Apache SSI 远程命令执行漏洞复现实验报告

原创

shidfe 于 2022-02-26 16:57:17 发布 3765 收藏
分类专栏： 笔记 文章标签： apache 安全 web安全

视频演示

ApacheSSI远程命令执行漏洞_哔哩哔哩_bilibiliBGM:《芳华慢》 《霜雪千年》(by等什么君)
https://www.bilibili.com/video/BV1Gm4y1R7Pm?spm_id_from=333.999.0.0

参考文章

Vulhub - Docker-Compose file for vulnerability environment https://vulhub.org/#/environments/httpd/ssi-rce/

漏洞形成原理

Apache服务器在上传文件时，很多时候不允许上传php文件，如果Apache服务器开启了SSI与CGI支持，我们可以上传一个shtml文件，并利用

```
<!--#exec cmd="id" -->
```

语法执行任意命令。

漏洞利用限制

服务器需要开启SSI与CGI

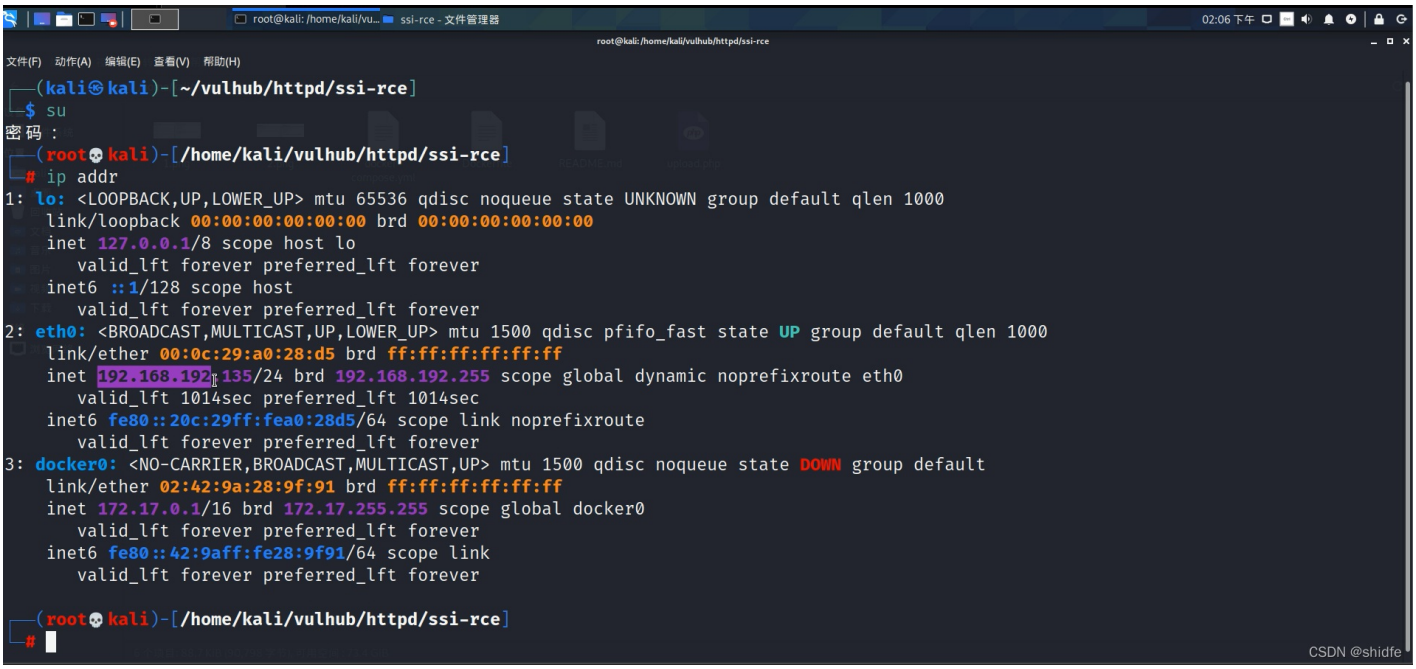
服务器当前用户权限限制

个人思考

我在复现漏洞时，上传php一句话木马服务器拦截，上传shtml文件并利用特殊的语法可以通过访问该shtml文件执行服务器系统命令，不过也取决于服务器当前用户权限，如果用户权限低，就不能执行访问高权限的文件和命令。另外我复现漏洞时尝试通过服务器命令写入一句话木马，不过失败了，可能是在shtml构造命令时格式失误吧

