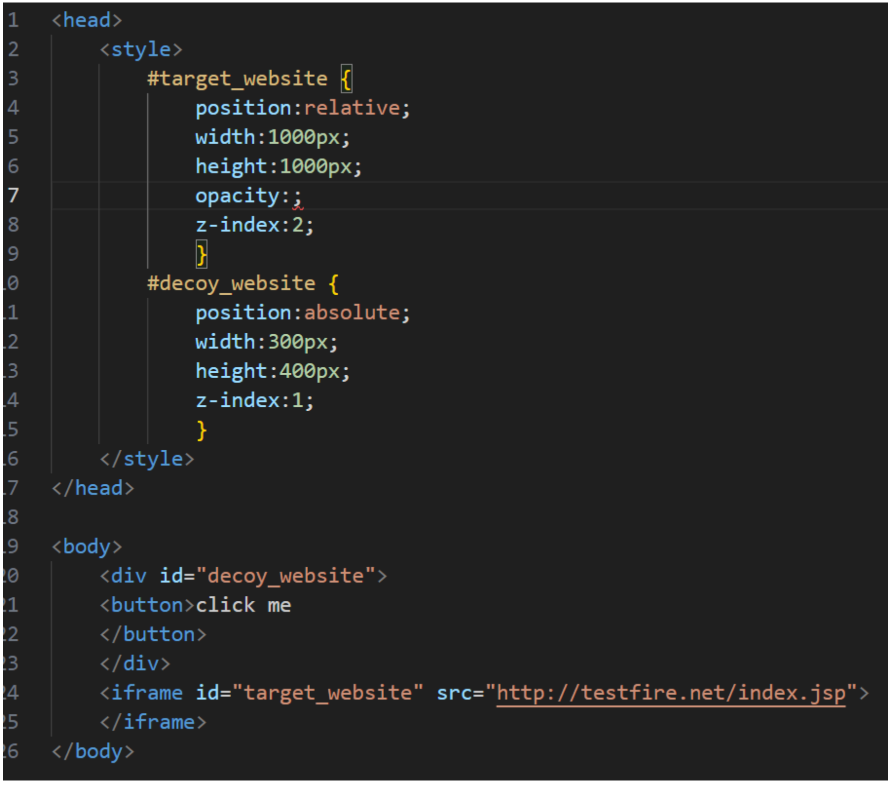
Step 1:- Access the URI


acunetix
acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
<body onload=
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook

welcome to our page

Test site for Acunetix WVS.

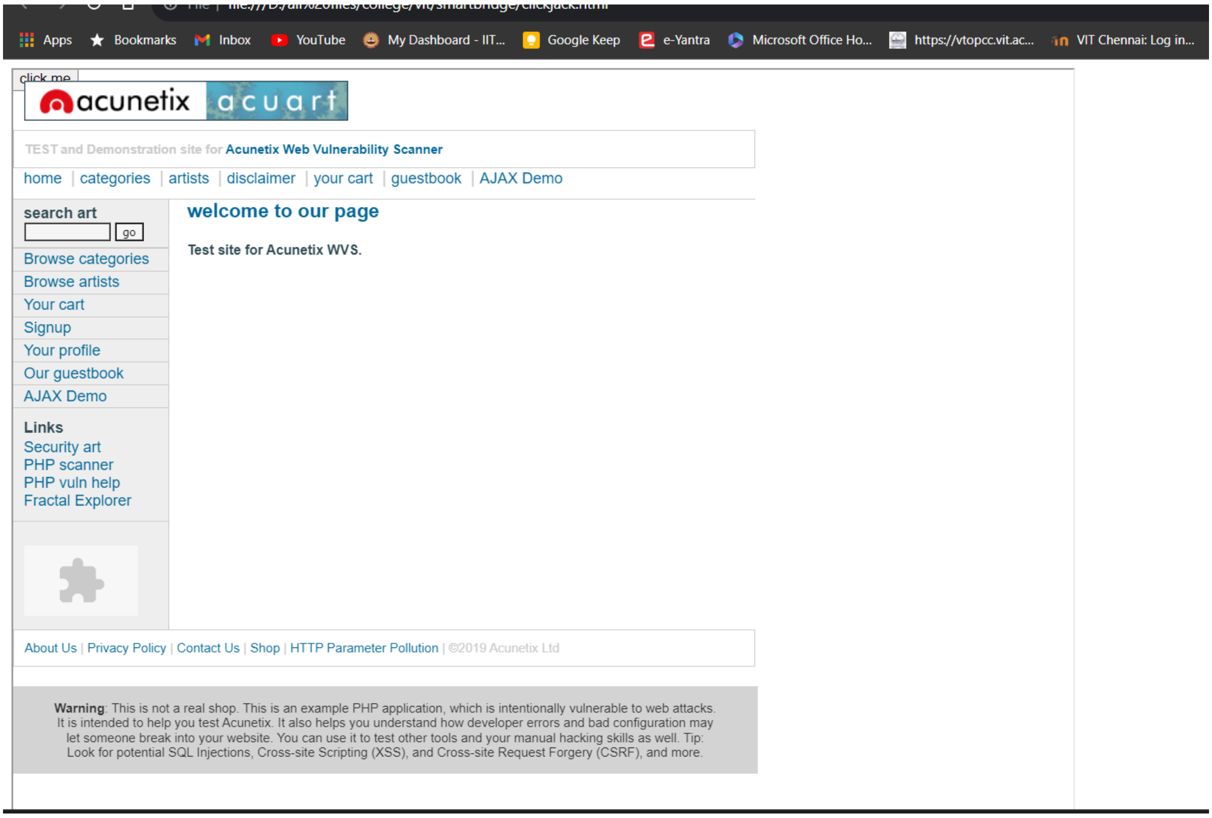
Step 2:- we write a html code as shown below when we run with the web address .



```html
<head>
    <style>
        #target_website {
            position:relative;
            width:1000px;
            height:1000px;
            opacity:;
            z-index:2;
            }
        #decoy_website {
            position:absolute;
            width:300px;
            height:400px;
            z-index:1;
            }
    </style>
</head>

<body>
    <div id="decoy_website">
    <button>click me
    </button>
    </div>
    <iframe id="target_website" src="http://testfire.net/index.jsp">
    </iframe>
</body>
```

