Web and Mobile Application Security

Chapter 3 — Web Application Security

Mr Laïdi FOUGHALI

l.foughali@univ-skikda.dz

(Website ⇒ www.al-moualime.com)

University of Skikda — Computer Science Department

2nd Year Master in Information Security (IS)

Academic Year 2026-2027

Updated on 2026-09-22 at 23:41:11

Outline

Chapter objectives

By the end of this chapter, you will be able to

- Know the major risks identified by OWASP
- Understand how injection, XSS, and CSRF work
- Master Web application protection techniques

3.1 — OWASP Top 10 risks (1/2)

The world's reference ranking

- **A01** — Broken Access Control
- **A02** — Cryptographic Failures
- **A03** — Injection (SQL, commands, XSS)
- **A04** — Insecure Design
- **A05** — Security Misconfiguration

3.1 — OWASP Top 10 risks (2/2)

Ranking continued

- **A06** — Vulnerable and Outdated Components
- **A07** — Identification and Authentication Failures
- **A08** — Software and Data Integrity Failures
- **A09** — Insufficient Logging and Monitoring
- **A10** — SSRF (*Server-Side Request Forgery*)

3.2 — Major Web attacks

The four attacks you must know

- **SQL injection** : inserting SQL code into an unfiltered input
- **XSS** (*Cross-Site Scripting*) : a script executed in another user's browser (reflected, stored, DOM-based)
- **CSRF** (*Cross-Site Request Forgery*) : an authenticated request forged without the victim's knowledge
- **Clickjacking** : an invisible frame tricking a click without the user's knowledge

The root cause of injection

Lack of strict separation between **code** and **data**.

3.3 — Protection techniques

Defenses to implement

- Input validation and sanitization
- Parameterized queries / ORM (against SQL injection)
- Output encoding (against XSS)
- Anti-CSRF tokens and the `SameSite` attribute
- Security headers: CSP, X-Frame-Options, HSTS
- Principle of least privilege, secure sessions
- WAF and SAST/DAST analysis

Key takeaways

The essentials of this chapter

- The OWASP Top 10 is the reference for Web risks; access control and injection top the list
- SQL injection, XSS, CSRF, clickjacking: the Web attacks you cannot skip
- Defense combines validation, parameterized queries, encoding, anti-CSRF tokens, security headers

Questions and exercises

To practice

1. Describe the three types of XSS and propose a countermeasure for each.
2. Why does a parameterized query prevent SQL injection?
3. Explain the mechanism of a CSRF attack and the role of the SameSite attribute.
4. Name five HTTP security headers and their purpose.