

CTFHUB刷题 密码口令/弱口令

原创

nuli1024 于 2021-09-05 14:59:12 发布 398 收藏 2

分类专栏: [CTFHub](#) 文章标签: [web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/m0_50829573/article/details/120114887

版权



[CTFHub 专栏收录该内容](#)

10 篇文章 1 订阅

订阅专栏

一、题目描述与分析

弱口令

X

所需金币: 30

题目状态: **未解出**

解题奖励: 金币:100 经验:5

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。

<http://challenge-3985702c7bdcac1c.sandbox.ctfhub.com:10800>

00:11:53

环境续期 v

停止并销毁环境

每分钟需要1个金币,请根据个人需求

Flag{.....}

提交Flag

WriteUp

觉得这个WP写的不好有更好的想法? [点我提交](#)

CSDN @nuli1024ws

由题意, 何为弱口令, 指的是通常认为容易被别人 (他们有可能对你很了解) 猜测到或破解工具的口令均为弱口令。这里我们可以尝试暴力破解

二、解题过程

1. 登入题目页面, 如图

CTFHub WriteUp 管理后台

 下次自动登录

CSDN @null1024ws

猜测需要提供2.用户名和密码，才能拿到flag,猜测用户名为admin

2.利用Burpsuite抓包

Request

Raw Params Headers Hex

```
POST / HTTP/1.1
Host: challenge-3985702c7bdcac1c.sandbox.ctfhub.com:10800
Content-Length: 35
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://challenge-3985702c7bdcac1c.sandbox.ctfhub.com:10800
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.63 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://challenge-3985702c7bdcac1c.sandbox.ctfhub.com:10800/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en-GB;q=0.8,en-US;q=0.7,en;q=0.6
Connection: close

name=admin&password=123456&referer=
```

CSDN @null1024ws

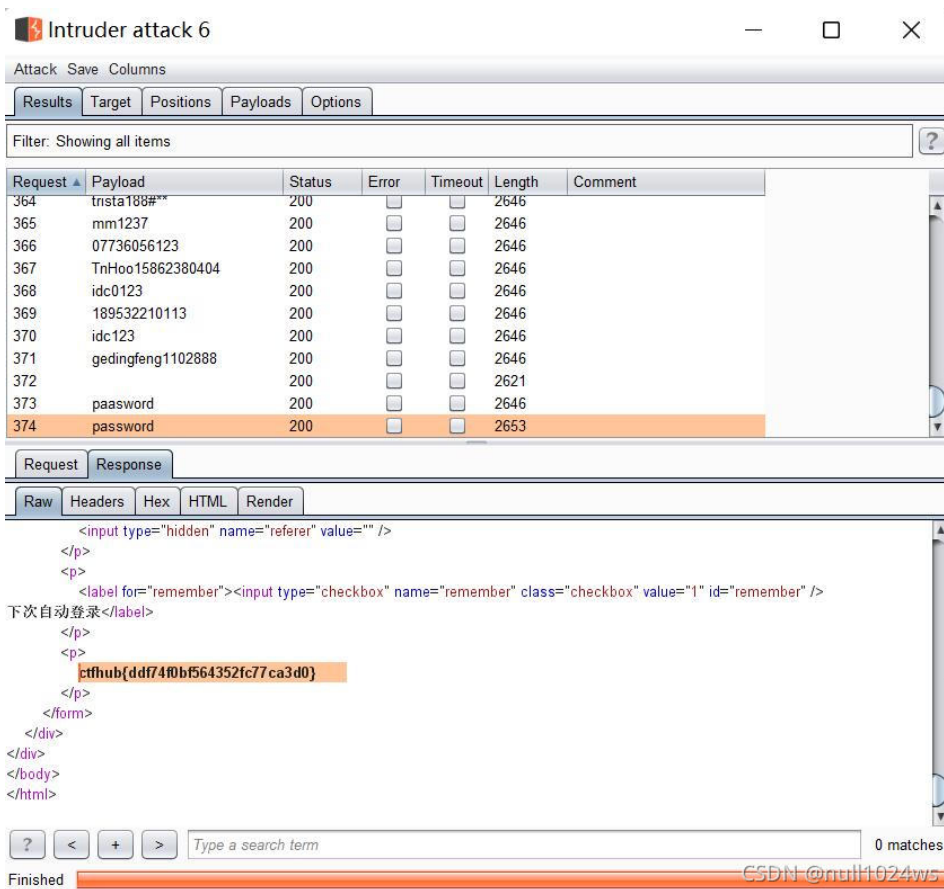
注意到

```
name=admin&password=123456&referer=
```

下面进行暴力破解

三.暴力破解

右键-->Send to intruder-->Intruder模块-->Positions选中爆破区域-->Payloads设置密码字典（这里选择常见的弱口令密码即可）-->start attack-->找到Length不一样的-->查看Response



Intruder attack 6

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

| Request | Payload | Status | Error | Timeout | Length | Comment |
|---------|-------------------|--------|--------------------------|--------------------------|--------|---------|
| 364 | tnsta188#** | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 2646 | |
| 365 | mm1237 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 2646 | |
| 366 | 07736056123 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 2646 | |
| 367 | TnHoo15862380404 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 2646 | |
| 368 | idc0123 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 2646 | |
| 369 | 189532210113 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 2646 | |
| 370 | idc123 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 2646 | |
| 371 | gedingfeng1102888 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 2646 | |
| 372 | | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 2621 | |
| 373 | paasword | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 2646 | |
| 374 | password | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 2653 | |

Request Response

Raw Headers Hex HTML Render

```
<input type="hidden" name="referer" value="" />
</p>
<p>
<label for="remember"><input type="checkbox" name="remember" class="checkbox" value="1" id="remember" />
下次自动登录</label>
</p>
<p>
ctfhub{ddf74f0bf564352fc77ca3d0}
</p>
</form>
</div>
</body>
</html>
```

0 matches

Finished CSDN @null1024ws

成功拿到flag√

三、题后反思

- 1.这题很简单，知道怎么使用Burpsuite暴力破解模块即可。
- 2.暴力破解密码时默认了用户名为admin,其实这不太严谨，纯属自己猜测。这里就涉及到Burpsuite暴力破解的四种模式了，具体学习链接[点击这里](#),查看writeup.



[创作打卡挑战赛](#)
赢取流量/现金/CSDN周边激励大奖