Step 3:- this will be the output of clickjacking the website with html code .



TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art [ ] go

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer

welcome to our page

Test site for Acunetix WVS.

About Us | Privacy Policy | Contact Us | Shop | HTTP Parameter Pollution | ©2019 Acunetix Ltd

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

Recommendation:

- Segment remote resource access functionality in separate networks to reduce the impact of SSRF
- Enforce “deny by default” firewall policies or network access control rules to block all but essential intranet traffic.
- Enforce the URL schema, port, and destination with a positive allow list
- Do not send raw responses to clients
- Disable HTTP redirection

Stage 2

Nesssus scan:

Overview:

Nessus is a widely used and powerful vulnerability scanning tool that helps organizations identify and assess security weaknesses in their systems, including websites. Here's an overview of Nessus and its uses for vulnerability testing on a website:

1. **What is Nessus**: Nessus is a commercial vulnerability scanner developed by Tenable, Inc. It is designed to scan networks, systems, and applications for security vulnerabilities, misconfigurations, and other potential risks. It provides a comprehensive assessment of a target's security posture.
2. **Features**:
   - **Remote Scanning**: Nessus can scan devices and services remotely, making it a versatile tool for both internal and external network assessments.
   - **Plugin Architecture**: Nessus uses a plugin-based architecture that allows it to perform a wide range of security tests, including known vulnerability checks, compliance checks, and more.
   - **Customization**: Users can customize scan policies to focus on specific vulnerabilities or compliance standards.
   - **Comprehensive Reporting**: Nessus generates detailed reports that highlight vulnerabilities, severity levels, and remediation steps.
3. **Uses for Website Vulnerability Testing**: When it comes to website security, Nessus can be employed for several purposes:
   - **Identifying Common Vulnerabilities**: Nessus can scan web servers, applications, and databases to identify common vulnerabilities like SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF), and more.
   - **SSL/TLS Configuration Analysis**: Nessus can check the SSL/TLS configuration of a website to ensure secure encryption practices are in place and to identify potential vulnerabilities like weak ciphers or expired certificates.
   - **Content Scanning**: It can analyze website content for sensitive information leakage or data exposure, which is particularly important for compliance with data protection regulations.

- **Web Application Scanning**: Nessus can conduct authenticated scans of web applications, testing not only the infrastructure but also the application layer for vulnerabilities.
- **Compliance Checks**: It can assess websites for compliance with various security standards and regulations, such as PCI DSS, HIPAA, and GDPR.

4. **Workflow for Website Vulnerability Testing**:

   - Configure Nessus: Set up a scan policy in Nessus, specifying the target website or IP address, scan options, and any authentication credentials if needed.
   - Run the Scan: Initiate the scan, and Nessus will actively probe the website to identify vulnerabilities and misconfigurations.
   - Review Results: Once the scan is complete, review the generated reports. Nessus provides information about the vulnerabilities found, their severity, and potential fixes.
   - Remediation: Take necessary steps to address the identified vulnerabilities, following best practices and security guidelines.
   - Regular Scanning: Website security is an ongoing process. Regularly scan your website with Nessus to detect new vulnerabilities as they emerge and to ensure continuous protection.

Nessus is an essential tool for website administrators and security professionals to maintain the security and integrity of their web assets. However, it's important to use Nessus responsibly and ethically, respecting privacy and legal requirements, and obtaining proper authorization before scanning websites that you don't own or have explicit permission to scan.

Target WebSite : VIT Chennai website vtopcc.vit.ac.in

Target IP : 115.240.194.17

S.no	vulnerability	synopsis	Description	solutoin	riskfactor	Plugin info
1	HTTP Methods Allowed (per directory)	This plugin determines which HTTP methods are allowed on various CGI	By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.	n/a	None	Severity:Info ID:43111 Version:1.12 Type:remote Family:Web Servers Published:December 10, 2009 Modified:April 11, 2022

		directories.	The following HTTP methods are considered insecure: PUT, DELETE, CONNECT, TRACE, HEAD Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticated Users' 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			
2	HTTP/2 Cleartext Detection	An HTTP/2 server is listening on the remote host.	The remote host is running an HTTP server that supports HTTP/2 running over cleartext TCP (h2c).	Limit incoming traffic to this port if desired.	None	Severity:Info ID:85805 Version:1.8 Type:remote Family:Web Servers Published:September 4, 2015 Modified:April 11, 2022
3	HyperText Transfer Protocol (HTTP) Information	Some information about the remote HTTP configuration can be extracted.	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	n/a	None	Severity:Info ID:24260 Version:1.14 Type:remote Family:Web Servers Published:January 30, 2007 Modified:November 22, 2019

