

# 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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/weixin\\_48400575/article/details/123150009](https://blog.csdn.net/weixin_48400575/article/details/123150009)

版权



[笔记](#) 专栏收录该内容

8 篇文章 0 订阅

订阅专栏

## 视频演示

Apache SSI 远程命令执行漏洞\_哔哩哔哩\_bilibili BGM: 《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](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

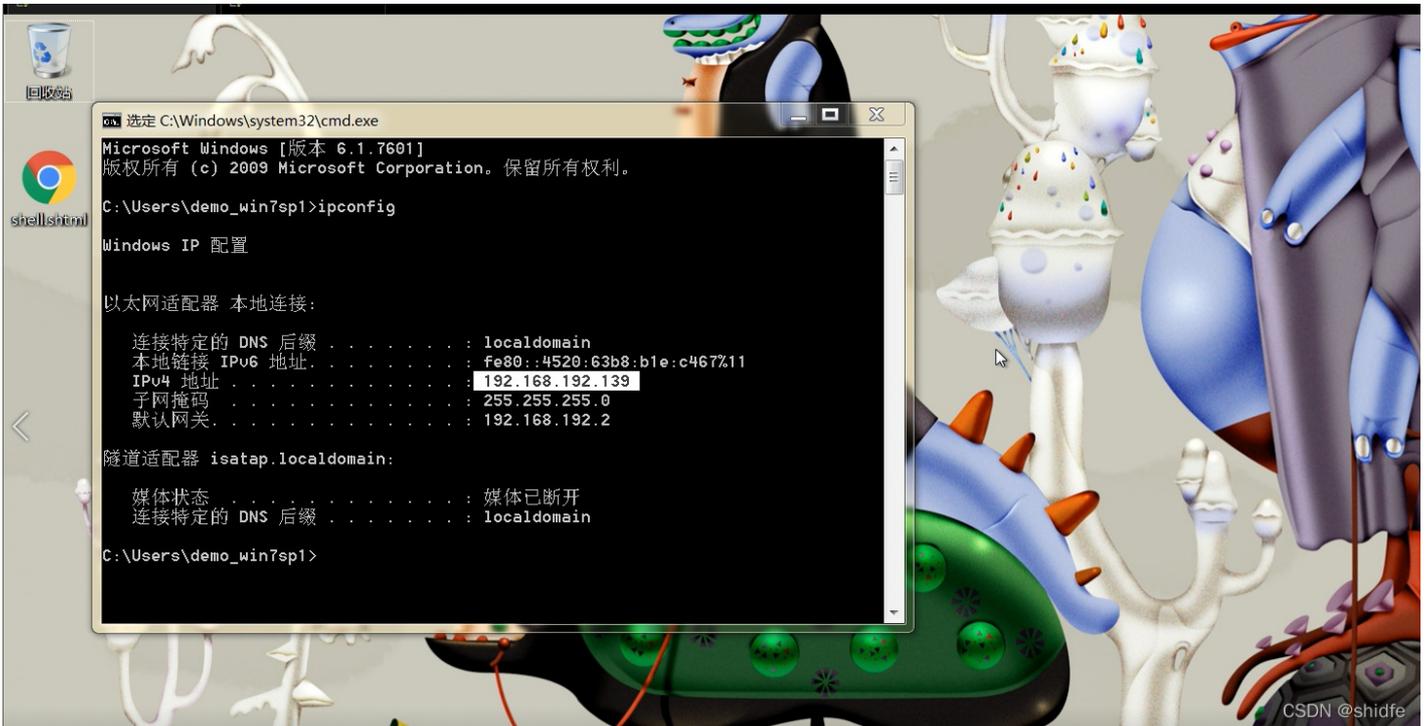
我在复现漏洞时, 上传 php 一句话木马服务器拦截, 上传 shtml 文件并利用特殊的语法可以通过访问该 shtml 文件执行服务器系统命令, 不过也取决于服务器当前用户权限, 如果用户权限低, 就不能执行访问高权限的文件和命令。另外我复现漏洞时尝试通过服务器命令写入一句话木马, 不过失败了, 可能是在 shtml 构造命令时格式失误吧

