

收到钓鱼网站链接：

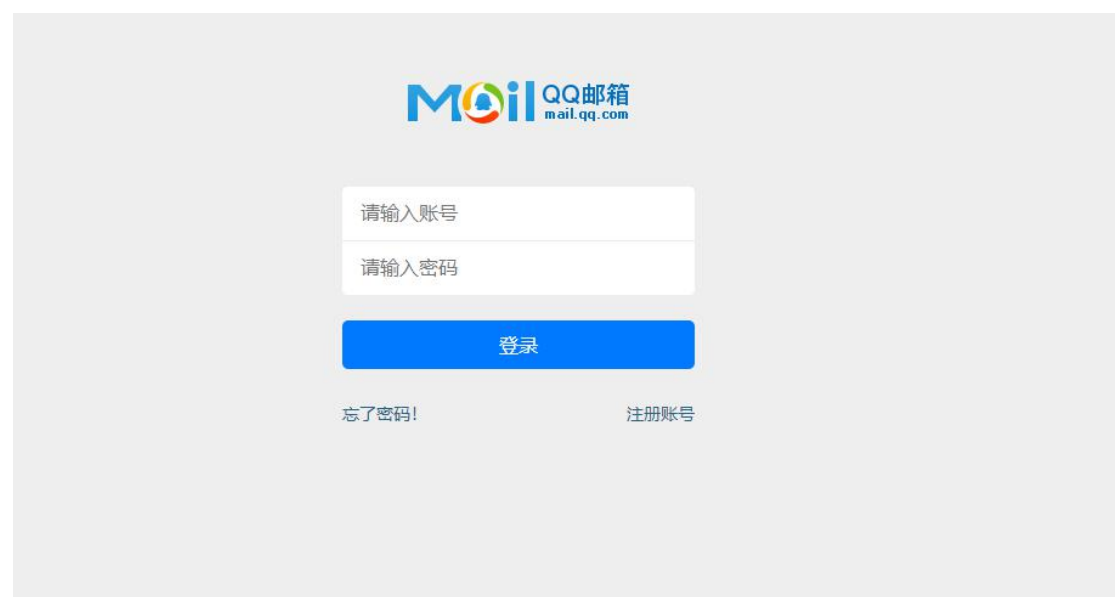


助学金补助名单：<http://www.yep.club/Fw-9ml?uid=62>

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

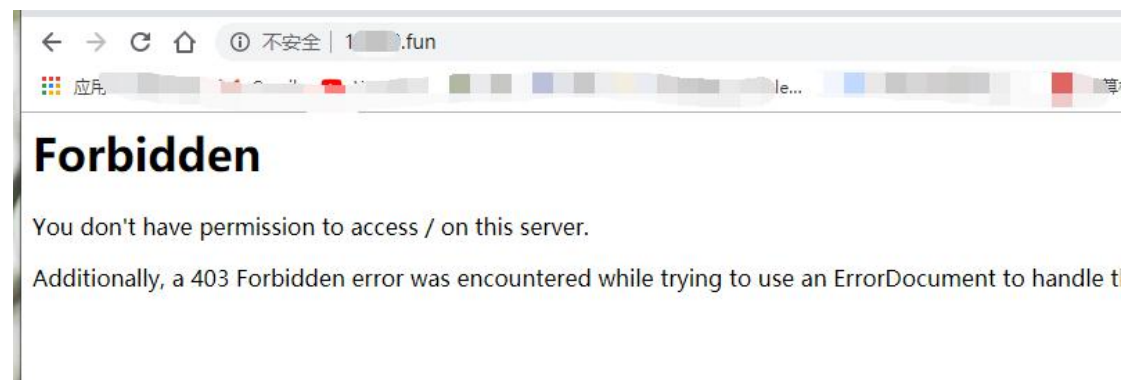
审计一下页面（也可以抓包），可以发现，数据提交的链接：

```

<div id="uid" id="login" class="login"><div id="logo" class="logo"></div>
<FORM method="post" name="form1" onsubmit="login();" action="http://www.1.fun/poss.php">
<div id="web_login"><ul id="g_list"><li id="g_u"><input name="tet_user" type="text" value="" placeholder="用户名" />
</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+

ID	账号	密码	URL	IP	添加时间	操作
651		744	http://www...club/Un-588.html...76	22.0.4.74 中国 广东 移动	2019-11-15 00:00:05	删除
651			http://www...club/Vv-...id=73	1.1.2.72 中国 广西 电信	2019-11-15 00:00:03	删除
651		51	http://www...club/Vv-...	3.2.72 中国 广西 电信	2019-11-15 00:00:06	删除
6519			http://www...club/Vv-...	1.1.7.74 中国 河南 移动	2019-11-15 00:00:04	删除
651		8	http://www...club/Vv-...	1.1.4.6 中国 广东 移动	2019-11-15 00:00:06	删除

