

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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/tangshuangsss/article/details/117458496>

版权



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

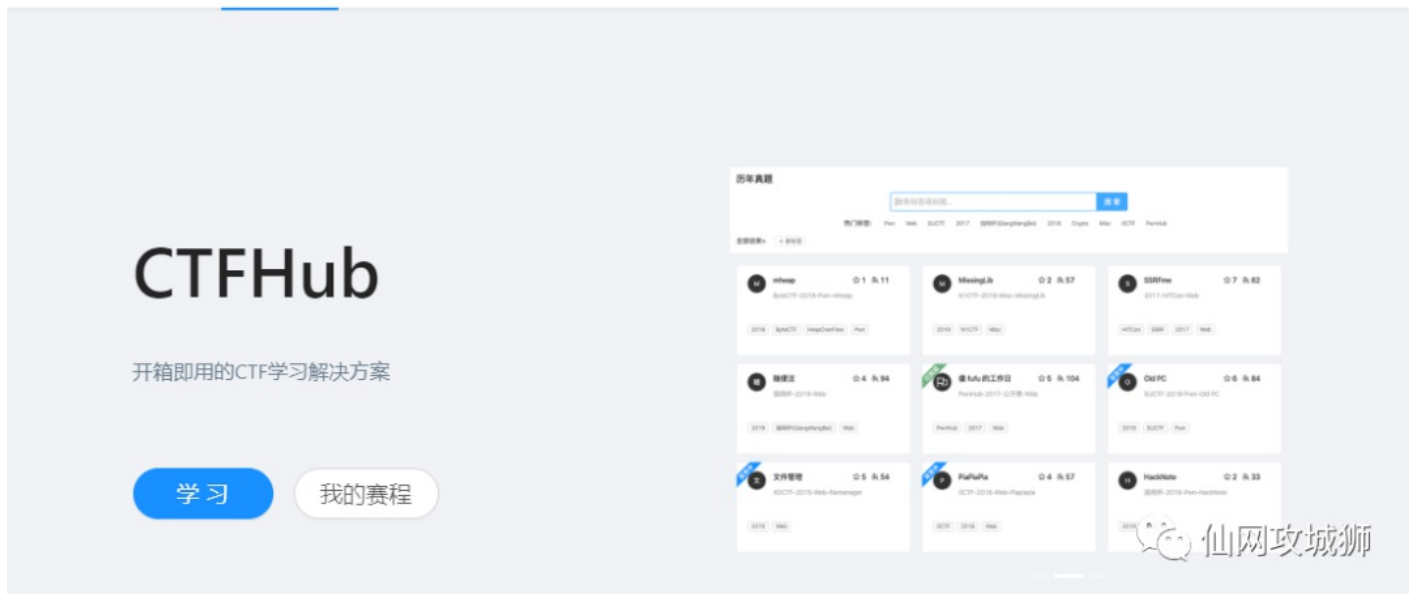
CTFHub 为网络安全工程师提供网络安全攻防技能培训、实战、技能提升等服务。

「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。

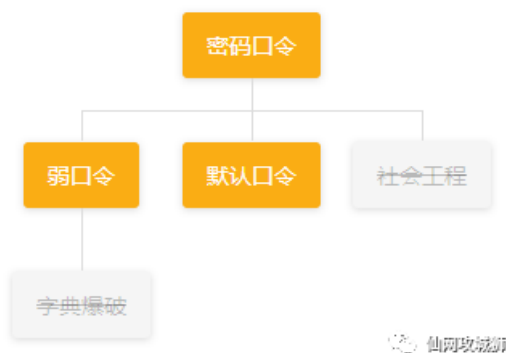
「历年真题」提供无限次赛后复盘, 边学边练。

「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

CTFHub WriteUp 管理后台

下次自动登录



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。

CTFHub WriteUp 管理后台

下次自动登录

user or password is wrong

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。

Target Positions Payloads Options

Start attack

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Cluster bomb

- Sniper
- Battering ram
- Pitchfork
- Cluster bomb

1 POST / B
2 Host: cl
3 User-Age
4 Accept:
5 Accept-
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 37
9 Origin: http://challenge-d62ac27a23822a1e.sandbox.ctfhub.com:10800
10 DNT: 1
11 Connection: close
12 Referer: http://challenge-d62ac27a23822a1e.sandbox.ctfhub.com:10800/
13 Upgrade-Insecure-Requests: 1
14
15 name= \$ admin \$ &password= \$ password \$ &referer= \$ \$

Add \$
Clear \$
Auto \$
Refresh

仙网攻城狮

5.添加用户和密码字典。

?) Payload Sets

You can define one or more payload sets. The number of payload sets and each payload type can be customized in different ways.

Payload set: 1 Payload count: 2
Payload type: Simple list Request count: 6,848

?) Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used in the request.

Paste user
Load ... admin
Remove

下面是密码

?) Payload Sets

You can define one or more payload sets. The number of payload sets and each payload type can be customized in different ways.

Payload set: 2 Payload count: 3,424
Payload type: Simple list Request count: 6,848

?) Payload Options [Simple list]

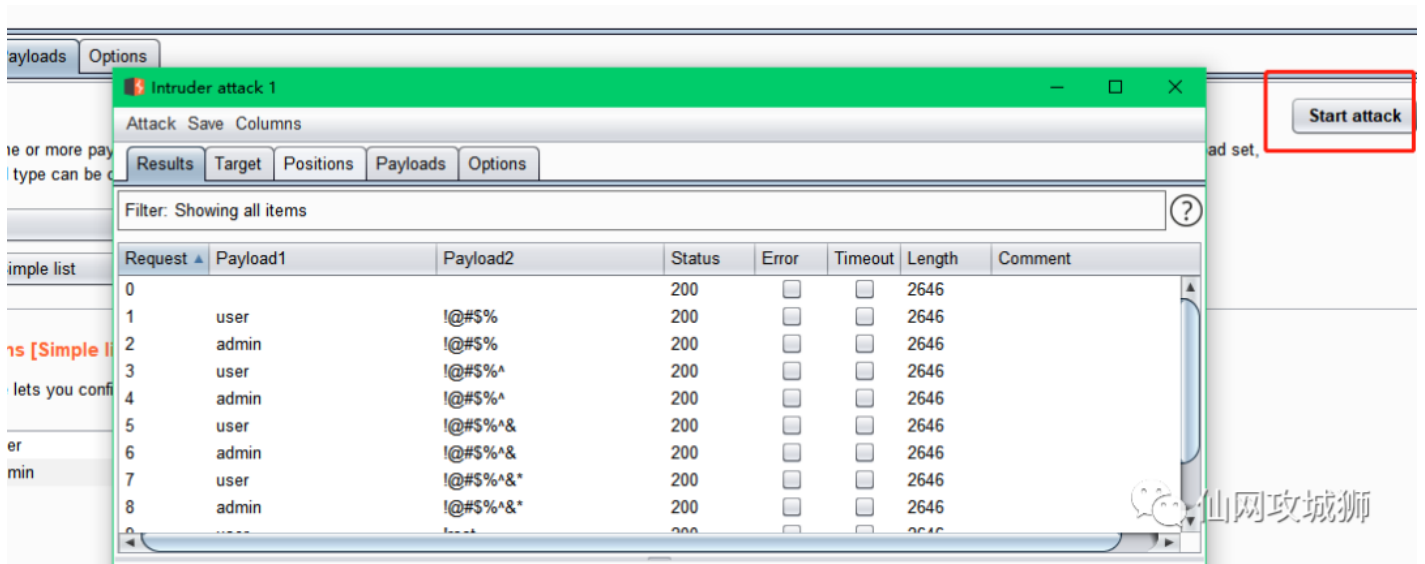
This payload type lets you configure a simple list of strings that are used in the request.

