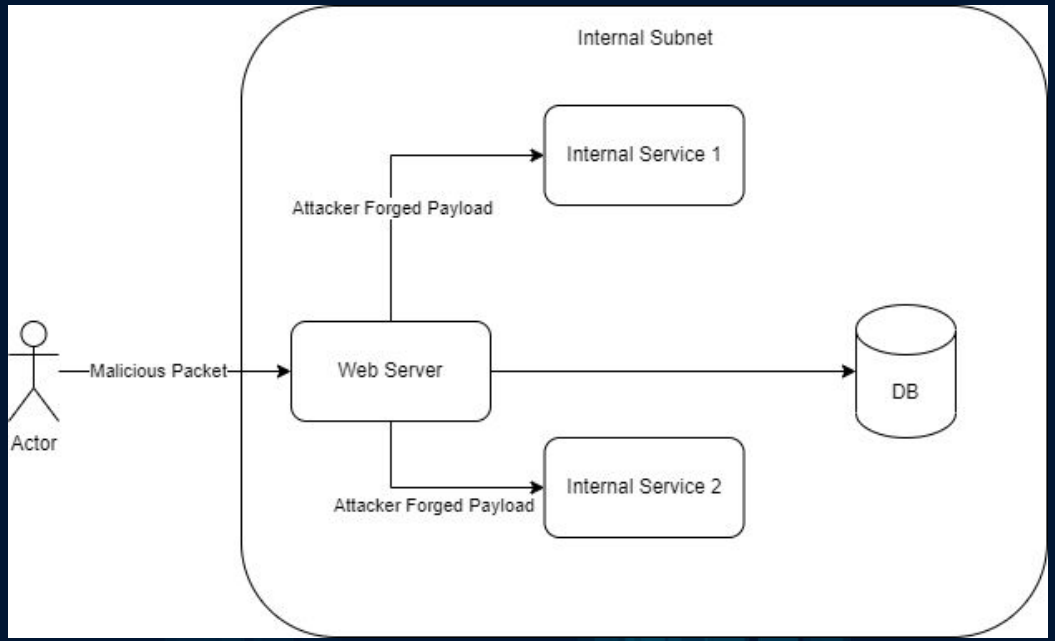
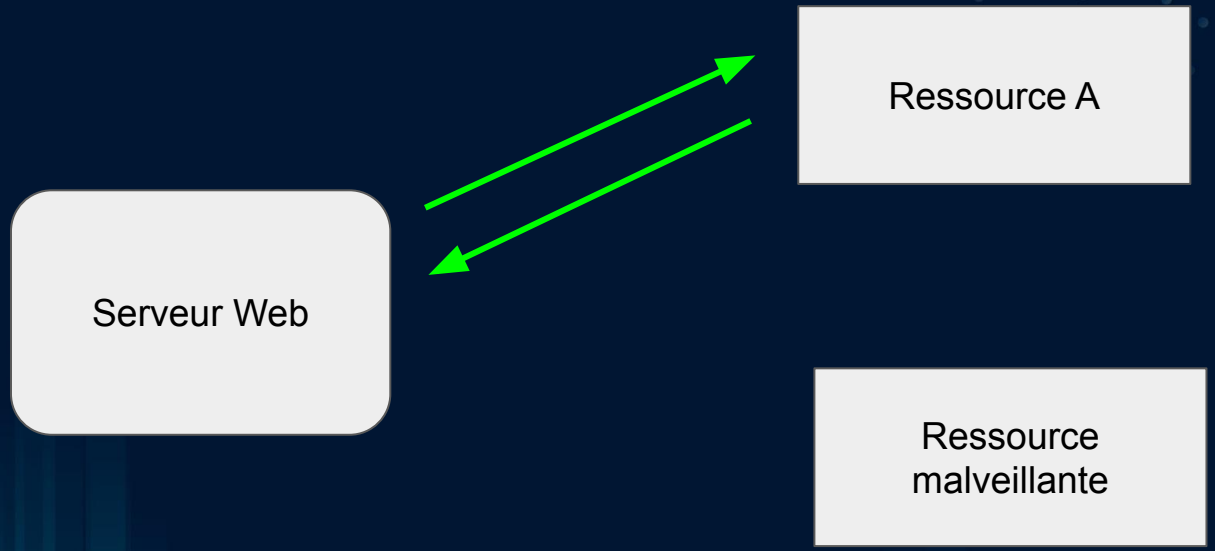
Intro to SSRF

