New issue

Jump to bottom

kkFileView XSS Vulnerability #366

Closed wxdx110 opened this issue on Jul 1 · 2 comments

wxdx110 commented on Jul 1

问题描述Description

kkFileview v4.1.0存在XSS漏洞，可能导致网站cookies泄露。

kkFileview v4.1.0 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71行、86行，"urls"、"currentUrl"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 75,86 in kkFileView/server/src/main/java/cn/keking/web/controller/OnlinePreviewController.java , The 'urls' and 'currentUrl' parameter is user-controllable, and it is output to the page without filtering special characters

```
@RequestMapping(value = "/picturesPreview")
public String picturesPreview(String urls, Model model, HttpServletRequest req) throws
UnsupportedEncodingException {
    String fileUrls;
    try {
        fileUrls = new String(Base64.decodeBase64(urls));
    } catch (Exception ex) {
        String errorMsg = String.format(BASE64_DECODE_ERROR_MSG, "urls");
        return otherFilePreview.notSupportedFile(model, errorMsg);
    }
    logger.info("预览文件url：{}，urls：{}", fileUrls, urls);
    // 抽取文件并返回文件列表
    String[] images = fileUrls.split("\\|");
    List<String> imgUrls = Arrays.asList(images);
    model.addAttribute("imgUrls", imgUrls);

    String currentUrl = req.getParameter("currentUrl");
    if (StringUtils.hasText(currentUrl)) {
        String decodedCurrentUrl = new String(Base64.decodeBase64(currentUrl));
        model.addAttribute("currentUrl", decodedCurrentUrl);
```

```
        } else {
            model.addAttribute("currentUrl", imgUrls.get(0));
        }
        return PICTURE_FILE_PREVIEW_PAGE;
    }
```

漏洞证明PoC

官方演示站点为最新4.1.0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/picturesPreview?urls=aHR0cDovLzEyNy4wLjAuMS8xLnR4dCI%2BPHN2Zy9vbmxvYWQ9YWxlcnQoMSk%2B
https://file.keking.cn/picturesPreview?urls=&currentUrl=PHN2Zy9vbmxvYWQ9YWxlcnQoMSk%2B

The official demo site is the latest version 4.1.0. Take this as a demo to access the vulnerability location (the URL parameter value needs to be Base64 encoded and URL encoded):
https://file.keking.cn/picturesPreview?urls=aHR0cDovLzEyNy4wLjAuMS8xLnR4dCI%2BPHN2Zy9vbmxvYWQ9YWxlcnQoMSk%2B
https://file.keking.cn/picturesPreview?urls=&currentUrl=PHN2Zy9vbmxvYWQ9YWxlcnQoMSk%2B

gaoxingzaq commented on Jul 3 • edited

fileUrls= HtmlUtils.htmlEscape(fileUrls);; 添加个转义方法

klboke commented on Jul 29 — Contributor

已修复，见： `acffcbf`

klboke closed this as completed on Jul 29

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

---

3 participants