Preventing SSRF

After discussing identifying and exploiting SSRF vulnerabilities, we will dive into SSRF prevention and mitigation techniques.

Prevention

Mitigations and countermeasures against SSRF vulnerabilities can be implemented at the web application or network layers. If the web application fetches data from a remote host based on user input, proper security measures to prevent SSRF scenarios are crucial.

The remote origin data is fetched from should be checked against a whitelist to prevent an attacker from coercing the server to make requests against arbitrary origins. A whitelist prevents an attacker from making unintended requests to internal systems. Additionally, the URL scheme and protocol used in the request need to be restricted to prevent attackers from supplying arbitrary protocols. Instead, it should be hardcoded or checked against a whitelist. As with any user input, input sanitization can help prevent unexpected behavior that may lead to SSRF vulnerabilities.

On the network layer, appropriate firewall rules can prevent outgoing requests to unexpected remote systems. If properly implemented, a restricting firewall configuration can mitigate SSRF vulnerabilities in the web application by dropping any outgoing requests to potentially interesting target systems. Additionally, network segmentation can prevent attackers from exploiting SSRF vulnerabilities to access internal systems.

For more details on the SSRF mitigation measures, check out the OWASP SSRF Prevention Cheat Sheet.

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