基础认证

发表于 2021-01-04 分类于 Skill， Web， Web前置技能， HTTP协议
Skill | Web | Web前置技能 | HTTP协议 | 基础认证

点击此处获得更好的阅读体验

题目考点

- *HTTP 基础认证*
- *脚本编写*
- *爆破*

解题思路

题目分析

本题考察了在HTTP中对于基础认证的一些知识，要求使用爆破的方法来获得基础认证的账号密码，之后登陆获得flag

解题过程

方法一

来自CTFHub官方

访问 /flag 发现需要登录

挂上 BurpSuite 的代理，随便输个账号密码（比如: 账号aaa 密码 bbb）访问，查看 HTTP 响应报文：

得到提示 `do u konw admin ?`，于是猜测账号是 `admin`，那么接下来就只需要爆破密码了

注意看到 HTTP 请求头部的 Authorization 字段:

```
1 Authorization: Basic YWFhOmJiYg==
```

Basic 表示是「基础认证」，后面的 `YWFhOmJiYg==` 用 `base64` 解码后是 `aaa:bbb`，也就是我们之前输入的 `账号:密码`

使用 BurpSuite 进行基础认证爆破

1. *将报文发送到 `Intruder`，将 `Basic` 后面 `base64` 部分添加为 `payload position`*

1. *在 `Payloads` 选项卡下，选择 `Payload Type` 为 `SimpleList`，然后在 `Payload Options` 中点击 `load` 加载密码字典*

1. *`Payload Processing` -> `Add` -> `Add Prefix`（添加前缀）-> 输入 `admin:`*

1. *`Payload Processing` -> `Add` -> `Encode`（添加一个编码方式）-> 选择 Base64 Encode*

1. *`Payload Encode` 取消勾选的 `URL-encode`，不然你会看到 base64 之后的 = 会被转成 `%3d`，你就算爆破到天荒地老也不会出来*

1. `Start Attack`，然后按 `Status` 排序，看到状态码出现 200 的，即爆破成功

查看 `Response` 得到flag

方法二

来自[wuj1n9](#)原创投稿

1. 打开题目链接，发现需要输入用户名和密码才能访问

1. 题目提供了常用密码top100，应该是爆破，~~因为范围很小，所以我们一个个试就好了，~~所以我们可以编写简单脚本
2. 写脚本前先了解一下基本认证是什么，照搬题目描述：

   在HTTP中，基本认证（英语：Basic access authentication）是允许http用户代理（如：网页浏览器）在请求时，提供 用户名 和 密码 的一种方式。详情请查看 [HTTP基本认证](#)关键的地方如下：

1. 使用 Burp 抓包，添加 `Authorization` 头字段，使用爆破模块

其中，payload 部分可以编写脚本生成

1. 根据提示，容易猜测用户名为 `admin`，那么 Authorization 头字段的格式就应该为

```
Authorization: Basic [base64(admin:密码)]
```


通过以下脚本将提供的密码列表按格式生成好

```
#!/usr/bin/env python3
import base64
# 字典文件路径
dic_file_path = '/Users/wujing/Downloads/10_million_password_list_top_100.txt'
with open(dic_file_path, 'r') as f:
    password_dic = f.readlines()
username = "admin" # 用户名
for password in password_dic:
    auth = str(username + ":" + password).encode("utf-8")
    encodestr = base64.b64encode(auth).decode()
    print(encodestr)
```

将结果放进爆破模块的 payload 中，进行爆破，解码得到密码

需要注意Burp会默认勾选payload进行URL编码，需要取消该选项

之后使用爆破出的密码登陆即可获得flag

#Skill #Web #Web前置技能 #HTTP协议
302跳转
响应包源代码