分享一次面试靶场笔记

原创

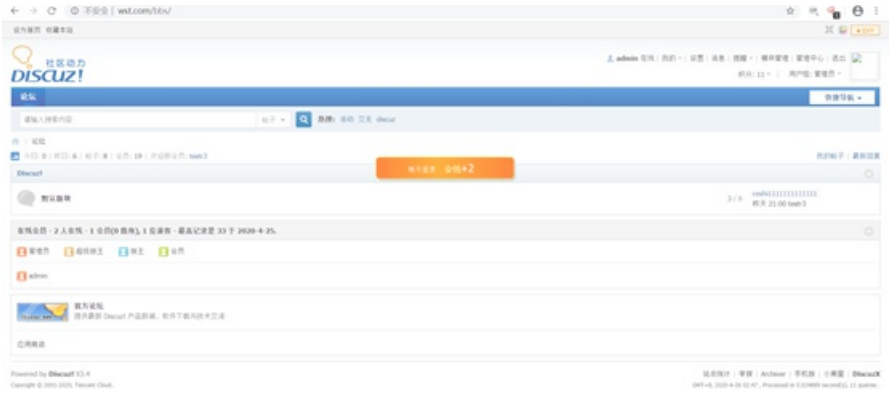
火线安全 于 2021-07-05 12:39:52 发布 97 收藏 1

文章标签： 网络安全

本文链接：https://blog.csdn.net/weixin_40418457/article/details/118487603

某面试靶场writeup

拿到站之后访问发现是一个phpinfo页面，大致看了一下内容，然后扫描目录，进入到bbs目录下，发现是用discuz3.4框架搭建的

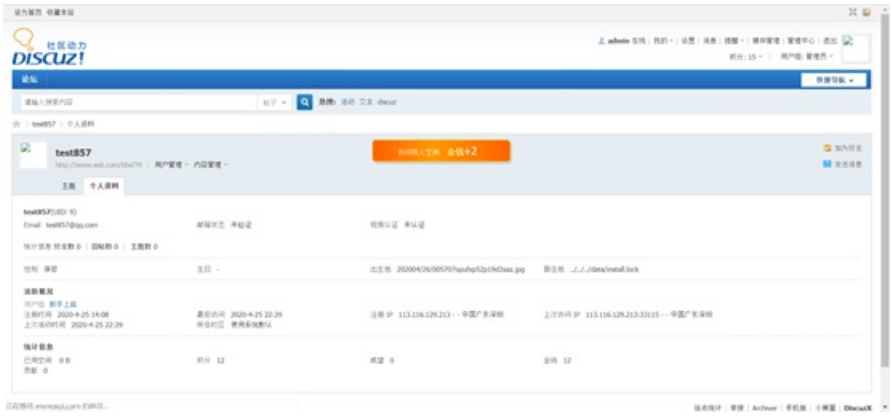


思路：

第一时间想到的就是利用网上已知的一些版本漏洞去入手，查了下该版本漏洞大概为四个，一个是刚出没多久的任意代码执行，但是因为是要cookie参数中有language参数然后再进行构造payload的，抓包的话发现站点并不存在这个参数，猜测可能会不会隐藏了参数？手动构造依然无果。

第二种就是一个是越权登录，一个是ssrf，这两个感觉对getshell可能帮助不大，最多是利用ssrf看下能不能探测到一些内网的敏感信息，后面测试发现这个漏洞其中一个前提是要在windows的环境中才有可能触发

最后一个任意文件删除漏洞，这个想了一下可以尝试删除install.lock文件，然后重置一遍站点在进后台getshell，尝试发现虽然在出生地的地方可以把要删除的文件的路径写上去，但是一直都无法删除install.lock文件

