渗透某骗子网站，X毛都没有，骗我九十九

原创r00tuser HACK学习呀
2019-10-21原文

前言

这几天在A市和B市奔波着，眼瞅着自己就要毕业了，必须得出来找份工作了。

和小伙伴在A市兜兜转转了几天，要不就是不合适没下文，要不就是给了offer，工资是在太低。心很累，然后就下B市了，看看B市还有没有一线生机。
(这篇文章是本人在面试的前一天，在B市某个咖啡馆写的，当时没有面试，在B市晃荡了一天，到最后只能在咖啡馆写文章了。直至今天重新写这篇文章时，网站已经不能访问了。)

网上冲浪？

和小伙伴合开了个房，晚上闲来无事，突发奇想就想着搜搜H的直播看看？（现在直播行业那么火，我们来看看小姐姐）

却误入了个萝莉吧？（首页图片很H这里就不放了）

想了想，首页这么暴露，必有诈。这种网站惯用套路就是注册需要转发链接，骗流量。还有就是骗钱，看个视频充个Vip之类的。

信息收集

本着为民除害(搞事情)的心态，我开始了拿站之旅。其实刚开始都没有收集什么信息，凭直觉我就随手测试了一下解析漏洞。（这里又有一个坑，因为之前认真复习了解析漏洞，从漏洞原理认真理解了一遍，也发现了一些东西。想写篇文章一直没写。先占个坑~）

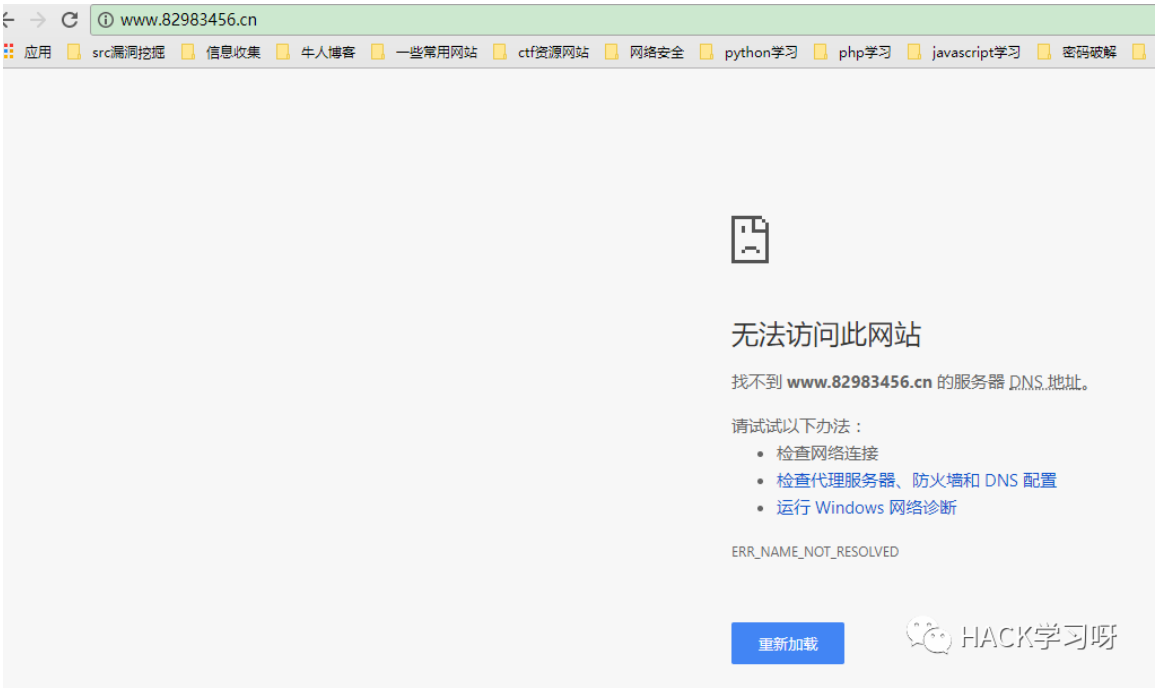
论坛的一些信息：dicuz论坛，nginx解析。

测试robots.txt正常，测试robots.txt/1.php返回不正常。

对比之处在于robots.txt返回的content-type:text/plain，

而robots.txt/1.php的content-type:text/html。

（过去了好久了，现在这个网站已经不能访问了。）



接下来就是找到一个上传点就好了。

先注册个账号，上传图像试试，发现图像是放在阿里的图床的，不放在服务器上面。

后来在测试发帖的时候成功上传图片马。拿到shell。

之后就是各种浏览了。

然后我发现进去之后浏览帖子，还要充钱？vip 99,超级vip,199?

