SSRF Cheat Sheet

Définition de la vulnérabilité SSRF

Vulnérabilité web qui permet d'interagir avec un serveur (réseau interne ou externe, ou la machine elle-même).
Peut donner accès : à des fichiers ; à des services (ex. Web, FTP, SMTP, SQL/NoSQL, etc.) sur le serveur vulnérable ou sur un autre serveur du réseau interne du serveur ; à d'autres serveurs ou réseaux ; à un routeur d'interface…

Où la trouver ?

Dès qu'une fonctionnalité interagit avec une ressource externe.
Par exemple :

- Uploads de fichiers
- Appels API
- Webhooks
- Redirection vers une page
- Parsers de documents
- Générateurs de documents (pdf…)

Types

- Content-based
- Boolean-based
- Error-based
- Time-based

Exploitation

√ Bypasser les filtres

- **0.0.0.0 variantes**
  - › 0
  - › [::]
  - › 0000
  - › 017700000001
  - › 0x7f000001
- **localhost & variantes**
  - › localhost
  - › 127.0.0.1
  - › Domaine avec une redirection vers 127.0.0.1
    - o le vôtre
    - o spoofed.burpcollaborator.net
    - o 127.0.0.1.nip.io
  - › Short IP
    - o 127.0.1
    - o 127.1
  - › Changement de base
    - o 2130706433 (decimal IP)
    - o 017700000001 (octal IP)
    - o 0x7f001 (hexadecimal IP)
  - › IP V6
    - o [::1]
    - o [::ffff:127.0.0.1]
    - o [::127.0.0.1]

√ Bypasser le protocole dans l'URL

- file://
- http://
- ftp://
- gopher://
- dict://
- idapt://

√ Bypasser les filtres DNS (DNS rebinding method)

- Rbndr

Exemple pour switcher entre 192.168.0.1 et 127.0.0.1 :
7f000001.c0a80001.rbndr.us

Protection

White-lister les ressources nécessaires :
- Définir les DNS /adresses IP autorisés
- Définir les protocoles autorisés

vaadata
Ethical Hacking Services
www.vaadata.com
v2022.1