

New issue

Jump to bottom

# 一个后台存储型xss漏洞 #3


🕒 Open

yazi7 opened this issue on Apr 1 · 0 comments

yazi7 commented on Apr 1

Affected version:<=1.2

[illegible]



电影推猴网

www.film1234.com

localhost:8080 显示1

确定

欢迎: admin

导航菜单

添加电影信息

电影信息管理

电影动态管理

网址信息管理

友情链接管理

安全退出






电影管理

修改

删除

电影名称:

搜索

<input type="checkbox"/>	编号	电影图片	电影名称	帖子标题	热门?	发布日期
6	<input type="checkbox"/> 44		惊天解密	惊天解密 迅雷下载 百度云下载	是	2017-08-28 14:37:22
7	<input type="checkbox"/> 45		星际特工：千星之城	星际特工：千星之城 迅雷下载 百度云下载	是	2017-08-28 14:43:40
8	<input type="checkbox"/> 46		极速车神	极 <div>正在处理, 请稍候, ...</div>	是	2017-08-28 14:55:02
9	<input type="checkbox"/> 47		敦刻尔克	敦刻尔克 迅雷下载 百度云下载	是	2017-08-28 15:05:04
10	<input type="checkbox"/> 48		杀破狼·贪狼	杀破狼·贪狼 迅雷下载 百度云下载	是	2017-08-28 15:11:37

10

第 3 共3页

显示21到24,共24记录

Copyright © 2019 倾心电影网

The main reason is that the code does not filter parameter values:

```
@PostMapping("/save")
public Map<String, Object> save(Movie movie,
                                @RequestParam("imageFile") MultipartFile file,
                                HttpServletRequest request) throws IOException {
    if (file != null && !file.isEmpty()) {
        // 获取文件名
        String fileName = file.getOriginalFilename();
        // 获取文件后缀名
        if (fileName != null) {
            String suffixName = fileName.substring(fileName.lastIndexOf( str: "."));
            String newFileName = DateUtils.getCurrentDateStr() + suffixName;
            // 保存图片到本地服务器
            FileUtils.copyInputStreamToFile(file.getInputStream(), new File( pathname: imagePath + newFileName));
            // 设置电影的图片名
            movie.setImageName(newFileName);
        }
    }
    // 设置发布时间
    movie.setPublishDate(new Date());

    // 保存电影到数据库
    boolean success = movieService.save(movie);
    // 刷新全局数据
    initSystem.loadData(request.getServletContext());
}
```

## Assignees

No one assigned

## Labels

None yet

## Projects

None yet

## Milestone

No milestone

## Development

No branches or pull requests

1 participant

