https://down.douphp.com/DouPHP_1.8_Release_20241203.zip

Xss storage type vulnerability in /admin/article.php

This line of code inserts the description parameter from the post request into the database

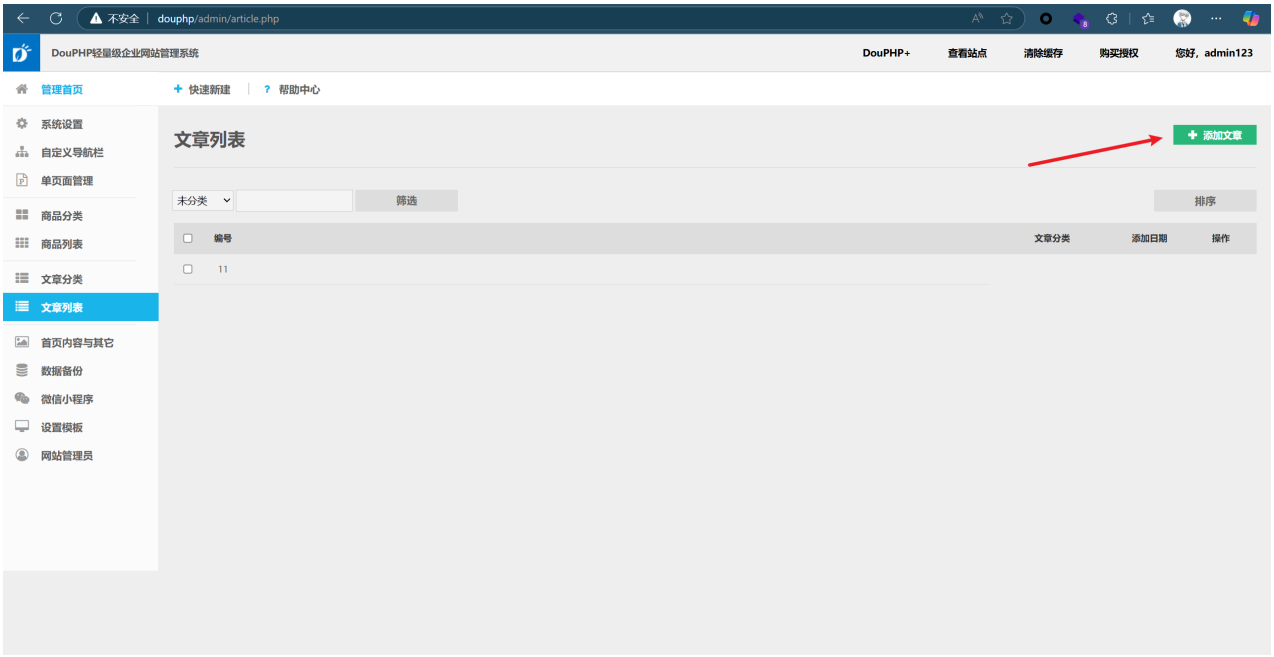
```
elseif ($rec == 'insert') {
    // 验证标题
    if (empty($_POST['title'])) $dou->dou_msg($_LANG['article_name'] . $_LANG['is_empty']);

    // 文件上传盒子
    $image = $file->box( module: 'article', $dou->auto_id( table: 'article'), file_field: 'image', type: 'main');

    // 数据格式化
    $add_time = $_POST['add_time'] ? strtotime($_POST['add_time']) : time();
    $_POST['defined'] = str_replace( search: "\r\n", replace: ',', $_POST['defined']);

    // CSRF防御令牌验证
    $firewall->check_token($_POST['token']);

    $sql = "INSERT INTO " . $dou->table( str: 'article') . " (id, cat_id, title, defined, content, image, keywords, de
    $dou->query($sql);

    $dou->create_admin_log( action: $_LANG['article_add'] . ': ' . $_POST['title']);
    $dou->dou_msg($_LANG['article_add_succes'], 'article.php');
```

