# CWE Detail – CWE-918

## Description

The web server receives a URL or similar request from an upstream component and retrieves the contents of this URL, but it does not sufficiently ensure that the request is being sent to the expected destination.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2023-32786: Chain: LLM integration framework has prompt injection
 (CWE-1427) that allows an attacker to force the service to retrieve
 data from an arbitrary URL, essentially providing SSRF (CWE-918) and
 potentially injecting content into downstream tasks.

**•** CVE-2021-26855: Server Side Request Forgery (SSRF) in mail server, as exploited in the wild per CISA KEV. (KEV)

**•** CVE-2021-21973: Server Side Request Forgery in cloud platform, as exploited in the wild per CISA KEV. (KEV)

**•** CVE-2016-4029: Chain: incorrect validation of intended decimal-based IP address format (CWE-1286) enables parsing of octal or hexadecimal formats (CWE-1389), allowing bypass of an SSRF protection mechanism (CWE-918).

**•** CVE-2002-1484: Web server allows attackers to request a URL from another server, including other ports, which allows proxied scanning.

**•** CVE-2004-2061: CGI script accepts and retrieves incoming URLs.

**•** CVE-2010-1637: Web-based mail program allows internal network scanning using a modified POP3 port number.

**•** CVE-2009-0037: URL-downloading library automatically follows redirects to file:// and scp:// URLs

## Related Attack Patterns (CAPEC)

* CAPEC-664

## Modes of Introduction

**•** Architecture and Design: N/A

**•** Implementation: N/A

## Common Consequences

**•** Impact: Read Application Data — Notes:

**•** Impact: Execute Unauthorized Code or Commands — Notes:

**•** Impact: Bypass Protection Mechanism — Notes: By providing URLs to unexpected hosts or ports, attackers can make it appear that the server is sending the request, possibly bypassing access controls such as firewalls that prevent the attackers from accessing the URLs directly. The server can be used as a proxy to conduct port scanning of hosts in internal networks, use other URLs such as that can access documents on the system (using file://), or use other protocols such as gopher:// or tftp://, which may provide greater control over the contents of requests.

## Applicable Platforms

**•** None (Class: Not Language-Specific, Prevalence: Undetermined)

## Notes

**•** Relationship: CWE-918 (SSRF) and CWE-611 (XXE) are closely related, because they both involve web-related technologies and can launch outbound requests to unexpected destinations. However, XXE can be performed client-side, or in other contexts in which the software is not acting directly as a server, so the "Server" portion of the SSRF acronym does not necessarily apply.