Exploitation

- Links
  - DNS
  - Request Interception
  - HTTPD
  - Conversion
  - Payloads

Links

DNS

https://nip.io/ Wildcard DNS

Request Interception

Tools:

- BurpSuite

Links:

- Requestbin: Interecepts HTTP Requests (useful for blind SSRF)

HTTPD

Busybox HTTPD

```
httpd [-ifv[v]] [-c CONFFILE] [-p [IP:]PORT] [-u USER[:GRP]] [-r REALM] [-h HOME] or httpd -d/-e/-m STRING

Listen for incoming HTTP requests

Options:

        -i              Inetd mode
        -f              Do not daemonize
        -v[v]           Verbose
        -c FILE         Configuration file (default httpd.conf)
        -p [IP:]PORT    Bind to ip:port (default *:80)
        -u USER[:GRP]   Set uid/gid after binding to port
        -r REALM        Authentication Realm for Basic Authentication
        -h HOME         Home directory (default .)
        -m STRING       MD5 crypt STRING
        -e STRING       HTML encode STRING
        -d STRING       URL decode STRING
```

Conversion

- CyberChef: Encode/Decode string formats with recipes

Payloads

- PayloadsAllTheThings: Misc payloads and bypasses