Experiment 10

Aim: Perform Cross-Site Scripting attack and analyse its impact on security

Tools: Kali Linux

Theory: Cross-Site Scripting Attack **(**XSS Attack)

Cross-site scripting (XSS) is a type of security vulnerability typically found in web applications. It occurs when a web application allows users to input data that is then included, unsanitized, in the output HTML content returned to other users. This can enable attackers to inject malicious scripts into web pages viewed by other users.

There are three main types of XSS attacks:

1. **Reflected XSS**: In this type of attack, the malicious script is injected into a web application, and the server reflects it back to the user in the response. For example, an attacker might craft a URL with a malicious script embedded in it and trick a user into clicking on it. When the user clicks the link, the script executes in the context of the victim's browser.

2. **Stored XSS**: In this scenario, the malicious script is stored on the server and then served to all users who access the compromised page or resource. This type of XSS attack is particularly dangerous because it can affect multiple users and persists over time. For example, an attacker might inject a script into a comment field on a website, and when other users view that comment, the script executes in their browsers.

3. **DOM-based XSS**: Unlike the other two types, DOM-based XSS does not involve server-side processing. Instead, the attack occurs entirely within the victim's browser. It exploits vulnerabilities in client-side scripts that manipulate the Document Object Model (DOM) of a web page. The attacker injects a malicious script that the client-side script unwittingly executes, leading to a security compromise.

4. **Client-Side Scripting**: XSS attacks primarily target web applications that involve client-side scripting languages such as JavaScript. Attackers exploit vulnerabilities in the way user input is processed and displayed in the browser.

5. **Cookie Theft and Session Hijacking**: One of the primary objectives of XSS attacks is to steal sensitive information such as session cookies or login credentials. Once an attacker gains access to session cookies, they can impersonate the victim and perform actions on their behalf, leading to session hijacking.

6. **Phishing and Malware Distribution**: XSS vulnerabilities can be leveraged to execute phishing attacks, where attackers mimic legitimate websites to trick users into revealing confidential information. Additionally, attackers may use XSS to distribute malware by injecting malicious scripts that redirect users to websites hosting exploit kits or malware downloads.

7. **Contexts Vulnerable to XSS**: XSS vulnerabilities often occur in various contexts within web applications, including input fields, URLs, HTTP headers, and even within JavaScript code itself. It's crucial for developers to identify and sanitize all user-controllable inputs to prevent XSS.

8. **Same-Origin Policy Bypass**: The Same-Origin Policy (SOP) is a security mechanism implemented by web browsers to restrict interactions between scripts from different origins (e.g., domains). However, XSS attacks can bypass SOP by executing within the context of a trusted origin, allowing attackers to access sensitive data or perform actions on behalf of the user across different domains.

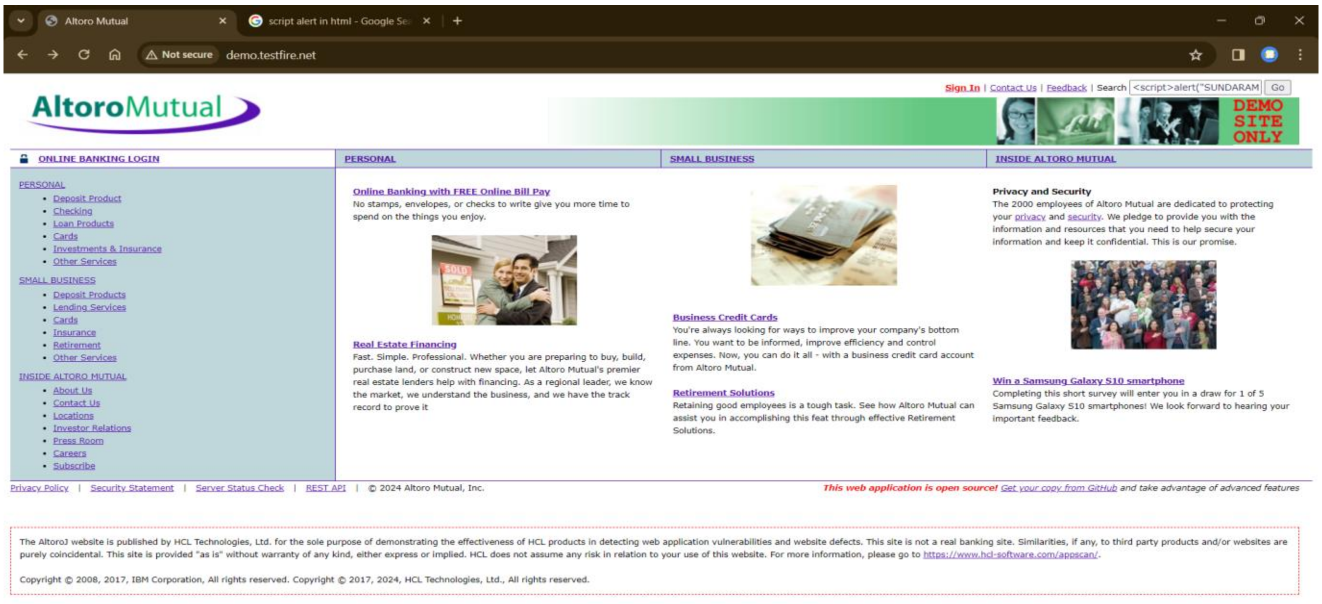
9. **XSS Worms**: In some cases, XSS vulnerabilities can be exploited to create self-propagating XSS worms. These worms automatically spread from one vulnerable page to another, infecting more users and amplifying the impact of the attack.

