CVE-2020-23520漏洞复现

前言

贴心猫（imcat）是一套基于PHP的开源建站系统。imcat 5.2 存在安全漏洞，该漏洞允许通过图片功能的认证文件上传和远程代码执行。

环境搭建

环境要求

- PHP5.4∽PHP7.4（推荐：PHP5.6∽PHP7.3）
- mysql5.1 +

我们登录Github下载源码：https://github.com/peacexie/imcat/tree/v5.2

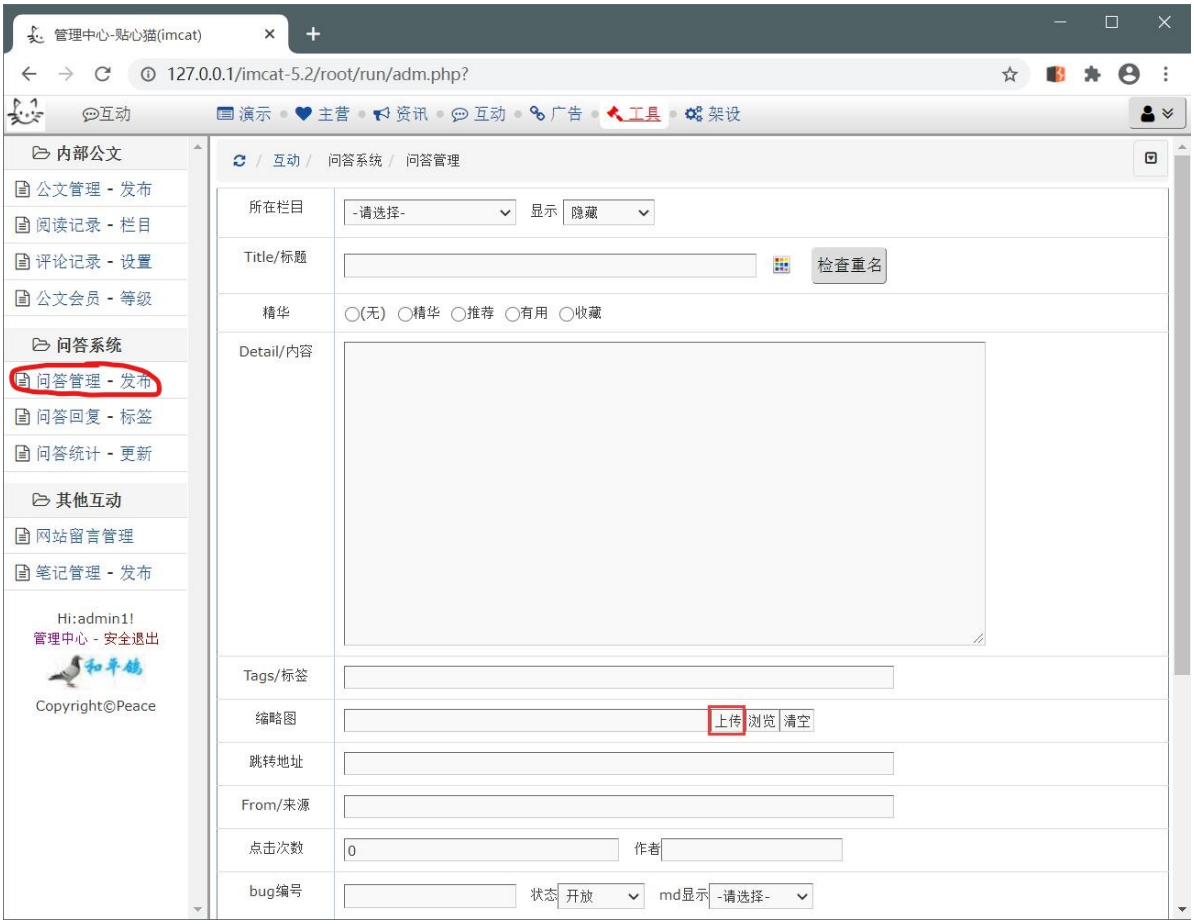
将文件放入服务器根目录进行访问，imcat默认会进行引导安装，按照引导完成安装！

