New issue

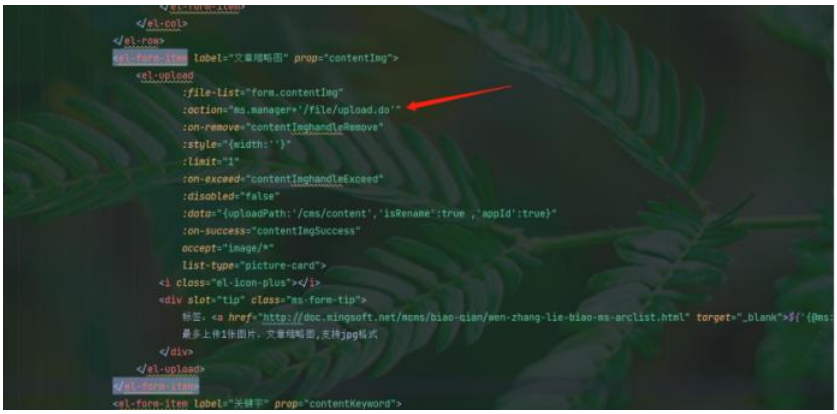
Jump to bottom

Mcms v5.2.8文件上传漏洞 #95

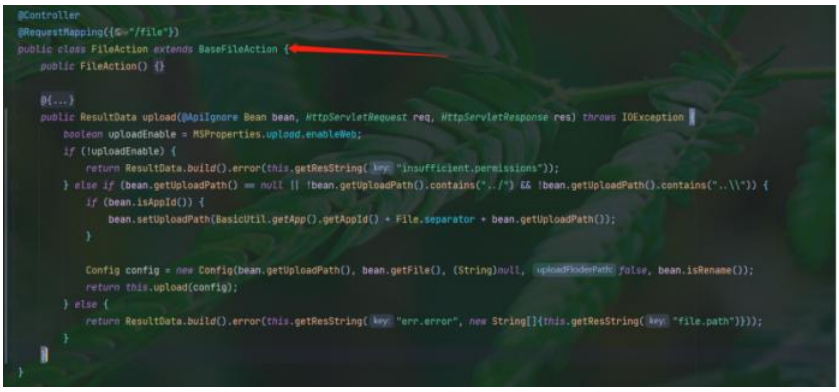
Closed **1orangeSky** opened this issue on May 27 · 3 comments

1orangeSky commented on May 27

1.代码分析
从铭飞官网https://gitee.com/mingSoft/MCMS把源码考下来之后
经过审计找到上传点，form.ftl这里有个文章缩略图上传点看他有没有做过滤然后根据action找到上传接口