			security problem			
4	HyperText Transfer Protocol (HTTP) Redirect Information	The remote web server redirects requests to the root directory.	The remote web server issues an HTTP redirect when requesting the root directory of the web server. This plugin is informational only and does not denote a security problem.	Analyze the redirect(s) to verify that this is valid operation for your web server and/or application.	None	Severity:Info ID:91634 Version:$Revision: 1.2 $ Type:remote Family:Web Servers Published:June 16, 2016 Modified:October 12, 2017
5	Nessus SYN scanner	It is possible to determine which TCP ports are open	This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.	Protect your target with an IP filter	None	Severity:Info ID:11219 Version:1.57 Type:remote Family:Port scanners Published:February 4, 2009 Modified:September 25, 2023
6	Nessus Scan	This plugin	This plugin displays, for	n/a	None	Severity:Info ID:19506

	Information□	displays information about the Nessus scan.	each tested host, information about the scan itself : - The version of the plugin set. - The type of scanner (Nessus or Nessus Home). - The version of the Nessus Engine. - The port scanner(s) used. - The port range scanned. - The ping round trip time - Whether credentialed or third-party patch management checks are possible. - Whether the display of superseded patches is enabled - The date of the scan. - The duration of the scan. - The number of hosts scanned in parallel. - The number of checks done in parallel.			Version:1.119 Type:summary Family:Settings Published:August 26, 2005 Modified:July 31, 2023
7	Web Server No 404	The remote web	The remote web server is configured	n/a	None	Severity:Info ID:10386 Version:1.100

	Error Code Check	server does not return 404 error codes.	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.			Type:remote Family:Web Servers Published:April 28, 2000 Modified:June 17, 2022

Stage 3 Report

Real-time protection against cyber threats using SOC and SIEM Integration

- **Soc (Security operations center)**

SOC is critical in continually monitoring a company's network, systems, and applications. It is capable of detecting and responding to possible security problems such as malware infections, data breaches, and so on. illegal access attempts. When a security event happens, time is of the essence. the essential. SOC teams are trained to respond quickly and effectively to incidents. Security breaches must be contained and mitigated. SOC does not exist. It does more than just respond to incidents; it proactively discovers weaknesses and threats. Infrastructure flaws in the organization. This proactive strategy allows businesses to improve their security posture and deploy precautions to avoid future assaults. SOC offers round-the-clock monitoring. ensuring that security analysts are always alert and prepared to respond regardless of the time of day, and respond to developing dangers.

SOC is an essential component of a strong cybersecurity strategy. It enables enterprises to identify, respond to, and avoid cyber attacks while also protecting sensitive data. sustaining business continuity and the organization's reputation reputation in an increasingly linked and risky digital world SOC serves as the focal center for incident coordination and response. communication. It makes it easier for multiple teams, such as IT, to collaborate. Legal, communications, and senior management ensure a unified front and efficient reaction to security problems.

- **SOC Cycle**

SOC life Cycle has three general categories.

1. **Preparation, planning, and prevention**

Asset Cataloging: An SOC must uphold a comprehensive inventory of all resources requiring protection, encompassing both in-house and external assets such as applications, databases, servers, cloud services, endpoints, and more. Additionally, all protective tools employed (firewalls, anti-malware software, monitoring utilities, etc) should be included in the inventory. Utilizing an asset discovery solution is a common practice among SOCs.

Ongoing Maintenance and Readiness: To enhance the efficacy of security protocols and tools in operation, the SOC implements routine preventative upkeep – from applying software patches and updates to persistently modifying firewalls, whitelists and blacklists, security policies, and procedures. The SOC may also establish system backups or guide in devising backup strategies to guarantee sustained business operations throughout data breaches or cybersecurity events.

Incident Reaction Coordination: The SOC assumes responsibility for devising the organization's incident response strategy – outlining actions, duties, and designated roles during potential threats or incidents while determining metrics to evaluate the effectiveness of incident management.

Frequent Evaluations: The SOC team conducts regular vulnerability assessments to gauge the susceptibility of each resource to probable hazards as well as associated costs. Penetration tests simulating targeted attacks on specific systems are also executed. Assessment outcomes inform consequential modifications to applications, security procedures, best practices as well and response strategies.

Current Developments: Continual vigilance characterizes SOC activity as they strive to stay informed about cutting-edge security solutions and technologies while monitoring recent threat intelligence. This involves tracking news on cyberattacks and relevant offenders using sources such as social media, industry insiders, or dark web communication channels.

2. Monitoring, detection and response

Round-the-clock security monitoring is essential for maintaining the integrity of an organization's IT infrastructure. The Security Operations Center (SOC) diligently oversees every facet of the system, including applications, servers, system software, computing devices, cloud workloads, and the network itself. This 24/7/365 supervision helps detect known exploits and identify any unusual activity.