漏洞复现

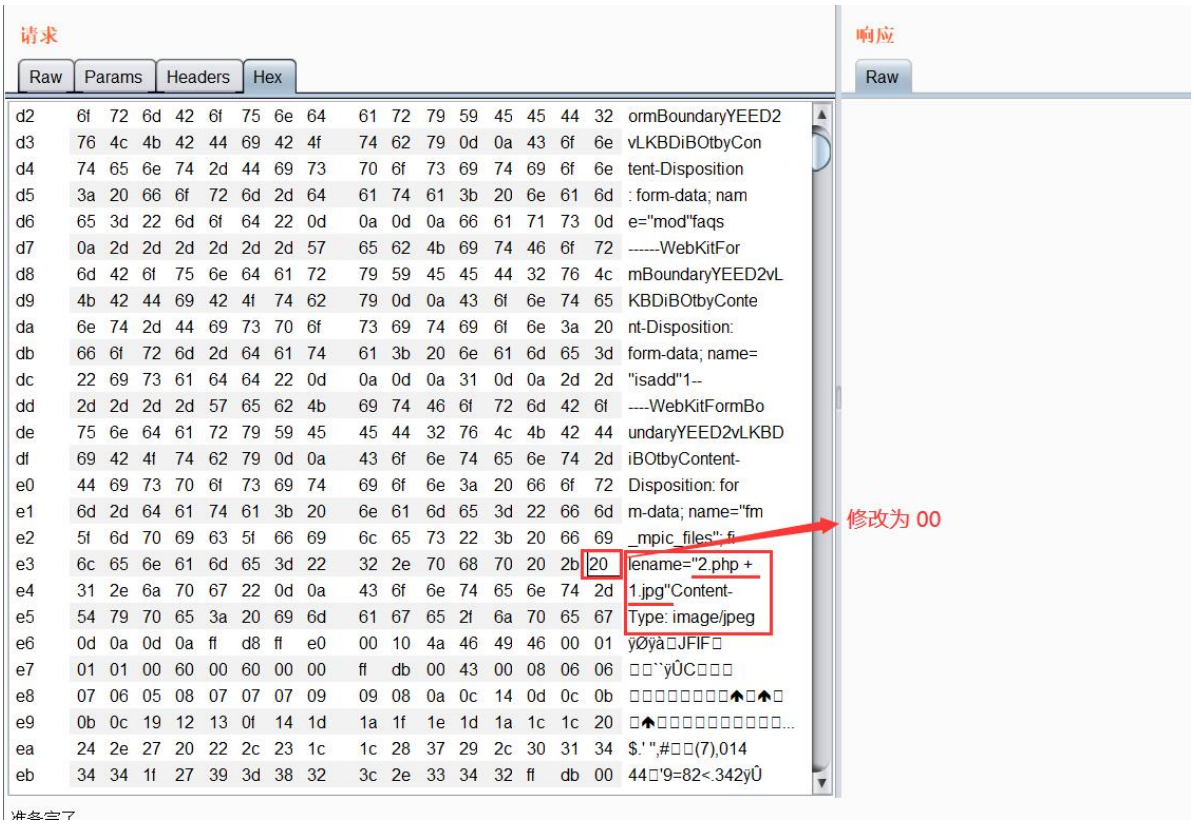
我们需要登录到

```
/root/run/adm.php?
```

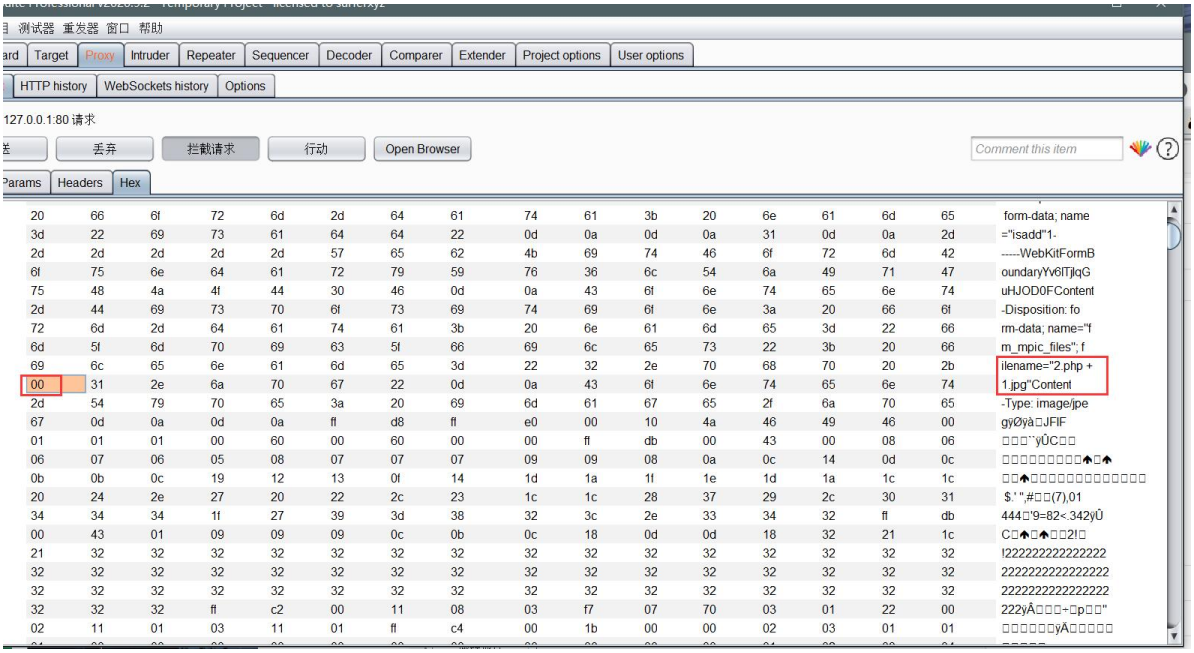
需要准备图片马，名称为：`2.php+ 1.jpg`



使用Burpsuite抓包上传，修改十六进制20-> 00：



修改为



蚁剑连接PHP文件：

```
127.0.0.1//xvars/dtmp/@udoc/a92f985b2414ed5cbdee2fb2e8565ec2/2021-42-m0fx.php+
```

小问题：

1. 这里我们绕过了文件上传的限制，上传了一个PHP代码，但是我们无法解析php+的文件。所以可能造成解析失败。
2. 如果你用的是Apache服务器，可能服务器会拒绝访问这个目录，因为无权限，所以需要修改 `\xvars\.htaccess` 文件为

```
<FilesMatch \.(?i:php|exe)$>
   Order allow,deny
   Allow from all
</FilesMatch>
```

漏洞分析

文件上传php代码路径为：

```
imcat\core\clib\comUpload.php
```

因为其中strpos()无法匹配.php +

```php
// 文件类型检测
private function checkType(){
    $ext = $this->getFileExt();
    $skips = '_.asp.aspx.jsp.php.exe.sh.bat.com.'; // asa.cdx.cer.php2.php3.php4.
    if(strpos($skips, $ext)){ // 超级管理员都不给上传这些文件？？？
        $this->stateInfo = "Error `$ext`!";
        return false; //"Error `$ext`!";
    }
    $flag = $this->config["allowFiles"]==='(supper)' ? true : in_array($ext, $this->config["allowFiles"]);
    return $flag;
}
```

upEnd()中，因为In_array()仅用于检查文件名是否有jpg。因此我们可以上传1.php + .jpg来绕过过滤。

```php
// 上传End
private function upEnd(){
    $this->stateInfo = $this->stateMap[0];
    if(in_array($this->fileType,array('.jpg','.jpeg'))){
        comImage::compress($this->fullName);
    }
}
```