CTFHub暴力破解WriteUP

原创

TaibaiXX1 于 2021-06-01 19:39:42 发布 172 收藏
文章标签： css html github 数据可视化 信息安全

点击"仙网攻城狮”关注我们哦~

不当想研发的渗透人不是好运维

让我们每天进步一点点

简介

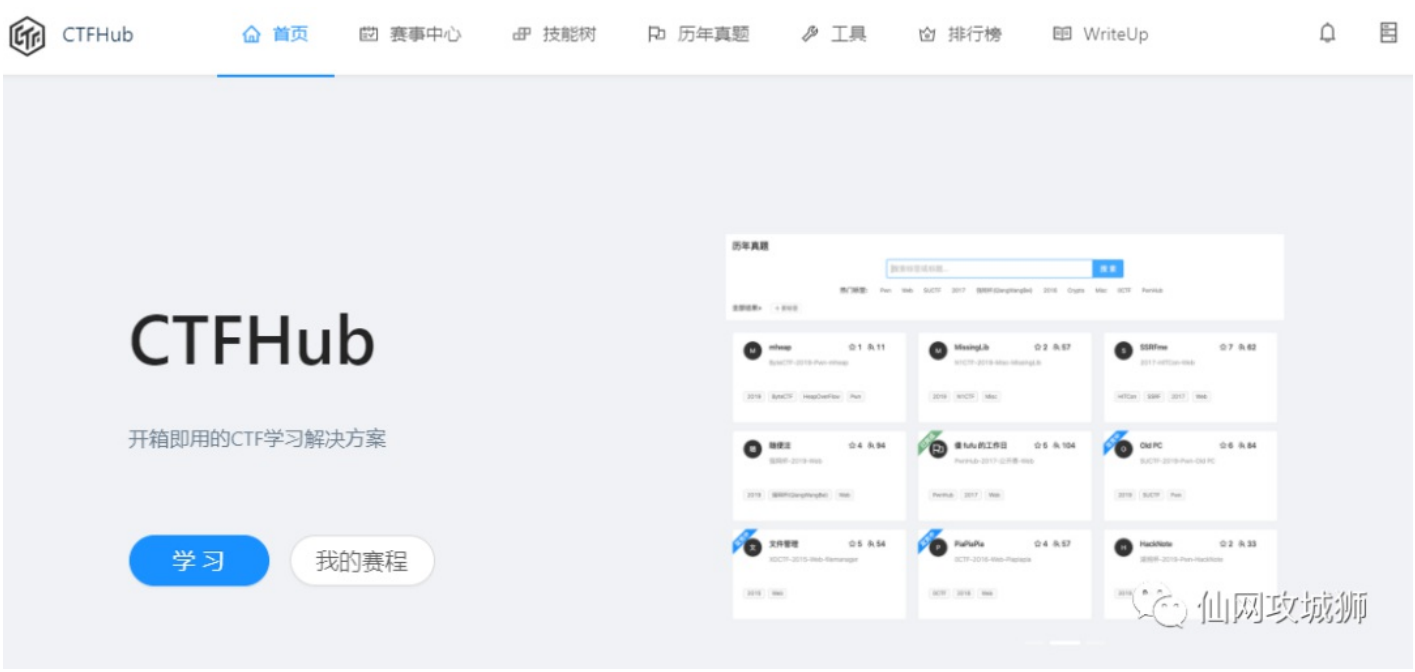
CTFHub 为网络安全工程师提供网络安全攻防技能培训、实战、技能提升等服务。

「赛事中心」提供全网最全最新的 CTF 赛事信息，关注赛事定制自己专属的比赛日历吧。

「技能树」提供清晰的 CTF 学习路线，想要变强就加点，哪里不会点哪里。