平台的子用户有 63 个

ID	账号	密码	URL	服务器	开通时间	操作
85					2019-11-15	修改 删除
84	www			空	2019-11-15	修改 删除
83	90				2019-11-15	修改 删除
82	3				2019-11-15	修改 删除
81	26				2019-11-15	修改 删除
80	21				2019-11-15	修改 删除
79	26				2019-11-15	修改 删除
78	24				2019-11-15	修改 删除

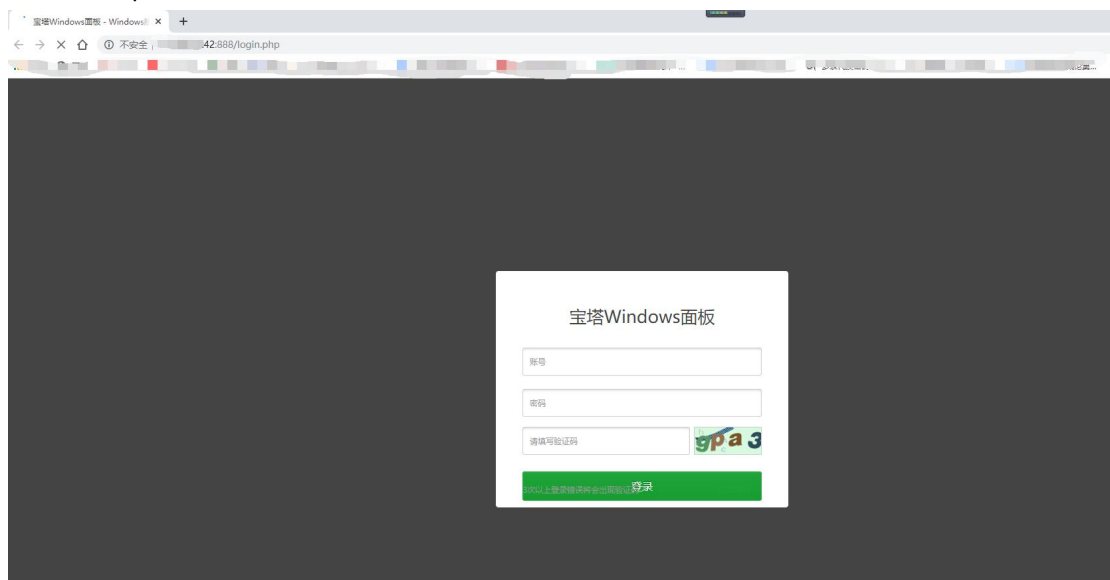
由于在这个站点上没有找到上传点,可以利用的服务还剩 ftp,由于对 ftp 不够了解,所以打算从其他方面入手,刚刚在审查用户的时候,我注意到了,每个链接都有对应的服务器。其中有个地址比较吸引我。

服务器 站点		
[REDACTED]t0q.w[REDACTED].com	20	20
[REDACTED]u9j8.w[REDACTED]	20	20
[REDACTED].42	20	20
[REDACTED]47.w[REDACTED]	20	20
l4[REDACTED]空间[REDACTED].com	20	20
[REDACTED]空间[REDACTED]	20	20
vi[REDACTED]空间[REDACTED].com	20	20
[REDACTED].42	20	20
[REDACTED]空间[REDACTED].pai[REDACTED].m	20	20
[REDACTED]空间[REDACTED]	20	20

尝试访问一下



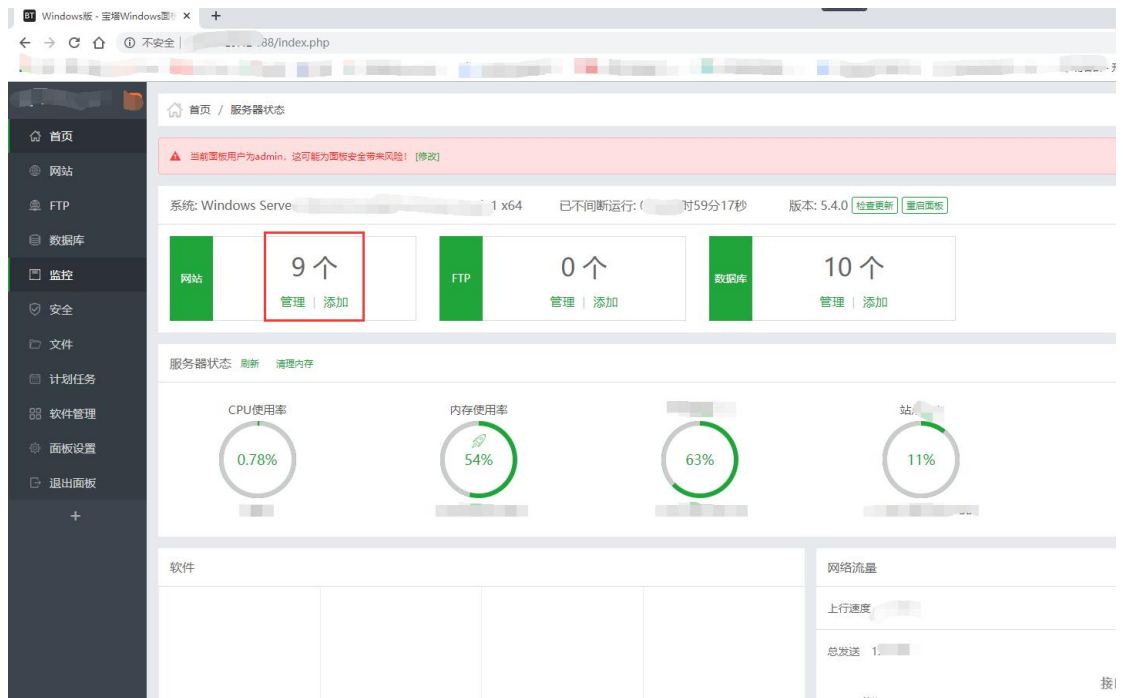
宝塔面板的界面，于是访问 888 端口，发现无响应，orz，再用 nmap 扫一下，扫出了 888 端口有 http，试着访问一下，发现了宝塔 win 的登录界面。



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。

用户列表: 共 63 个用户						
<div>全选 删除 一键清空 一键导出 admin 搜索链接 搜索用户</div>						
