Penetration Testing Report – XML/XXE Injection (Lab Environment)

Target Application: Vulnerable XML Parser (Lab Application)
Test Type: XML/XXE Injection Vulnerability Assessment
Date: 15 Aug 2025
Tester: Waleed Elsmedsey

1. Executive Summary

The objective of this penetration test was to simulate XML Injection and XXE (XML External Entity) attacks against a vulnerable lab application. The test successfully demonstrated how insecure XML parser configurations could allow external entity injection, data disclosure, and file access in a controlled environment.

2. Scope

- **In Scope:** XML request parsing in the vulnerable lab application.
- **Out of Scope:** Any production or internet-facing applications.
- **Environment:** Docker-based vulnerable XML/XXE lab, isolated network.

3. Methodology

1. Reconnaissance: Identified XML input points in the lab application.
2. Manual Testing: Injected XML payloads with custom entities.
3. Exploitation: Used external entity payloads to simulate data retrieval and local file inclusion.
4. Analysis: Observed parser behavior and application responses.
5. Documentation: Recorded payloads, results, and recommendations.

4. Findings

Finding ID	Vulnerability	Severity	Description
XML-001	XML Injection	Medium	Improper XML input handling allowed injection of custom XML en
XML-002	XXE Injection	High	The XML parser accepted external entities, enabling data disclos

5. Impact

If present in production, XML/XXE Injection could allow attackers to read local files, perform SSRF attacks, or exfiltrate sensitive data. In this lab test, the vulnerability demonstrated data disclosure and file read capabilities.

6. Recommendations

- Disable external entity (DTD) processing in XML parsers.
- Use secure XML parsers (e.g., defusedxml, lxml with secure settings).
- Implement strict input validation and whitelisting.
- Apply least privilege to the application’s service account.

- Regularly test XML endpoints for injection vulnerabilities.

7. Tools Used

- Burp Suite
- OWASP ZAP
- Custom XXE Payloads
- Docker vulnerable XXE application

8. Conclusion

The test confirmed that the lab application was vulnerable to XML and XXE Injection. Applying secure parser configurations and disabling external entity resolution will mitigate the risk of such attacks.