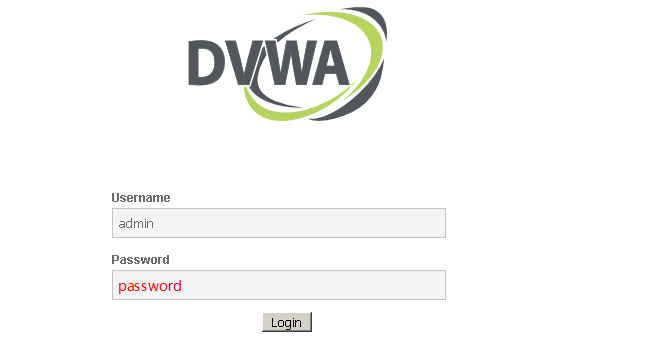
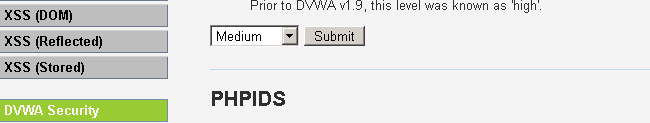
登录DVWA 账号 admin 密码password



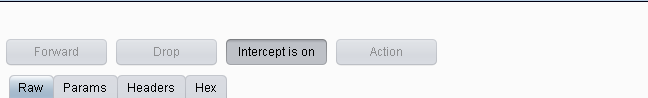
进入安全级别模块设置等级为中等



准备好php图片木马



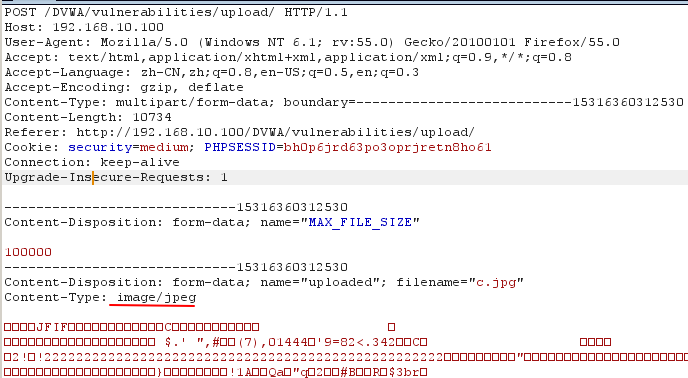
开启Burp，浏览器也开启127.0.0.1:8080代理



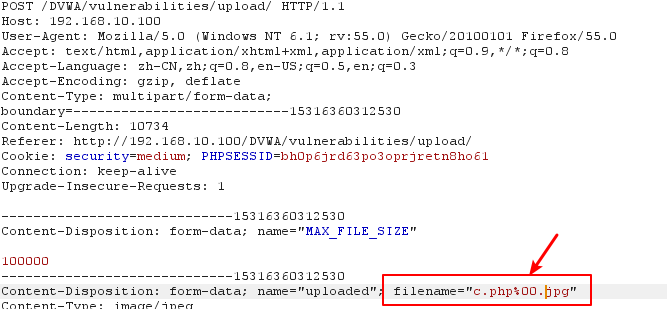
然后点击File Upload 模块，浏览选择图片马，然后点击上传



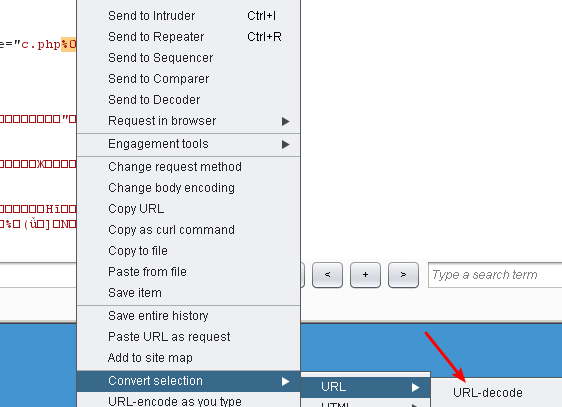
然后在Burp找到上传文件的包，Ctrl+R 将包转到Repeater模式并切换到该模式下面



将filename="c.jpg" 改为 filename="c.php%00.jpg"



选中%00，右键URL解密，如下图所示也可以直接Ctrl +Shift + U

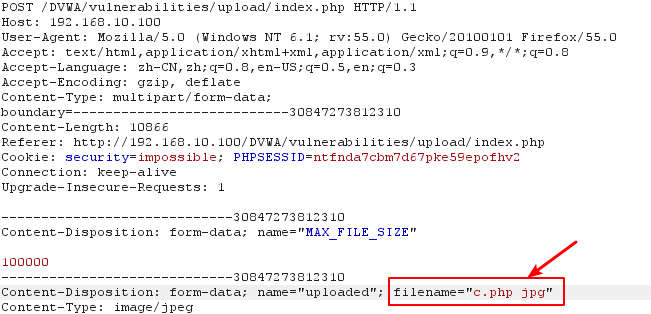


解密后%00就会变成一个方框，这就是00截断了

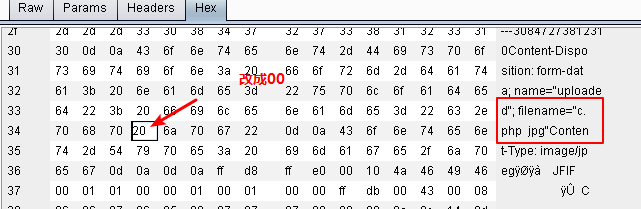


%00 截断除了可以使用右键URL解密外，还可以是用十六进制模式改成00

将 filename="c.jpg" 改成 filename="c.php .jpg" 中间有个空格



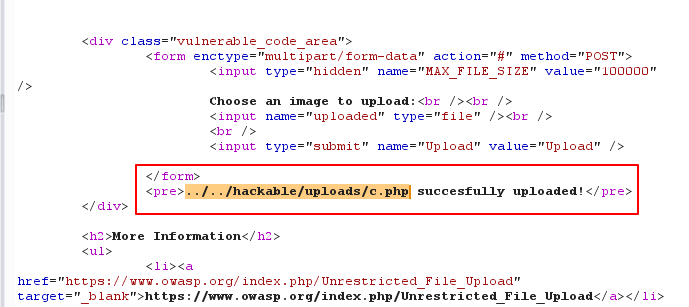
然后进入十六进制模式，找到空格的位置值为20改成00，切换回row模式



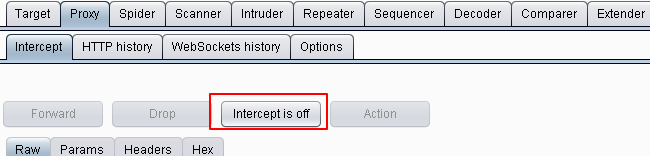
可以看到这种方法也出现了方框，两种选一即可



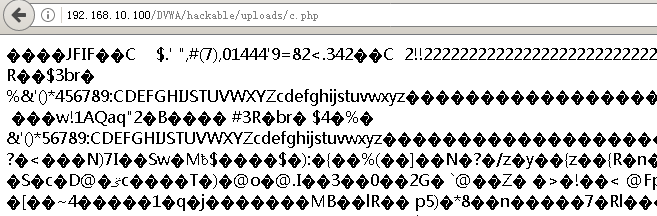
点击go发生请求，再返回框框当做找到输出的上传文件路径，如下图



找到之后将其复制，并将捕捉拦截功能关闭



访问：http://192.168.10.100/DVWA/vulnerabilities/upload/../../hackable/uploads/c.php



菜刀连接