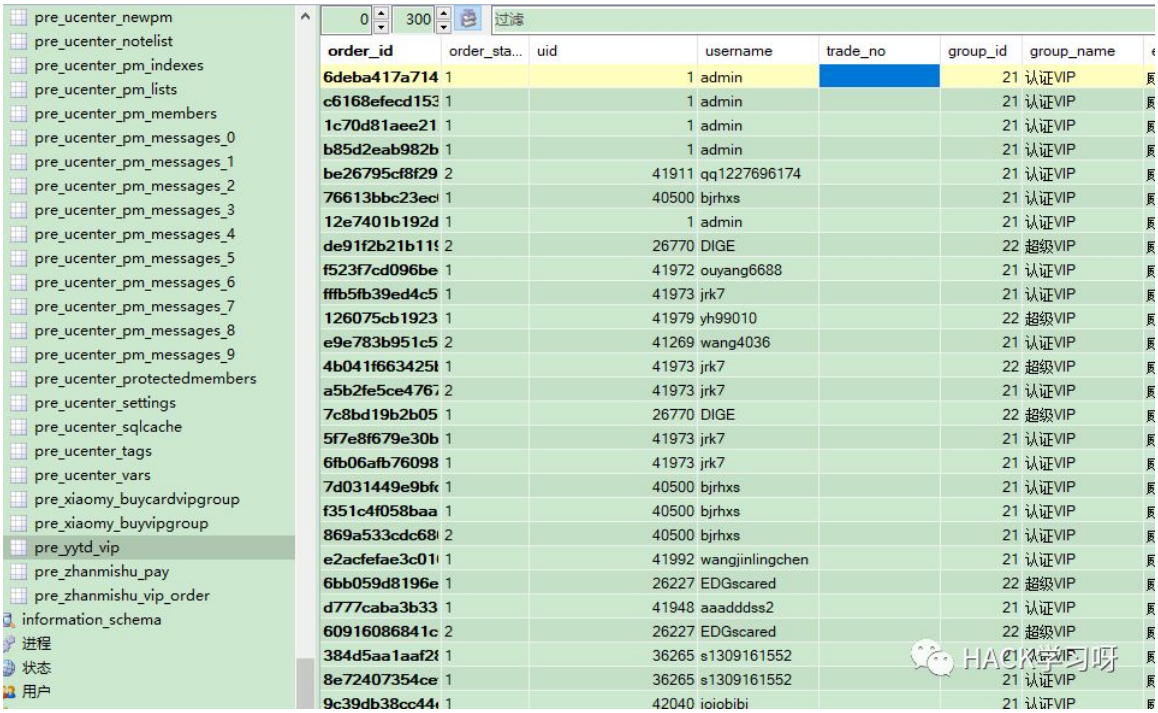
找了个超级vip的账号。

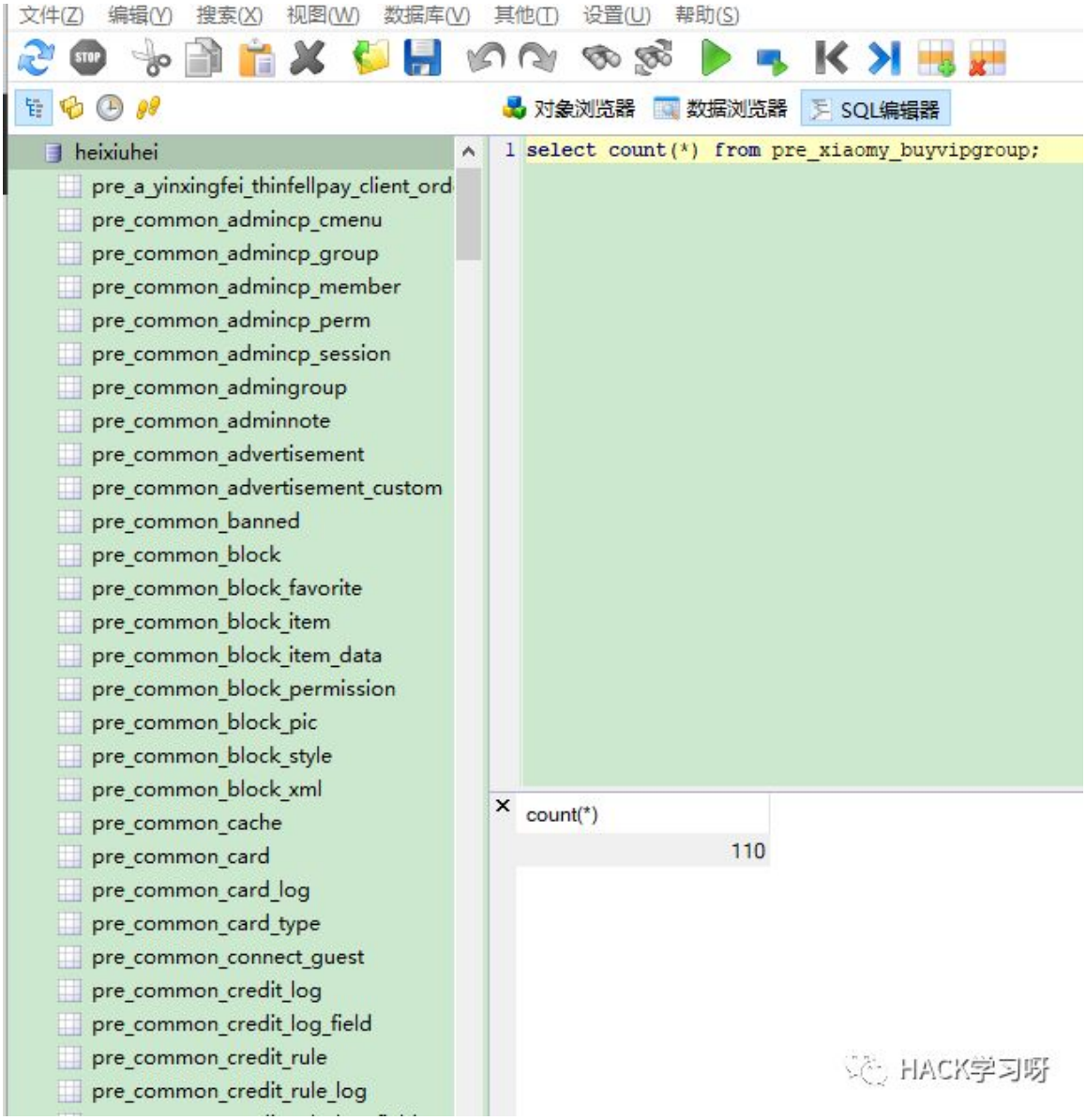
然后我就笑了。

为什么会这样呢？然后我看了一下所谓的H视频

就tm标题出骨一点，其实就是街头的一些跟拍而已。

然后我又看一下vip，和超级vip的人数：





也是有一百多号的水鱼啊！！

笑死~

网上那么多免费资源你不看，偏要给钱人家？？想不懂！！

还有这个网站的管理员发表的所谓声明。。。

这两天网站被黑客入侵，原因大家想必都知道！黑客小子尽然威胁我们要现金，不然删除所有萝莉数据！没办法，只能让他删除！但是他并不知道我们还有备份！因为萝莉数据被删除，所以VIP会员现在暂时看不到！如果现在马上上资源，肯定立马又被删除。为了VIP会员的权益，我们决定三天后再从新恢复数据！这样黑客就可以避免黑客的再次攻击！萝莉吧365天都可以正常打开。所以请网站请VIP会员一定要记得收藏好本网址，一定一定要记得！随时关注我们，绝对不让你们失望！！！被迫无奈，我们也没招，好在我们萝莉吧之偷拍美女裙底、偷拍屁股等珍稀视频资源没被删除。目前还可以继续下载观看！下载视频资源，请移步我们论坛极品萝莉专区以及超级VIP专享板块，即可在线下载超清4K视频，每一部都是摄影师冒死偷拍，价格不菲！最后希望VIP会员耐心等待三天！

