ONE PAGE SUMMARY

IT & Software › Web Development › Web Security

Introduction to Web Security

Mastering web security is essential for safe online experiences.

DEFINITION

> Web security involves protecting websites and online services from cyber threats and attacks. It ensures the safety of data and user interactions on the internet.

KEY CONCEPTS

SSL/TLS Encryption

SSL/TLS encrypts data between the user's browser and the web server, ensuring secure communication.

Cross-Site Scripting (XSS)

XSS is a vulnerability that allows attackers to inject malicious scripts into web pages viewed by users.

SQL Injection

SQL injection occurs when attackers manipulate a web application's database queries to gain unauthorized access.

Authentication

Authentication verifies the identity of users before granting access to sensitive information or services.

Firewalls

Firewalls monitor and control incoming and outgoing network traffic based on predetermined security rules.

EXAMPLES

→ Using HTTPS instead of HTTP for secure browsing.

→ Implementing input validation to prevent XSS attacks.

→ Utilizing prepared statements to defend against SQL injection.

MEMORY TIPS

★ Remember 'SSL' for 'Secure Socket Layer' to recall encryption importance.

★ Think 'XSS' as 'eXtra Script Security' to remember XSS vulnerabilities.

★ Use 'A-F-F' for Authentication, Firewalls, and Filtering as key security components.

COMMON MISTAKES

✗ Neglecting to update software and security patches regularly.

✗ Using weak passwords or not enforcing strong password policies.

✗ Overlooking the importance of user education on security best practices.

QUICK RECAP

Web security is crucial for protecting online data and user interactions. Key concepts include encryption, authentication, and common vulnerabilities like XSS and SQL injection. Always stay updated on security practices to prevent attacks.