Web and Mobile Application Security

Chapter 5 — Content Security Policy (CSP)

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 23:41:27

Outline

Chapter objectives

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

- Understand the role of Web workers
- Define a Content Security Policy (CSP)
- Use iframe isolation (sandboxed iframes)

5.1 — Web workers

Running JavaScript in the background

- Background threads, outside the main UI thread
- Isolated context, no direct DOM access
- Communication via message passing

Service workers

A network-oriented variant: a programmable proxy between the page and the network (caching, offline mode). High power ⇒ **restricted to HTTPS**.

5.2 — Content Security Policy (CSP)

An HTTP header that restricts allowed sources

The server declares to the browser the allowed sources per resource type (scripts, styles, images, frames, etc.)

- Directives: `default-src`, `script-src`, `style-src`, `frame-src`
- *Nonces* or hashes for identified scripts
- "Report-only" mode to test without blocking

Complementary defense, not a single solution

CSP mitigates mainly XSS (chapter 3) but does not replace input validation and output encoding.

5.3 — Frame isolation (sandboxed iframes)

The `sandbox` attribute

By default, disables:

- Script execution
- Form submission
- Top-level navigation
- Access to the parent origin

Capabilities re-granted explicitly

`allow-scripts`, `allow-forms`, `allow-same-origin`, etc. Essential for safely embedding third-party content (ads, widgets).

Key takeaways

The essentials of this chapter

- Web workers run DOM-isolated code; service workers require HTTPS
- CSP declares allowed sources and mitigates mainly XSS
- The sandbox attribute of iframes confines third-party content by default

Questions and exercises

To practice

1. What is the difference between a Web worker and a service worker?
2. Write a CSP directive allowing only same-origin scripts.
3. Name three restrictions imposed by default on a sandboxed iframe.
4. Why is CSP a "defense in depth" rather than a single solution against XSS?