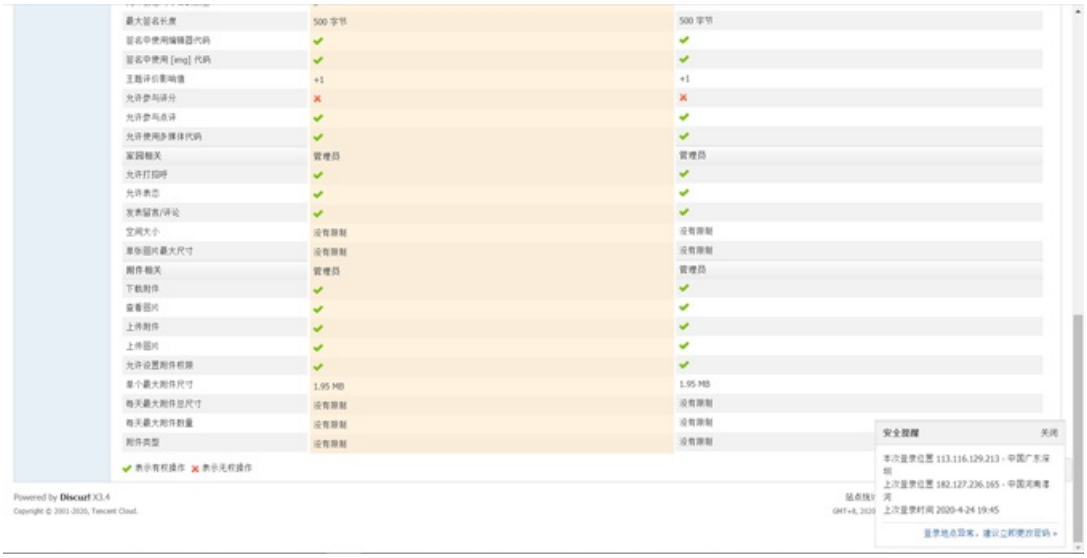


到这里一时间陷入的困境，对这种很成熟的框架，除了已经漏洞的利用，难道还是用0day？也有可能是漏洞利用的姿势不对，为此还特地下载了个同版本的框架，本地搭建复现了一下这个任意文件删除漏洞，发现本地搭建的环境也是无法删除到文件

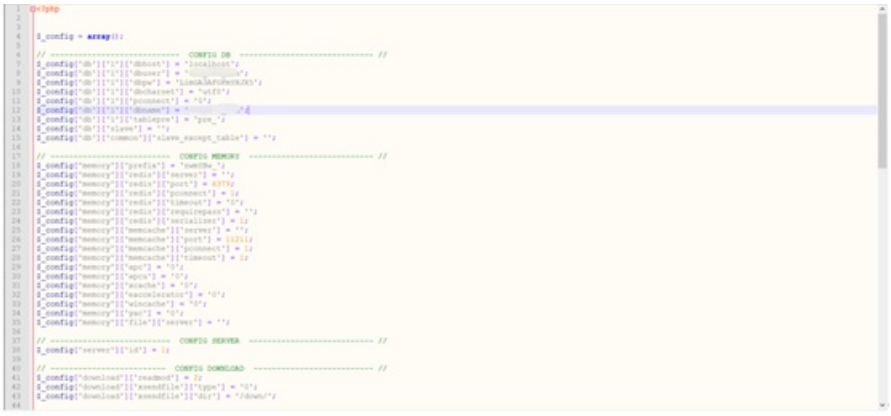
陷入僵局就先浏览了一下该框架，通过查看个人信息，可以发现原来有的几个账号，admin,whit,ceshizhanghao，发现了这三个账号，其中ceshizhanghao这个账号随便输入了一个弱口令123456竟然登录成功了，而且还是管理员的前台账号，但是回头一想前台的管理员账号也没有Getshell的点，然后就继续尝试这三个账号弱口令去登录后台的账号，发现还是不行，这就很难受了呀！！！