The key technology for many SOCs is Security Information and Event Management (SIEM), which serves as the cornerstone of monitoring, detection, and response. By monitoring and aggregating real-time alerts and telemetry data from network software and hardware components, SIEM analyzes this information to pinpoint potential threats. Moreover, some SOCs have started adopting Extended Detection and Response (XDR) technology to enhance their telemetry monitoring capabilities and streamline incident detection and response operations.

Log management deserves its place as a critical subset of security monitoring. Collecting and scrutinizing log data generated during various network events provides a baseline of activity that helps uncover any deviations suggestive of suspicious activities. Many hackers rely on organizations neglecting to analyze log data thoroughly, allowing their viruses or malware to remain undetected for prolonged periods. Most SIEM platforms offer integrated log management functionality.

Within threat detection operations at the SOC, discerning genuine cyber threats from benign false positives is vital. Teams triage identified threats based on severity.

State-of-the-art SIEM systems feature artificial intelligence that streamlines detection processes while improving threat recognition accuracy over time.

When facing an imminent threat or actual security incident, SOC teams deploy various measures to mitigate its impact:

- Identifying the root cause to determine technical vulnerabilities exploited by hackers as well as uncovering other contributing factors such as poor password practices or inadequate policy enforcement
- Isolating compromised endpoints or disconnecting them from the network
- Securing compromised sections of the network or redirecting network traffic
- Temporarily suspending or terminating affected applications or processes
- Removing damaged or contaminated files
- Executing antivirus or anti-malware software
- Revoking passwords for internal and external users

Many XDR platforms empower SOCs to automate and expedite these and other incident response operations, elevating overall security efficacy.

3. Recovery, refinement, and compliance

Recovery and Remediation: Following the containment of a security incident, the Security Operations Center (SOC) neutralizes the threat and restores affected assets to their pre-incident state. This may involve wiping, restoring, and reconnecting disks, devices, endpoints, network traffic, applications, and processes. In cases of data breaches or ransomware attacks, recovery could also require switching to backup systems and resetting passwords and authentication credentials.

Post-Mortem and Refinement: To mitigate the likelihood of future occurrences, the SOC leverages new intelligence acquired from incidents to address vulnerabilities more effectively. Updating procedures, policies, and cybersecurity tools, or revising the incident response plan are essential steps in these processes. Furthermore, the SOC team aims to identify emerging or evolving cybersecurity trends based on incident analysis to enhance preparedness.

Compliance Management: The responsibility of ensuring that applications, systems, security tools, and procedures adhere to data privacy regulations falls under the purview of SOC. These regulations include GDPR (Global Data Protection Regulation), CCPA (California Consumer Privacy Act), PCI DSS (Payment Card Industry Data Security Standard), and HIPAA (Health Insurance Portability and Accountability Act). Following an incident, the SOC ensures proper notification of users, regulators, law enforcement agencies, and other relevant parties as mandated by regulations while retaining necessary incident data for evidence and auditing purposes.

- **SIEM (**Security Information and Event Management**)**

Security Information and Event Management (SIEM) is an essential and highly effective technology in the domain of cybersecurity, acting as the unwavering protector of an organization's digital assets. It persistently monitors the extensive and intricate digital environments, safeguarding against emerging threats, vulnerabilities, and possible security breaches. At its essence, SIEM is a comprehensive solution integrating two crucial functionalities: security information management (SIM) and security event management (SEM). The SIM facet concentrates on gathering, examining, and correlating data from various sources like log files, security events, and network traffic – all of which generate valuable insights into an organization's security posture. In contrast, SEM centers around real-time event correlation and threat detection, promptly detecting anomalies and potential breaches necessitating immediate action.

The role of a SIEM system is multifaceted. Its primary objective is to offer centralized visibility across an organization's entire IT infrastructure, encompassing networks, devices, applications, and user activities. This all-encompassing perspective equips security teams to monitor real-time events and rapidly identify anomalies. By aggregating data from multiple sources, SIEM creates a unified and coherent understanding of the security landscape – essential in today's distributed and complicated IT environments. Threat detection remains a fundamental aspect of SIEM. Leveraging advanced analytics and correlation techniques, SIEM systems proficiently detect security threats by scrutinizing data from diverse sources. This analytical capability aids in pinpointing unusual patterns or actions that could signify a security incident. SIEM's real-time alerting mechanisms ensure that security teams receive prompt notification when potential threats are detected. Compliance is a significant consideration across various industries, with SIEM systems playing a valuable supporting role. They aid organizations in complying with regulatory requirements by efficiently collecting, storing, and reporting security-related data. This not only guarantees compliance but also streamlines the auditing process – saving time and resources.

SIEM platforms also excel in their log management capabilities, adeptly gathering and storing log information from a variety of sources – a critical aspect for forensic analysis and reconstructing security incidents. This log data proves indispensable when attempting to comprehend an attack's progression or demonstrating compliance with security standards.

Lastly, SIEM shines in monitoring insider threats. By observing user activities and behavioral patterns, SIEM systems can discern potential internal threats involving employees or contractors. This ability has become ever more valuable in the modern landscape, where insider threats continue to grow as a major concern.

