

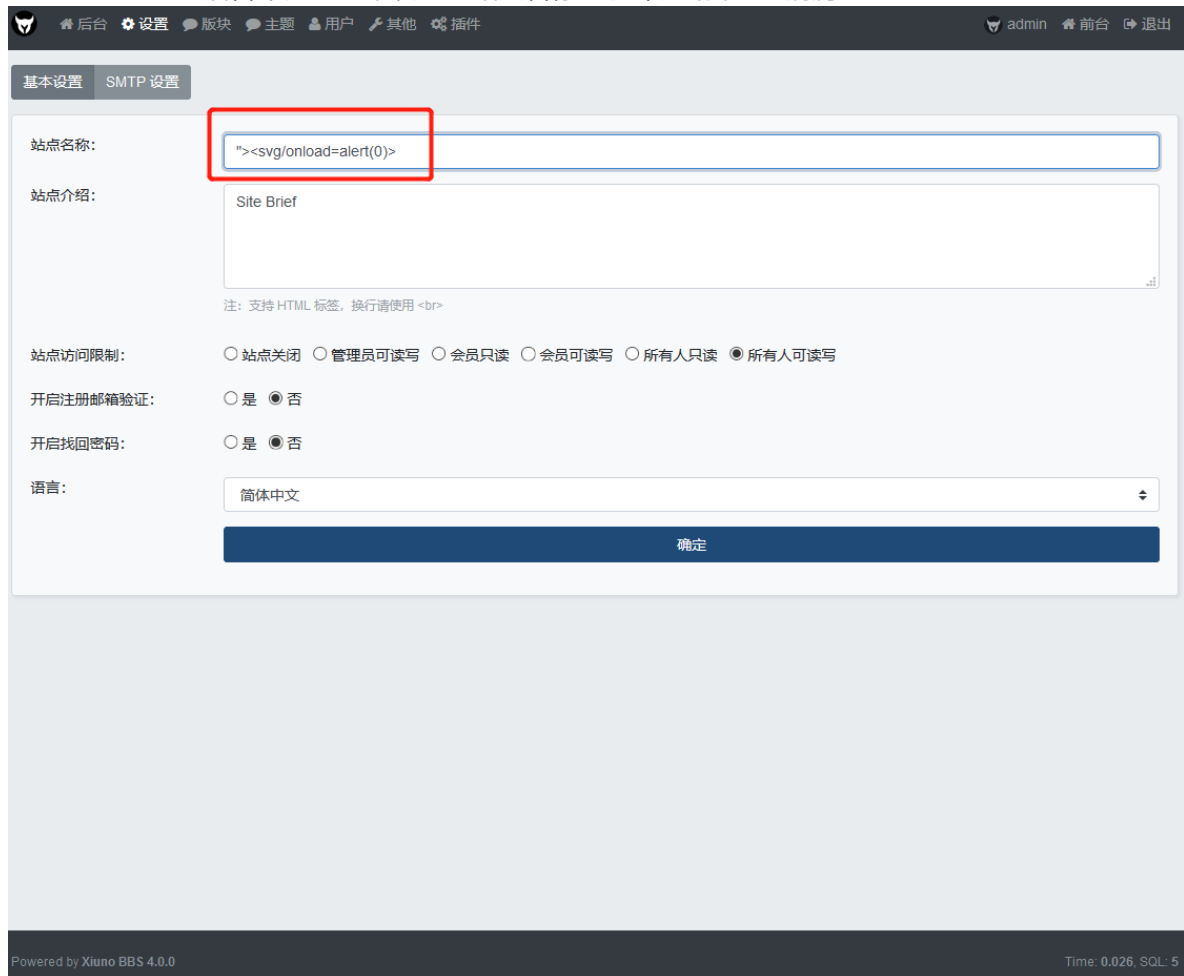
# Xiuno BBS 4.0.0 后台xss 漏洞

## 1、什么是 Xiuno BBS 4.0?

它是一款国产、小巧、稳定、支持在大数据量下仍然保持高负载能力的轻论坛。它只有 20 多个表，源代码压缩后 1M 左右，运行速度非常快，处理单次请求在 0.01 秒级别，在有 APC、Yac、XCache 的环境下可以跑到 0.00x 秒，对第三方类库依赖少，作者认为它就像一辆纯手工打造的法拉利，动力强劲，没有一丝赘肉，方便部署和维护，是一个非常好的二次开发的基石。

## 2、漏洞详情

Xiuno BBS 4.0.0 后台 设置->基本设置-> 站点名称 过滤不严 存在xss漏洞。



The screenshot shows the 'Basic Settings' (基本设置) tab in the Xiuno BBS 4.0.0 admin interface. The 'Site Name' (站点名称) field is highlighted with a red box and contains the payload `<svg/onload=alert(0)>`. The 'Site Introduction' (站点介绍) field contains 'Site Brief'. Below the introduction field, there is a note: '注: 支持 HTML 标签, 换行请使用 <br>'. The 'Access Restrictions' (站点访问限制) section has radio buttons for 'Site Closed', 'Admins Read/Write', 'Members Read Only', 'Members Read/Write', 'Everyone Read Only', and 'Everyone Read/Write' (selected). The 'Registration Email Verification' (开启注册邮箱验证) and 'Password Recovery' (开启找回密码) sections have radio buttons for 'Yes' and 'No' (selected). The 'Language' (语言) dropdown is set to 'Simplified Chinese'. A 'Confirm' (确定) button is at the bottom.

Powered by Xiuno BBS 4.0.0 Time: 0.026 SQL: 5