

Please support the OWASP mission to improve software security through open source initiatives and community education. [Donate Now!](#)



Store

ACTS CHAPTERS

Donate



Store

Join

Donate

This website uses cookies to analyze our traffic and only share that information with our analytics partners.

Accept



# Server Side Request Forgery

Author: Eoftedal

Contributor(s): ErezYalon, kingthorin

## Overview

In a Server-Side Request Forgery (SSRF) attack, the attacker can abuse functionality on the server to read or update internal resources. The attacker can supply or modify a URL which the code running on the server will read or submit data to, and by carefully selecting the URLs, the attacker may be able to read server configuration such as AWS metadata, connect to internal services like http enabled databases or perform post requests towards internal services which are not intended to be exposed.

## Description

The target application may have functionality for importing data from a URL, publishing data to a URL or otherwise reading data from a URL that can be tampered with. The attacker modifies the calls to this functionality by supplying a completely different URL or by manipulating how URLs are built (path traversal etc.).

When the manipulated request goes to the server, the server-side code picks up the manipulated URL and tries to read data to the manipulated URL. By selecting target URLs the attacker may be able to read data from services that are not directly exposed on the internet.

This website uses cookies to analyze our traffic and only share that information with our analytics partners.

Accept

Join

Watch 190

Star 1,163

**The OWASP® Foundation** works to improve the security of software through its community-led open source software projects, hundreds of chapters worldwide, tens of thousands of members, and by hosting local and global conferences.

## Important Community Links

[Community](#)

[Attacks \(You are here\)](#)

[Vulnerabilities](#)

[Controls](#)

## Upcoming OWASP Global Events

[OWASP Global AppSec EU 2025](#)

◦ May 26-30, 2025

[OWASP Global AppSec US 2025 - Washington, DC](#)

◦ November 3-7, 2025

`http://105.254.105.254/` where important configuration and sometimes even authentication keys can be extracted.

◦ November 2-6, 2026

- Database HTTP interfaces - NoSQL database such as MongoDB provide REST interfaces on HTTP ports. If the database is expected to only be available to internally, authentication may be disabled and the attacker can extract data.
- Internal REST interfaces.
- Files - The attacker may be able to read files using `file://` URIs.

The attacker may also use this functionality to import untrusted data into code that expects to only read data from trusted sources, and as such circumvent input validation.

## Prevention

See the [Server-Side Request Forgery Prevention Cheat Sheet](#).

---

[Edit on GitHub](#)

## Spotlight: Tenable, Inc



Tenable® is the Exposure Management company. Approximately 40,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include approximately

This website uses cookies to analyze our traffic and only share that information with our analytics partners.

Accept





## Become a corporate supporter

[HOME](#) [PROJECTS](#) [CHAPTERS](#) [EVENTS](#) [ABOUT](#)



[PRIVACY](#) [SITEMAP](#) [CONTACT](#)

OWASP, the OWASP logo, and Global AppSec are registered trademarks and AppSec Days, AppSec California, AppSec Cali, SnowFROC, OWASP Boston Application Security Conference, and LASCON are trademarks of the OWASP Foundation, Inc. Unless otherwise specified, all content on the site is Creative Commons Attribution-ShareAlike v4.0 and provided without warranty of service or accuracy. For more information, please refer to our [General Disclaimer](#). OWASP does not endorse or recommend commercial products or services, allowing our community to remain vendor neutral with the collective wisdom of the best minds in software security worldwide. Copyright 2025, OWASP Foundation, Inc.

This website uses cookies to analyze our traffic and only share that information with our analytics partners.

Accept

