Web for pentester_writeup之File Upload篇

转载

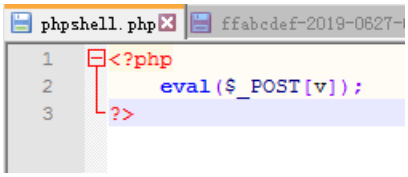
ditanji3425 于 2019-08-08 18:01:00 发布 109 收藏
文章标签： php
原文链接：http://www.cnblogs.com/liliyuanshangcao/p/11322761.html

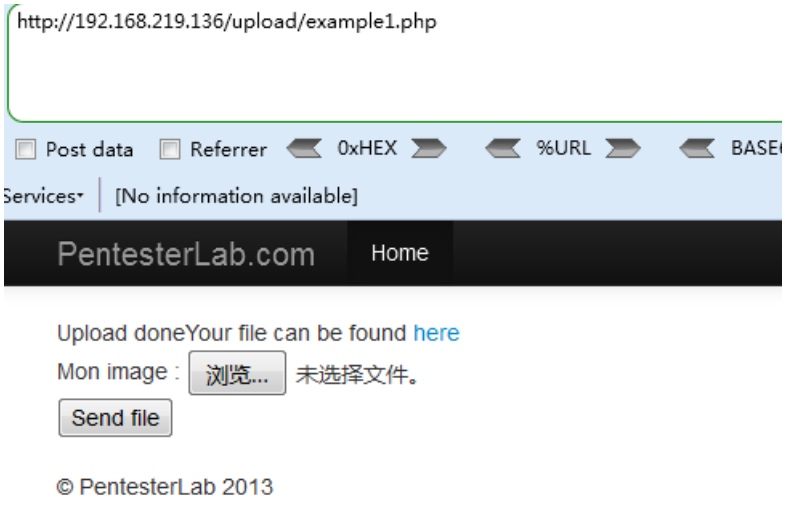
