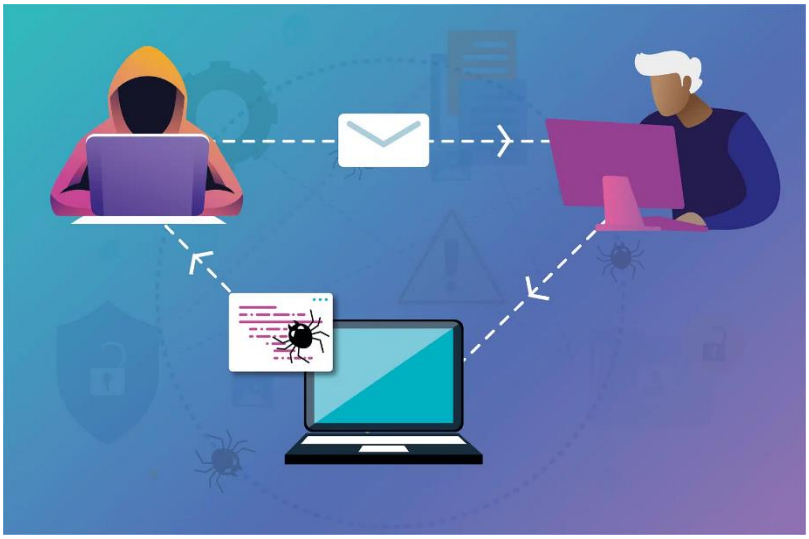
OCTOBER 26, 2023

CROSS-SITE SCRIPTING (XSS)

SAKTHI AYYAPPAN

CROSS-SITE SCRIPTING(XSS)



Cross-site scripting (XSS) Cross-site scripting (XSS) is an attack in which an attacker injects malicious executable scripts into the code of a trusted application or website.

- When a user visits the vulnerable website, their browser executes the malicious code, which can then perform a variety of malicious actions, such as stealing cookies, redirecting users to malicious websites, or taking over the user's account.
- XSS attacks are possible because web applications often rely on user input to generate dynamic content.

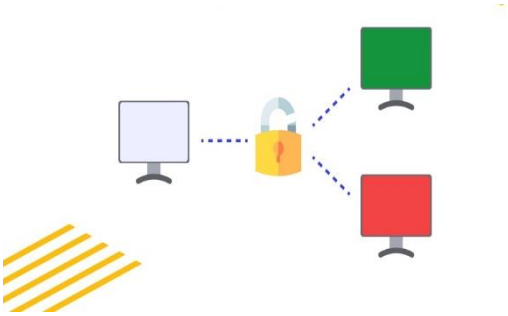
For example, a web application might use user input to generate a search results page or to display comments on a blog post. If the web application

does not properly validate and sanitize user input, an attacker can inject malicious code into the web application's output.

Examples of crosss-site scripting:

- ✓ Stealing user cookies: An attacker can use XSS to steal a user's cookies, which can then be used to impersonate the user and gain access to their account.

- ✓ Redirecting users to malicious websites: An attacker can use XSS to redirect users to malicious websites that may contain malware or phishing attacks.



- ✓ Taking over user accounts: An attacker can use XSS to take over user accounts by stealing cookies or by injecting malicious code that can be used to change the user's password.
- ✓ Defacing websites: An attacker can use XSS to deface websites by injecting malicious code that can change the content of the website.

TYPES OF CROSS SITE SCRIPTING ATTACKS:

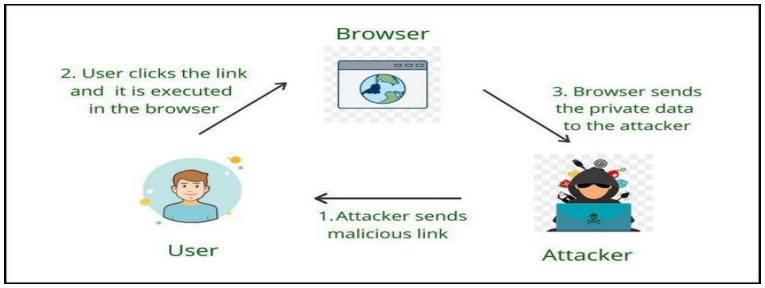
Reflected XSS

- ✓ Reflected XSS attacks occur when malicious code is injected into a web application request and then reflected back to the user in the response.
- ✓ This type of attack is often carried out by exploiting vulnerabilities in search forms, comment forms, and other input fields.