Qu'est-ce qu'un SSRF

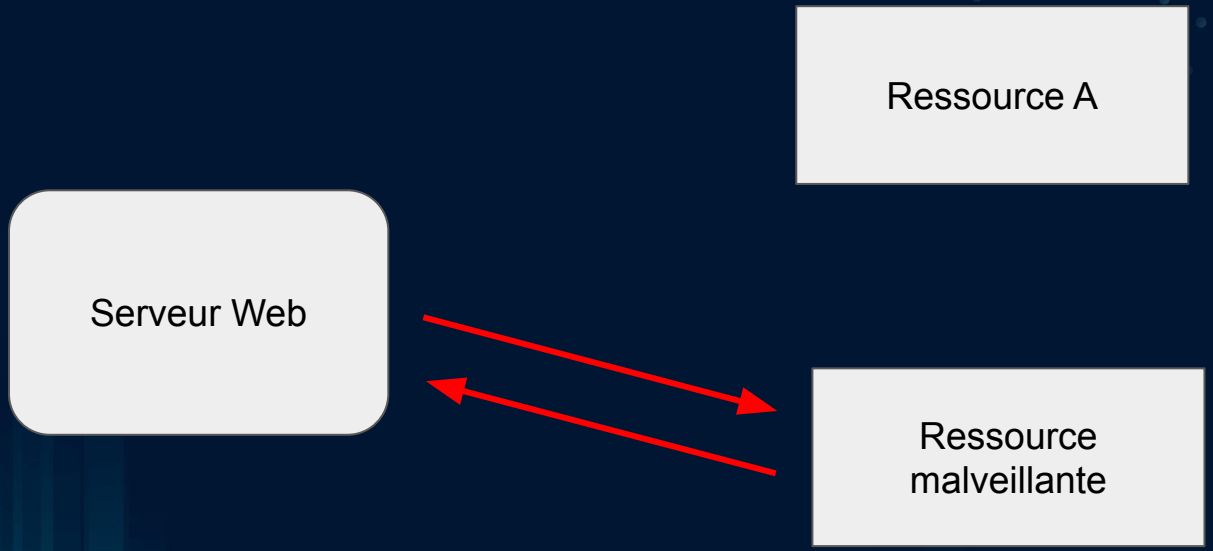
Envoyer des requêtes (HTTP, HTTPS ...) depuis un serveur cible vers des ressources internes ou externes.



Pourquoi ca existe



Pourquoi ca existe



Où trouver des SSRFs

Où trouver des SSRFs

Generator de pdf

Où trouver des SSRFs

Generator de pdf

LFI = SSRF ? (file_get_contents, fopen ...)

Où trouver des SSRFs

Generator de pdf

Ajout de webhooks

LFI = SSRF ? (file_get_contents, fopen ...)

Où trouver des SSRFs

Generator de pdf

Import en xml (XXE)

Ajout de webhooks

LFI = SSRF ? (file_get_contents, fopen ...)

Où trouver des SSRFs

Generator de pdf

Import en xml (XXE)

Ajout de webhooks

LFI = SSRF ? (file_get_contents, fopen ...)

Headers HTTP (Host, X-Forward-For, Referer)

Où trouver des SSRFs

Generator de pdf

Import en xml (XXE)

Photo de profile

Ajout de webhooks

LFI = SSRF ? (file_get_contents, fopen ...)

Headers HTTP (Host, X-Forward-For, Referer)

Où trouver des SSRFs

Generator de pdf

Import en xml (XXE)

Photo de profile

Ajout de webhooks

LFI = SSRF ? (file_get_contents, fopen ...)

Server status

Headers HTTP (Host, X-Forward-For, Referer)

Où trouver des SSRFs

Generator de pdf

Import en xml (XXE)

Photo de profile

Ajout de webhooks

Config email

LFI = SSRF ? (file_get_contents, fopen ...)

Server status

Headers HTTP (Host, X-Forward-For, Referer)

Où trouver des SSRFs

Generator de pdf

Import en xml (XXE)

Photo de profile

Ajout de webhooks

Preview de lien dans chat

Config email

LFI = SSRF ? (file_get_contents, fopen ...)

Server status

Headers HTTP (Host, X-Forward-For, Referer)

Où trouver des SSRFs

Generator de pdf

Import en xml (XXE)

Photo de profile

Ajout de webhooks

Import url

Preview de lien dans chat

Config email

LFI = SSRF ? (file_get_contents, fopen ...)

Server status

Headers HTTP (Host, X-Forward-For, Referer)

Où trouver des SSRFs

Generator de pdf

Import en xml (XXE)

Photo de profile

Ajout de webhooks

Import url

Preview de lien dans chat

Config email

Upload de fichiers (svg)

LFI = SSRF ? (file_get_contents, fopen ...)

Server status

Headers HTTP (Host, X-Forward-For, Referer)

Impact des SSRFs

- Scanner des ports/ips
- Taper des services sur le localhost / reseau interne
- Exfiltrer des fichiers/contenu privé
- Accès aux métadonnées cloud
- RCE??
- Command injection si dev stupide

Types de SSRFs Content Based (Classic)

GET lucashanson.fr/ssrf.php?url=http://localhost/admin.php

Réponse:

Html blah blah admin page

Types de SSRFs Boolean-Based / Error Based (Semi blind)

GET lucashanson.fr/ssrf.php?url=http://localhost:22

Page affiche html / code 200

GET lucashanson.fr/ssrf.php?url=http://localhost:23

Page affiche erreur / code 500

Types de SSRFs Time based (Blind)

GET lucashanson.fr/ssrf.php?url=http://localhost:22

Réponse rapide: Ouvert

GET lucashanson.fr/ssrf.php?url=http://localhost:23

Réponse lente: Fermé