Preventing XSLT Injection

After discussing how to identify and exploit XSLT injection vulnerabilities in the previous sections, we will conclude this module by discussing how to prevent them.

Prevention

Similarly to all injection vulnerabilities discussed in this module, XSLT injection can be prevented by ensuring that user input is not inserted into XSL data before processing by the XSLT processor. However, if the output should reflect values provided by the user, user-provided data might be required to be added to the XSL document before processing. In this case, it is essential to implement proper sanitization and input validation to avoid XSLT injection vulnerabilities. This may prevent attackers from injecting additional XSLT elements, but the implementation may depend on the output format.

For instance, if the XSLT processor generates an HTML response, HTML-encoding user input before inserting it into the XSL data can prevent XSLT injection vulnerabilities. As HTML-encoding converts all instances of `<` to `<` and `>` to `>`, an attacker should not be able to inject additional XSLT elements, thus preventing an XSLT injection vulnerability.

Additional hardening measures such as running the XSLT processor as a low-privilege process, preventing the use of external functions by turning off PHP functions within XSLT, and keeping the XSLT library up-to-date can mitigate the impact of potential XSLT injection vulnerabilities.

Previous Next

Mark Complete & Next

Cheat Sheet

Table of Contents

Introduction

Introduction to Server-side Attacks

SSRF

Introduction to SSRF

Identifying SSRF

Exploiting SSRF

Blind SSRF

Preventing SSRF

SSTI

Template Engines

Introduction to SSTI

Identifying SSTI

Exploiting SSTI - Jinja2

Exploiting SSTI - Twig

SSTI Tools of the Trade & Preventing SSTI

SSI Injection

Introduction to SSI Injection

Exploiting SSI Injection

Preventing SSI Injection

XSLT Injection

Intro to XSLT Injection

Exploiting XSLT Injection

Preventing XSLT Injection

Skills Assessment

Server-Side Attacks - Skills Assessment

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left

Powered by HACKTHEBOX