i春秋-web-Code

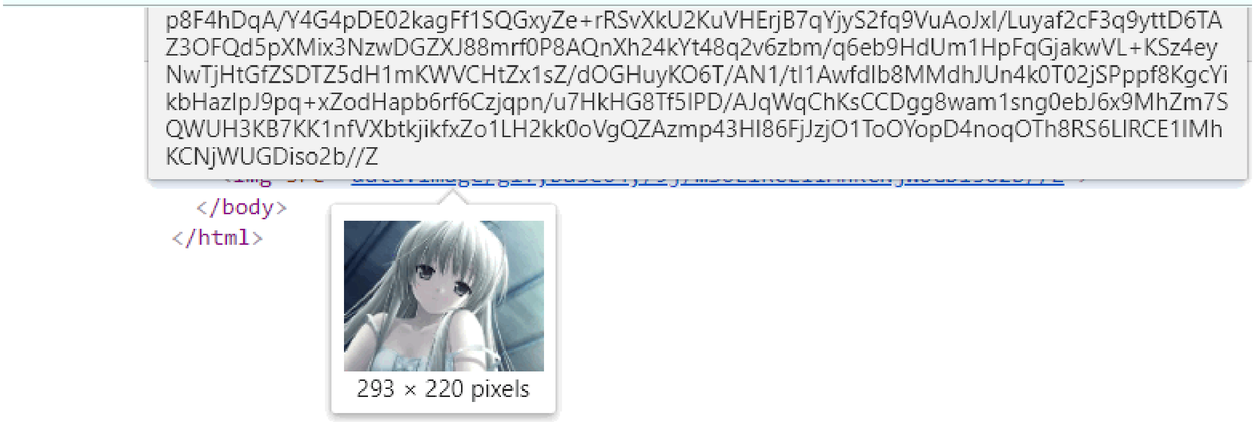
原创

超级神兽小金刚 于 2020-04-14 20:44:59 发布 130 收藏

题目要点

- 文件包含
- 脑洞

题目内容

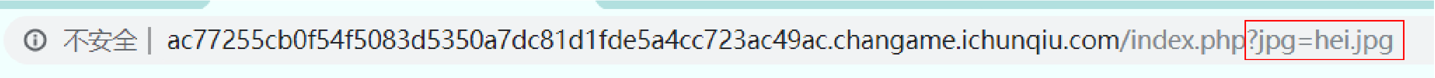


p8F4hDqA/Y4G4pDE02kagFf1SQGxyZe+rRSvXkU2KuVHErjB7qYjyS2fq9VuAoJxl/Luyaf2cF3q9yttD6TA
Z3OFQd5pXMix3NzwDGZXJ88mrf0P8AQnXh24kYt48q2v6zbm/q6eb9HdUm1HpFqGjakwVL+KSz4ey
NwTjHtGfZSDTZ5dH1mKWVCHtZx1sZ/dOGHuyKO6T/AN1/tl1Awfdlb8MMdhJUn4k0T02jSPppf8KgcYi
kbHazlpJ9pq+xZodHapb6rf6Czjqpn/u7HkHG8Tf5IPD/AJqWqChKsCCDgg8wam1sng0ebJ6x9MhZm7S
QWUH3KB7KK1nfVXbtkjikfxZo1LH2kk0oVgQZAzmp43HI86FjJzjO1ToOYopD4noqOTh8RS6LIRCE1IMh
KCNjWUGDiso2b//Z

```
  </body>
</html>
```

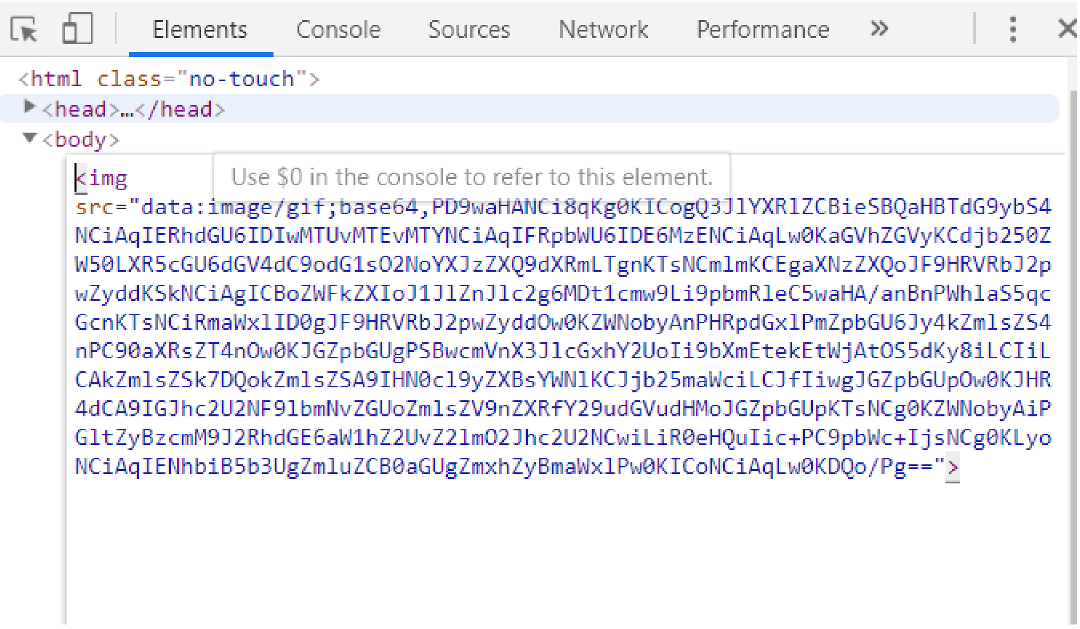
解题

打开页面，是一张**base64加密**的动漫图片
在URL中可以看到图片名



ac77255cb0f54f5083d5350a7dc81d1fde5a4cc723ac49ac.changame.ichunqiu.com/index.php?jpg=hei.jpg

