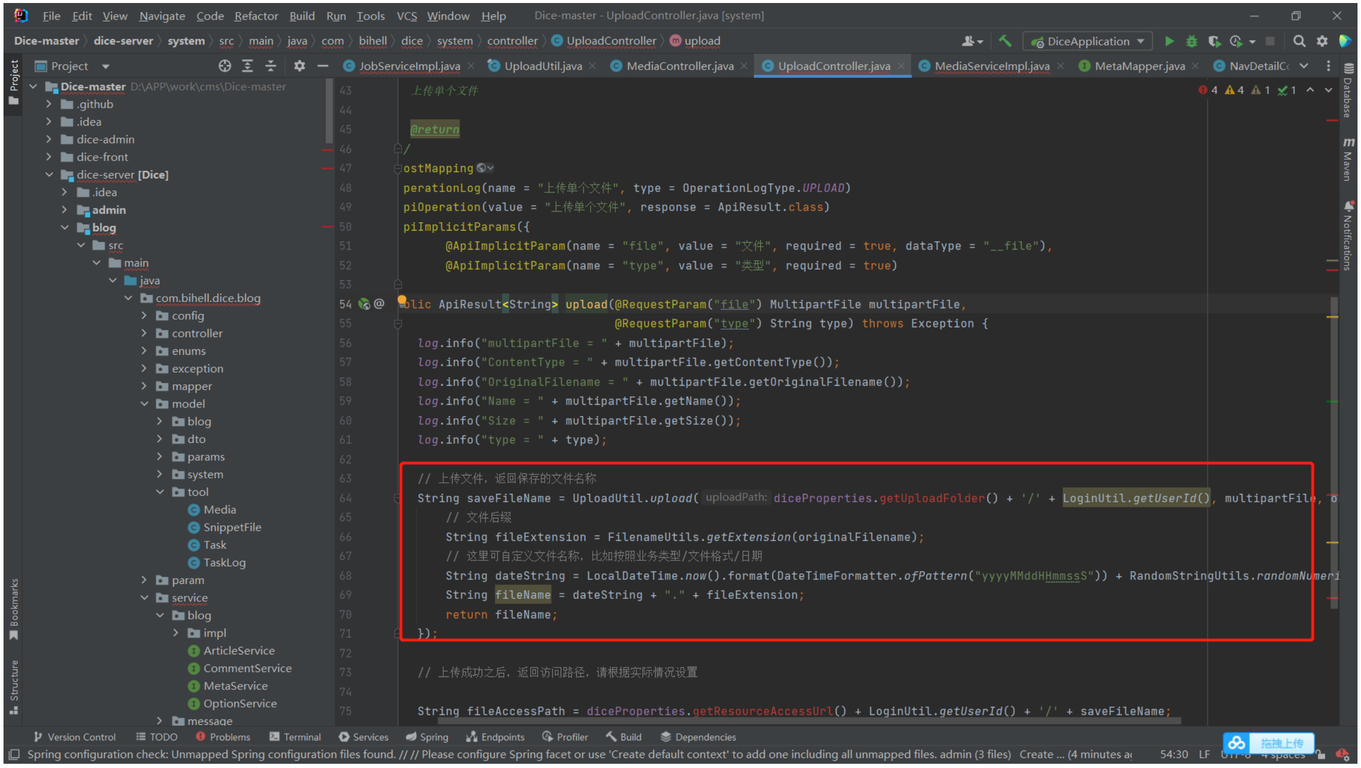
# any file upload vuln #157

Open lanfei-4 opened this issue on Jun 1 · 0 comments

lanfei-4 commented on Jun 1

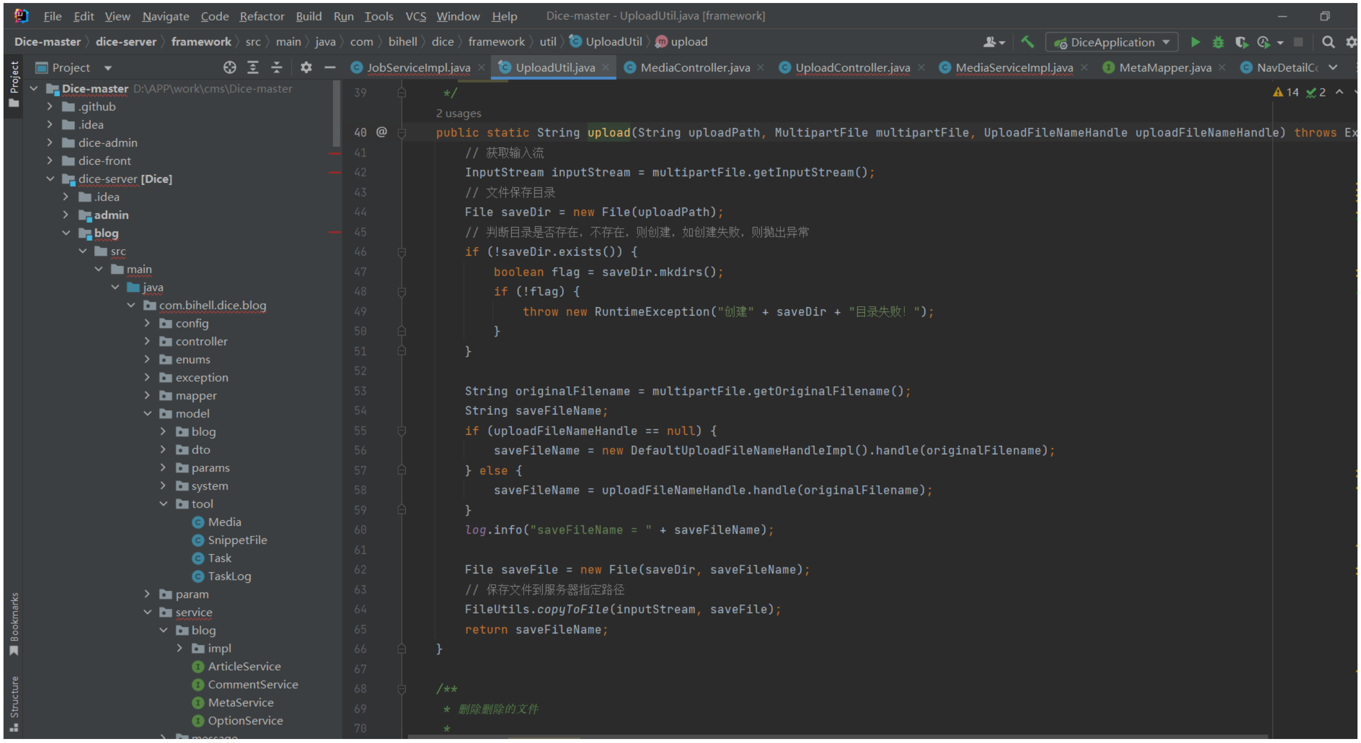
1、 Any file upload vulnerability in the following code can cause RCE



```
 上传单个文件

 @return
/
ostMapping
perationLog(name = "上传单个文件", type = OperationLogType.UPLOAD)
piOperation(value = "上传单个文件", response = ApiResult.class)
piImplicitParams({
      @ApiImplicitParam(name = "file", value = "文件", required = true, dataType = "__file"),
      @ApiImplicitParam(name = "type", value = "类型", required = true)

blic ApiResult<String> upload(@RequestParam("file") MultipartFile multipartFile,
                              @RequestParam("type") String type) throws Exception {
  log.info("multipartFile = " + multipartFile);
  log.info("ContentType = " + multipartFile.getContentType());
  log.info("OriginalFilename = " + multipartFile.getOriginalFilename());
  log.info("Name = " + multipartFile.getName());
  log.info("Size = " + multipartFile.getSize());
  log.info("type = " + type);

  // 上传文件，返回保存的文件名称
  String saveFileName = UploadUtil.upload( uploadPath: diceProperties.getUploadFolder() + '/' + LoginUtil.getUserId(), multipartFile, o
      // 文件后缀
      String fileExtension = FilenameUtils.getExtension(originalFilename);
      // 这里可自定义文件名称，比如按照业务类型/文件格式/日期
      String dateString = LocalDateTime.now().format(DateTimeFormatter.ofPattern("yyyyMMddHHmmssS")) + RandomStringUtils.randomNumeri
      String fileName = dateString + "." + fileExtension;
      return fileName;
  });

  // 上传成功之后，返回访问路径，请根据实际情况设置