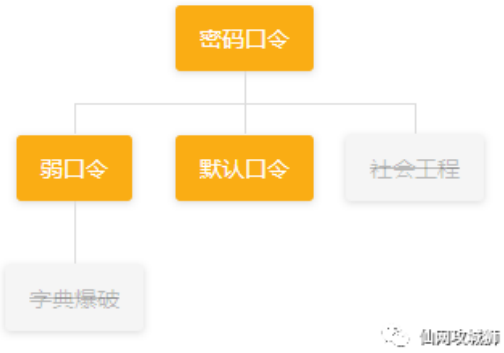
「历年真题」提供无限次赛后复盘，边学边练。

「工具」提供各类常用工具，打仗没有一把趁手的武器怎么行。



实战

下面内容将为大家讲解常见的暴力破解密码的各种姿势，用CTFHub中的靶机进行演示。



一、弱口令

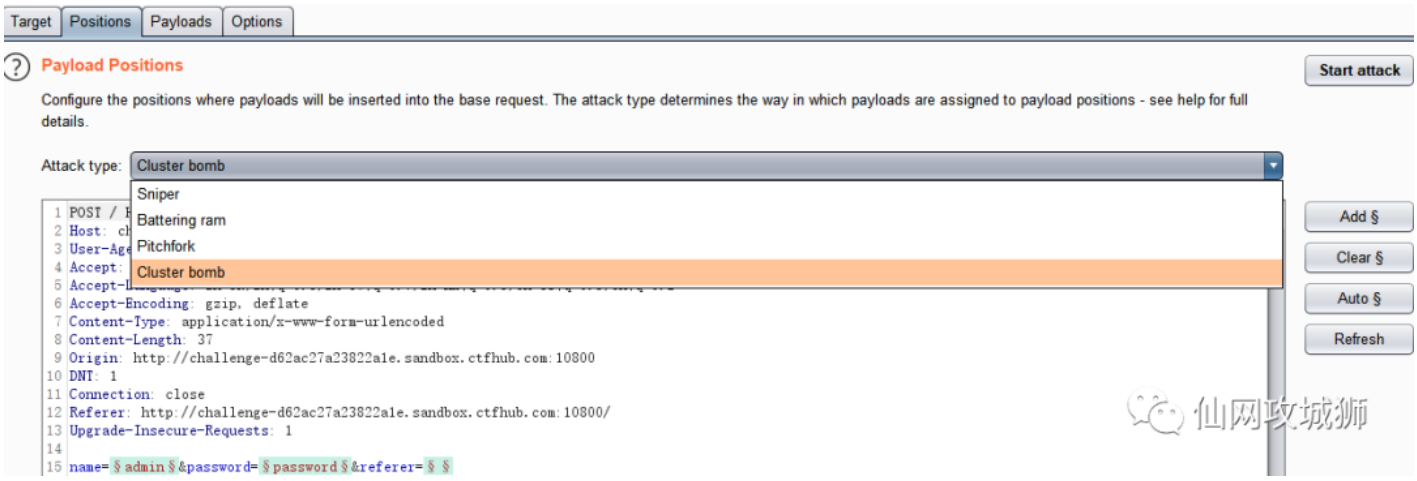
弱口令(weak password) 没有严格和准确的定义，通常认为容易被别人（他们有可能对你很了解）猜测到或被破解工具破解的口令均为弱口令。弱口令指的是仅包含简单数字和字母的口令，例如“123”、“abc”等，因为这样的口令很容易被别人破解，从而使用户的计算机面临风险，因此不推荐大家使用。

