渗透测试报告

通过渗透测试发现了以下漏洞：

前端

（1）注册界面存在存储型XSS

先利用burp进行抓包，正常的输入注册信息，然后将数据包拦截，修改数据包，加入XSS语句，如在邮件处修改成以下语句：aaa1<script>alert(XXS)<script>11356qq.com，结果：语句被执行，出现弹窗，显示XXS。

（2）注册界面存在SQL注入

（3）登录

万能密码可以成功登录，存在SQL注入

（4）我的个人资料处存在存储型XSS

在修改资料处，在电子邮件地址中输入<script>alert('xss')</script>语句，点击确认修改后。

结果：代码被执行，出现弹窗，当再次访问该页面，代码会再次执行，出现弹窗。

后台

(1)添加新会员处存在存储型XSS

在电子邮件中输入<script>alert('1111')</script>语句，点击提交。

结果：代码被执行，出现弹窗，显示1111，当再次访问该页面，代码会再次执行，出现弹窗。

(2)在广告管理的添加新广告处存在存储型XSS

在广告名称中输入<script>alert('8')</script>语句，点击提交

结果：代码被执行，出现弹窗，显示8，当再次访问该页面，代码会再次执行，出现弹窗。

（3）在友情链接的添加新链接处存在存储型XSS

在链接名称中输入<script>alert('xsssll')</script>语句，点击提交

结果：代码被执行，出现弹窗，显示xsssll，当再次访问该页面，代码会再次执行，出现弹窗。

（4）在电话广告位的添加新电话广告中存在存储型XSS

在显示名称中输入<script>alert('xssss')</script>语句，点击提交

结果：代码被执行，出现弹窗，显示xssss，当再次访问该页面，代码会再次执行，出现弹窗。

（5）发布本地新闻处存在存储型XSS漏洞，

在新闻标题中填写<script>alert('1')</script>，然后选择分类，输入新闻内容，点击提交。

结果：代码被执行，出现弹窗，显示1，当再次访问该页面，代码会再次执行，出现弹窗。

（6）在首页flash的添加新flash中存在反射型XSS

浏览并插入图片，在图片链接中填写<script>alert('11')</script>，然后点击提交。

结果：代码被执行，出现弹窗，显示11，当再次访问该页面，代码会再次执行，出现弹窗。

（7）在导航管理的添加新连接处存在存储型XSS

在导航名称中输入<script>alert('1233')</script>，输入导航链接，点击提交。

结果：代码被执行，出现弹窗，显示1233，当再次访问该页面，代码会再次执行，出现弹窗。

输入导航名称，在导航链接中输入<script>alert('1233')</script>，点击提交。

结果：代码被执行，出现弹窗，显示1233，当再次访问该页面，代码会再次执行，出现弹窗。

（8）在新闻分类的添加栏目中存在存储型XSS

在分类名称中输入<script>alert('1233')</script>，点击提交。

结果：代码被执行，出现弹窗，显示1233，当再次访问该页面，代码会再次执行，出现弹窗。

(9) 在系统组用户中存在存储型XSS

进入系统组用户，点击编辑，在电子邮件中输入<script>alert('123456')</script>，输入密码，点击提交。

结果：代码被执行，出现弹窗，显示123456，当再次访问该页面，代码会再次执行，出现弹窗。