尝试访问index源码(修改 **hei.jpg** 为 **index.php**)，得到base64加密的源码。



```
<html class="no-touch">
▶<head>…</head>
▼<body>
    <img
    src="data:image/gif;base64,PD9waHANCi8qKg0KICogQ3JlYXRlZCBieSBQaHBTdG9ybS4
    NCiAqIERhdGU6IDIwMTUvMTEvMTYNCiAqIFRpbWU6IDE6MzENCiAqLw0KaGVhZGVyKCdjb250Z
    W50LXR5cGU6dGV4dC9odG1sO2NoYXJzZXQ9dXRmLTgnKTsNCmlmKCEgaXNzZXQoJF9HRVRbJ2p
    wZyddKSkNCiAgICBoZWFkZXIoJ1JlZnJlc2g6MDt1cmw9Li9pbmRleC5waHA/anBnPWhlaS5qc
    GcnKTsNCiRmaWxlID0gJF9HRVRbJ2pwZyddOw0KZWNobyAnPHRpdGxlPmZpbGU6Jy4kZmlsZS4
    nPC90aXRsZT4nOw0KJGZpbGUgPSBwcmVnX3JlcGxhY2UoIi9bXmEtekEtWjAtOS5dKy8iLCIiL
    CAkZmlsZSk7DQokZmlsZSA9IHN0cl9yZXBsYWNlKCJjb25maWciLCJfIiwgJGZpbGUpOw0KJHR
    4dCA9IGJhc2U2NF9lbmNvZGUoZmlsZV9nZXRfY29udGVudHMoJGZpbGUpKTsNCg0KZWNobyAiP
    GltZyBzcmM9J2RhdGE6aW1hZ2UvZ2lmO2Jhc2U2NCwiLiR0eHQuIic+PC9pbWc+IjsNCg0KLyo
    NCiAqIENhbiB5b3UgZmluZCB0aGUgZmxhZyBmaWxlPw0KICoNCiAqLw0KDQo/Pg==">
```

解密得到如下代码：

```php
<?php
/**
 * Created by PhpStorm.
 * Date: 2015/11/16
 * Time: 1:31
 */
header('content-type:text/html;charset=utf-8');
if(! isset($_GET['jpg']))
    header('Refresh:0;url=./index.php?jpg=hei.jpg');
$file = $_GET['jpg'];
echo '<title>file:'.$file.'</title>';
$file = preg_replace("/[^a-zA-Z0-9.]+/","", $file);
$file = str_replace("config","_", $file);
$txt = base64_encode(file_get_contents($file));

echo "<img src='data:image/gif;base64,".$txt."'></img>";

/*
 * Can you find the flag file?
 *
 */

?>
```

代码大意为将传入jpg这个变量的参数进行了过滤，只允许大小写字母与数组，否则会被替换成空。将config这个字符替换成了"_"。
但是下一步我们该怎么做？发现注释中有信息说是用PhpStorm写的，PhpStorm有个问题，它存在于一个.idea的文件夹，里面存储了一些配置文件

> 构造URL访问
> http://16f8b7fc777444e38af9e234404cec95d069d121e5d7435a.game.ichunqiu.com/.idea/workspace.xml

在workspace.xml我们可看到 **fl3g_ichuqiu.php** ，这应该就是关键

```
fl3g_ichuqiu.php源码

<?php
/**
 * Created by PhpStorm.
 * Date: 2015/11/16
 * Time: 1:31
 */
error_reporting(E_ALL || ~E_NOTICE);
include('config.php');
function random($length, $chars = 'ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789abcdefghijklmnopqrstuvwxyz') {
    $hash = '';
    $max = strlen($chars) - 1;
    for($i = 0; $i < $length; $i++) {
        $hash .= $chars[mt_rand(0, $max)];
    }
    return $hash;
}

function encrypt($txt,$key){
    for($i=0;$i<strlen($txt);$i++){
        $tmp .= chr(ord($txt[$i])+10);
    }
    $txt = $tmp;
    $rnd=random(4);
    $key=md5($rnd.$key);
    $s=0;
    for($i=0;$i<strlen($txt);$i++){
        if($s == 32) $s = 0;
        $ttmp .= $txt[$i] ^ $key[++$s];
    }
    return base64_encode($rnd.$ttmp);
}
function decrypt($txt,$key){
    $txt=base64_decode($txt);
    $rnd = substr($txt,0,4);
    $txt = substr($txt,4);
    $key=md5($rnd.$key);

    $s=0;
    for($i=0;$i<strlen($txt);$i++){
        if($s == 32) $s = 0;
        $tmp .= $txt[$i]^$key[++$s];
    }
    for($i=0;$i<strlen($tmp);$i++){
        $tmp1 .= chr(ord($tmp[$i])-10);
    }
    return $tmp1;
}
$username = decrypt($_COOKIE['user'],$key);
if ($username == 'system'){
    echo $flag;
}else{
    setcookie('user',encrypt('guest',$key));
    echo "╮(╯▽╰)╭";
}
?>
```