ID	账号	密码	URL	服务器	开通时间	操作
22	admin		http://www.		2022-10-10	修改 删除

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。。。



使用宝塔Windows面板创建网站时会默认创建权限配置, 统一使用www用户, 此用户统一使用应用程序池用户。

添加站点 修改默认 默认站点

域名	网站状态	备份	网站目录	创建日期	备注	操作
www.fun	运行中	无备份	wwwroot\80	2019-11-11	默认站点	设置   删除
www.fun	运行中	无备份	wwwroot\802	2019-11-11	默认站点	设置   删除
www.fun	运行中	无备份	wwwroot\80	2019-11-11	默认站点	设置   删除
www.fun	运行中	无备份	wwwroot\80	2019-11-11	默认站点	设置   删除
www.fun	运行中	无备份	wwwroot\80	2019-11-11	默认站点	设置   删除
www.fun	已停止	无备份	wwwroot\80	2019-11-11	默认站点	设置   删除
www.fun	运行中	无备份	wwwroot\80	2019-11-11	默认站点	设置   删除
www.fun	运行中	无备份	wwwroot\80	2019-11-11	默认站点	设置   删除

1 共计9条数据

添加数据库 root密码 phpMyAdmin

数据库名	用户名	密码	类型	打包文件	备注	操作
20			无备份		空	管理   权限   删除
12			无备份		空	管理   权限   删除
11			无备份		空	管理   权限   删除
5			无备份		空	管理   权限   删除
3			无备份		空	管理   权限   删除
1			无备份		空	管理   权限   删除
4			无备份		空	管理   权限   删除
3			无备份		空	管理   权限   删除
8			无备份		空	管理   权限   删除
5			无备份		空	管理   权限   删除

同步选中 同步所有 从服务器同步

1 共计10条数据