## 漏洞复现

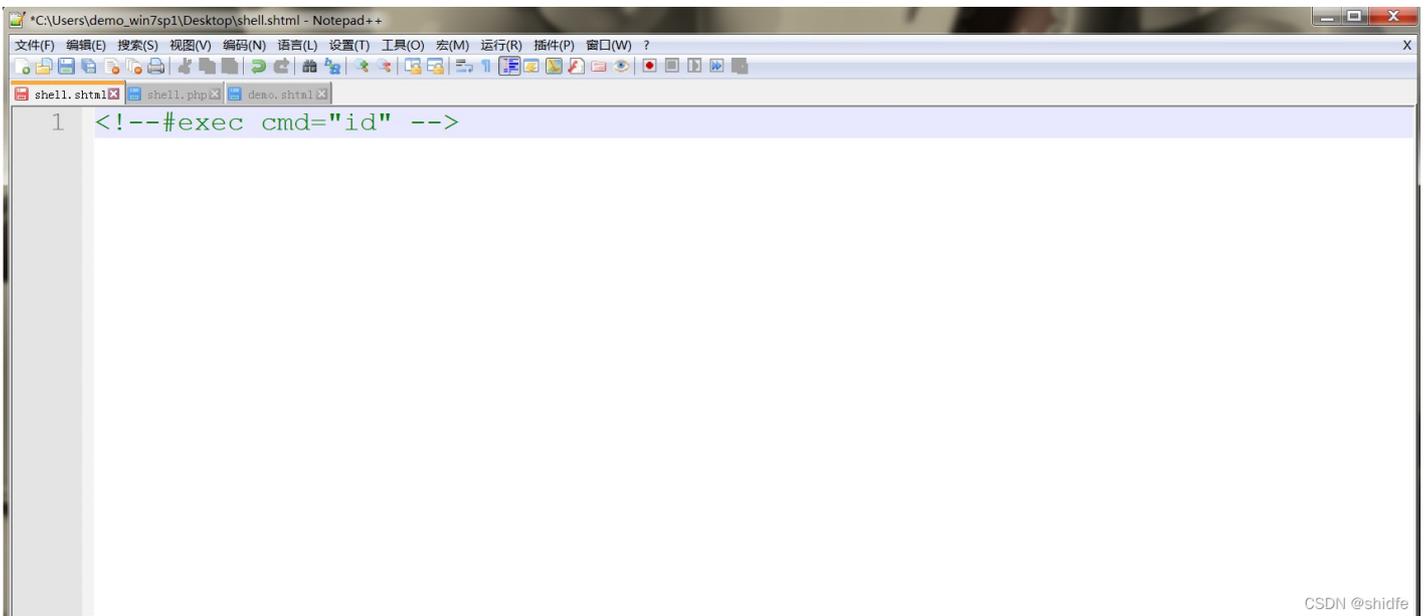
靶机 IP: 192.168.192.135

```
root@kali: /home/kali/vulhub/ssi-rce - 文件管理器
root@kali: /home/kali/vulhub/httpd/ssi-rce
(kali@kali) - [~/vulhub/httpd/ssi-rce]
$ su
密码:
(root@kali) - [~/home/kali/vulhub/httpd/ssi-rce]
# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
   inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
   link/ether 00:0c:29:a0:28:d5 brd ff:ff:ff:ff:ff:ff
   inet 192.168.192.139/24 brd 192.168.192.255 scope global dynamic noprefixroute eth0
       valid_lft 1014sec preferred_lft 1014sec
   inet6 fe80::20c:29ff:fea0:28d5/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
   link/ether 02:42:9a:28:9f:91 brd ff:ff:ff:ff:ff:ff
   inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
       valid_lft forever preferred_lft forever
   inet6 fe80::42:9aff:fe28:9f91/64 scope link
       valid_lft forever preferred_lft forever
(root@kali) - [~/home/kali/vulhub/httpd/ssi-rce]
#
```