10. **Client-Side Defenses**: While server-side input validation and output encoding are crucial for mitigating XSS vulnerabilities, client-side defenses such as Content Security Policy (CSP) can also help prevent XSS attacks. CSP allows web developers to define a whitelist of trusted sources for scripts, stylesheets, and other resources, thereby limiting the execution of potentially malicious scripts.

XSS attacks can have serious consequences, including theft of sensitive information (such as session cookies or credentials), defacement of websites, or redirection to malicious websites. To prevent XSS attacks, web developers should implement proper input validation and output encoding techniques, such as escaping special characters and using frameworks that automatically handle these security measures. Additionally, web application firewalls and security scanning tools can help detect and mitigate XSS vulnerabilities.

Implementation:

a. XSS Attack –



Sign In | Contact Us | Feedback | Search <script>alert("SUNDARAM

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

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.

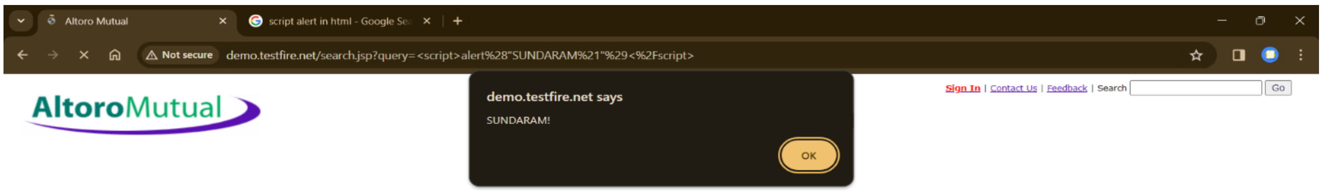
Win a Samsung Galaxy S10 smartphone
Completing this short survey will enter you in a draw for 1 of 5 Samsung Galaxy S10 smartphones! We look forward to hearing your important feedback.

Privacy Policy | Security Statement | Server Status Check | REST API | © 2024 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 HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL 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. HCL does not assume any risk in relation to your use of this website. For more information, please go to https://www.hcl-software.com/appscan/.

Copyright © 2008, 2017, IBM Corporation, All rights reserved. Copyright © 2017, 2024, HCL Technologies, Ltd., All rights reserved.