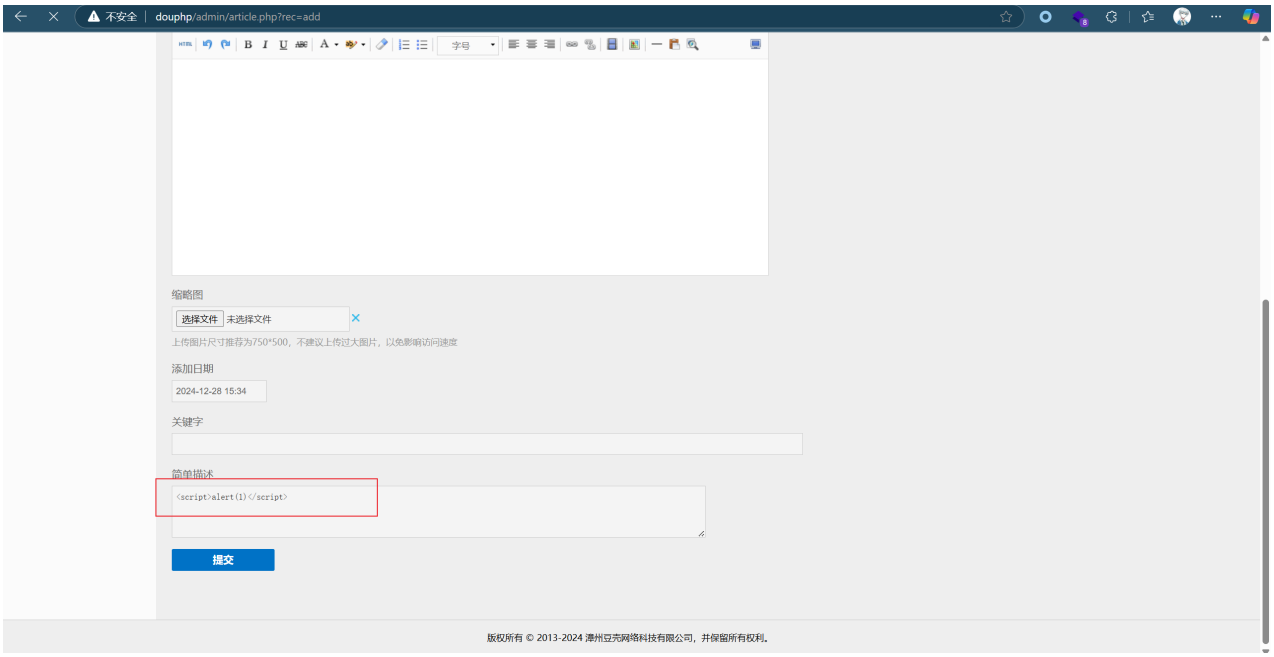
```
$sql = "INSERT INTO " . $dou->table('article') . " (id, cat_id, title, defined, content, image, keywords, description, sort, add_time)" . " VALUES (NULL,
'$_POST[cat_id]', '$_POST[title]', '$_POST[defined]', '$_POST[content]', '$image', '$_POST[keywords]', '$_POST[description]', '$_POST[sort]', '$add_time')";
```

