kali linux渗透测试

第27课 Burp Suite利用服务器文件上传漏洞，成功上传一句话木马

文件上传漏洞

文件上传漏洞，通常是由于对上传文件的类型、内容没有进行严格的过滤、检查，使得攻击者可以通过上传木马获取服务器的webshell权限，因此文件上传漏洞带来的危害常常是毁灭性的，Apache、Tomcat、Nginx等都曝出过文件上传漏洞。

漏洞利用

文件上传漏洞的利用是有限制条件的，首先当然是要能够成功上传木马文件，其次上传文件必须能够被执行，最后就是上传文件的路径必须可知。

Content-Type

multipart/form-data

当action为post且Content-Type类型是multipart/form-data，浏览器会把整个表单以控件为单位分割，并为每个部分加上Content-Disposition(form-data或者file),Content-Type(默认为text/plain),name(控件name)等信息，并加上分割符(boundary)。

Content-Type，内容类型，一般是指网页中存在的Content-Type，用于定义网络文件的类型和网页的编码，决定浏览器将以什么形式、什么编码读取这个文件

谢谢观赏