- **SIEM Cycle**

The life cycle of a Security Information and Event Management (SIEM) system encompasses various integral stages that guarantee the proficient implementation, operation, and preservation of the SIEM solution. The SIEM life cycle usually comprises the subsequent phases:

1. Planning and Assessment:

Outline the objectives and scope for the SIEM implementation, taking into account the organization's security requisites and compliance aims. Perform an extensive evaluation of the current security infrastructure, data sources, and log management tactics to pinpoint disparities and indispensable enhancements. Formulate a meticulous plan for deploying the SIEM solution, encompassing resource distribution, schedule, and accountabilities.

2. Design and Architecture:

Construct the SIEM architecture grounded on the organization's requirements and data sources, contemplating elements such as scalability, redundancy, and performance. Ascertain the optimal deployment model (on-premises, cloud-based, or hybrid) that corresponds with the organization's preferences and resources. Organize the incorporation of data sources into the SIEM, guaranteeing pertinent security events are gathered and centralized for examination.

3. Data Collection and Integration:

Employ data collectors and agents to amass logs and events from a range of sources, including firewalls, network devices, servers, applications, and endpoints.

Standardize and augment the gathered data to enable effective analysis and association.

Establish connectors and parsers to assimilate data streams from security apparatuses and other sources into the SIEM framework.

4. Event Correlation and Analysis:

Formulate and refine correlation rules and use cases to recognize malicious activity patterns and security risks. Carry out real-time event association and analysis to produce actionable alerts concerning potential security incidents. Leverage threat intelligence feeds to bolster the SIEM's capacity for detecting emerging hazards and establishing attack vectors.

5. Incident Detection and Response:

Launch incident response measures, encompassing containment, elimination, and restoration.

Undertake comprehensive forensic scrutiny to comprehend incident origins and assailant methodologies. Safeguard and document evidence for prospective legal or regulatory purposes.

6. Forensics and Investigation:

Address generated warnings by examining potential security occurrences.

Execute in-depth analysis to ascertain the extent and implications of identified security incidents.

7. Reporting and Compliance:

Generate and convey security reports and dashboards for various stakeholders such as IT management, executives, auditors, as well as regulatory authorities. Guarantee compliance with pertinent industry standards and regulations through constant monitoring and reporting of security events and incidents.

8. Continuous Monitoring & Maintenance:

Persistently oversee SIEM infrastructure while adjusting configurations as required for optimal performance. Update correlation rules and threat intelligence feeds, along with other components regularly to ensure sustained SIEM effectiveness against emerging threats. Perform systematic reviews & assessments of SIEM's performance & efficacy for improvement identification.

9. Training & Knowledge Transfer:

Educate SOC staff & IT personnel in proficient utilization of the SIEM solution.

Encourage knowledge exchange & best practices across the organization through incident investigations & analyses.

The SIEM lifecycle is a perpetual, iterative process whereby each phase is informed by insights & experiences gleaned from previous stages. This methodology guarantees the continued relevance, efficiency, & effectiveness of the SIEM solution in aiding organizations to detect & respond to security dangers.

- MISP (Malware Information Sharing Platform & Threat Sharing)

MISP (Malware Information Sharing Platform and Threat Sharing) is a sophisticated and all-encompassing threat intelligence platform engineered to address the ever-changing cybersecurity landscape. It functions as a central repository for exchanging, preserving, and correlating a diverse range of indicators of compromise (IoCs) associated with targeted attacks, threat intelligence, financial fraud, vulnerability information, and counter-terrorism data. This invaluable instrument presents organizations with a collaborative environment to bolster their joint defense against cyber threats.

MISP's core functions comprise Security Information Management (SIM) and Security Event Management (SEM). SIM is dedicated to collecting and analyzing data from various sources, such as log files, security events, and network traffic, to deliver a comprehensive perspective on an organization's security posture. Conversely, SEM excels in real-time event correlation and threat detection, facilitating the swift identification of anomalies necessitating immediate action.

Central to MISP's capabilities is its efficient incident response mechanism. This feature empowers security teams to accurately assess alerts, establish the extent of incidents, and swiftly respond to neutralize threats. In the rapidly evolving domain of cybersecurity, this prompt reaction can delineate the distinction between a minor security event and a significant data breach.MISP's distinctive advantage lies in its compliance capabilities. It assists organizations in fulfilling regulatory requirements by effectively accumulating, preserving, and reporting security-related data. This compliance support streamlines the auditing process and guarantees adherence to security standards.MISP emerges as an expert in threat detection by employing state-of-the-art analytics and correlation techniques to identify security threats through the examination of data from multiple sources. By detecting atypical patterns or behaviors that might signify a security incident, MISP's real-time alerting mechanisms assure that security teams are promptly notified when potential threats surface.

Furthermore, MISP occupies a crucial position in monitoring insider threats. By scrutinizing user activities and behavioral patterns, it can identify possible insider threats involving employees or contractors. This function is increasingly vital in the contemporary landscape, where insider threats are a mounting concern.MISP's collaboration features foster efficient information sharing and collective analysis. It enables users to suggest modifications or updates to attributes and indicators. Its data-sharing feature facilitates automated exchange and synchronization with other parties and trust groups utilizing MISP. The platform's feed import functionality eases the integration of third-party threat intelligence and open-source intelligence feeds, augmenting an organization's capacity to remain current on emerging threats.MISP's integration capabilities with various systems are remarkably smooth and efficient. The platform can generate Intrusion Detection System (IDS) rules for Snort, Suricata, and Bro, demonstrating its versatility. Additionally, it facilitates exports in a diverse range of formats like OpenIOC, plain text, CSV, MISP XML, or JSON. This broad compatibility targets seamless integration with an array of security tools such as network IDS, host IDS, and bespoke applications. Moreover, MISP offers a robust and flexible free-text import tool designed to simplify the incorporation of unstructured reports into the platform.