攻击机IP: 192.168.192.139

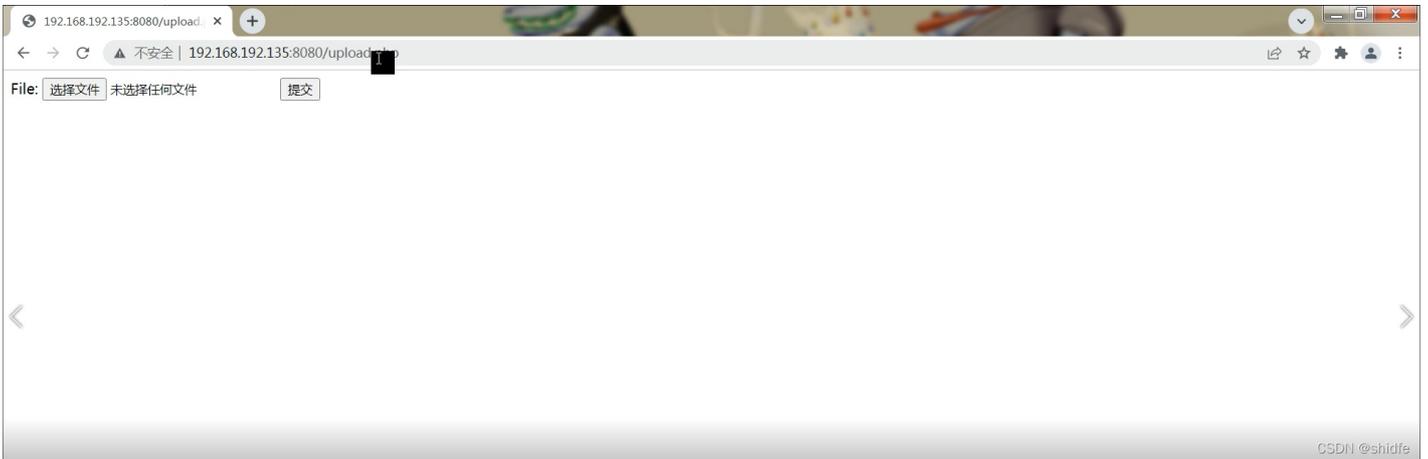


shtml文件

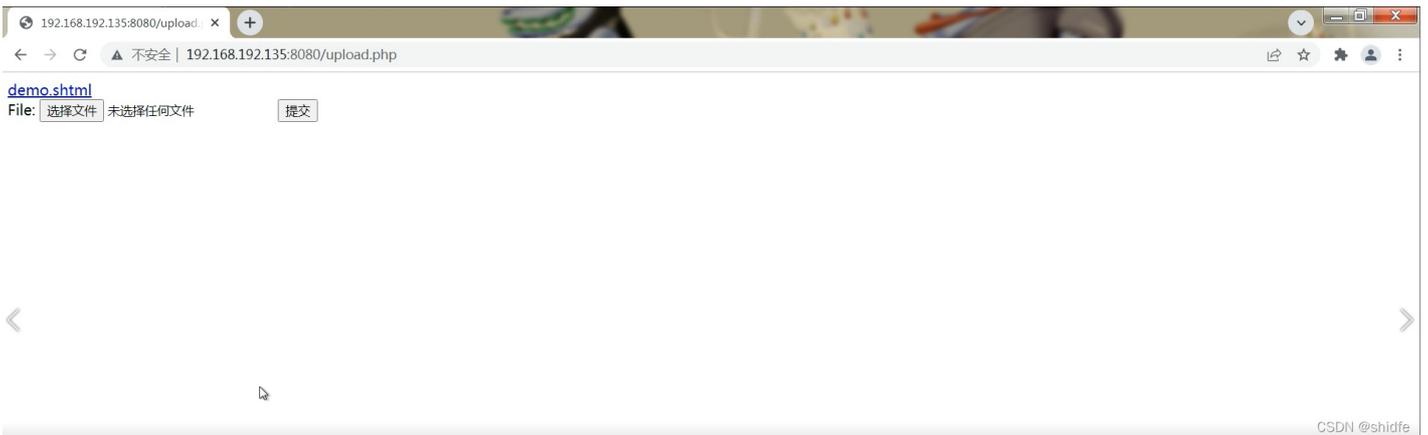


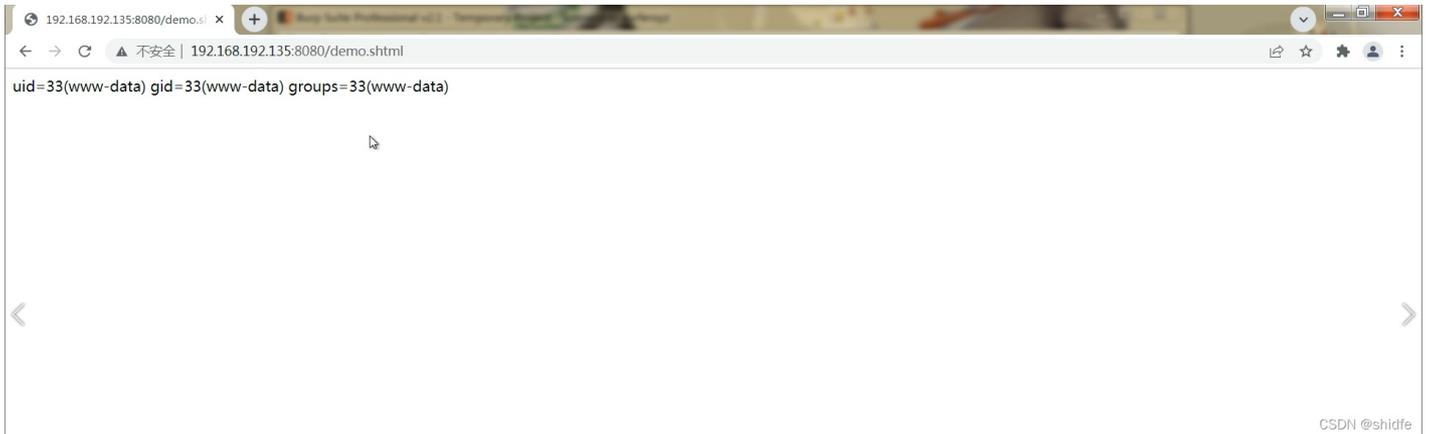
CSDN @shidfe

## 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