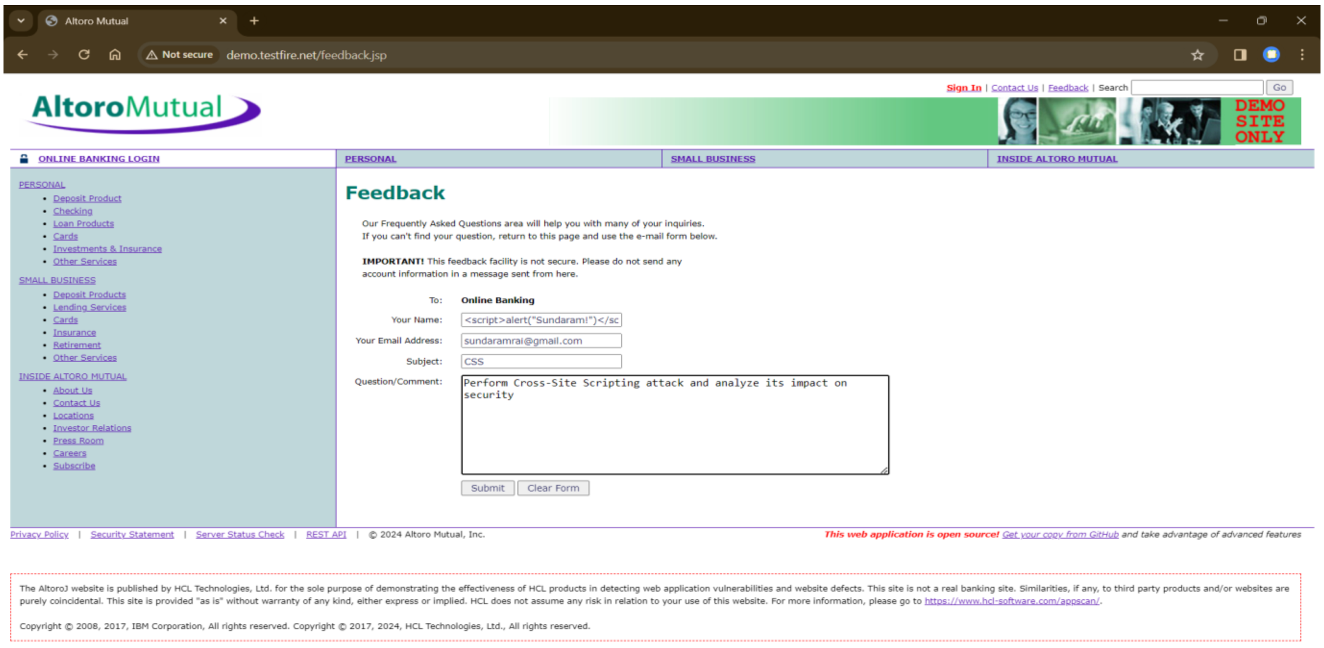

Altoro Mutual | script alert in html - Google Se

Not secure demo.testfire.net/search.jsp?query=<script>alert%28"SUNDARAM%21"%29<%2Fscript>

Sign In | Contact Us | Feedback | Search Go

demo.testfire.net says
SUNDARAM!
OK

b. Reflected XSS Attack -


Altoro Mutual

Not secure demo.testfire.net/feedback.jsp

Sign In | Contact Us | Feedback | Search Go

AltoroMutual 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

Feedback

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

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

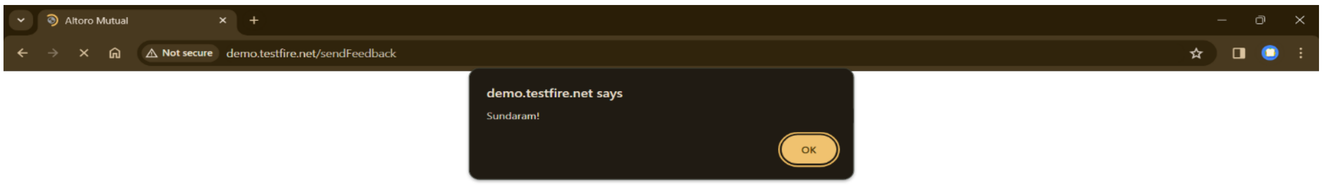
To:	**Online Banking**
Your Name:	<script>alert("Sundaram!")</sc
Your Email Address:	sundaramrai@gmail.com
Subject:	CSS
Question/Comment:	Perform Cross-Site Scripting attack and analyze its impact on security

Submit | Clear Form

Privacy Policy | Security Statement | Server Status Check | REST API | © 2024 Altoro Mutual, Inc.   *This web application is open source! Get your copy from GitHub and take advantage of advanced features*