For example, an attacker might inject the following malicious code into a search form on a website:

<script>alert("This is a malicious script!");</script>

- ✓ When the user submits the form, the web application will reflect the malicious code back to the user in the search results page.
- ✓ When the user views the search results page, their browser will execute the malicious code, displaying an alert message.



STORED XSS

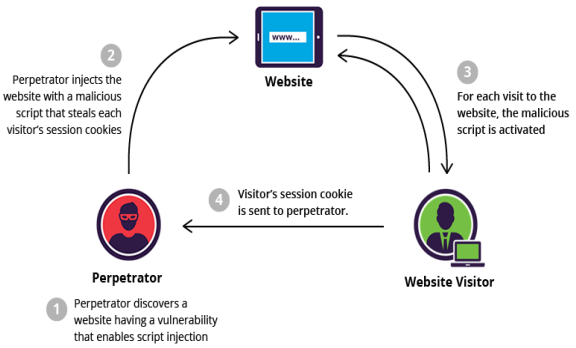
- ✓ Stored XSS attacks occur when malicious code is injected into a web application's database and then stored for later retrieval.

- ✓ This type of attack is often carried out by exploiting vulnerabilities in blog posts, wikis, and other user-generated content.

For example, an attacker might inject the following malicious code into a comment on a blog post:

```
<script>alert("This is a malicious script!");</script>
```

- ✓ When another user visits the blog post, their browser will retrieve the malicious code from the database and execute it.
- ✓ This can allow the attacker to steal the user's cookies, redirect them to a malicious website, or take over their account.



DOM-based XSS

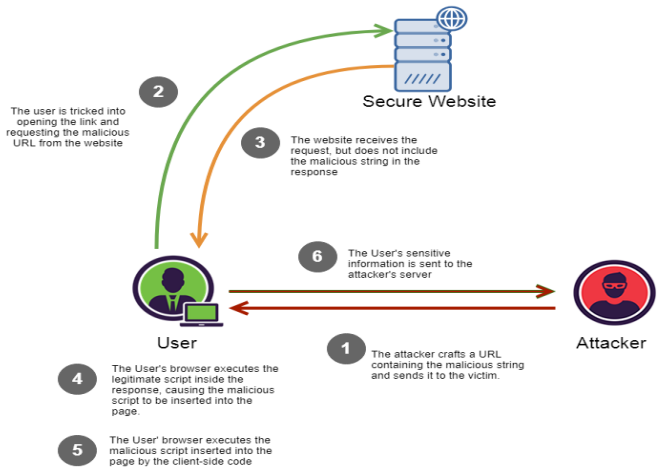
- ✓ DOM-based XSS attacks occur when malicious code is injected into the Document Object Model (DOM) of a web page.

- ✓ The DOM is a representation of the web page's structure, and it can be manipulated by JavaScript.

For example, an attacker might inject the following malicious code into a web page's cookies:

```
<script>alert("This is a malicious script!");</script>
```

- ✓ When the user visits the web page, their browser will load the malicious code from the cookies and execute it.
- ✓ This can allow the attacker to steal the user's cookies, redirect them to a malicious website, or take over their account.



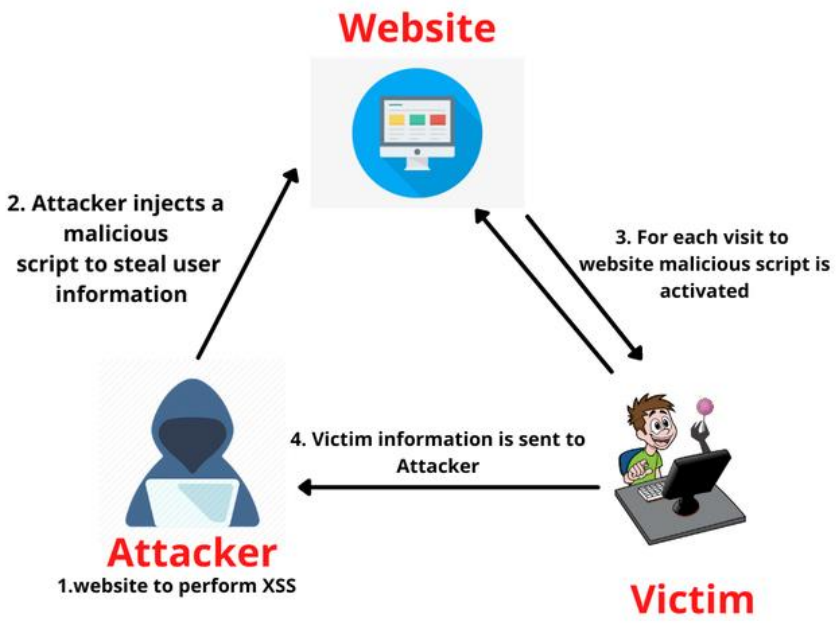
BLIND XSS:

