Web and Mobile Application Security

Chapter 7 — XML and Web Services 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 23:41:43

Outline

Chapter objectives

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

- Recall Web services (SOAP, REST) and the role of XML
- Understand XML-specific vulnerabilities (XXE, XML bomb)
- Introduce AJAX and know its attacks and defenses

7.1 — Recap on Web services

Two major families

- **SOAP** : structured XML messages, described by a WSDL contract
- **REST** : lightweight APIs, frequently exchanging JSON

A full-fledged attack surface

These interfaces directly expose server-side functionality accessible from the network.

7.2 — XML security

Risks specific to XML processing

- **XML injection** : tags/content hijacking the parser's interpretation
- **XXE** (*XML External Entity*) : reading local files, probing internal networks, denial of service
- **XML bomb** (*billion laughs*) : exponential entity expansion ⇒ memory exhaustion

Defenses

WS-Security (XML signing/encryption), disabling external entities, strict document validation.

7.3 — Introducing AJAX technology

Asynchronous client-server exchanges

Asynchronous JavaScript and XML — via `XMLHttpRequest` or `fetch`, data often exchanged as JSON today.

The other side of the coin

AJAX multiplies client-side data entry points, subject to the SOP and CORS (chapter 2).

7.4 — Attacks against AJAX and defenses

Attacks

- XSS via unsanitized AJAX responses
- CSRF on AJAX endpoints
- JSON hijacking, data leakage
- Overly permissive CORS configuration

Defenses

Systematic DOM encoding, anti-CSRF tokens, restrictive server-controlled CORS, strict input/output validation.

Key takeaways

The essentials of this chapter

- Web services (SOAP/XML, REST/JSON) expose a full attack surface
- XXE and XML bombs are the emblematic risks of XML processing
- AJAX falls under the SOP and depends on careful CORS configuration
- AJAX attacks: encoding, anti-CSRF tokens, restrictive CORS

Questions and exercises

To practice

1. Describe an XXE attack and its countermeasure.
2. What is an XML bomb and what kind of threat does it represent?
3. How can an overly permissive CORS configuration be exploited?
4. Name three defenses applicable to AJAX endpoints.