i春秋php代码审计-xss漏洞

原创

Tools-only 于 2017-04-02 11:51:57 发布

记录一下在i春秋的学习过程，感谢Virink老师，希望能出更多更好的作品。

审计代码：

如图，可以看到get_client_ip()这个函数是可能存在注入的，因为HTTP_CLIENT_IP和HTTP_X_FORWARDED_FOR是用户可控的。如果网站没有对xss进行防范，攻击者就可以构造一段js进行攻击。

进一步我们对get_client_ip()函数进行全局查找，发现出现在logCheck.php文件中，可以看到对其进行了sqlwaf过滤，去查看sqlwaf()函数，发现它并没有对xss的关键字以及<>进行过滤。接下来一行是一个sql语句，通过用户传递的ip进行查找。

对login_ip进行全局查找，可以看到在manageUser.php文件中，即当管理员执行用户管理操作时，就会显示login_ip。如果用户传递的ip为js代码，则在此处就会执行。

实施攻击：

构造Payload，在本地创建一个payload文件，其作用是在manageAdmin.php页面执行POST，添加一个管理员用户xss，密码为123456

使用Modify Headers修改X-Forwarded-For，在Value栏写入js语句，这里url没有加双引号，在浏览器端会自动识别添加。由于payload.js文件是写在本地，所以这里是127.0.0.1

点击Start开启，并使用普通用户进行登陆。

使用管理员账号登陆，并点击管理用户选项。此时页面就执行了我们构造的payload

我们使用payload中添加的xss用户进行登陆，可以看到，xss具有管理员权限。

xss并不是一个弹窗那么简单，也并不仅仅局限于留言板、论坛发表等位置，通过审计代码可以发现，在一些其他位置，只要用户可控，也是可能存在xss漏洞的。