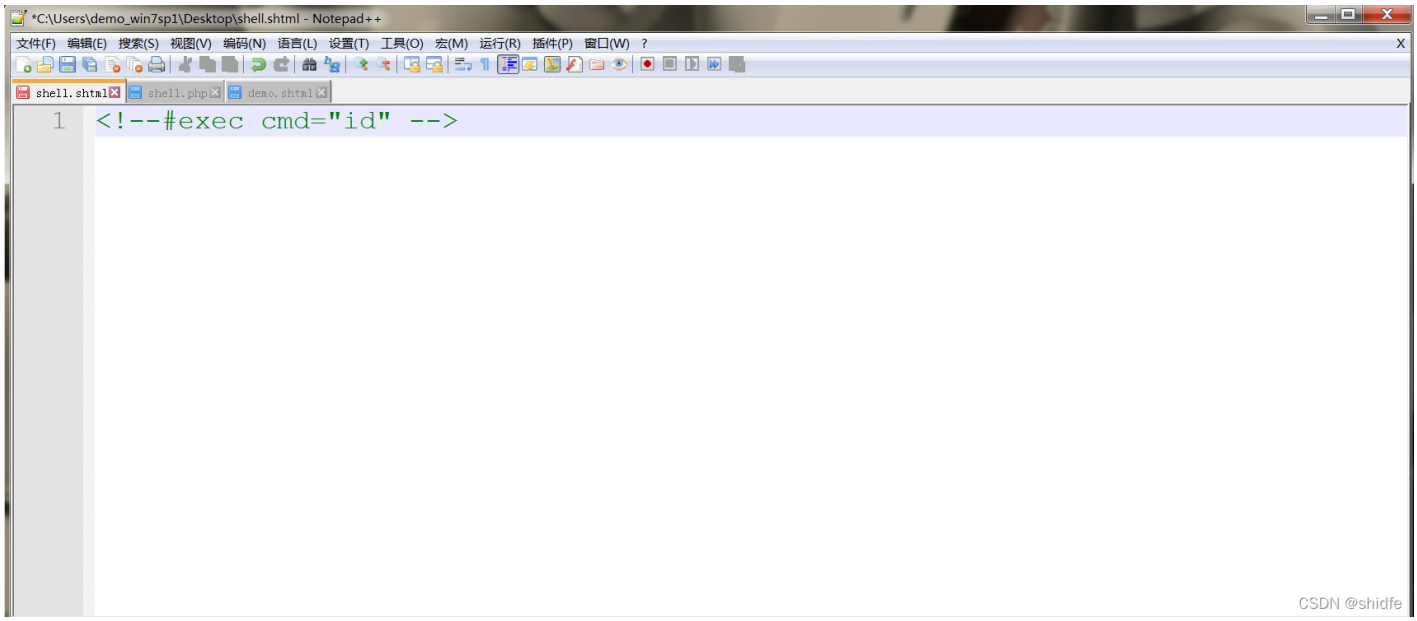
漏洞复现

靶机IP：192.168.192.135

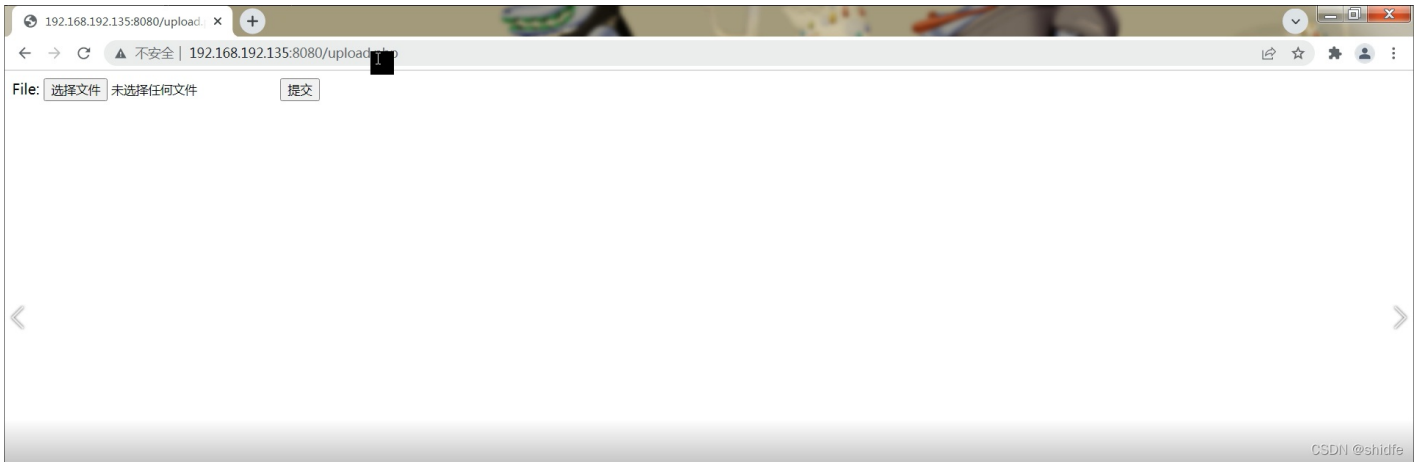


攻击机IP：192.168.192.139

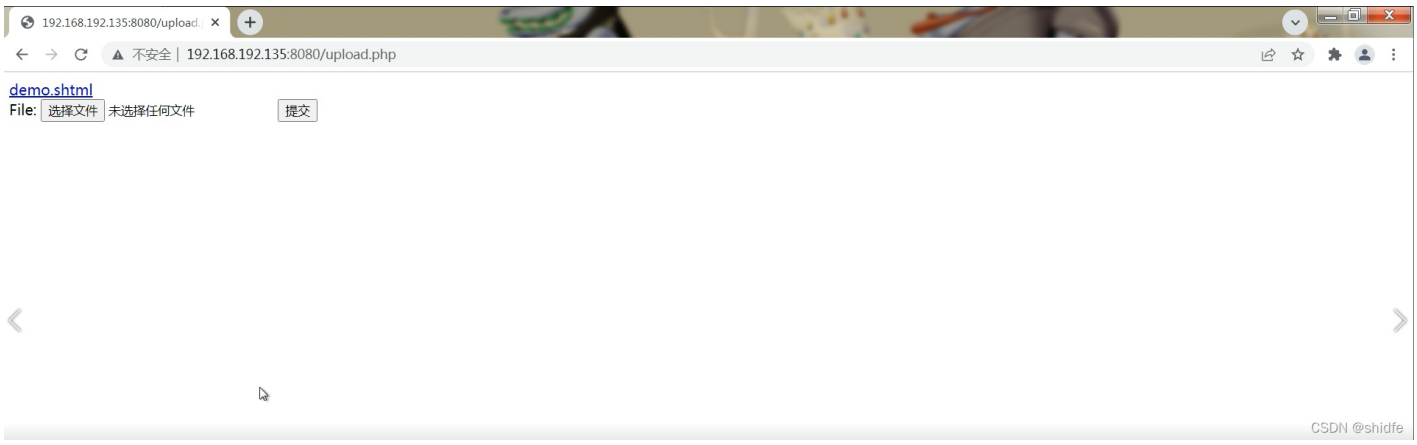