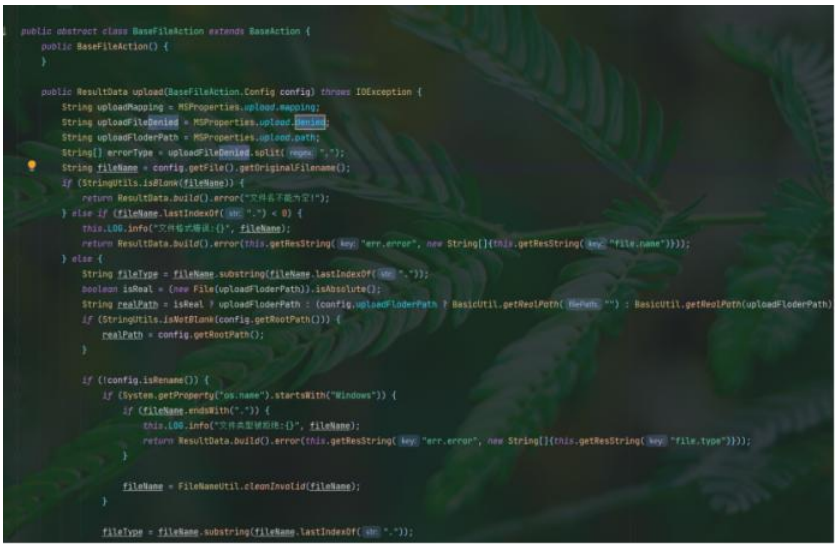


经过查找在FileAction.class这里只判断了../防止目录跳跃，继续往下看点击继承的那个类



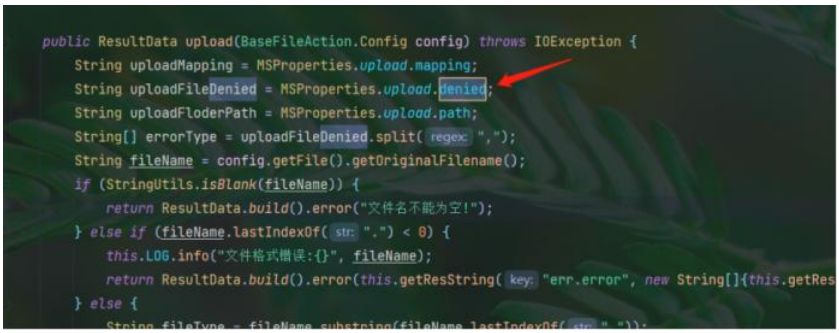
```
@Controller
@RequestMapping({"/file"})
public class FileAction extends BaseFileAction {
    public FileAction() {}

    @{...}
    public ResultData upload(@ApiIgnore Bean bean, HttpServletRequest req, HttpServletResponse res) throws IOException {
        boolean uploadEnable = MSProperties.upload.enableWeb;
        if (!uploadEnable) {
            return ResultData.build().error(this.getResString( key: "insufficient.permissions"));
        } else if (bean.getUploadPath() == null || !bean.getUploadPath().contains("../") && !bean.getUploadPath().contains("..\\")) {
            if (bean.isAppId()) {
                bean.setUploadPath(BasicUtil.getApp().getAppId() + File.separator + bean.getUploadPath());
            }

            Config config = new Config(bean.getUploadPath(), bean.getFile(), (String)null, uploadFloderPath: false, bean.isRename());
            return this.upload(config);
        } else {
            return ResultData.build().error(this.getResString( key: "err.error", new String[]{this.getResString( key: "file.path")}));
        }
    }
}
```

BaseFileAction.class发现他这做了后缀判断接着看是在哪调用的过滤



```
public abstract class BaseFileAction extends BaseAction {
    public BaseFileAction() {
    }

    public ResultData upload(BaseFileAction.Config config) throws IOException {
        String uploadMapping = MSProperties.upload.mapping;
        String uploadFileDenied = MSProperties.upload.denied;
        String uploadFloderPath = MSProperties.upload.path;
        String[] errorType = uploadFileDenied.split( regex: ",");
        String fileName = config.getFile().getOriginalFilename();
        if (StringUtils.isBlank(fileName)) {
            return ResultData.build().error("文件名不能为空!");
        } else if (fileName.lastIndexOf( str: ".") < 0) {
            this.LOG.info("文件格式错误:{}", fileName);
            return ResultData.build().error(this.getResString( key: "err.error", new String[]{this.getResString( key: "file.name")}));
        } else {
            String fileType = fileName.substring(fileName.lastIndexOf( str: "."));
            boolean isReal = (new File(uploadFloderPath)).isAbsolute();
            String realPath = isReal ? uploadFloderPath : (config.uploadFloderPath ? BasicUtil.getRealPath( filePath: "") : BasicUtil.getRealPath(uploadFloderPath));
            if (StringUtils.isNotBlank(config.getRootPath())) {
                realPath = config.getRootPath();
            }

            if (!config.isRename()) {
                if (System.getProperty("os.name").startsWith("Windows")) {
                    if (fileName.endsWith(".")) {
                        this.LOG.info("文件类型被拒绝:{}", fileName);
                        return ResultData.build().error(this.getResString( key: "err.error", new String[]{this.getResString( key: "file.type")}));
                    }

                    fileName = FileNameUtil.cleanInvalid(fileName);
                }

                fileType = fileName.substring(fileName.lastIndexOf( str: "."));
```

我们复制denied全局搜索，application.yml发现他是在配置文件里写了过滤，过滤了 exe,jsp,jspx,sh那说明除了这四个其他都可以上传



```
public ResultData upload(BaseFileAction.Config config) throws IOException {
    String uploadMapping = MSProperties.upload.mapping;
    String uploadFileDenied = MSProperties.upload.denied;
    String uploadFloderPath = MSProperties.upload.path;
    String[] errorType = uploadFileDenied.split( regex: ",");
    String fileName = config.getFile().getOriginalFilename();
    if (StringUtils.isBlank(fileName)) {
        return ResultData.build().error("文件名不能为空!");
    } else if (fileName.lastIndexOf( str: ".") < 0) {
        this.LOG.info("文件格式错误:{}", fileName);
        return ResultData.build().error(this.getResString( key: "err.error", new String[]{this.getRes
    } else {
```

```
manager:
  path: /ms
  check-code: true
xss:
  xssEnable: true
  filterUrl: /**
  excludeUrl: /ms**,/static**,/template**,/file/upload.do,/static/plugins/ueditor/1.4.3.3/jsp/editor.do
upload:
  enable-web: true
  template: template
  path: upload
  mapping: /upload/**
  denied: .exe,.jsp,.jspx,.sh
  back-up: /upload_back
  multipart:
    max-file-size: 10240
```

