

0x01 背景

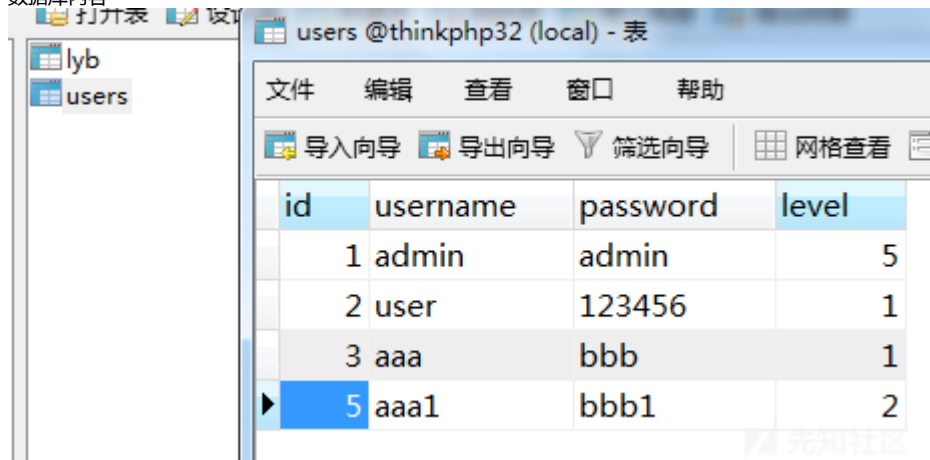
最近研究Laravel框架的代码审计,因为3月份爆出过一个ignore函数的一个漏洞,网上找了些文章,看了下,自己搭建环境测试,一直没有成功,自己就详细的审计了一遍

0x02 laravel介绍

Laravel 在全球范围内有着众多用户。该框架在国外很受欢迎,国外用户量远大于国内。当然,国内也有大型企业使用该框架。此次曝出的 SQL 注入漏洞,并不是太通用,需要一定的条件。[直接复制粘贴]

0x03 漏洞测试环境搭建

数据库内容



| id | username | password | level |
|----|----------|----------|-------|
| 1 | admin | admin | 5 |
| 2 | user | 123456 | 1 |
| 3 | aaa | bbb | 1 |
| 5 | aaa1 | bbb1 | 2 |

代码测试:

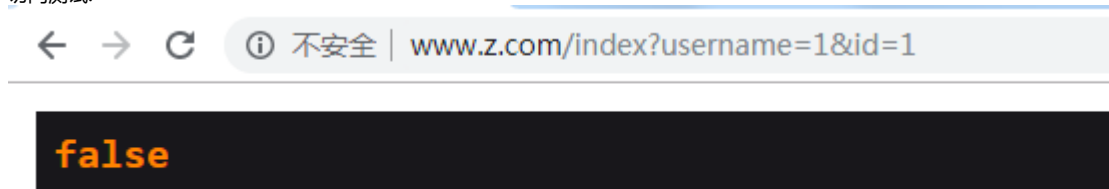
```
$validator = Validator::make($request->input(), [
    'username' => [
        'required',
        Rule::unique("users")->ignore($request->input("id"),$request->input("column"))
    ],
]);

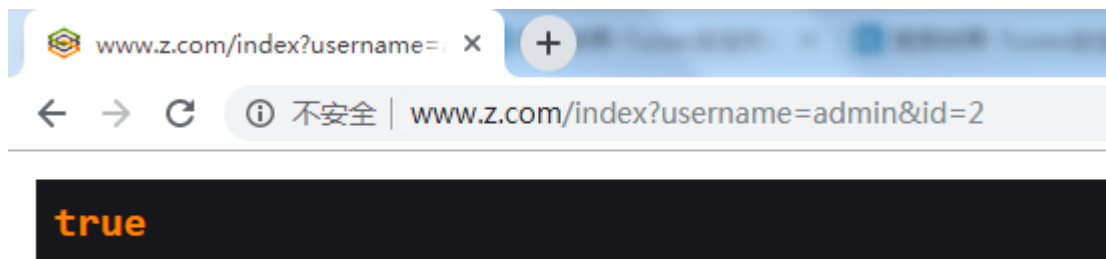
dump($validator->fails());
```

路由定义:

```
Route::any("index", "UserController@index");
```

访问测试:





先知社区

理解这个漏洞之前,需要了解laravel的自动验证机制

Rule::unique("users")->ignore(\$request->input("id"),\$request->input("column")) 这种写法不常见,常见的是

