SSRF (Server-Side Request Forgery)

Inhaltsverzeichnis

SSRF bringt einen Server dazu, Anfragen an interne oder geschützte Ziele zu stellen. So werden Firewall-Grenzen umgangen und Metadaten- oder Intranet-Dienste erreichbar.

1 Funktionsweise

Die Anwendung akzeptiert eine URL oder ein Ziel und holt Daten serverseitig ab. Ein Angreifer lenkt das Ziel auf interne IPs, Cloud-Metadaten oder lokale Dienste um.

- **URL-Fetching:** Preview, Webhooks, Importer
- **Internal Reach:** Zugriff aus Server-Perspektive
- **Protocol Abuse:** file://, gopher:// u. Ä. je nach Stack

2 Typische Einsatzbereiche

- Cloud-Umgebungen mit Metadaten-APIs
- Microservices hinter internen Netzen
- Funktionen zum Laden externer Ressourcen

3 Wichtige Hinweise

- Allowlists statt Blocklisten bevorzugen.
- Private IP-Ranges und Link-Local sperren.
- Netzwerksegmentierung begrenzt Blast Radius.

4 Fazit

SSRF missbraucht das Vertrauensprivileg des Servers – besonders kritisch in Cloud- und Intranet-nahen Architekturen.