Exhibiting excellent scalability, MISP is aptly suited to cater to organizations with diverse sizes and complexities. It serves as an indispensable resource for sharing information and fostering collaboration on security events and attributes. Consequently, this enhances the ease of data exchange via different distribution models.

- How do you think you would deploy soc in your college?

Establishing a Security Operations Center (SOC) within an organization necessitates meticulous planning, strategic resource distribution, and a systematic methodology. The following pivotal steps will aid in the successful implementation of a SOC:

1. Appraisal and Requirements Collection:

- Perform an exhaustive evaluation of the company's existing cybersecurity stance, encompassing current safety measures, tools, and workflows.

- Recognize the distinct security issues, risks, and compliance obligations that the SOC will confront.

- Ascertain the aims and objectives of the SOC implementation to synchronize with the organization's comprehensive security plan.

2. Budgeting and Resource Distribution:

- Calculate the financial and resource prerequisites for creating and sustaining the SOC.

- Assign staff, hardware, software, and other indispensable resources to bolster SOC functions.

3. Assemble a Competent Team:

- Hire or designate proficient security experts to compose the SOC ensemble.

- The group should comprise security analysts, incident responders, threat pursuers, and SOC managerial personnel.

4. Infrastructure and Technological Configuration:

- Construct the physical or virtual foundation for the SOC, including servers, networking equipment, and storage facilities.

- Implement crucial security technologies such as SIEM, intrusion detection and prevention systems (IDS/IPS), firewalls, endpoint protection, and threat intelligence channels.

5. Integration and Data Accumulation:

- Consolidate security apparatuses and systems with the SIEM to centralize log and event data acquisition.

- Confirm that vital data sources like firewalls, servers, network devices, and applications are contributing logs to the SIEM.

6. Establishment of Processes and Protocols:

- Formulate standard operating procedures (SOPs) for an array of SOC tasks like incident management, response methods, escalation processes, and communication guidelines.

- Adopt incident classification and prioritization mechanisms.

7. Implementation of Monitoring and Notification:

- Tailor the SIEM to generate instantaneous alerts based on established correlation rules and security use cases.

- Refine alerting thresholds to mitigate false positives and concentrate on critical notifications.

8. Incident Management and Escalation:

- Devise a formal incident response strategy, detailing action steps for addressing security incidents.
- Specify roles and accountabilities for incident management, and establish a transparent escalation route for severe incidents.

9. Training and Expertise Enhancement:

- Deliver comprehensive education to the SOC team in areas such as security tool usage, incident investigation, threat hunting, and best practices in incident response.

10. Staying Informed on Cybersecurity Developments:

- Ensure the team remains well-informed about the latest cybersecurity trends, emerging attack methods, and pertinent certifications.

11. Testing and Ongoing Enhancement:

- Implement periodic tabletop exercises and simulated cyber attack scenarios to assess the SOC team's capabilities in handling incidents.
- Utilize the knowledge obtained from these tests to optimize and refine the SOC's processes and methodologies.

12. Performance Monitoring and Communication:

- Continuously evaluate the SOC's effectiveness in detecting and addressing security incidents.
- Generate comprehensive reports and performance metrics to demonstrate the SOC's value to stakeholders and facilitate communication.

13. Collaboration with IT and Business Operations:

- Encourage a cooperative relationship between the SOC, IT, and business departments for a unified approach to security.
- Engage with executive management and board members to obtain support for SOC initiatives.

14. Constant Adaptation and Improvement:

- Recognize that operating a SOC is an ongoing commitment that demands adaptability and continuous enhancement. Frequent evaluations, training sessions, and updates are crucial to ensure the SOC remains proficient in addressing the organization's dynamic security landscape.

- Threat Intelligence

Threat intelligence, often referred to as 'cyber threat intelligence' (CTI) or simply 'threat intel,' comprises data that imparts extensive knowledge regarding the cybersecurity risks aimed at an organization. By adopting threat intelligence, security teams can act more proactively—facilitating well-informed, data-driven decisions that help prevent cyber attacks before they even transpire. Furthermore, threat intelligence can significantly aid organizations in detecting and responding to ongoing attacks.

To generate threat intelligence, security analysts gather raw threat data and security-related information from numerous sources. They then process this data through correlation and analysis techniques to identify trends, patterns, and connections that yield a comprehensive understanding of actual or potential threats. The resultant intelligence is characterized by the following traits:

1. Organization-specific: Instead of relying on generalities (e.g., commonly known malware strains), threat intelligence zeroes in on the unique vulnerabilities present within an organization's attack surface, examining the enabled attacks and exposed assets.

2. Detailed and contextual: This intelligence covers not only threats targeted at a company but also the potential threat actors who might execute these attacks. Additionally, it encompasses the tactics, techniques, and procedures (TTPs) employed by such threat actors, as well as the indicators of compromise (IoCs) that may signify a specific cyber attack.

