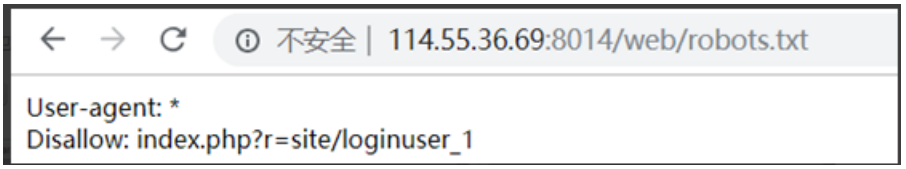
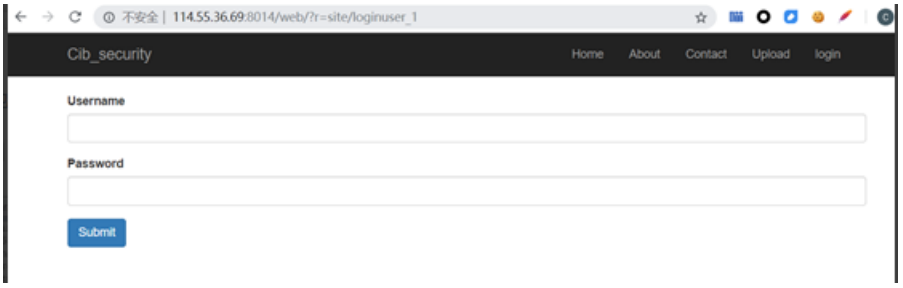
完整赛题参考连接：http://www.thecosmos.cn/index.php/archives/90/

秘密的系统

首先扫目录，发现robots.txt

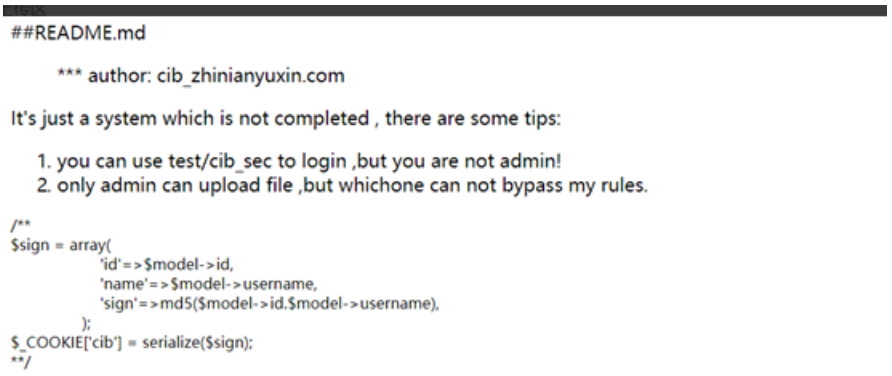




然后查看源代码，发现一段提示

```
24          <!--
25  *** author: cib_zhinianyuxin.com
26  *** code: github.com
27  -->
```

显然是要去github找源代码了(xswl还以为是恶心的代码审计)



就给了一个游客账号，和一小段代码，这段代码显然就是设置登陆的cookie了。先登录游客账号，发现cookie里面果然有一个cib，是一段经过serialize()序列化后的字符串，非字母数字部分都经过了url编码，解码后得到：

`a:3:{s:2:"id";i:2;s:4:"name";s:4:"test";s:4:"sign";s:32:"7cbab5cea99169139e7e6d8ff74ebb77";}`

根据上面给的代码，后面32位的就是md5后的id拼上用户名，

游客账号的id为2，显然admin的id为1。

然后生成1admin的md5

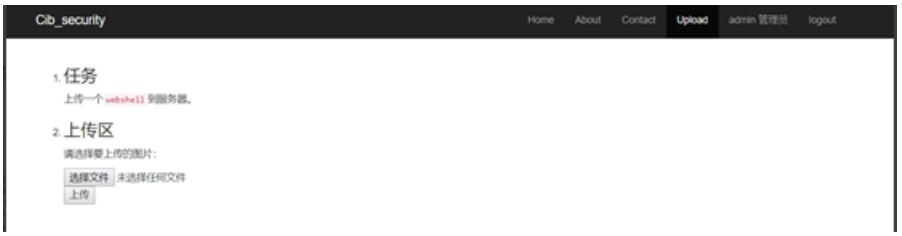
```php
<?php
    $id="1";
    $name="admin";
    $sign=md5($id.$name);
    print_r($sign);
?>
```

然后按照游客账号的cib构造admin的cib

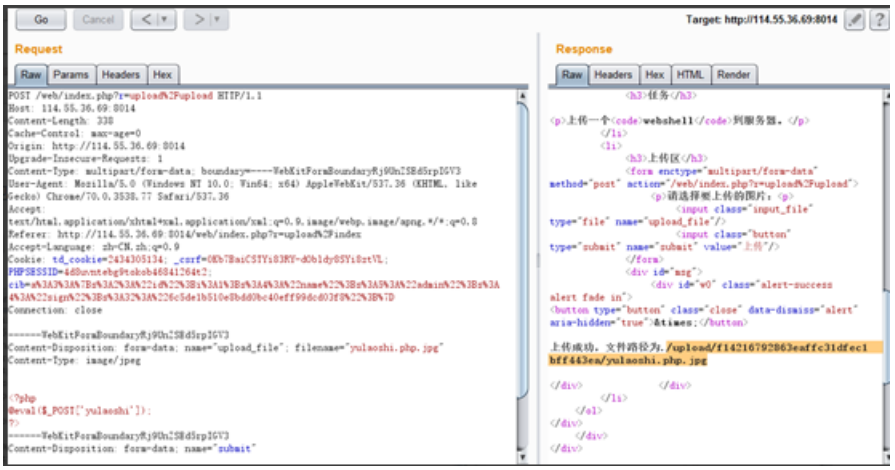
a:3:

{s:2:"id";i:1;s:4:"name";s:5:"admin";s:4:"sign";s:32:"6c5de1b510e8bdd0bc40eff99dcd03f8";}

url编码后加到cookie里，然后刷新页面，发现上传页面可以访问了。



这里也是用到了apache解析漏洞



直接上传后缀为.php.jpg的一句话木马就可以运行。