Web for pentester_writeup之File Upload篇

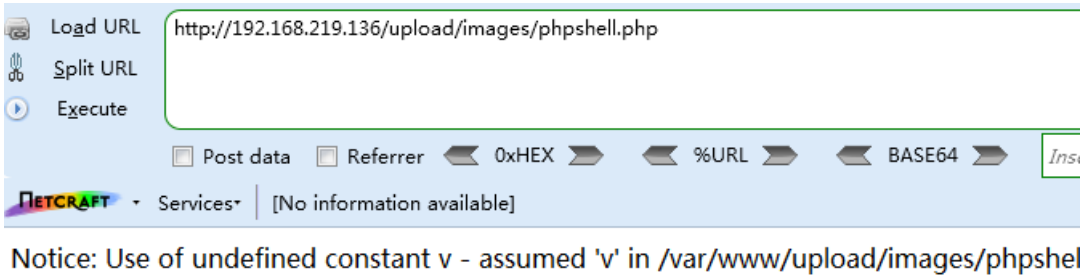
File Upload（文件上传）

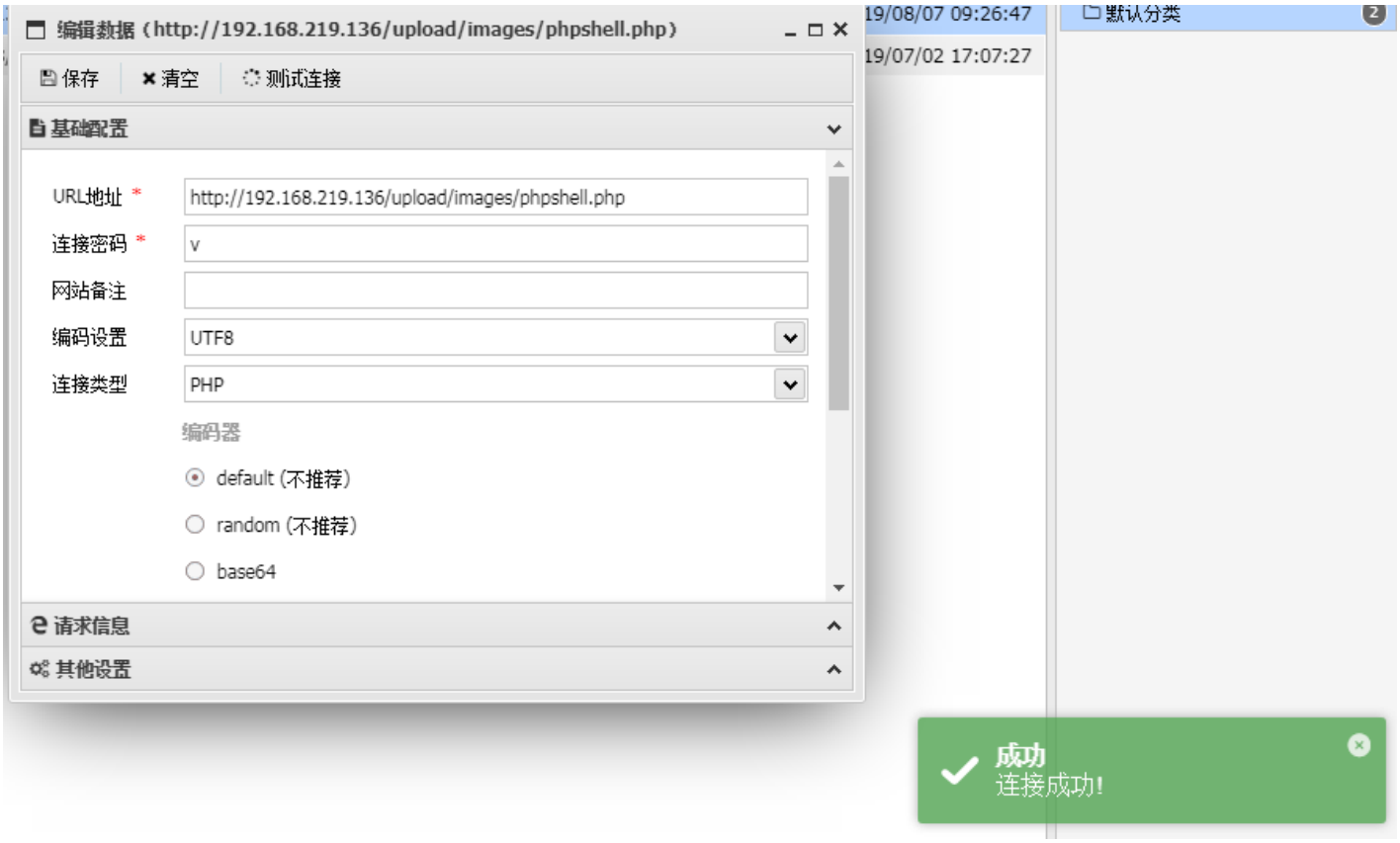
Example 1

直接上传一句话木马，使用蚁剑连接

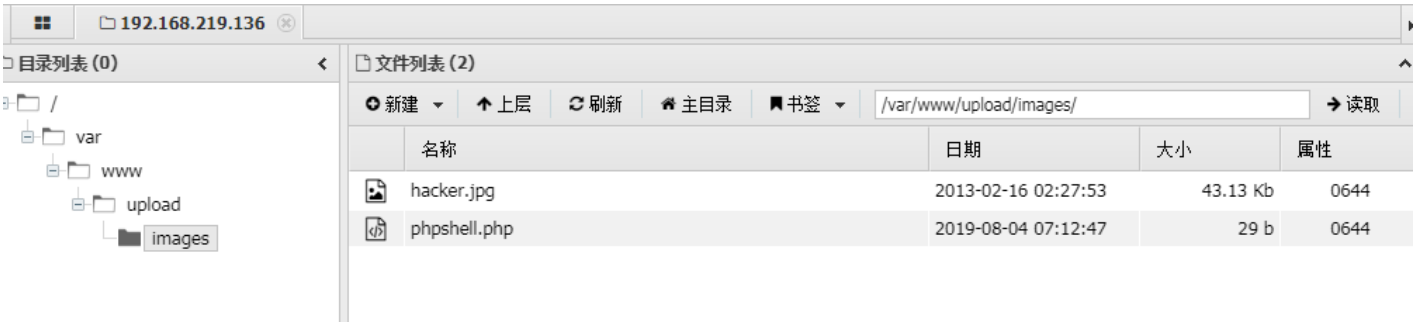






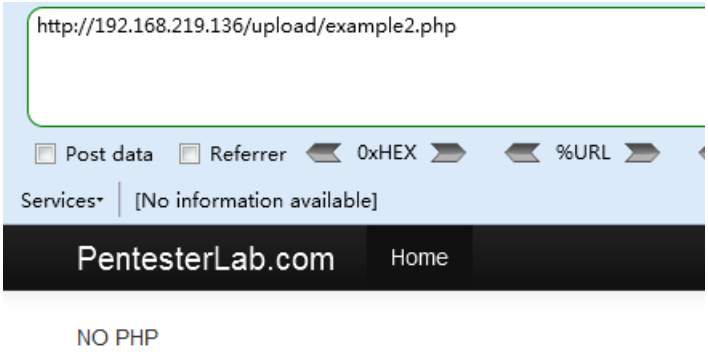