Rule::unique("users")->ignore(\$request->input("id")) 这种写法,后面的变量如果不写,默认是id,写上去代表自定义查询字段。

我们可以把测试环境更改为 Rule::unique("users")->ignore(\$request->input("id")) 然后进行代码跟踪调试

0x04 代码跟踪调试

参数提交内容

?username=admin&id=2

直接下断点

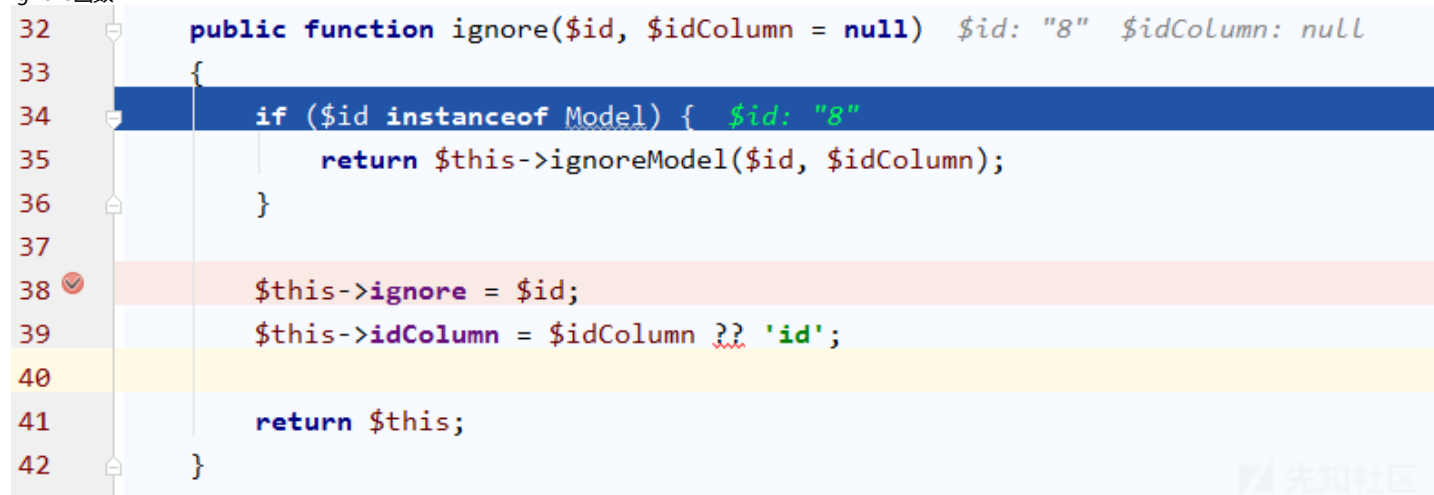


先知社区

跟踪进入,注意几个关键点函数即可

关键点1:

ignore函数



先知社区

直接对ignore 和 idColumn进行赋值 如果idColumn没有传入,默认为id ,然后进入另一个 toString方法

```
64 public function __toString()
65 {
66     return rtrim(sprintf('unique:%s,%s,%s,%s,%s',
67         $this->table,
68         $this->column,
69         $this->ignore ? "'".$this->ignore."' : 'NULL',
70         $this->idColumn,
71         $this->formatWheres()
72     ), ',');
73 }
74 }
```

漏洞也是主要对这里进行修复

修复后的代码

```
64 public function __toString()
65 {
66     return rtrim(sprintf('unique:%s,%s,%s,%s,%s',
67         $this->table,
68         $this->column,
69         $this->ignore ? "'".addslashes($this->ignore)."' : 'NULL',
70         $this->idColumn,
71         $this->formatWheres()
72     ), ',');
73 }
74 }
```

laravel社区对这种修复,讨论很多,认为addslashes 无法根本防止注入, 因为ignore的有些写法还是会引起问题.

