New issue

Jump to bottom

XSS Vulnerability #347

Open **Snrt7** opened this issue on Apr 13 · 0 comments

Snrt7 commented on Apr 13

kkFileView XSS Vulnerability

问题描述Description

kkFileview v4.0.0存在XSS漏洞，可能导致网站cookies泄露。

kkFileview v4.0.0 has an XSS vulnerability, which may lead to the leakage of website cookies.

漏洞位置vulerable code location

`kkFileView/server/src/main/java/cn/keking/web/controller/OnlinePreviewController.java` 文件59行，url参数用户可控，且没有过滤特殊字符就输出到了页面

The vulnerability code is located at line 59 in `kkFileView/server/src/main/java/cn/keking/web/controller/OnlinePreviewController.java` , The url parameter is user-controllable, and it is output to the page without filtering special characters

```
public String onlinePreview(String url, Model model, HttpServletRequest req) {
    String fileUrl;
    try {
        fileUrl = new String(Base64.decodeBase64(url), StandardCharsets.UTF_8);
    } catch (Exception ex) {
        String errorMsg = String.format(BASE64_DECODE_ERROR_MSG, "url");
        return otherFilePreview.notSupportedFile(model, errorMsg);
    }
    if (!allowPreview(fileUrl)) {
        return otherFilePreview.notSupportedFile(model, "该文件不允许预览：" + fileUrl);
    }
    FileAttribute fileAttribute = fileHandlerService.getFileAttribute(fileUrl, req);
    model.addAttribute("file", fileAttribute);
    FilePreview filePreview = previewFactory.get(fileAttribute);
    logger.info("预览文件url：{}，previewType：{}", fileUrl, fileAttribute.getType());
    return filePreview.filePreviewHandle(fileUrl, model, fileAttribute);
}
```

漏洞证明PoC

官方演示站点为最新4.0.0版本，以此为演示，访问漏洞位置（url参数值需要经过base64编码和url编码）：
https://file.keking.cn/onlinePreview?url=aHR0cDovL3d3dy54eHguY29tL3h4eC50eHQiPjxpbWcgc3JjPTExMSBvbmVycm9yPWFsZXJ0KDEpPjEyMw%3D%3D

The version of official demo site is v4.0.0. Visit https://file.keking.cn/onlinePreview?url=aHR0cDovL3d3dy54eHguY29tL3h4eC50eHQiPjxpbWcgc3JjPTExMSBvbmVycm9yPWFsZXJ0KDEpPjEyMw%3D%3D and the concept is proofed. (The url parameter value needs to be base64 encoded and url encoded.)

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant