New issue

Jump to bottom

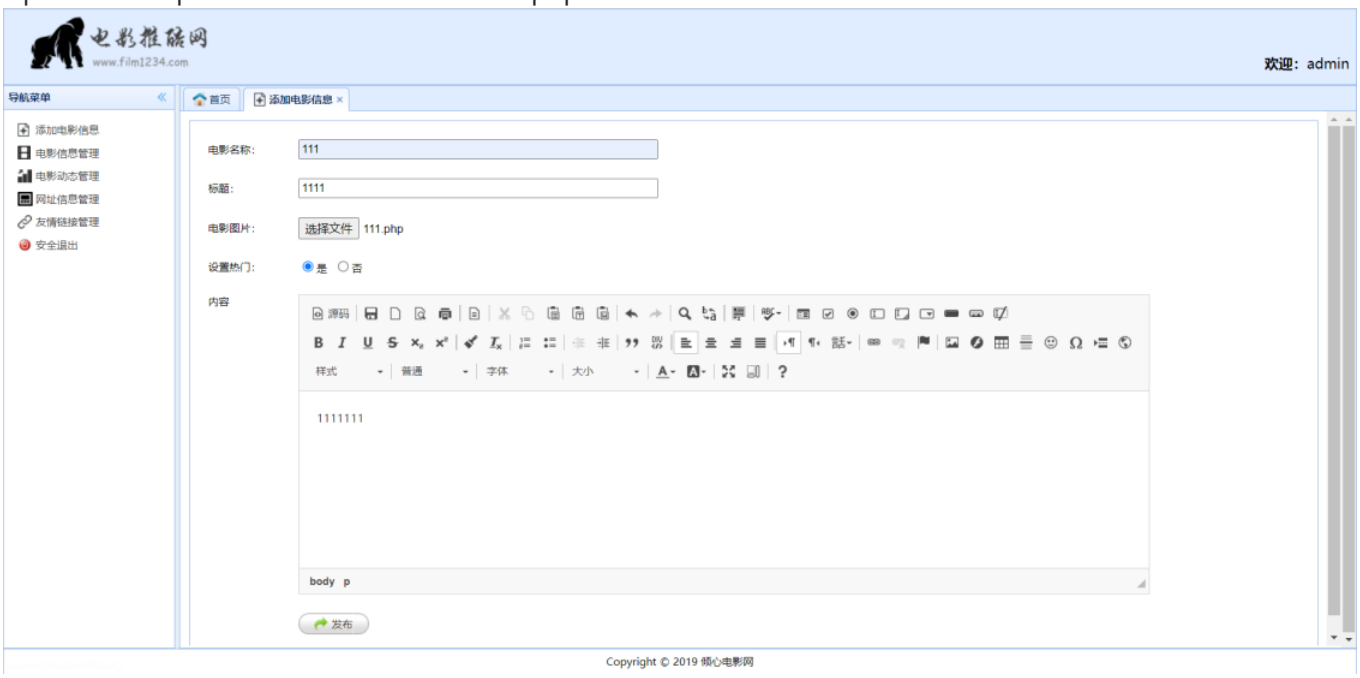
Arbitrary file upload vulnerability #4

Open yazi7 opened this issue on Apr 8 · 0 comments

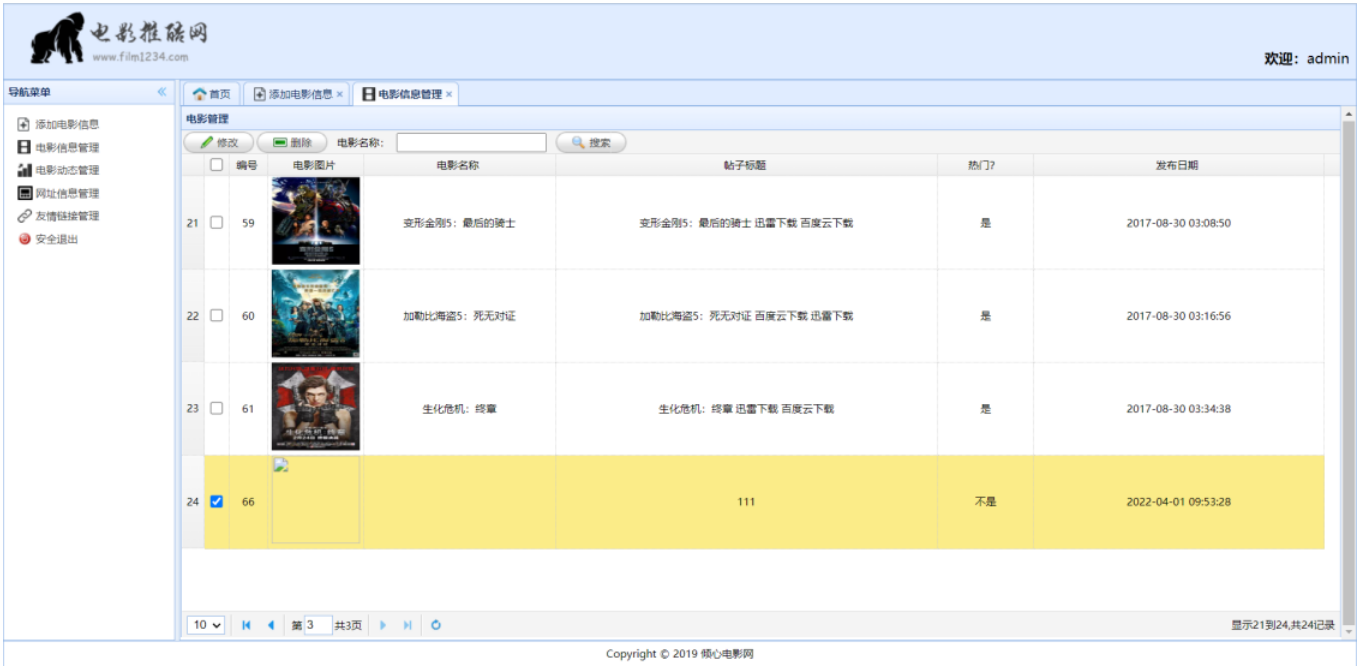
yazi7 commented on Apr 8

Affected version： <=1.2

Upload a compromised file with the suffix .php



Published successfully



Vulnerable code：

```
*/
@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: imageFilePath + 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());

    Map<String, Object> resultMap = new HashMap<>();
    resultMap.put("success", success);
```

The reason for the vulnerability is that the file suffix is not filtered here

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant