

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过滤然后根据action找到上传接口

```
</el-col>
</el-row>
<el-form-item label="文章缩略图" prop="contentImg">
  <el-upload
    :file-list="form.contentImg"
    :action="ms.manager+'/file/upload.do'"
    :on-remove="contentImghandleRemove"
    :style="{width:'100%'}"
    :limit="1"
    :on-exceed="contentImghandleExceed"
    :disabled="false"
    :data="{uploadPath:'/cms/content/', 'isRename':true, 'appId':true}"
    :on-success="contentImgSuccess"
    accept="image/*"
    list-type="picture-card">
    <i class="el-icon-plus"></i>
    <div slot="tip" class="ms-form-tip">
      标签: <a href="http://doc.mingsoft.net/mcms/biao-qian/wen-zhang-lie-biao-ms-arclist.html" target="_blank">${' '}</a>
      最多上传1张图片，文章缩略图，支持jpg格式
    </div>
  </el-upload>
</el-form-item>
<el-form-item label="关键词" prop="contentKeyword">
```

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, uploadFolderPath 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 uploadFolderPath = 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(uploadFolderPath)).isAbsolute();
            String realPath = isReal ? uploadFolderPath : (config.uploadFolderPath ? BasicUtil.getRealPath(uploadFolderPath) : BasicUtil.getRealPath(uploadFolderPath));
            if (StringUtils.isBlank(config.getRootPath())) {
                realPath = config.getRootPath();
            }

            if (!config.isRename()) {
                if (System.getProperty("os.name").startsWith("Windows")) {
                    if (fileName.endsWith(str: ".")) {
                        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 = FileUtils.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,jsp,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 uploadFolderPath = 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: "."));
    }
}
```

```
manager:
  path: /ms #前台管理的路径，如http://项目/ms/login.do，生产的时候建议修改
  check-code: true #默认开启验证码验证，false验证码不验证
xss:
  xssEnable: true #xss过滤器的开关
  filterUrl: /** #过滤的url，多个用逗号分开
  excludeUrl: /ms**,/static**,/template**,/file/upload.do,/static/plugins/ueditor/1.4.3.3/jsp/editor.do #排除的url，多个用逗号分开
upload:
  enable-web: true #是否web端的上
  template: template #模板文件支持重命名，不支持移动
  path: upload #文件上传路径，可以根据实际情况进行配置
  mapping: /upload/** #修改需要谨慎，系统第一次部署可以随意修改，如果已经有了上传数据，再次修改会导致之前上传的文件404
  denied: .exe,.jsp,.jspx,.sh
  back-up: /upload_back
multipart:
  #最大上传文件大小，单位：KB
  max-file-size: 10240
  #文件上传超时时间
```

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。



## 2.根据分析的代码操作

找到文章缩略图地址，点击上传zip

MCms v5.2.8

内容管理

文章管理

栏目管理

静态化

工作台

文章管理

全部

公司产品

开源产品

行业产品

平台产品

新闻动态

文章编辑

\* 文章标题

BIMCms施工管理软件

标签: \${field.title}

\* 所属栏目

行业产品

标签: \${field.type.title} 不能选择时

文章类型

推荐

标签: \${flag} 通过自定义字典可扩展, 通常用在 arclist 标签的 flag 属性上进行过滤文章

\* 发布时间

2022-02-27 11:42:04

标签: \${field.date?string("yyyy-M")}

文章作者

请输入文章作者

标签: \${field.author}

文章来源

请输入文章来源

标签: \${field.source}

是否显示

是 否

选择否后编辑将不显示, 需要重新生成才有效果

文章缩略图

+

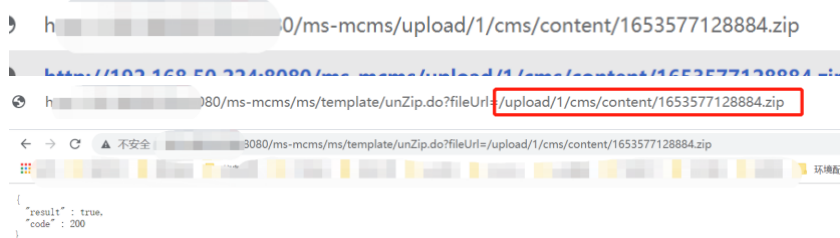
标签: { @ms:file field.itpic/ }

最多上传1张图片, 文章缩略图, 支持jpg格式

关键字

请输入文章关键字

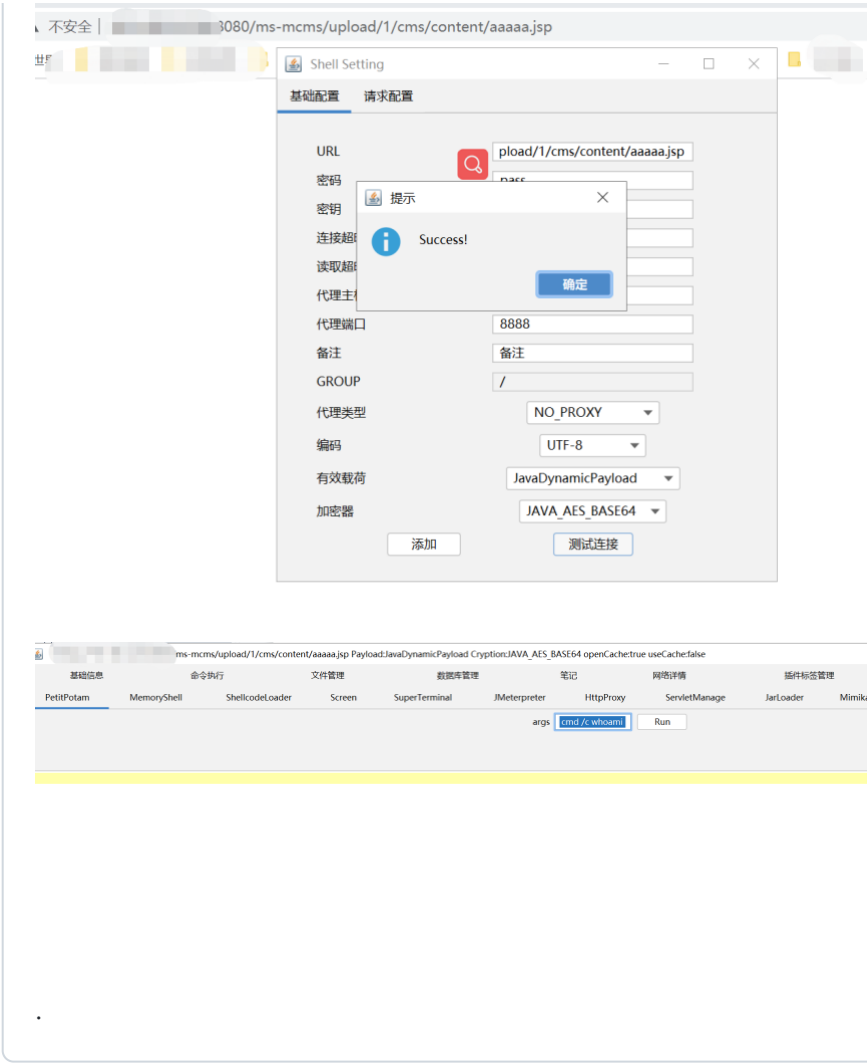
上传上去之后右键复制图片路径，然后通过上面分析的调用解析zip的接口fileUrl=刚刚上传的zip回车提示执行成功



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

« apache-tomcat-8.5.68 » webapps » ms-mcms » upload » 1 » cms » content

名称	修改日期	类型	大小
1653577128884.zip	2022/5/26 22:58	360压缩 ZIP 文件	2 KB
aaaaa.jsp	2022/5/26 23:07	JSP 文件	3 KB



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

