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:

Important Community Links

Community
Attacks (You are here)
Vulnerabilities
Controls

http://169.254.169.254/ where important configuration and sometimes even authentication keys can be extracted.
- 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

- November 2-6, 2026

Become a corporate supporter