shtml文件

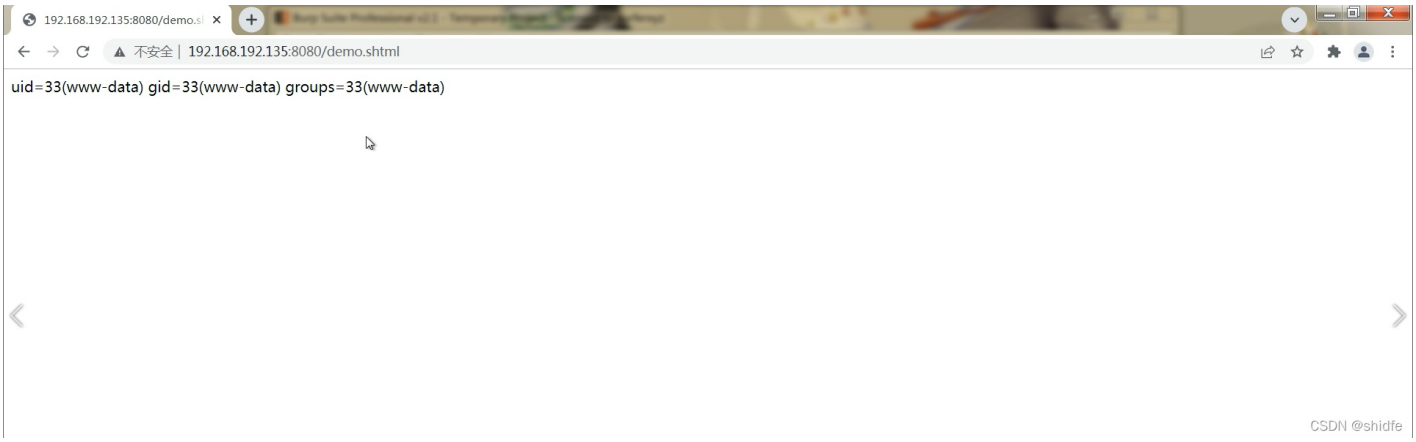


在靶场表单上传shtml文件



访问shtml文件





可以看到服务器执行shtml的系统命令并返回执行结果，通过此种方式可以执行不同的命令，具体请看**视频演示**，至此漏洞复现完成

写在最后

有任何错误或失误的地方，请各位指正