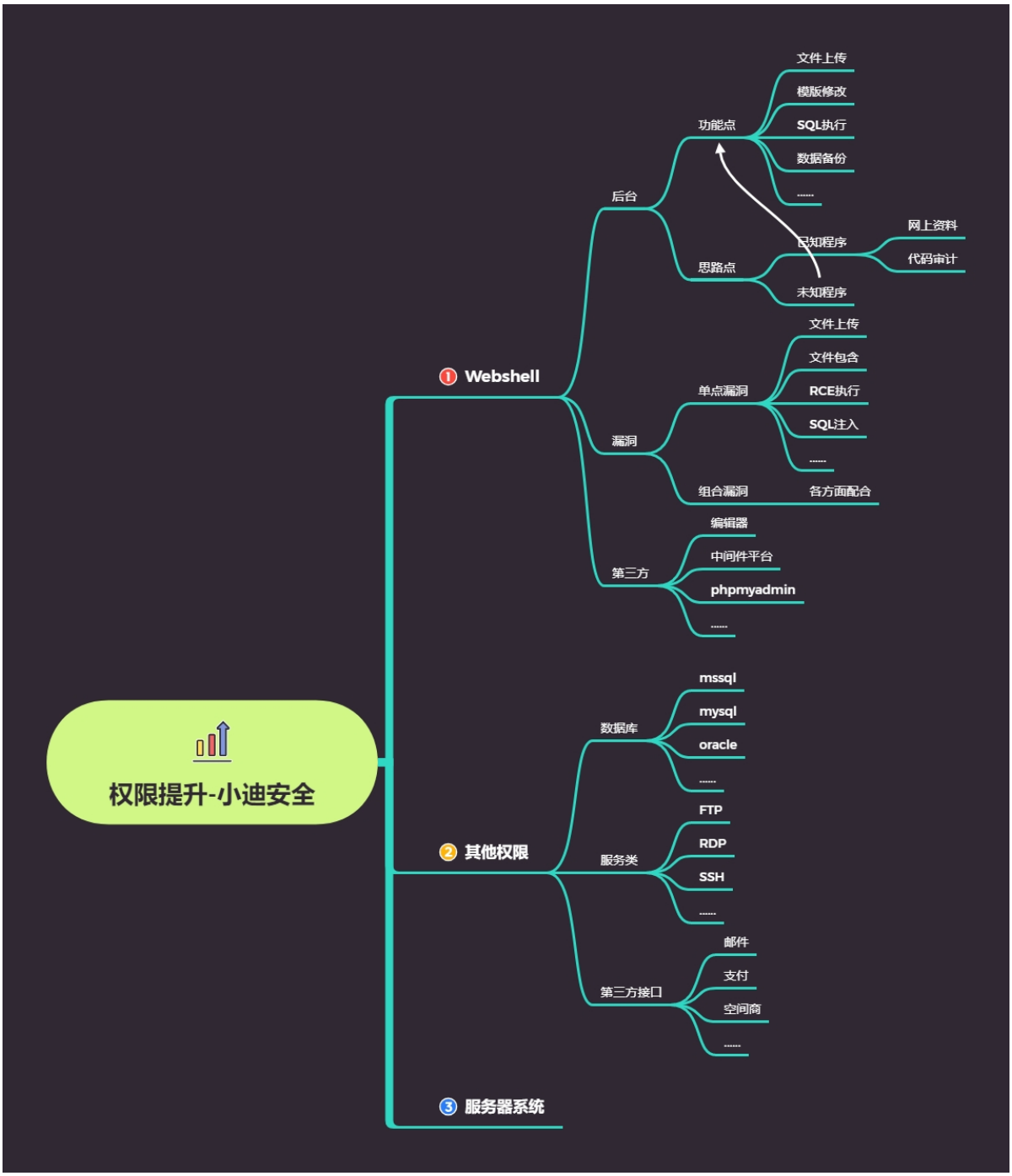
Day58　权限提升–网站权限后台漏洞第三方获取



58.1 权限提升

> 此处提权指的不是让网站的普通用户获取到管理员的权限（那属于网站的逻辑漏洞）而是我们已经利用网站的漏洞拿到了一些权限乃至webshell后如何利用网站权限进而获取到数据库、操作系统、服务器等的权限。

```
#当前知识点在渗透流程中的点
前期-中期-后期对应的知识关系

#当前知识点在权限提升的重点
知识点顺序,理解思路、分类介绍等

#当前知识点权限提升权限介绍
注重理解当前权限对应可操作的事情

#利用成功后的思路需要总结的思路
相关的操作被拒绝无法实现的时候就会涉及到权限提升
```

58.2 具体权限

后台权限、网站权限、数据库权限、接口权限、系统权限、域控权限等，一般正常的权限由小到大的顺序。

```
1）后台权限(获得方式:爆破、注入猜解、弱口令等)：一般网站或应用后台只能操作应用的界面内容、数据图片等信息,无法操作程序的源代码或服务器上的资源文件。(但是如果后台功能存在文件操作的话也可以操作文件数据拿到shell)
```

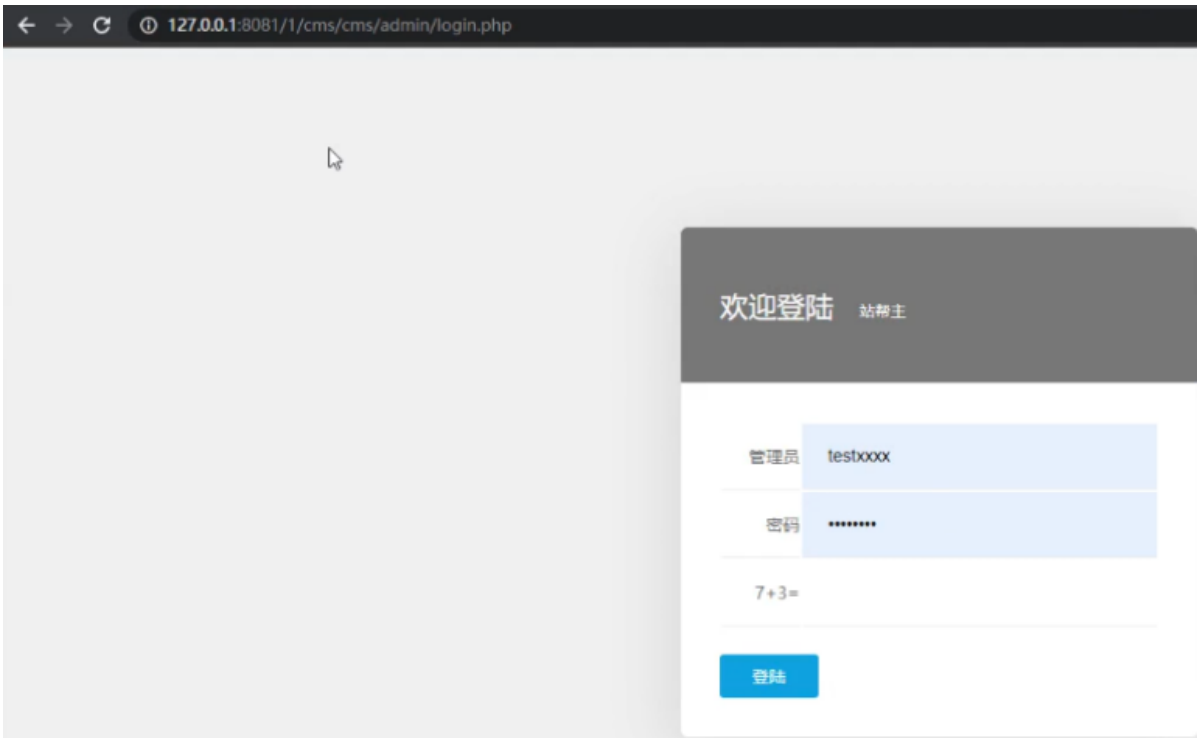
2）网站权限(获得方式:漏洞、曝光的exp获取)：查看或修改(还要看有没有锁权)程序源代码,可以进行网站或应用的配置文件读取(接口配置信息、数据库配置信息等),还能收集服务器操作系统等相关的信息,为后续系统提权做准备。

3）数据库权限：操作数据库的权限,数据库的增删改查等,源码或配置文件泄露,也可能是网站权限(webshell)进行的数据库配置文件读取获得。

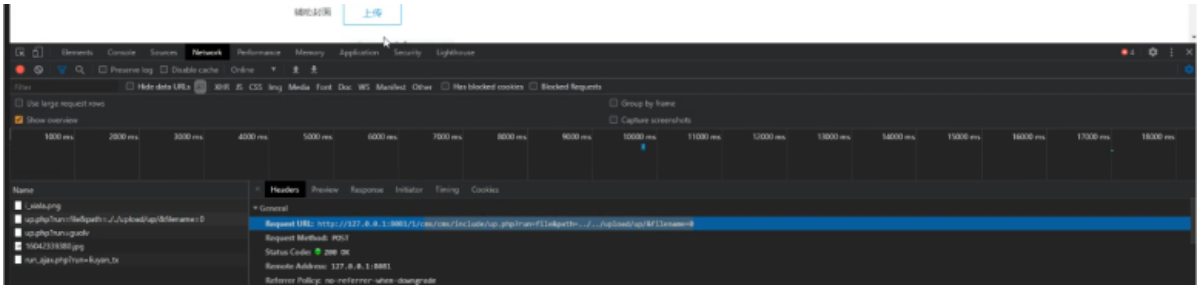
4）第三方/接口权限：(邮件、短信、支付、登录等)：后台或网站权限后的获取途径：后台(修改配置信息功能点)，网站权限(查看配置文件获取)进而可能获取到其它个人的敏感信息，社工...。