哎呀，厉害了。

网站上不去，估计是被人举报，网警叔叔干事了。

看看域名信息（不打码）

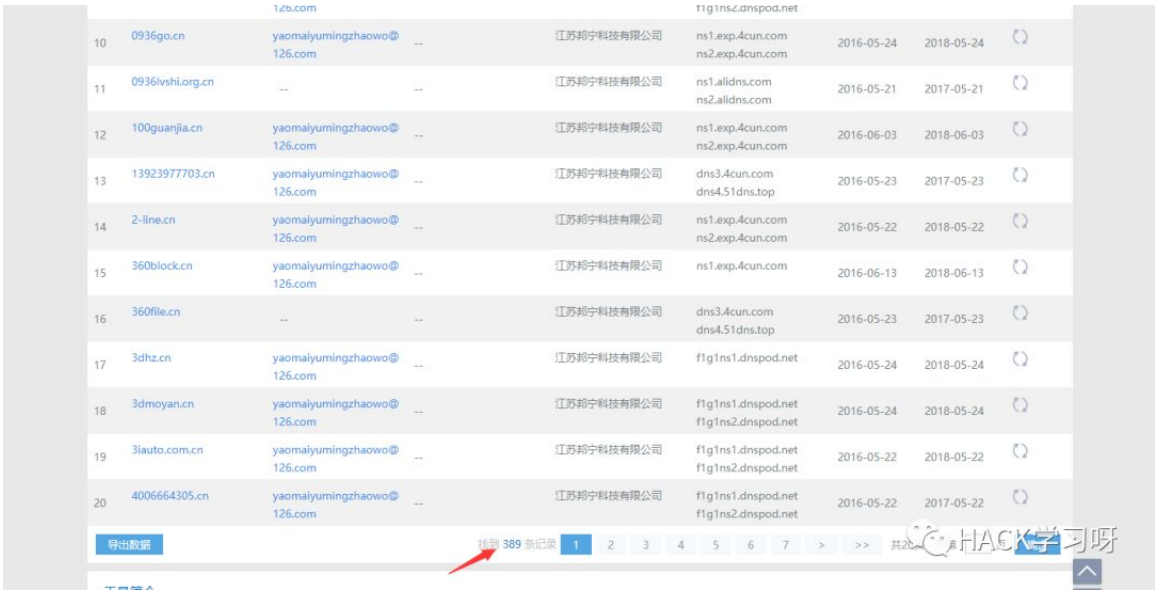
域名 82983456.cn 的信息 以下信息更新时间：2017-08-23 13:19:00 立即更新

域名	82983456.cn [whois 反查] 其他常用域名后缀查询： cn com cc net org
注册商	江苏邦宁科技有限公司
联系人	姜燕宁 [whois反查]
联系邮箱	yaomaiyumingzhaowo@126.com [whois反查]
创建时间	2016年05月22日
过期时间	2018年05月22日
DNS	f1g1ns1.dnspod.net f1g1ns2.dnspod.net
状态	域名普通状态(ok)

-------站长之家 Whois查询--------

Domain Name: 82983456.cn
ROID: 20160522s10001s83375595-cn
Domain Status: clientTransferProhibited
Domain Status: clientHold
Registrant ID: bn1462856128623
Registrant: 姜燕宁
Registrant Contact Email: yaomaiyumingzhaowo@126.com[whois反查]
Sponsoring Registrar: 江苏邦宁科技有限公司
Name Server: f1g1ns1.dnspod.net
Name Server: f1g1ns2.dnspod.net
Registration Time: 2016-05-22 04:07:40
Expiration Time: 2018-05-22 04:07:40
DNSSEC: unsigned

