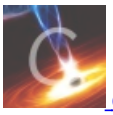
XCTF攻防世界web新手练习_ 7_weak_auth

原创

Dar1in9 于 2019-04-28 23:15:54 发布 12369 收藏 21

分类专栏： ctf_web

本文链接：https://blog.csdn.net/silence1_/article/details/89648135



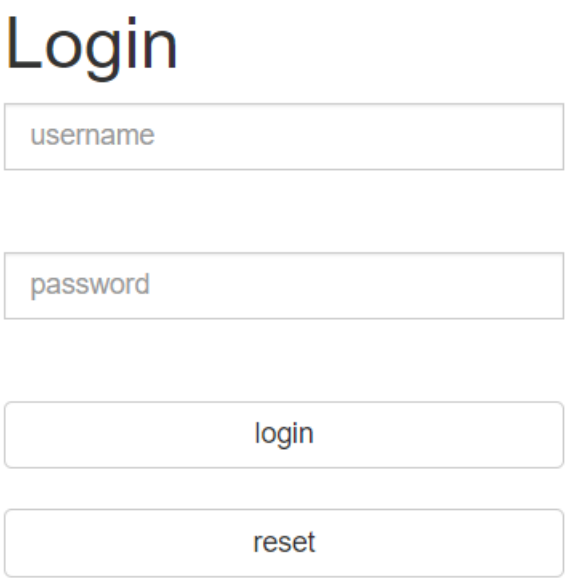
XCTF攻防世界web新手练习—weak_auth

题目

题目为weak_auth，描述信息，重点：随手就设了一个密码

小宁写了一个登陆验证页面，随手就设了一个密码。

进入题目，看到需要登录，随便输入一个用户名和密码试试



弹出弹窗提示用admin账户登录

于是用确定用户名为admin
F12看看源码，提示需要一个字典，意思是要进行爆破

```
  <script>alert('please login as admin');</script>
  <!--maybe you need a dictionary-->
</body>
```

于是用burp进行爆破，当密码为123456时返回长度不同

Request	Payload	Status	Error	Timeout	Length	Comment
3	123456	200	☐	☐	437	
25	123456.	200	☐	☐	437	
0		200	☐	☐	434	baseline request
1	123456789	200	☐	☐	434	

查看此时返回响应得到flag！

```
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>weak auth</title>
</head>
<body>
```

cyberpeace{32ccebc9e3346cbb90ac65986550e7e4} *<!--maybe you need a dictionary-->*

关于弱密码的爆破

弱密码

弱密码是易于猜测的密码，主要有以下几种：

- 1. 顺序或重复的字相邻字母：“111111”、“abcdefg”、“asdf”、“qwer”键盘上的
- 2. 使用数字或符号的仅外观类似替换，例如使用数字“1”、“0”替换英文字母“i”、“O”，字符“@”替换字母“a”等；
- 3. 登录名的一部分：密码为登录名的一部分或完全和登录名相同；
- 4. 常用的单词：如自己和熟人的名字及其缩写，常用的单词及其缩写，宠物的名字等；
- 5. 常用数字：比如自己或熟人的生日、证件编号等，以及这些数字与名字、称号等字母的简单组合。

下面是一些常见的弱密码：

```
admin ——太容易猜出
123 ——同上
abcde ——同上
abc123 ——同上
123456 ——由于文化因素极其常用
1234 ——同上
888888 ——同上
1234567890 ——同上
susan ——常见人名
BarackObama ——高知名度人物
monkey ——常见动物名且正好六位
password ——经常被使用，极易猜出
p@$$\/\/0rd ——简单的字母替换，易被黑客软件破译
rover ——宠物的常用名称，也是一个单词
12/3/75 ——日期
nbusr123 ——可能是用户名，如果是这样的话很容易被猜出
asdf ——常用键盘的键排列
qwerty ——常用键盘的键排列
aaaaa ——重复的字母，极易被破解
Taiwan ——地名
administrator——太容易猜出
```

用burpsuite进行暴力破解密码

参考 https://blog.csdn.net/u011781521/article/details/54772795

附上一个字典 https://github.com/rootphantomer/Blasting_dictionary