后面继续跟踪调试, 就会进入 laravel的PDO操作处理

跟踪的出来的sql语句为:

```
66
67     return $sql;
68 }
69
70 /**
71  * Compile the components necessary for a select clause.
```

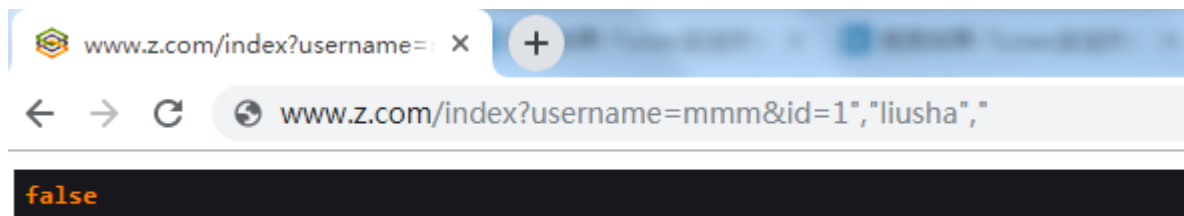
后续就是进行 PDO查询操作, 因为没有带入exp,所以会正常执行

0x05 注入演示

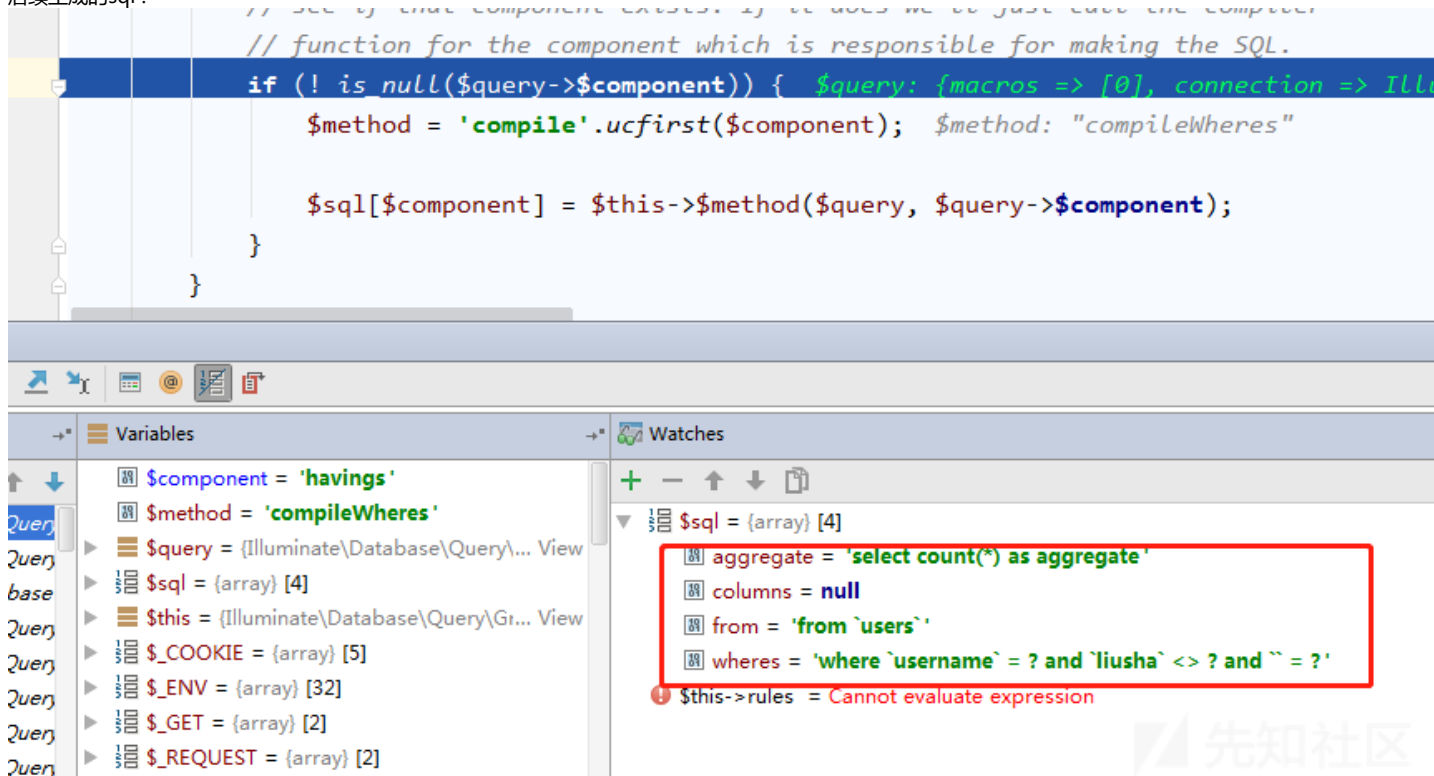
因为如果是pdo操作, 注入通常是对键名 进行带入, 如果带入进键值的话, 没有任何效果, 这里关键的突破点就是 ignore函数中的 idColumn 变量, 以及 toString() 在处理 ignore中的处理方式