反查看看，389条记录，这么多垃圾域名。细极思恐~~



10	0936go.cn	yaomaiyumingzhaowo@126.com	--	江苏邦宁科技有限公司	ns1.exp.4cun.com ns2.exp.4cun.com	2016-05-24	2018-05-24
11	0936lvshi.org.cn	--	--	江苏邦宁科技有限公司	ns1.alidns.com ns2.alidns.com	2016-05-21	2017-05-21
12	100guanjia.cn	yaomaiyumingzhaowo@126.com	--	江苏邦宁科技有限公司	ns1.exp.4cun.com ns2.exp.4cun.com	2016-06-03	2018-06-03
13	13923977703.cn	yaomaiyumingzhaowo@126.com	--	江苏邦宁科技有限公司	dns3.4cun.com dns4.51dns.top	2016-05-23	2017-05-23
14	2-line.cn	yaomaiyumingzhaowo@126.com	--	江苏邦宁科技有限公司	ns1.exp.4cun.com ns2.exp.4cun.com	2016-05-22	2018-05-22
15	360block.cn	yaomaiyumingzhaowo@126.com	--	江苏邦宁科技有限公司	ns1.exp.4cun.com	2016-06-13	2018-06-13
16	360file.cn	--	--	江苏邦宁科技有限公司	dns3.4cun.com dns4.51dns.top	2016-05-23	2017-05-23
17	3dhz.cn	yaomaiyumingzhaowo@126.com	--	江苏邦宁科技有限公司	f1g1ns1.dnspod.net	2016-05-24	2018-05-24
18	3dmoyan.cn	yaomaiyumingzhaowo@126.com	--	江苏邦宁科技有限公司	f1g1ns1.dnspod.net f1g1ns2.dnspod.net	2016-05-24	2018-05-24
19	3iauto.com.cn	yaomaiyumingzhaowo@126.com	--	江苏邦宁科技有限公司	f1g1ns1.dnspod.net f1g1ns2.dnspod.net	2016-05-22	2018-05-22
20	4006664305.cn	yaomaiyumingzhaowo@126.com	--	江苏邦宁科技有限公司	f1g1ns1.dnspod.net f1g1ns2.dnspod.net	2016-05-22	2017-05-22

导出数据 找到 389 条记录 1 2 3 4 5 6 7 > >>

最后

还请网警叔叔加大力度，打击这些虚晃的黄网，拯救我国广大的花季少年啊！！

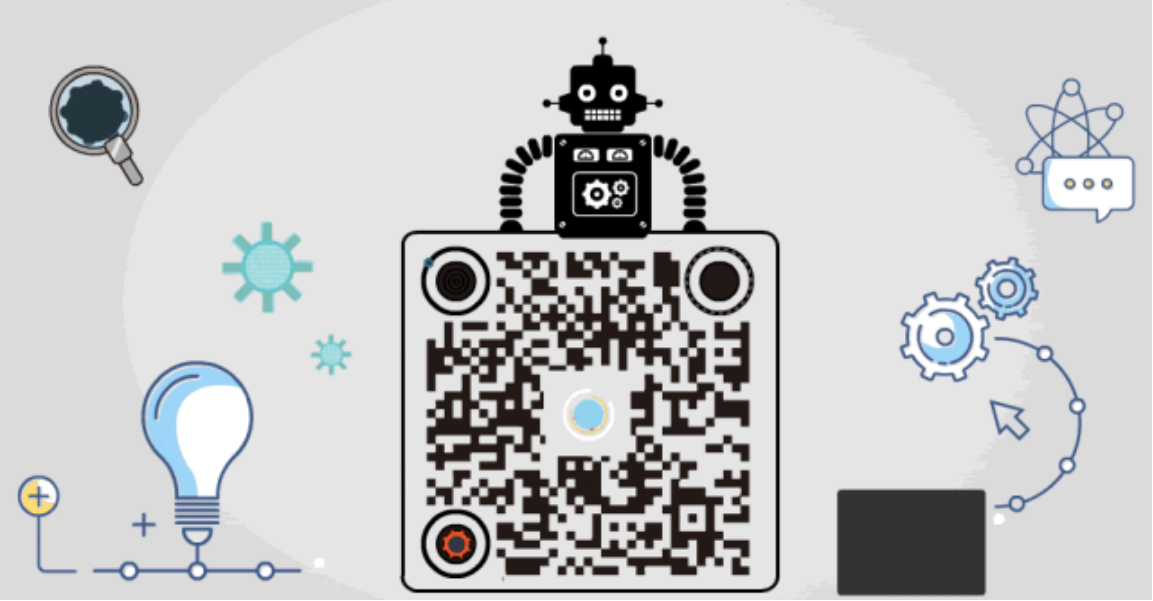
本篇文章没有什么技术含量，仅作为记录。（对了，网警叔叔这个就不要查水表了。）

现在这个82983456.cn现在已经是301跳转一个BC网站了

各位就不要自己再打开去看了

原创投稿作者：r00tuser

博客地址：https://www.cnblogs.com/r00tuser/p/7444139.html



精选留言

用户设置不下载评论