3. Actionable: Threat intelligence furnishes information that enables security teams to pinpoint vulnerabilities, prioritize and mitigate threats, as well as assess existing or novel cybersecurity tools.

As per IBM's Cost of a Data Breach 2022 report, the average financial impact of a data breach is approximately USD 4.35 million—with detection and escalation fees constituting the largest expense at USD 1.44 million. Therefore, by leveraging threat intelligence, security teams can access vital information that helps them identify attacks earlier on—effectively diminishing detection costs while mitigating the consequences of successful breaches.

- Incident Response

Incident response, also known as cybersecurity incident response, encompasses an organization's methodologies and technological systems for the detection and management of cyber threats, security violations, and cyber assaults. The primary objective of an incident response strategy is to proactively prevent cyberattacks while minimizing the financial and operational consequences arising from any that do transpire.

A comprehensive incident response plan (IRP) should be established by an organization to outline the specific procedures and technologies required for identifying, mitigating, and resolving various types of cyberattacks. A proficient IRP allows cybersecurity teams to detect, contain, and recover from cyber threats more rapidly while reducing the financial losses, regulatory penalties, and other expenses associated with these threats. As demonstrated in IBM's 2022 Cost of a Data Breach Report, organizations equipped with incident response teams and routinely tested IRPs experienced data breach costs that were USD 2.66 million lower on average than those without such teams or plans.

- Qradar & understanding of this tool

The QRadar security intelligence platform operates through a three-layered framework, applicable to any deployment configuration, independent of its dimensions or intricacy. The subsequent illustration exhibits the layers constituting the QRadar infrastructure.

Despite the size or quantity of components within a deployment, the QRadar architecture maintains consistent functionality. The diagram displays three key layers that encapsulate the fundamental operations of all QRadar systems.

1. Data Collection

As the initial layer, data collection encompasses retrieving data such as events or flows from your network. The All-in-One appliance is capable of extracting this data directly or through collectors, such as QRadar Event Collectors or QRadar QFlow Collectors for event and flow data. Upon collection, data undergoes parsing and normalization before entering the processing layer. The parsed raw data transforms into a structured and accessible format.

QRadar SIEM's primary functionality lies in collecting event and flow data. Event data signifies occurrences at specific moments within the user's environment, including user logins, emails, VPN connections, firewall denies, proxy connections, and other logged events. Flow data represents network activity information or session details between two hosts and translates into flow records within QRadar. This conversion incorporates IP addresses, ports, byte and packet counts, and additional information into flow records that depict a session between two hosts. Additionally, full packet capture is available via the QRadar Incident Forensics component when using Flow Collectors.

2. Data Processing

The second layer involves processing collected event and flow data through the Custom Rules Engine (CRE), generating offenses and alerts before writing this data to storage. This processing can occur on an All-in-One appliance without necessitating Event Processors or Flow Processors.

However, if the processing capacity of an All-in-One appliance becomes exceeded, incorporating Event Processors, Flow Processors, or other processing appliances may become necessary to accommodate increased requirements. Additional storage capacity is achievable through the integration of Data Nodes.

3. Extended Functionality

QRadar also features other tools such as QRadar Risk Manager (QRM), QRadar Vulnerability Manager (QVM), and QRadar Incident Forensics, which collect diverse data types and offer expanded functionality.

QRadar Risk Manager is designed to gather and analyze network infrastructure configurations while generating a comprehensive map of your network topology. By employing this data, you can effectively manage risk by simulating various network situations via modifying configurations and deploying rules across your network. Utilize QRadar Vulnerability Manager for scanning your network and processing vulnerability data or overseeing the information collected from alternative scanners like Nessus and Rapid7. The amassed vulnerability data is crucial for detecting potential security threats within your network.

QRadar Incident Forensics offers a platform for conducting in-depth forensic investigations and replaying entire network sessions. In the uppermost layer, QRadar provides users with access to collected and processed data for search, analysis, reporting, and alerts or offense inquiries. Users are enabled to search and administer security tasks for their networks via the user interface located on the QRadar Console.

In an All-in-One system, all data collection, processing, and storage takes place within the All-in-One appliance. In distributed environments, the QRadar Console does not engage in event or flow processing, or storage functions. The Console primarily serves as a user interface for executing searches, reports, alerts, and investigations.

Leverage IBM QRadar components to expand your QRadar deployment and manage data collection as well as processing in distributed networks. IBM QRadar appliances boast certification for supporting specific maximum events per second (EPS) rates. Factors such as data type being processed, system configuration, and system load determine maximum EPS.

IBM QRadar SIEM's core functions involve overseeing network security by monitoring events and flows across the network. This refined content captures the original structure while presenting it professionally and engagingly to enhance fluency.

Conclusion

Phase 1: *Understanding Web Application Testing*

Web application testing is a comprehensive process designed to certify the security, reliability, and functionality of a web application. The objective is to uncover and rectify potential vulnerabilities, glitches, and usability issues that could compromise application performance and user experience. An effective web application testing strategy delivers the following outcomes:

- Identification of Security Risks
- Bug Discovery and Resolution
- Verification of Functional Specifications
- Usability and User Experience Assessment
- Appraisal of Performance and Load Handling Abilities
- Compatibility Testing Observations
- Adherence to Accessibility Standards
- Security Compliance and Risk Mitigation Measures
- Optimization Suggestions
- Augmented Quality Assurance
- Boosted Customer Confidence
- Compliance to Regulatory Mandates

In essence, the end-result of rigorous web application testing is an advanced, secure, and reliable web application that fulfills user expectations and offers a seamless interaction for its users. It equips developers and stakeholders with the assurance that the application is primed for deployment, capable of warding off potential security threats, and equipped to handle performance bottlenecks.

