XSS injection

Jessica Longane

01

Introduction to XSS injection

02

Understanding website functionality

03

Types of XSS injection

04

Demo - Reflected XSS

05

Preventions

06

Conclusion

01 Introduction to XSS injection

1.Understanding XSS Injection Basics

What is XSS injection?

= Cross-Site Scripting

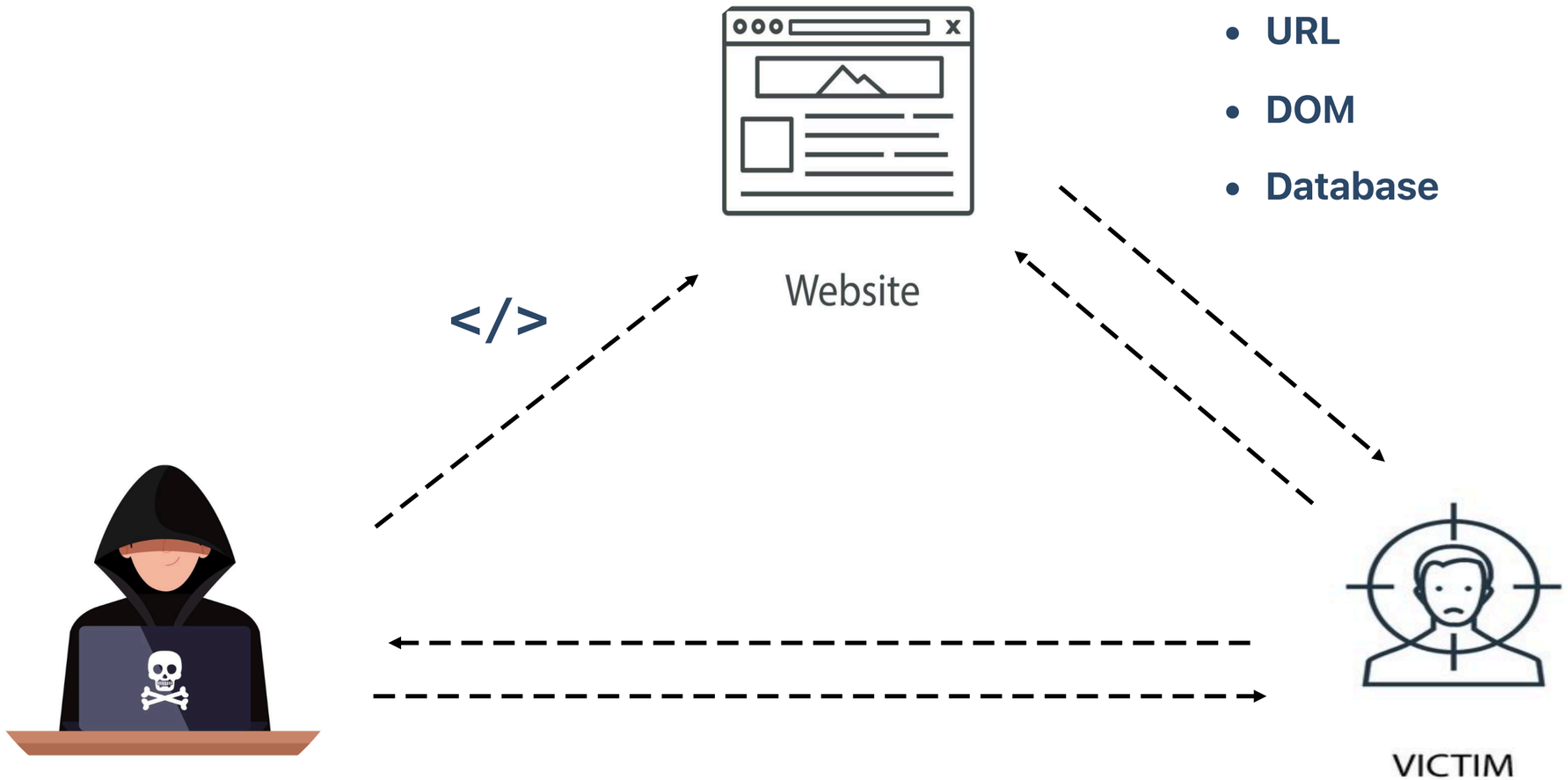
What?

- Attack on a website
- inject malicious JavaScript code
- victim's browser executes the code

Why?

- cookies session
- data stolen

XSS Attack Process



- URL
- DOM
- Database

02 Understanding website functionality

How a website works

HTML: provides the structure and content of a web page.

CSS: style the HTML elements and provide a visually appealing layout.

JavaScript: JavaScript adds interactivity to web pages, allowing for dynamic content and user interactions.

03 Types of XSS injection: DOM-Based, Stored and Reflected

Types of XSS injection

DOM-Based XSS

DOM-Based XSS occurs when the attacker modifies the **DOM structure** of a web page, which is then rendered by the browser.

Stored XSS

Stored XSS involves storing malicious scripts in the **web application**, which are then served to users when they access the site.

Reflected XSS

Reflected XSS occurs when the malicious script is reflected off the web server in an **HTTP response**, and the user is tricked into clicking a link or submitting a form.

04 Demo

Reflected XSS

05 Preventions

05 Preventions

measures

Output Encoding

Input validation & sanitization

Use secure HTTP headers

Regular manual or automated security scans

Use modern frameworks that auto-escape user input

Goal

Prevent injected code from being interpreted as HTML/JS

Remove or reject dangerous characters/code as soon as the user submits data.

Strengthen browser-side protection.

Block unauthorized script loading or execution.

tools

- textContent
- DOMPurify, bleach.clean()
- React, Angular, Vue.js
- CSP (Content Security Policy)
- OWASP ZAP, Burp Suite, SonarQube, Bright Security

Conclusion

Understanding XSS

Understanding the different types of XSS and their prevention methods is crucial for securing web applications.

The importance of security

Implementing proper security measures, such as input validation and CSP, is essential to protect users from XSS attacks.

Q&A

Thank You for Your Attention

Any questions ?

Sources

- https://itsocial.fr/contenus/articles-decideurs/breches-de-code-plus-exploitees/
- https://www.youtube.com/watch?v=Bkg7JoBs2ac&t=435s
- https://www.youtube.com/shorts/pd3m8RvOmg8
- https://www.brightsec.com/blog/reflected-xss/
- https://www.youtube.com/watch?v=yJSnggHSH1U
- https://www.youtube.com/watch?v=ABwS2MIxFPQ
- https://www.geeksforgeeks.org/javascript/dom-based-cross-site-scripting-attack-in-depth/
- https://www.brightsec.com/blog/dom-based-xss/
- https://www.researchgate.net/figure/The-process-of-stored-XSS-Attack_fig1_338000205