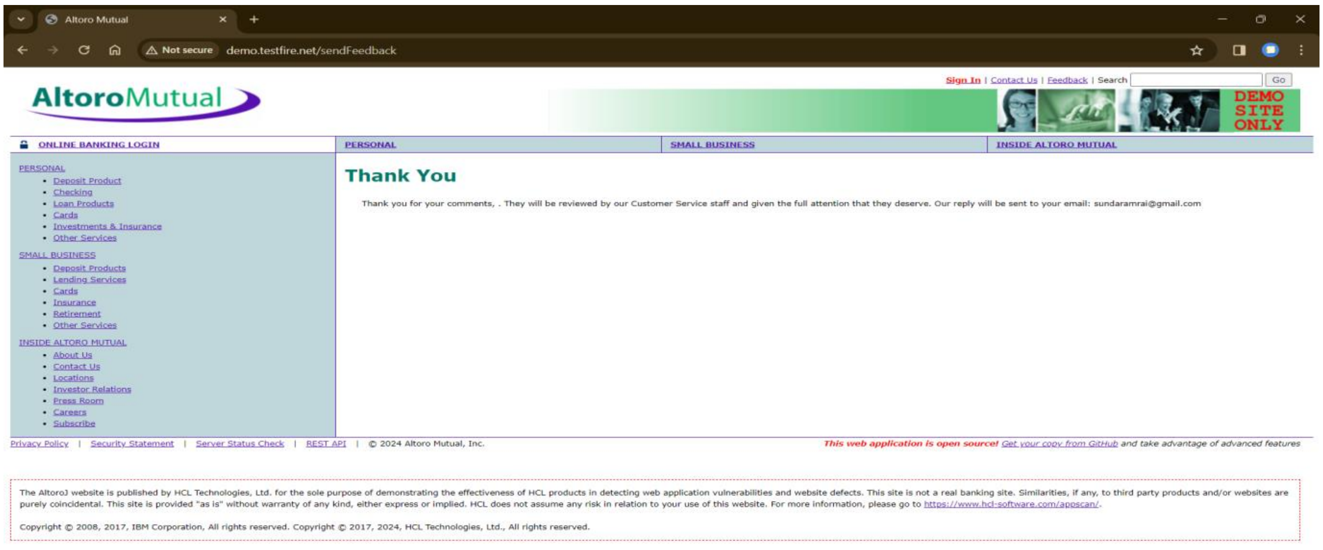
The AltoroJ website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are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

Copyright © 2008, 2017, IBM Corporation, All rights reserved. Copyright © 2017, 2024, HCL Technologies, Ltd., All rights reserved.


Altoro Mutual

Not secure demo.testfire.net/sendFeedback

demo.testfire.net says
Sundaram!
OK


Altoro Mutual
Not secure demo.testfire.net/sendFeedback

Sign In | Contact Us | Feedback | Search Go

AltoroMutual

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

Thank You

Thank you for your comments, . They will be reviewed by our Customer Service staff and given the full attention that they deserve. Our reply will be sent to your email: sundaramrai@gmail.com

Privacy Policy | Security Statement | Server Status Check | REST API | © 2024 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 HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL 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. HCL does not assume any risk in relation to your use of this website. For more information, please go to https://www.hcl-software.com/appscan/.

Copyright © 2008, 2017, IBM Corporation, All rights reserved. Copyright © 2017, 2024, HCL Technologies, Ltd., All rights reserved.

Learning Outcomes:

LO1. Understanding of Web Security Fundamentals: Learners will gain a foundational understanding of web security concepts, including common vulnerabilities like XSS, the impact they can have on web applications, and the importance of implementing robust security measures.
LO2. Knowledge of XSS Attack Techniques: Students will learn about the various techniques used by attackers to exploit XSS vulnerabilities, including reflected XSS, stored XSS, and DOM-based XSS. They will understand how attackers craft malicious payloads and exploit user input to execute unauthorized scripts.
LO3. Ability to Identify XSS Vulnerabilities: Upon completing their studies, learners will be able to identify potential XSS vulnerabilities in web applications by analyzing code, input validation processes, and output encoding mechanisms. They will develop the skills to conduct manual and automated security assessments to detect XSS flaws.

Conclusion:

For Faculty Use

Correction Parameters	**Formative Assessment [40%]**	**Timely Completion of Practial [40%]**	**Attendace/ Learning Attitude [20%]**	**Total**
Marks Obtained				