- ✓ Blind XSS is a subtype of stored XSS where the attacker cannot see the results of their attack immediately.
- ✓ This is because the attacker's malicious payload is stored on the web server and then executed later, when the user visits a different page or when the web application performs a certain action.
- ✓ Blind XSS attacks are often carried out by exploiting vulnerabilities in contact forms, feedback forms, and other input fields that allow users to submit data to the web server.
- ✓ The attacker injects their malicious payload into one of these fields and then submits the form. The web server then stores the attacker's payload in its database.

Later, when a user visits the web application, the attacker's payload is executed, and the attacker can steal the user's cookies, redirect them to a malicious website, or take over their account.

- ✓ Blind XSS attacks are more difficult to exploit than traditional stored XSS attacks because the attacker cannot see the results of their attack immediately.
- ✓ However, blind XSS attacks can still be very dangerous, especially if the attacker is able to target a vulnerable web application that is used by a large number of users.

Here’s how blind xss works,



IMPACTS OF CROSS SITE SCRIPTING :

XSS attacks can have a variety of negative consequences for both individuals and organizations, including:

Identity theft:

XSS attacks can be used to steal user cookies, which can then be used to impersonate the user and gain access to their accounts. This can lead to identity theft, financial loss, and damage to the user's reputation.

Malware infection:

- ✓ XSS attacks can be used to redirect users to malicious websites that may contain malware.
- ✓ If the user downloads and installs the malware, it can infect their computer and steal their personal information or cause damage to their system.

Financial loss:

- ✓ XSS attacks can be used to steal credit card numbers and other financial information from users.
- ✓ This can lead to financial loss and fraud.

Privacy violations:

- ✓ XSS attacks can be used to steal personal information from users, such as their name, address, phone number, and email address.
- ✓ This information can then be used for marketing purposes, sold to third parties, or used to commit identity theft.

In the organizations point of view ,it may affect by:

Damage to reputation:

- ✓ XSS attacks can damage an organization's reputation by making it look like the organization is not taking security seriously.
- ✓ This can lead to lost customers and business partners.

Financial losses:

XSS attacks can lead to financial losses for organizations in a number of ways, such as through credit card fraud, identity theft, and malware infections.

Compliance violations:

Organizations that are subject to data protection regulations, such as the General Data Protection Regulation (GDPR), may face fines and other penalties if they are found to have been compromised by an XSS attack.

Additionally,

1. Deface websites
2. Spread disinformation
3. Support phishing attacks
4. Launch denial-of-service attacks

MITIGATIONS

For example a company's website has a contact form that allows users to submit feedback.

The company wants to prevent XSS attacks on the contact form, so they implement the following security measures:

1. Validate and sanitize all user input: The company uses a secure coding framework to validate and sanitize all user input on the contact form. This ensures that any malicious code injected into the

form is removed before it is stored in the database or displayed on the website.

2. Use a content security policy: The company implements a CSP to restrict the types of scripts that can be executed on the contact form. This helps to prevent attackers from injecting malicious scripts into the form.
3. Test for XSS vulnerabilities: The company regularly tests the contact form for XSS vulnerabilities. This helps to identify and fix any vulnerabilities before they can be exploited by attackers.

Additionally the mitigations steps for an individual may be :

- ✓ Keep your web browser and operating system up to date.Software updates often include security patches that can help to protect against XSS attacks.
- ✓ Be careful about clicking on links: Do not click on links in emails, social media posts, or on websites unless you are sure that they are safe. If you are unsure about the safety of a link, hover your mouse over the link to see the actual URL.
- ✓ Use a password manager: A password manager can help you to create and manage strong, unique passwords for all of your online accounts. This can help to protect your accounts from being compromised by XSS attacks.

REFERENCES:

1. https://www.synopsys.com/glossary/what-is-cross-site-scripting.html#:~:text=Cross%2Dsite%20scripting%20(XSS)%20is%20an%20attack%20in%20which,the%20user%20to%20click%20it.
2. https://www.trendmicro.com/en_za/devops/23/e/cross-site-scripting-xss-attacks.html#:~:text=highly%20damaging%20attacks.-,Types%20of%20XSS%20attacks,Object%20Model%20(DOM)%20XSS.