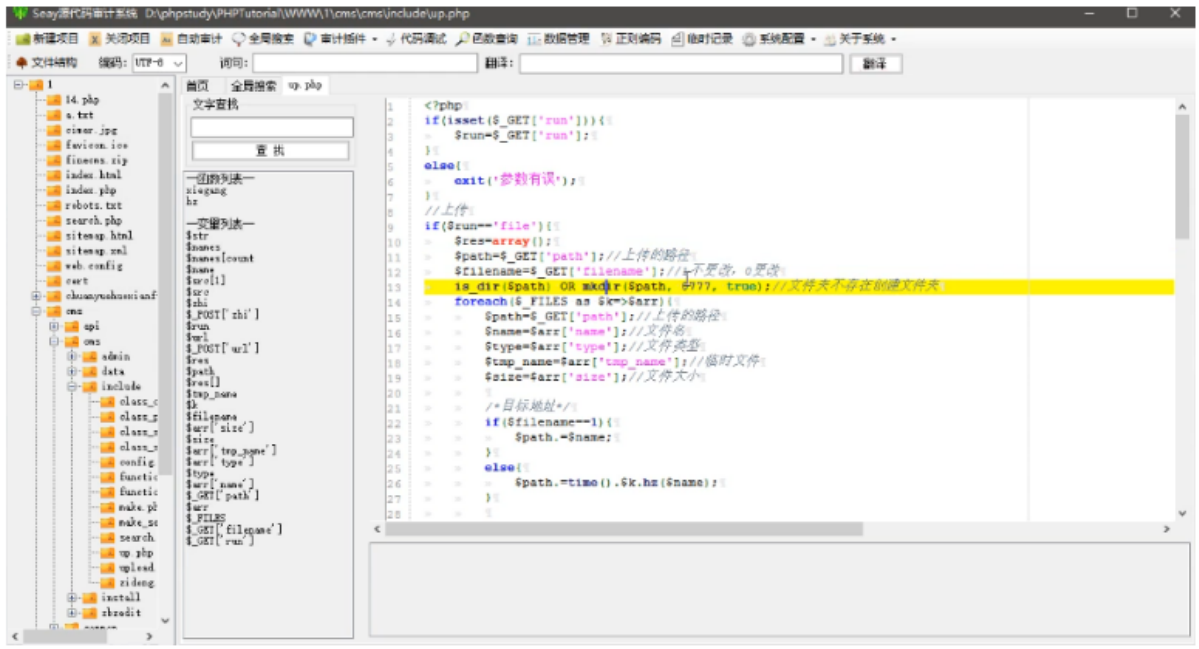
58.3 某挂壁程序后台权限提升-后台功能

后台地址:



抓包分析：

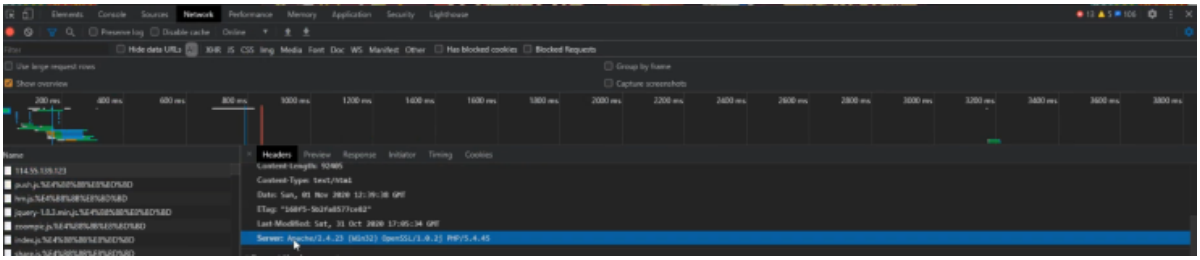




没有任何过滤,直接任意文件上传，如果没有代码,我们可以找功能点，SQL执行，文件操作、文件读取、文件写入

58.4 某BC广告导航页权限提升-漏洞层面

抓包分析：



通过分析中间件分析,该网站是phpstudy搭建的，先前phpstudy曝过漏洞，漏洞利用时使用postman软件

58.5 苏丹大西瓜GlassFish中间件-第三方

第三方glassfish服务器漏洞，苏丹的网站,fofa收集，寻找exp

fofa收集信息：

发现漏洞：