Server Side Request Forgery

Server-side request forgery is a web security vulnerability that allows an attacker to cause the server-side application to make requests to an unintended location.

Do you know ?

dnsFookup	DNS rebinding toolkit
rbndr	Simple DNS Rebinding Service
dref	DNS Rebinding Exploitation Framework
dns-rebind-toolkit	A front-end JavaScript toolkit for creating DNS rebinding attacks.
whonow	A "malicious" DNS server for executing DNS Rebinding attacks on the fly (public instance running on rebind.network:53)
singularity	A DNS rebinding attack framework.
lorsrf	Bruteforcing on Hidden parameters to find SSRF vulnerability using GET and POST Methods
sentrySSRF	Tool to searching sentry config on page or in javascript files and check blind SSRF
grafana-ssrf	Authenticated SSRF in Grafana
SSRFmap	Automatic SSRF fuzzer and exploitation tool
Gopherus	This tool generates gopher link for exploiting SSRF and gaining RCE in various servers
ground-control	A collection of scripts that run on my web server. Mainly for debugging SSRF, blind XSS, and XXE vulnerabilities.
SSRFire	An automated SSRF finder. Just give the domain name and your server and chill! ;) Also has options to find XSS and open redirects
B-XSSRF	Toolkit to detect and keep track on Blind XSS, XXE & SSRF
gaussrf	Fetch known URLs from AlienVault's Open Threat Exchange, the Wayback Machine, and Common Crawl and Filter Urls With OpenRedirection or SSRF Parameters.
ssrfDetector	Server-side request forgery detector

www.hackingarticles.in

@hackinarticles

https://in.linkedin.com/company/hackingarticles

https://github.com/Ignitetechnologies