ezlight

发表于 2021-05-25 更新于 2021-05-26 分类于 Challenge， 2021， 第四届红帽杯网络安全大赛， Web
Challenge | 2021 | 第四届红帽杯网络安全大赛 | Web | ezlight

点击此处获得更好的阅读体验

WriteUp来源

来自颖奇L'Amore的博客

题目描述

> *easy cms for you.*

题目考点

- *LightCMS RCE*

解题思路

0x00 前言

LightCMS 是一款基于 Laravel 框架的 CMS，但前台没什么东西，主要作为一个后台管理系统。这个 CMS 我在春节期间就挖过了，但是因为全部都是一些数据库操作，最终放弃了。今天在伟大的郭院士的指导下，终于调出了这个郭院士挖到的 0day。

0x01 文件上传

这个 0day 是一个 Phar 反序列化打 Laravel RCE 的洞，因此需要能够将 phar 文件上传，在后台的内容管理中不难发现图像上传位点

查看其 HTML 源代码，js Event 提交图片到一个上传接口

跟进其模板中来看一下 `resources/views/admin/content/add.blade.php`

上传接口是渲染的一个 Laravel 的路由，来看一下这个路由，使用了 `NEditorController` 这个控制器

跟到控制器，`uploadImage` 方法处理图像上传，没啥可以利用的

`app/Http/Controllers/Admin/NEditorControllers.php`

0x02 继续深入

尽管这个上传没找到什么有价值的东西，我们可以在这个控制器下找到另一个比较有趣的方法

`catchImage()` 方法接收 file 参数并传入 `fetchImageFile()`，跟进

在 `fetchImageFile()` 中，它会 curl 访问这个 url 并将读取到的内容传入 `Image::make()` 中

通过 debug 的不断跟进，最终来到了这个 `init()`，然后传入 `decoder->init()`

vendor/intervention/image/src/intervention/Image/AbstractDriver.php

而接下来的这个 `init()` 则是一个 switch case，根据传入内容的类型返回不同的东西

注意我们现在传入 `init()` 中的 `$data` 是提交的一个 url 的 curl 读取结果，而 `case $this->isUrl()` 看上去很有趣，因为 url 的内容似乎还可以是 url。那么不妨我们就直接将 url 的内容设置为一个新的 url 并传入，来看看 `initFormUrl()` 到底做了什么。

这里它继续读取了这个 url 的内容，然后作为 binary 数据处理

然后我们来看看这个 `case` 的判断函数 `isUrl` 做了什么

```
1 public function isUrl()
2 {
3     return (bool) filter_var($this->data, FILTER_VALIDATE_URL);
4 }
```

这个方法只是利用 FILTER VAR 判断是否为 url，这意味着前面的 http 协议可以替换成其他协议，比如 phar 协议。

于是我们将 url 内容改成一个 phar，再次下断点，果然依旧进到了这里并且传给了 `file_get_contents()`

然后就会触发 phar 反序列化了。

0x03 利用

首先去网上找一个现成的 Laravel RCE 的 gadget，生成 phar 文件

然后来到内容管理 - 新增文章内容，上传文件，就会得到一个这样的图片 url：

```
1 http://127.0.0.1:12334/upload/image/202105/cbf1k61csMcM1pAheP34DxrcUIjDS1kF5bPaCYnC.gif
```

然后来到我们自己的 vps，新建一个 txt，内容为：

```
1 phar://./upload/image/202105/cbf1k61csMcM1pAheP34DxrcUIjDS1kF5bPaCYnC.gif
```

然后 POST 提交到这个路由即可触发 phar 反序列化

0x04 后记

这个洞还是比较容易被忽视的，虽然利用起来并不复杂，但是触发思路比较新颖，不容易被发现。只能说郭院士太强了。

Challenge # 2021 # Web # 第四届红帽杯网络安全大赛
PicPic
WebsiteManger