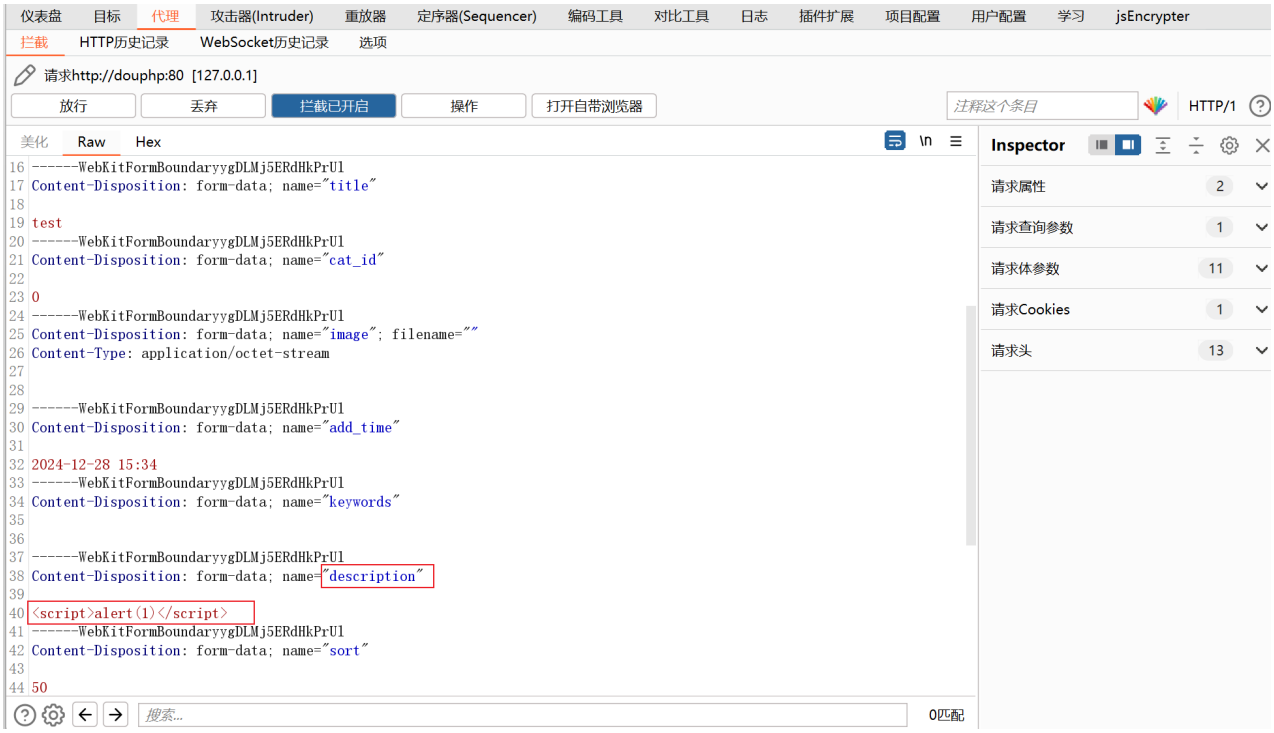
The filtering of post requests is done in /include/firewall.class.php, with only single quotes, double quotes, and backslashes escaped

```
function dou_magic_quotes() {
    if (PHP_VERSION >= 6 || !@get_magic_quotes_gpc()) {
        $_GET = $_GET ? $this->addslashes_deep($_GET) : '';
        $_POST = $_POST ? $this->addslashes_deep($_POST) : '';
        $_COOKIE = $this->addslashes_deep($_COOKIE);
        $_REQUEST = $this->addslashes_deep($_REQUEST);
    }
}
```

Add an article and fill in the payload


不安全 | douphp/admin/article.php
DouPHP轻量级企业网站管理系统
DouPHP+
查看站点
清除缓存
购买授权
您好，admin123
管理首页
快速新建
帮助中心
系统设置
自定义导航栏
单页面管理
商品分类
商品列表
文章分类
文章列表
首页内容与其它
数据备份
微信小程序
设置模板
网站管理员
文章列表
添加文章
未分类
筛选
排序
编号
文章分类
添加日期
操作
11


不安全 | douphp/admin/article.php?rec=add
缩略图
选择文件
未选择文件
上传图片尺寸推荐为750*500，不建议上传过大图片，以免影响访问速度
添加日期
2024-12-28 15:34
关键字
简单描述
<script>alert(1)</script>
提交
版权所有 © 2013-2024 漳州豆壳网络科技有限公司，并保留所有权利。



Then visit http://douphp/?module=article&s=test ,**The test in the URL is the article name**

Successful pop-up window