1.点击弱口令题目开始解题。

2.打开后是这样的

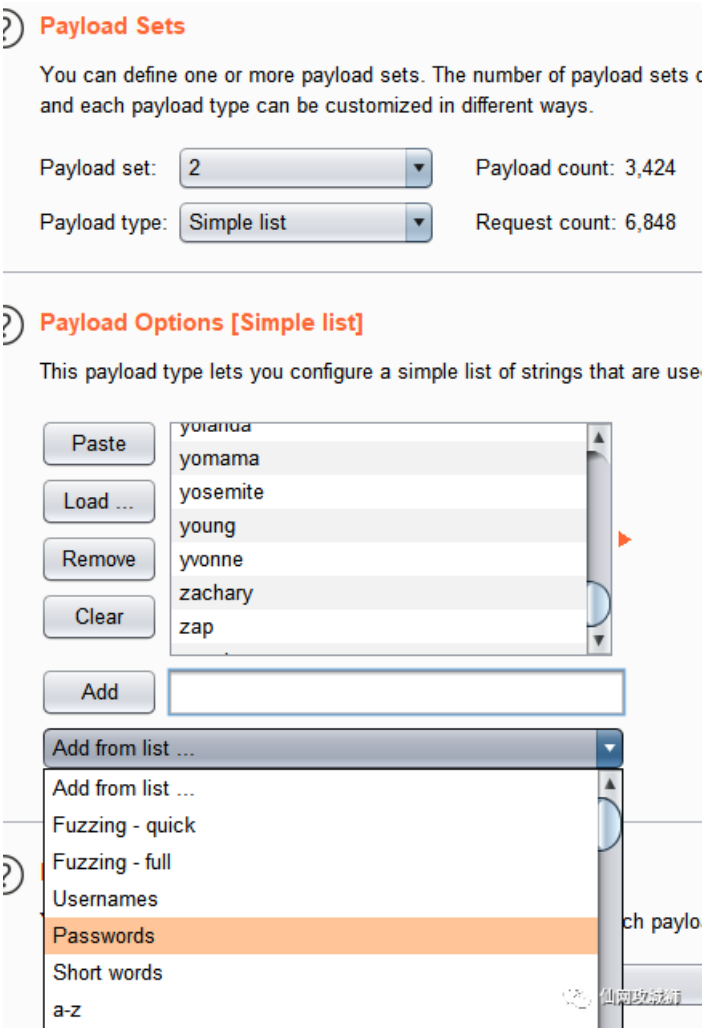
3.查看一下页面源码看看有没有什么提示，然后手动尝试一波，用户名user、admin，密码1234、abcd、abc123、admin、password等看看，提示用户密码错误，这里就有点方了还以为直接手动敲敲就过了呢。