接着看看他有没有可利用的接口来实现上传jsp，经过查找TemplateAction.class里有个专门解析zip的接口。那么结合上面的过滤 可以上传zip，可以通过zip包含jsp恶意文件上传上去 然后调用这个接口去解析zip并解析树

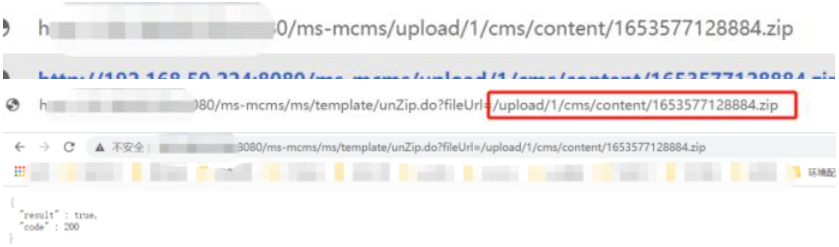
jsp并访问。


@ApiOperation("解压zip模板文件")
@ApiImplicitParam(
name = "fileUrl",
value = "文件路径",
required = true,
paramType = "query"
)
@Logger(
title = "解压zip模板文件",
businessType = BusinessTypeEnum.OTHER
)
@GetMapping("/unZip")
@ResponseBody
@RequiresPermissions({"template:upload"})
public ResultData unZip(@ApiIgnore ModelMap model, HttpServletRequest request) throws IOException, BusinessException {
String fileUrl = request.getParameter(s: "fileUrl");
if (fileUrl == null && (fileUrl.contains("../") || fileUrl.contains("..\\"))) {
ResultData.build().error();
}
File zipFile = new File(BasicUtil.getRealTemplatePath(fileUrl));
this.unzip(zipFile, zipFile.getParent());
FileUtil.del(zipFile);
return ResultData.build().success();

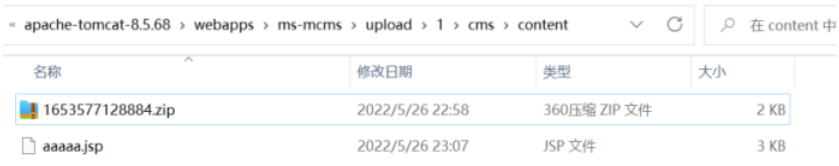
2.根据分析的代码操作

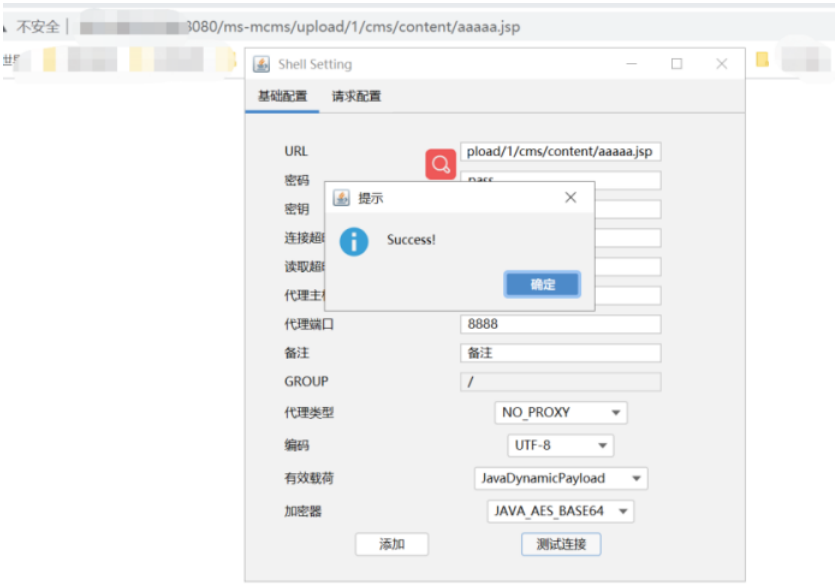
找到文章缩略图地址，点击上传zip

上传上去之后右键复制图片路径，然后通过上面分析的调用解析zip的接口fileUrl=刚刚上传的zip回车提示执行成功



之后查看上传目录的地方，发现成功解压了在通过路径访问aaaaa.jsp，然后利用哥斯拉去连接他发现执行成功





.

IMBALaunched commented on Jul 4

您是如何配置环境的，我用idea搭建环境后，存放上传文件的目录下不对jsp文件进行解析

killfen commented on Sep 8 Contributor

5.2.9 fix it

killfen closed this as completed on Sep 8

1orangeSky commented on Oct 11 Author

需要tomcat启动

...

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants