Introduction to SSRF

SSRF vulnerabilities are part of OWASPs Top 10. This type of vulnerability occurs when a web application fetches additional resources from a remote location based on user-supplied data, such as a URL.

Server-side Request Forgery

Suppose a web server fetches remote resources based on user input. In that case, an attacker might be able to coerce the server into making requests to arbitrary URLs supplied by the attacker, i.e., the web server is vulnerable to SSRF. While this might not sound particularly bad at first, depending on the web application's configuration, SSRF vulnerabilities can have devastating consequences, as we will see in the upcoming sections.

Furthermore, if the web application relies on a user-supplied URL scheme or protocol, an attacker might be able to cause even further undesired behavior by manipulating the URL scheme. For instance, the following URL schemes are commonly used in the exploitation of SSRF vulnerabilities:

- `http://` and `https://`: These URL schemes fetch content via HTTP/S requests. An attacker might use this in the exploitation of SSRF vulnerabilities to bypass WAFs, access restricted endpoints, or access endpoints in the internal network
- `file://`: This URL scheme reads a file from the local file system. An attacker might use this in the exploitation of SSRF vulnerabilities to read local files on the web server (LFI)
- `gopher://`: This protocol can send arbitrary bytes to the specified address. An attacker might use this in the exploitation of SSRF vulnerabilities to send HTTP POST requests with arbitrary payloads or communicate with other services such as SMTP servers or databases

For more details on advanced SSRF exploitation techniques, such as filter bypasses and DNS rebinding, check out the Modern Web Exploitation Techniques module.

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