This Is Forgery

SSRF Execute Payloads

Server-Side Request Forgery attacks execute payload commands through an exploited application/system targeting that system or other back-end systems.

SSRF-Mailcious-HTTP-Request

A Server-Side Request Forgery attack sends malicious HTTP requests to vulnerable applications/systems to use that system as a vessel to conduct other malicious actions.

SSRF Internal Scanning

An attacker may gather critical system/network information (scanning and enumeration) by conducting Server-Side Request Forgery attacks.

SSRF Dangers

Server-Side Request Forgery attacks are dangerous because they allow the remote retrieval of files, remote execution of applications and system commands, and other malicious actions.

SSRF Evade Firewalls and Network Security

Server-Side Request Forgery attacks allow attackers to evade network firewalls and other network security devices.

SSRF Prevention

Server-Side Request Forgery attacks may be prevented by implementing network access control policies, response handling, input validation, internal communication (zero-trust) authentication, and disabling unnecessary URLs.

SSRF Enablers

The lack of server hardening, input validation, response handling, and network access security policy enables Server-Side Request Forgery attacks to be.

Print Share