Paste yoranda
Load ... yomama
Remove yosemite
Clear young
yonne
zachary
zap

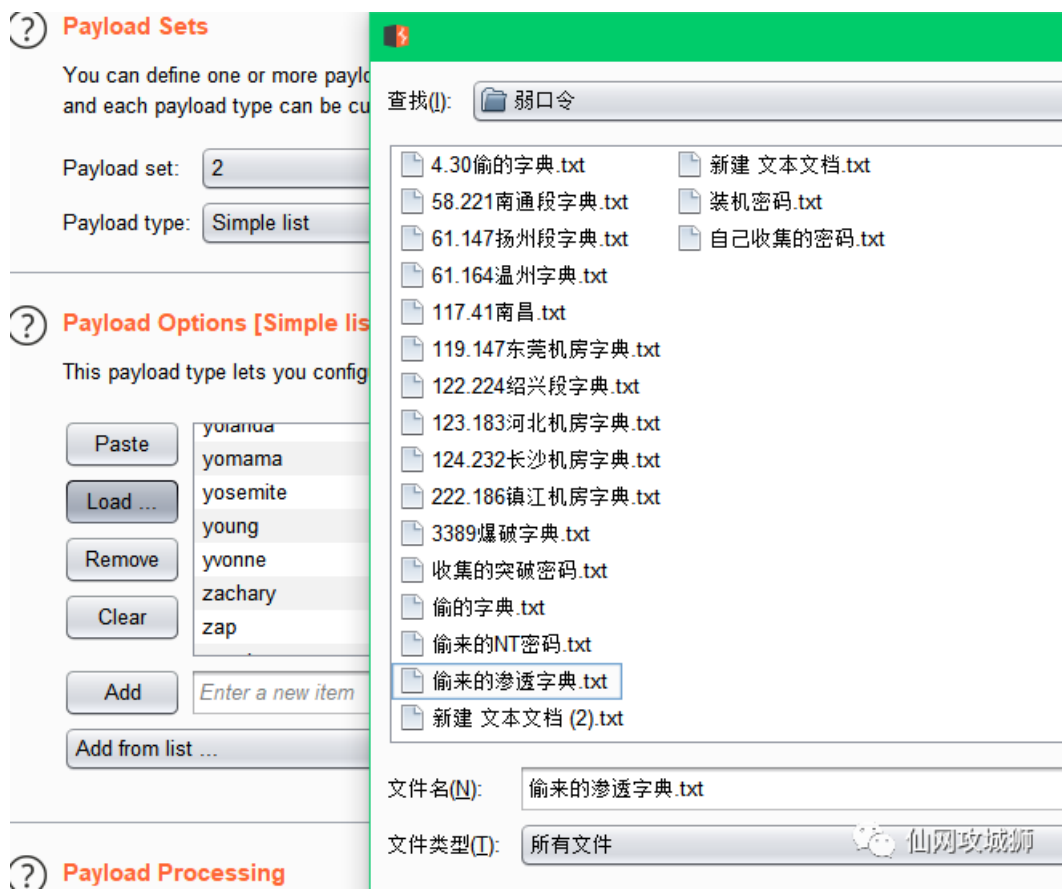
Add

Add from list ...
Add from list ...
Fuzzing - quick
Fuzzing - full
Usernames
Passwords
Short words
a-z

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。

ATTACK Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload1	Payload2	Status	Error	Timeout	Length	Comment
184	admin	admin666	200	<input type="checkbox"/>	<input type="checkbox"/>	2653	
0			200	<input type="checkbox"/>	<input type="checkbox"/>	2646	
1	user	0p9o8i7u6y	200	<input type="checkbox"/>	<input type="checkbox"/>	2646	
2	admin	0p9o8i7u6y	200	<input type="checkbox"/>	<input type="checkbox"/>	2646	
3	user	147258369	200	<input type="checkbox"/>	<input type="checkbox"/>	2646	
4	admin	147258369	200	<input type="checkbox"/>	<input type="checkbox"/>	2646	
5	user	webserver	200	<input type="checkbox"/>	<input type="checkbox"/>	2646	
6	admin	webserver	200	<input type="checkbox"/>	<input type="checkbox"/>	2646	
7	user	qwertyuiop	200	<input type="checkbox"/>	<input type="checkbox"/>	2646	
8	admin	qwertyuiop	200	<input type="checkbox"/>	<input type="checkbox"/>	2646	

