Falsificación de solicitudes del lado del servidor (Server-Side Request Forgery, SSRF)

Se está en riesgo de sufrir ataques SSRF cuando una aplicación permite obtener un recurso remoto sin validar la URL que proporciona el usuario. Este tipo de ataque puede evitar la protección que brinda el cortafuegos, la VPN o los controles de acceso.

Por ejemplo, cuando una aplicación permite especificar una URL a la que será redirigida la petición inicial, si no filtramos la URL a la que se redireccionará, el atacante podría aprovechar para indicar una dirección cualquiera.

Los ataques podrían consistir en peticiones del tipo:

GET /?url=http://localhost/server-status HTTP/1.1

o

GET /?url=file:///etc/passwd HTTP/1.1