Server-Side Request Forgery (SSRF) Overview

Server-Side Request Forgery (SSRF) attacks, listed in the OWASP top 10, allow us to abuse server functionality to perform internal or external resource requests on behalf of the server. To do that, we usually need to supply or modify URLs used by the target application to read or submit data. Exploiting SSRF vulnerabilities can lead to:

- Interacting with known internal systems
- Discovering internal services via port scans
- Disclosing local/sensitive data
- Including files in the target application
- Leaking NetNTLM hashes using UNC Paths (Windows)
- Achieving remote code execution

We can usually find SSRF vulnerabilities in applications that fetch remote resources. When hunting for SSRF vulnerabilities, we should look for:

- Parts of HTTP requests, including URLs
- File imports such as HTML, PDFs, images, etc.
- Remote server connections to fetch data
- API specification imports
- Dashboards including ping and similar functionalities to check server statuses

Note: Always keep in mind that web application fuzzing should be part of any penetration testing or bug bounty hunting activity. That being said, fuzzing should not be limited to user input fields only. Extend fuzzing to parts of the HTTP request as well, such as the User-Agent.

Previous Next Mark Complete & Next

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left