  String fileAccessPath = diceProperties.getResourceAccessUrl() + LoginUtil.getUserId() + '/' + saveFileName;
```

Spring configuration check: Unmapped Spring configuration files found. // // Please configure Spring facet or use 'Create default context' to add one including all unmapped files. admin (3 files) Create ... (4 minutes a

2、 Follow up the code、 Files are directly uploaded to the server without filtering



```
     */
    2 usages
    public static String upload(String uploadPath, MultipartFile multipartFile, UploadFileNameHandle uploadFileNameHandle) throws Ex
        // 获取输入流
        InputStream inputStream = multipartFile.getInputStream();
        // 文件保存目录
        File saveDir = new File(uploadPath);
        // 判断目录是否存在，不存在，则创建，如创建失败，则抛出异常
        if (!saveDir.exists()) {
            boolean flag = saveDir.mkdirs();
            if (!flag) {
                throw new RuntimeException("创建" + saveDir + "目录失败！");
            }
        }

        String originalFilename = multipartFile.getOriginalFilename();
        String saveFileName;
        if (uploadFileNameHandle == null) {
            saveFileName = new DefaultUploadFileNameHandleImpl().handle(originalFilename);
        } else {
            saveFileName = uploadFileNameHandle.handle(originalFilename);
        }
        log.info("saveFileName = " + saveFileName);

        File saveFile = new File(saveDir, saveFileName);
        // 保存文件到服务器指定路径
        FileUtils.copyToFile(inputStream, saveFile);
        return saveFileName;
    }

    /**
     * 删除删除的文件
     *
```

## Assignees

No one assigned

## Labels

None vet

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant