
THE UNIVERSITY
of ADELAIDE
Web and Database Computing
adelaide.edu.au
Web Security: Common Threats/Vulnerabilities

3 Common Threats/Vulnerabilities

1) Cross Site Scripting (XSS)

XSS can occur when a user's input is stored and displayed to other users of the same site.

- If the input is not properly sanitized, an attacker can write JavaScript code instead of normal input, that gets run when another user interacts with the page displaying .
- This attack is mitigated by sanitizing the input and output of user data.

The following videos provide one of the best, detailed breakdowns of XSS:

- Introduction to XSS: https://www.youtube.com/watch?v=L5l9lSnNMxg?t=198
- Example of XSS in Twitter: https://www.youtube.com/watch?v=zv0kZKC6GAM

2) SQL Injection

SQL Injection can occur when a user's input is used as part of a SQL query.

- If the input is not properly sanitized, an attacker can write SQL code instead of normal input to extract data from, or manipulate the database in ways they shouldn't be authroised to.
- This attack is mitigated using Prepared Statements (which we've already been using).

The following videos provide one of the best, detailed breakdowns of SQL Injection:

- Introduction to SQL Injection: https://www.youtube.com/watch?v=_jKylhJtPmI
- Example of : https://www.youtube.com/watch?v=ciNHn38EyRc

3) Cross Site Request Forgery (CSRF/XSRF)

CSRF can occur when a website allows requests that originated from other websites.

- If a user is logged-in to a vulnerable site, and then accesses a malicious site, a HTTP request sent from the maliscious site will contain the user's session token.
- The malicious site can make requests as that user via the user's browser (using AJAX or just a regualar form input).
- This attack is mitigated by preventing requests from outside your own website (acheived using a special header sent by all browsers), or by using a single-use token with all forms.
    - Express has this funcitonality built-in and will protect against this type of attack unless it is explicitly disabled.
    - This attack is becoming less effective as browsers and servers are building in protections against it.

The following video provides one of the best, detailed breakdowns of CSRF:

- Introduction to CSRF: https://www.youtube.com/watch?v=vRBihr41JTo

Summary

- XSS, SQL Injection & CSRF are 3 of the most prevalent attacks against web applications.

THE UNIVERSITY
of ADELAIDE