4.用burpsutie中的暴力破解模块跑一波，这里使用Cluster bomb来进行，该模式可以进行交叉遍历来爆破。

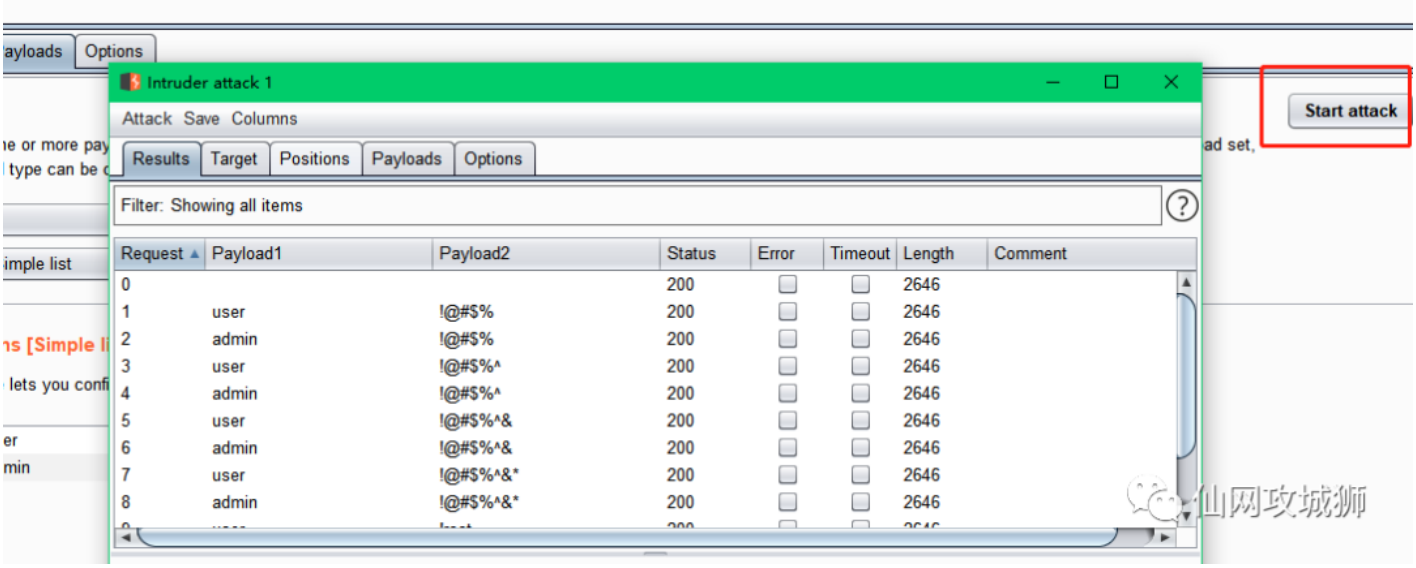


5.添加用户和密码字典。

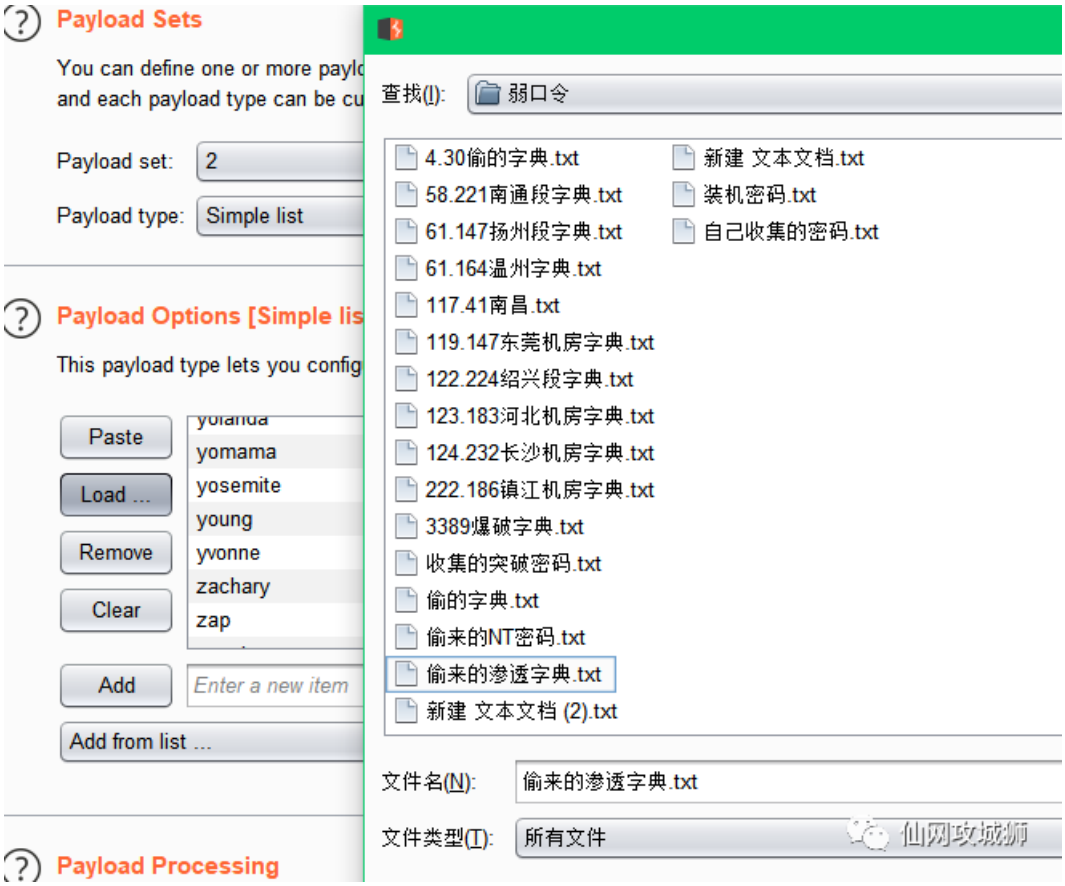
下面是密码



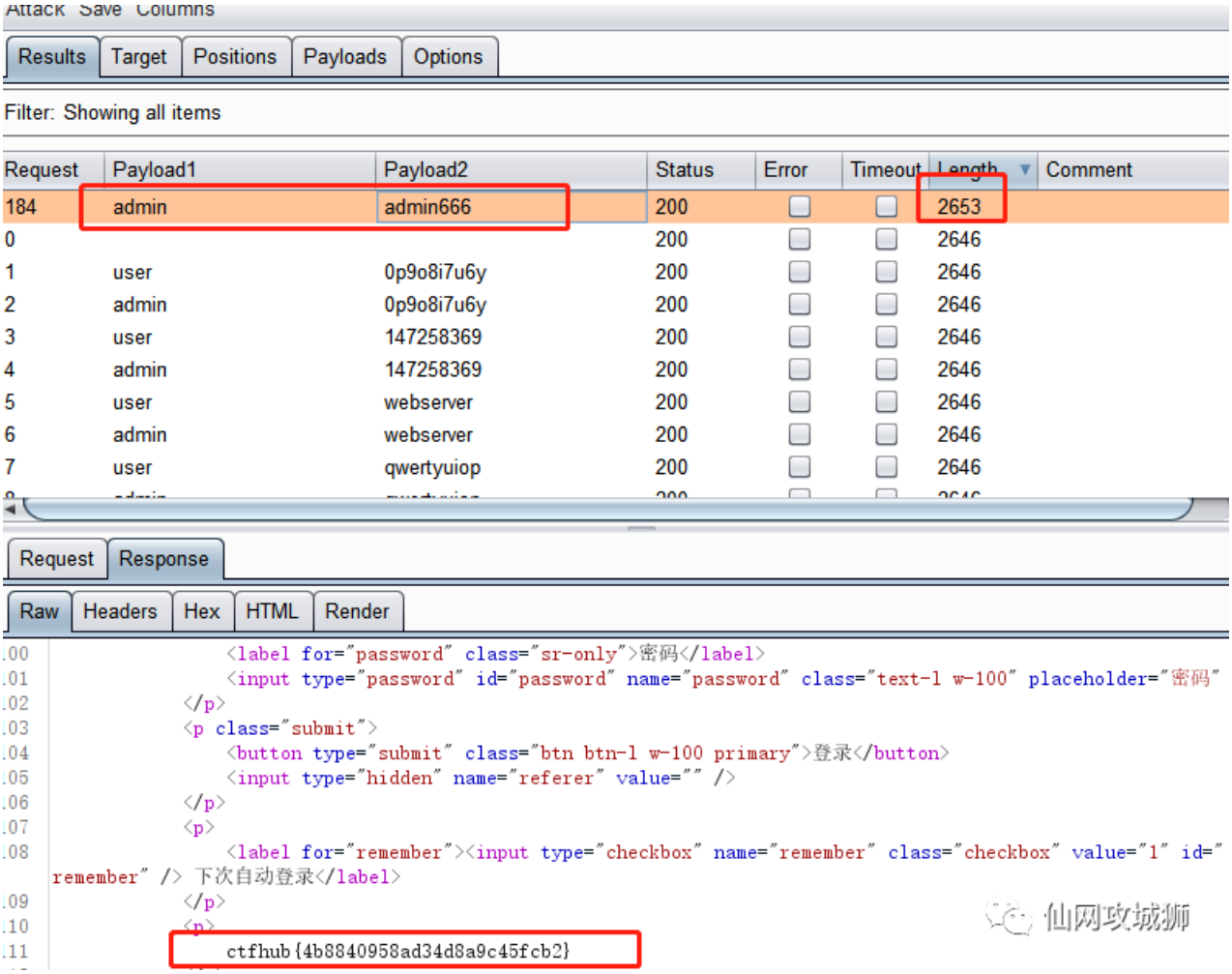
6.开跑，出人意料TM居然没有跑成功，说好的弱口令呢喂。只能拿出我珍藏的字典了