成功连接，获取网站根目录

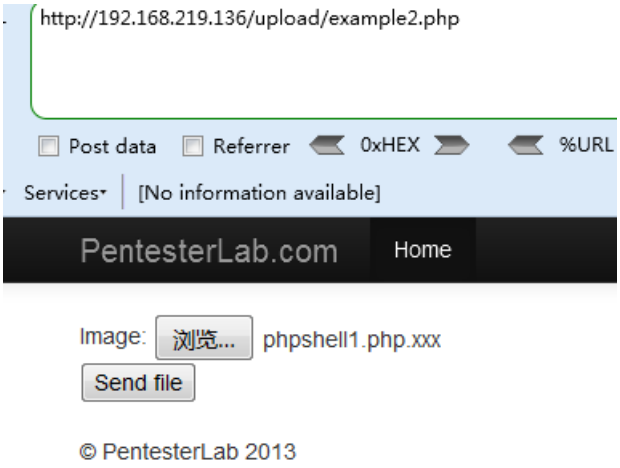


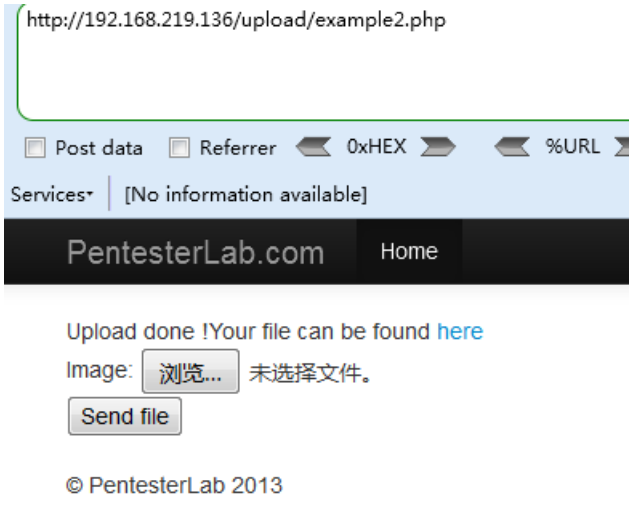
Example 2

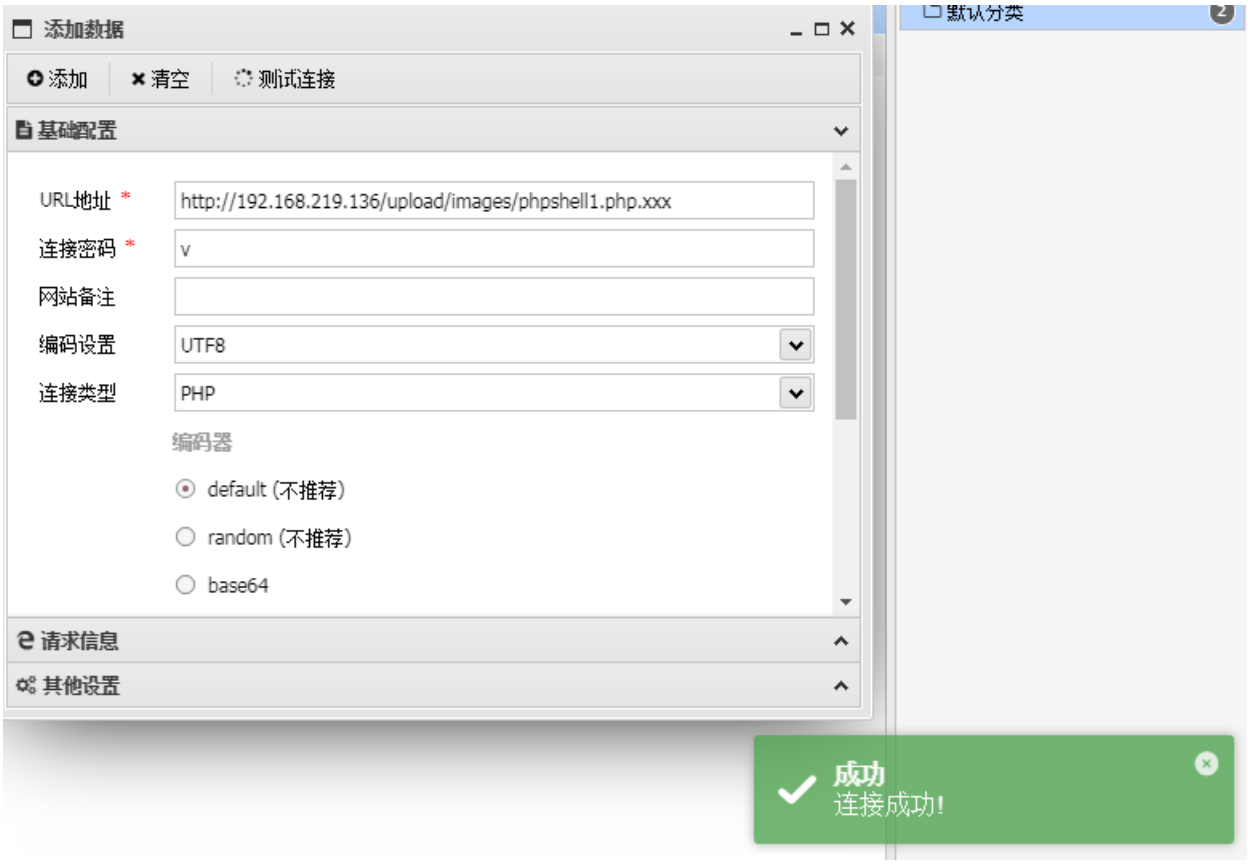
可以看到上传文件做了相关限制，不允许上传PHP文件，



修改后缀名为linux不识别的xxx，上传







同样成功连接，我们还可以修改后缀名为.php3，有些系统.php4，.php5也能成功执行
文件上传绕过方式有很多，包含

- 前台脚本检测扩展名绕过
- Content-Type检测文件类型绕过
- 文件系统00截断绕过
- 服务器端扩展名检测黑名单绕过
- JS检测上传文件绕过
- 重写解析规则绕过
- 后缀名大小写绕过
- 双写后缀名绕过
- 特殊后缀名绕过

大家可以根据实际环境选择其中的一种或者多种方式结合来绕过文件上传限制，这里就不过多阐述。

转载于:https://www.cnblogs.com/liliyuanshangcao/p/11322761.html