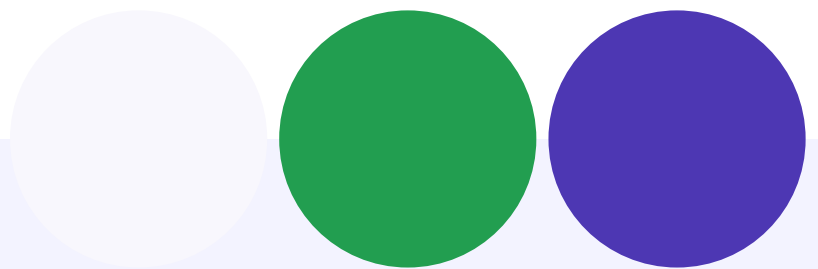


Web Security

Web Programming Report

Author: Yousif Khaled, C5, 12500088

Instructor: Abdelftah





Introduction

Most of what we depend on today lives on the web — our accounts, our money, our work, our conversations, even our identities.

We trust websites with information that we would never hand to a stranger in real life. But this trust only makes sense if the systems behind the scenes are actually protected.

Without proper security, all of that data can be exposed, stolen, or manipulated in seconds. That is why security is not an add-on or a decoration — it is a core part of building anything online.

A website is only as strong as the way it protects the people using it.

Definition

Web security refers to all techniques, tools, and standards used to prevent unauthorized access, data theft, malicious activity, and system damage on websites and web applications.

"The greatest vulnerability is the belief that nothing can touch you."



SSL & TLS

- SSL (Secure Sockets Layer) and TLS (Transport Layer Security) are protocols used to protect data sent between a user and a website.
- They encrypt the communication so that even if someone intercepts it, the data cannot be read or changed.
- TLS is the newer and more secure version that replaced SSL in most modern systems.
- Websites using SSL/TLS show https:// and a lock icon in the browser.
- They are especially important for login pages, bank transactions, and any site that handles personal or financial information.

Common Threats

- Phishing — tricking users into giving passwords or data.
- SQL Injection — inserting malicious code into databases.
- XSS (Cross-Site Scripting) — injecting scripts into web pages.
- Man-in-the-Middle (MITM) — intercepting communication.
- DDoS Attacks — overwhelming servers to make them crash.
- Brute Force Attacks — guessing passwords repeatedly.



Pros

- Protects user data and privacy
- Builds trust and credibility
- Prevents financial and reputational loss
- Keeps websites stable and available
- Helps meet legal and security standards

Challenges

- Requires constant updates and monitoring
- Can be expensive to implement at scale
- Needs skilled people and proper planning
- Sometimes affects speed or convenience
- One small mistake can create big vulnerabilities

Conclusion:

Web security is essential for trust, privacy, and safe communication online. By applying strong defenses, using standards like TLS, and staying aware of new threats, we reduce risks and protect both systems and users from harm.