7.导入珍藏的字典。



8.跑了半个小时WC，没辙暴力破解就是费时间，终于跑出来了admin、admin666。



二、默认口令

1.点击默认口令题目开始解题。

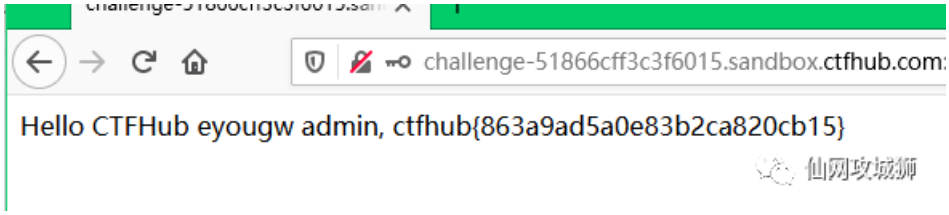
2.点击进入发现是一个eyou的服务器。

3.在网上寻找eyou的默认口令，网上操作手册中的默认口令不行，默认口令查询网站也查不到，有点方。

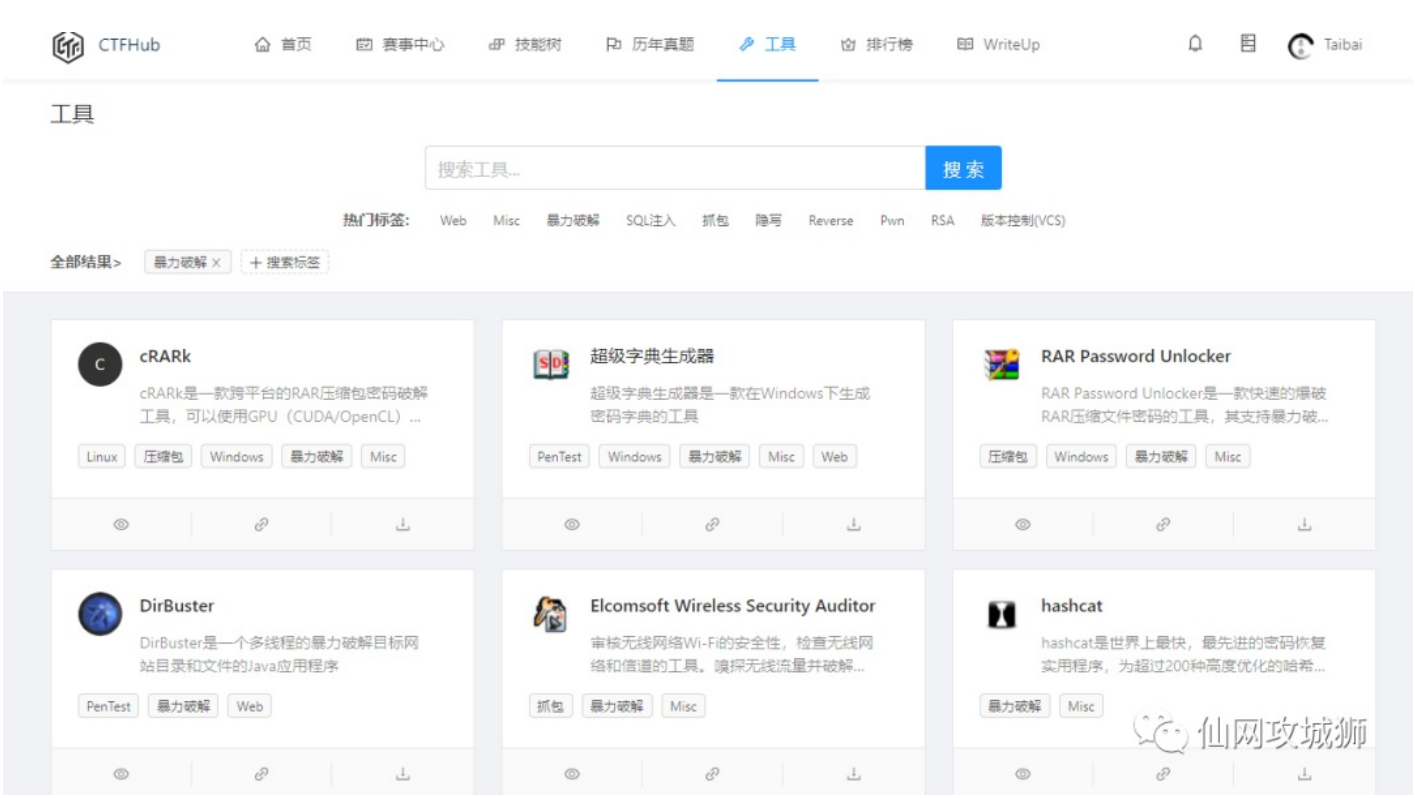
4.经过多次尝试终于找到了，admin@(eyou)

亿邮邮件网关	eyouuser	eyou_admin
	eyougw	admin@(eyou)
	admin	+-ccccc
	admin	cyouadmin

5.复制提交



在CTFHub里面有很多好用的暴力破解的工具



往期内容

CTFHub信息泄露WriteUP

ATT&CK实战-红队评估之二

网站被挂马？？文件上传漏洞上传木马后门

更多资讯长按二维码 关注我们

觉得不错点个“赞”呗