管理员账号：

ceshizhanghao 123456

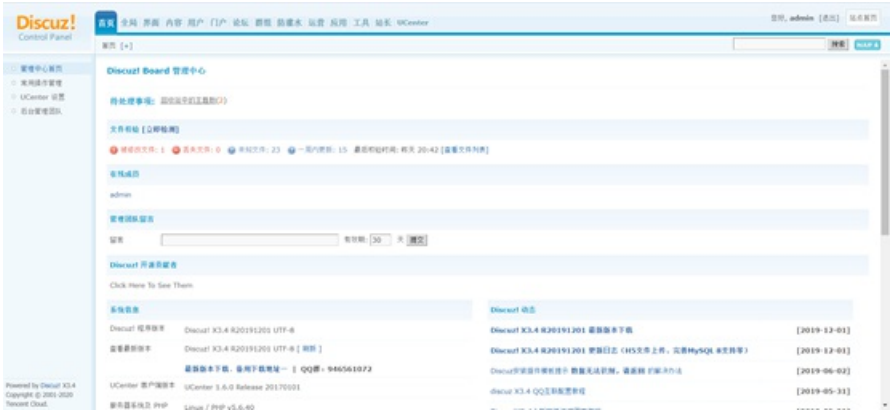


测试到这里就一直僵持了很久，没有入手点只能尽量的先收集一下信息了，把网址爬了一下，找到了一个bbs.tar.gz文件，下载下来发现是源码，在源码中找到了数据库账号密码



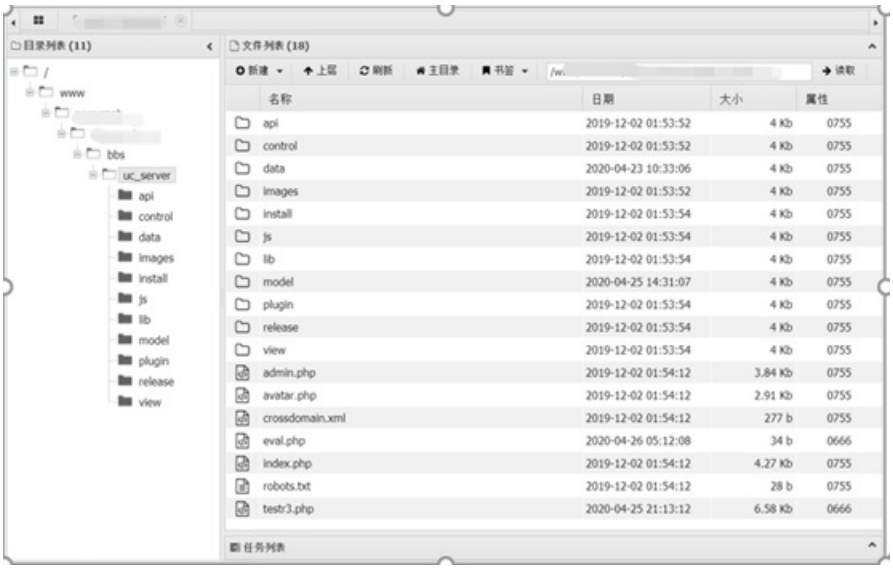
但是没有对外开放端口，这样知道账号密码也没有用，后面突然发现了根目录下有个admin.php,还有个adminer.php，访问发现是一个类似数据库管理的软件，然后成功用账号密码登录进去，查找到了后台的账号密码

成功登录到后台



后面在ucenter管理页面找到了一个本地文件包含漏洞可以成功利用

成功拿下



总结：

因为是靶场，可能会有大佬有其他的更快速的解题思路，不过在我测试过程中，其实关键点就是在源码的下载上，一开始拿到这种框架的站点有点太固定思维想着去利用历史漏洞，导致浪费了不少时间，没有一开始就去下到这个源码文件，要不然可以少走很多没必要的路，然后还有个任意文件删除的漏洞当时因为赶时间没去深究，后面要在搭建研究一下是啥问题。