Request Response

Raw Headers Hex HTML Render

```

.00 <label for="password" class="sr-only">密码</label>
.01 <input type="password" id="password" name="password" class="text-l w-100" placeholder="密码"
.02 </p>
.03 <p class="submit">
.04 <button type="submit" class="btn btn-l w-100 primary">登录</button>
.05 <input type="hidden" name="referer" value="" />
.06 </p>
.07 <p>
.08 <label for="remember"><input type="checkbox" name="remember" class="checkbox" value="1" id="
remember" /> 下次自动登录</label>
.09 </p>
.10 <p>
.11 ctfhub {4b8840958ad34d8a9c45fcb2}

```

仙网攻城狮

二、默认口令

1. 点击默认口令题目开始解题。

默认口令 X

所需金币: 30 题目状态: **未解出** 解题奖励: 金币:100 经验:5

<http://challenge-51866cf3c3f6015.sandbox.ctfhub.com:10800>

00:28:54

仙网攻城狮

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。



默认密码在线查询网站

CIRT.net

<https://cirt.net/passwords>

默认密码列表

<https://datarecovery.com/rd/default-passwords/>

工具猫路由器默认密码查询

<https://toolmao.com/baiduapp/routerpwd/>

路由器默认密码查询

<https://www.cleancss.com/router-default/>

Internet上最全面的默认路由器密码列表

<https://portforward.com/router-passwords/>

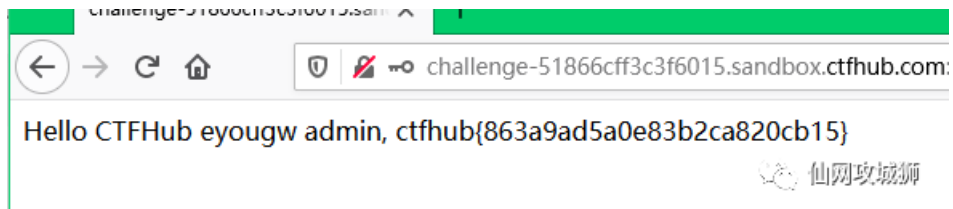
仙网攻城狮

4. 经过多次尝试终于找到了，admin@(eyou)

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

仙网攻城狮

5. 复制提交








在CTFHub里面有很多好用的暴力破解的工具

工具

搜索工具...

搜索

热门标签: [Web](#) [Misc](#) [暴力破解](#) [SQL注入](#) [抓包](#) [隐写](#) [Reverse](#) [Pwn](#) [RSA](#) [版本控制\(VCS\)](#)全部结果> [暴力破解 X](#) [+ 搜索标签](#)

 cRARK cRARK是一款跨平台的RAR压缩包密码破解工具,可以使用GPU (CUDA/OpenCL) ... Linux 压缩包 Windows 暴力破解 Misc	 超级字典生成器 超级字典生成器是一款在Windows下生成密码字典的工具 PenTest Windows 暴力破解 Misc Web	 RAR Password Unlocker RAR Password Unlocker是一款快速的爆破RAR压缩文件密码的工具,其支持暴力破... 压缩包 Windows 暴力破解 Misc
 DirBuster DirBuster是一个多线程的暴力破解目标网站目录和文件的Java应用程序 PenTest 暴力破解 Web	 Elcomsoft Wireless Security Auditor 审核无线网络Wi-Fi的安全性,检查无线网络和信道的工具。嗅探无线流量并破解... 抓包 暴力破解 Misc	 hashcat hashcat是世界上最快,最先进的密码恢复实用程序,为超过200种高度优化的哈希... 暴力破解 Misc

仙网攻城狮

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](#)

糟糕，~~~
是心动的感觉!!!



长按关注



更多资讯长按二维码 关注我们

觉得不错点个“赞”呗 🍷