Phase 2: *Comprehending the Nessus Report*

Nessus serves as a potent vulnerability scanning instrument that detects and reports security lapses in computer systems and networks. The output of a Nessus report is contingent on the specific target scanned and the vulnerabilities unearthed. Typically, a Nessus report enumerates the identified vulnerabilities, categorizing them based on their severity levels, provides intricate descriptions, and recommends remediation strategies. Severity levels are generally classified as critical, high, medium, and low, based on the potential impact and exploitability of the vulnerability.

Phase 3: *Decoding the SOC / SEIM / Qradar Dashboard*

The SOC (Security Operations Center) is fundamentally designed to monitor and shield an organization's IT infrastructure from security threats and incidents. SOC analysts employ a variety of tools and technologies to detect, analyze, and react to security incidents in real time. The anticipated outcomes of a high-performing SOC encompass:

a. Enhanced Threat Detection: SOC analysts vigilantly monitor network traffic, log data, and security alerts, enabling swift identification of potential threats and security incidents.

b. Expedited Incident Response: A well-set-up SOC empowers organizations to react swiftly to security incidents, thereby mitigating the impact of data breaches or cyber-attacks.

c. Fortified Security Posture: A proactive SOC aids organizations in implementing robust security measures and continually enhancing their overall cybersecurity framework.

d. Diminished Downtime and Financial Losses: Swift detection and mitigation of security incidents can significantly reduce downtime and financial losses ensuing from cyber-attacks.

Future Scope

Phase 1: *Future Scope of Web Application Testing for Malware Detection and Classification*

The future scope of malware detection and classification within web application testing is promising and crucial in our increasingly digital world. With the rapid growth of web applications, both in number and complexity, there is a pressing need for more advanced and proactive measures to detect and classify malware. Artificial intelligence and machine learning are likely to play a significant role in this context. These technologies can analyze vast datasets to identify patterns and anomalies, enabling the detection of previously unseen malware variants. Moreover, the integration of threat intelligence feeds and the development of sophisticated behavioral analysis techniques will become essential to keep up with the evolving threat landscape. Additionally, the automation of testing processes and the use of sandboxing environments for testing will improve the efficiency of malware detection in web applications.

Phase 2: *Future Scope of Testing Processes for Malware Detection and Classification*

In the domain of malware detection and classification, the future scope of testing processes will involve streamlining and enhancing the methodologies used to identify, isolate, and analyze malicious software. One key area of development lies in the incorporation of DevSecOps practices, where security is seamlessly integrated into the software development lifecycle. This approach ensures that potential vulnerabilities and malware are detected and addressed at the earliest stages of application development. Additionally, the use of containerization and microservices architectures will require innovative testing approaches, as malware can potentially propagate within such environments. The adoption of continuous testing and security testing automation tools will become indispensable for ensuring that software remains free from malware throughout its lifecycle

Phase 3: *Future Scope of SOC and SIEM in Malware Detection and Classification*

The future scope of Security Operations Centers (SOC) and Security Information and Event Management (SIEM) systems in the context of malware detection and classification is poised for significant evolution. SOC teams will increasingly leverage advanced analytics and machine learning algorithms to detect complex and stealthy malware threats in real time. The integration of threat intelligence from various sources and the development of predictive analytics will be vital for proactive threat detection. Moreover, SIEM systems will continue to evolve, offering improved correlation and automation capabilities. They will play a pivotal role in aggregating and analyzing security event data to identify potential malware incidents. SIEM systems will also be more closely integrated with SOC operations, enabling seamless incident response and threat mitigation.

Topics explored

The content explores a range of topics within the field of cybersecurity, including an introduction to the subject and its growing importance. It delves into the concept of data sanity, cloud services, and the associated security measures. It further discusses the implications of data breaches and protective measures like firewalls and antivirus software.

An understanding of the digital ecosystem is given, emphasizing data protection, various types of cyber attacks, and key terminologies. The content also introduces networking concepts, web APIs, webhooks, and web shell concepts. A detailed exploration of the vulnerability stack is provided, along with a study of the top 10 applications listed by OWASP. The concepts of QRadar, SOC, and SIEM are also presented.

Tools Explored

The instructional content utilizes a variety of tools to facilitate learning. These include Nessus, cybermap.kaspersky.com, thehackersone.com, chaptgpt, and wepik.com, an AI image editor. It also introduces Gamma, an AI-based PowerPoint tool, and the top 10 vulnerabilities listed by OWASP for 2021.

Other resources such as thehackersnews.com, CWE, exploitDB, virtual box, live websites like bugcrowd, nslookup.io, OSINT framework, mitre framework, IBM fix central, and QRadar Installation are also discussed. Additionally, tools like mobaxterm, tools-nmtui, Nmap, sqlmap, Identify fixes-wincollect agent, metasploitable, malware bytes, Linux cheatsheet, QRadar for SOC dashboard presentation, and Kali Linux are explored.