Server Side Template Injection

mh4ckt3mh4ckt1c4s

Avant de commencer

- Qui je suis : mh4ckt3mh4ckt1c4s, étudiant à Télécom SudParis
- Le TP : minimum d'installation requise, fait pour expérimenter librement (il suffit d'avoir Python et Internet)
- Les questions : n'hésitez pas à m'interrompre, les seules questions idiotes sont celles qu'on ne pose pas

Qu’est-ce qu’un template ?

- Avant, on écrivait du code directement dans le code HTML (PHP)

- Besoin de faciliter la personnalisation de sites web sans mettre du code partout

- Permet de créer des pages web adaptables à l’aide d’un langage

Exemple : un site en Jinja

- {{ variable }} pour afficher une variable ou exécuter du code
- {% for ... %} et {% endfor %} pour des boucles (syntaxe Python)
- {% if ... %} et {% endif %} pour des conditions (syntaxe Python)
- Et bien d’autres !

Démonstration

- Dossier exemple

Qu’est-ce qu’une injection de template ?

- Exécution de code lors du rendering
- Que se passe-t-il si l’entrée utilisateur contient du code ?
- Peut-on s’empêcher de faire du rendering sur des entrées utilisateur ?

Où trouve-t-on des SSTI ?

- tl;dr : Partout !
- De nombreux langages : PHP, Java, NodeJS, Python, Ruby...
- De nombreux moteurs : Twig, Smarty, Jinjava, Jinja, Mako...
- Problème : compliqué d’identifier le bon template !

Quel est l’impact d’une SSTI ?

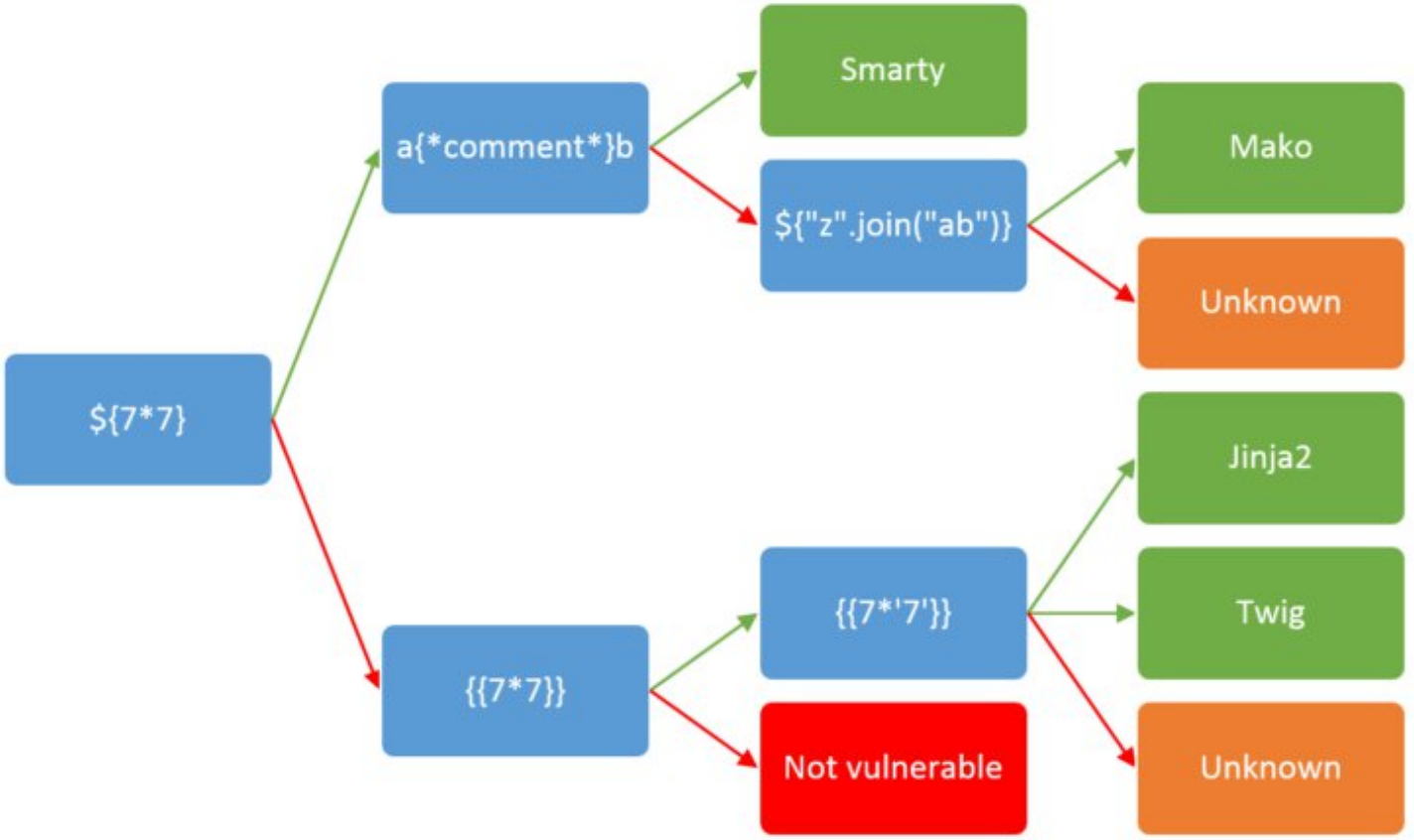
- Beaucoup trop de choses

- En général, une SSTI permet de :
  - Faire leak des variables
  - Lire des fichiers arbitraires (LFI)
  - Exécuter des commandes
  - Et parfois encore plus

Exploiter une SSTI

- Trouver un template...
- Trouver une erreur : ${{<%[%’”}}%\.
- Identifier le moteur de template
- Exploiter !

Exploiter une SSTI



Exploiter une SSTI

- PayloadAllTheThings et cie
- La doc
- Votre tête
- Expérimentez !

A vous de jouer !

- TP avec 2 niveaux (+1 bonus)

- Vous êtes sur votre machine, ne faites pas rm –rf

- Essayez les choses suivantes :
  - Faire leak la valeur de la variable “secret”
  - Lire des fichiers sur votre système (/etc/passwd)
  - Lire des fichiers binaires (/bin/bash)
  - Exécuter des commandes
  - Obtenir un reverse shell