讲传入的id参数修改为: 1,"liusha",

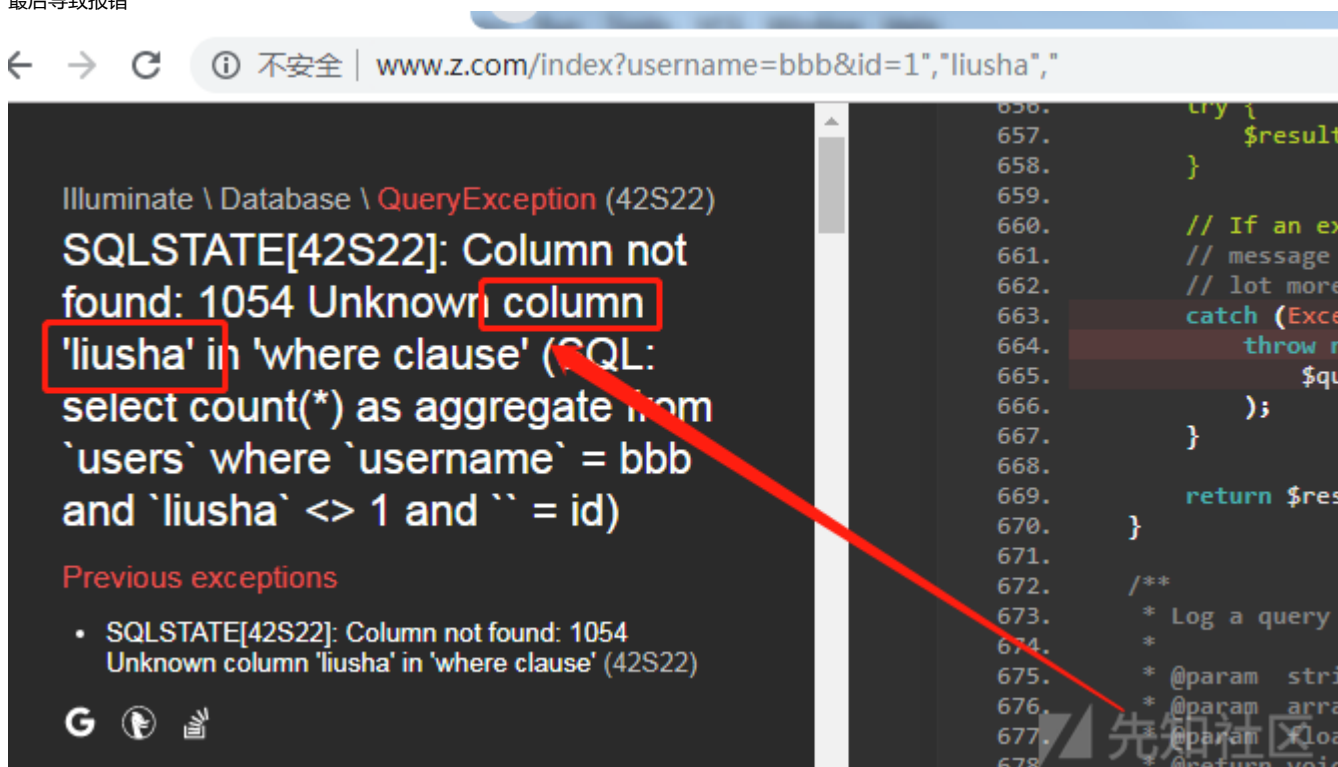
url为:



这样传入id,就会对 idColumn 进行覆盖, 默认是id, 现在column 就变为 liusha, 如果这个字段不存在表中, 这个键名 就会对带入PDO查询操作中,导致报错. 后续生成的sql:



sql的键值带入了我们出入的 liusha 非法字段 最后导致报错



提示不存在 liusha这个column.

ok,演示完成.

0x06 总结

这个漏洞是今年3月份爆出来的, 实际开发中, ignore函数用的比较少, laravel的代码审计 , 大部分还是审计一些开发作者在开发中的一些不规范写法导致的漏洞.

点击收藏 | 0 关注 | 1

[上一篇 : android so加固之sect...](#) [下一篇 : 【第二弹】使用2FA保护你的Win...](#)

1. 0 条回复
- 动动手指，沙发就是你的了！

[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](#)