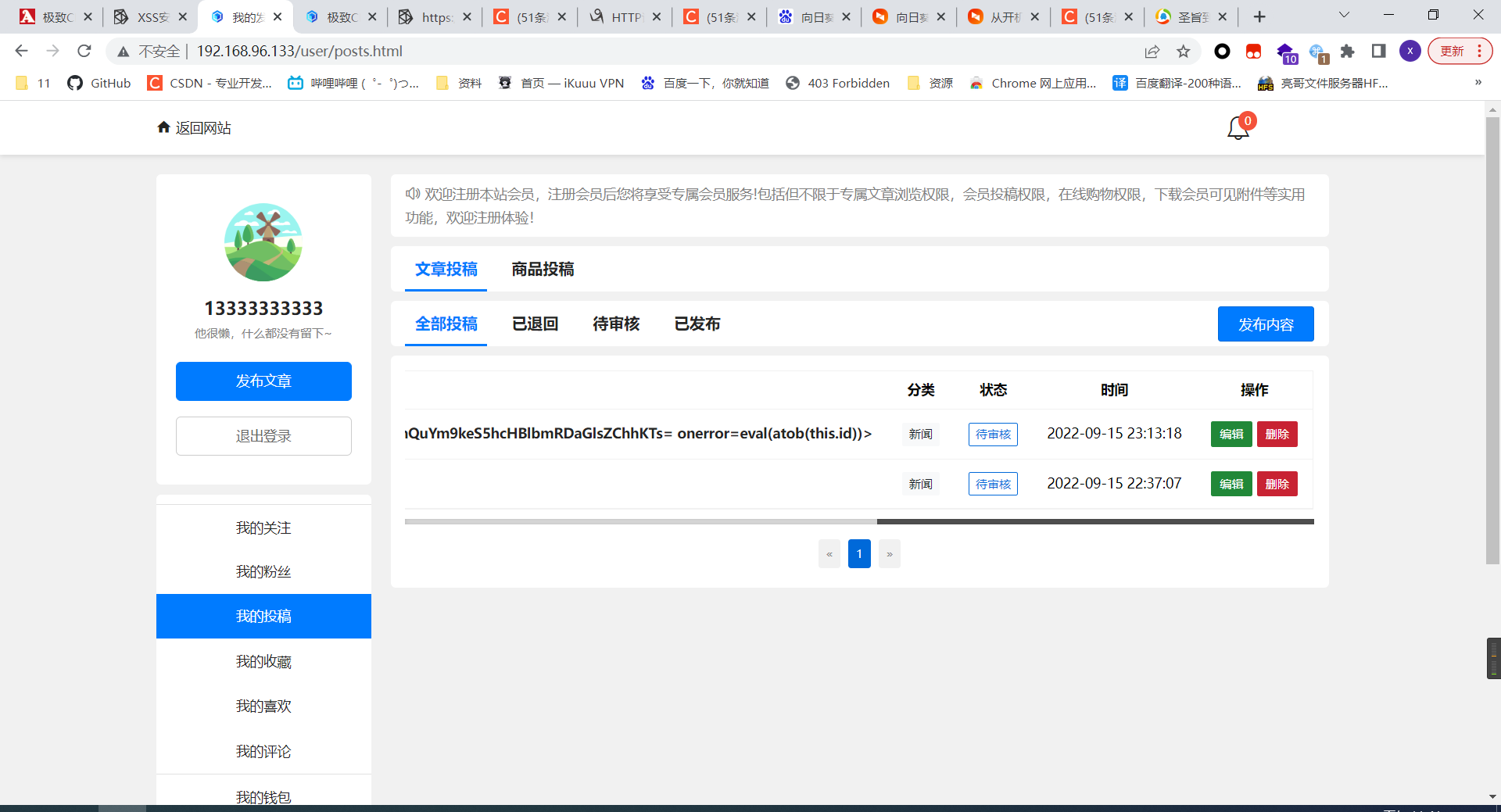
拿到1.7版本的jizhicms,在本地部署项目。寻找输入点，注册后发现可以发布文章



尝试发布文章，发现文章提交后需要审核，



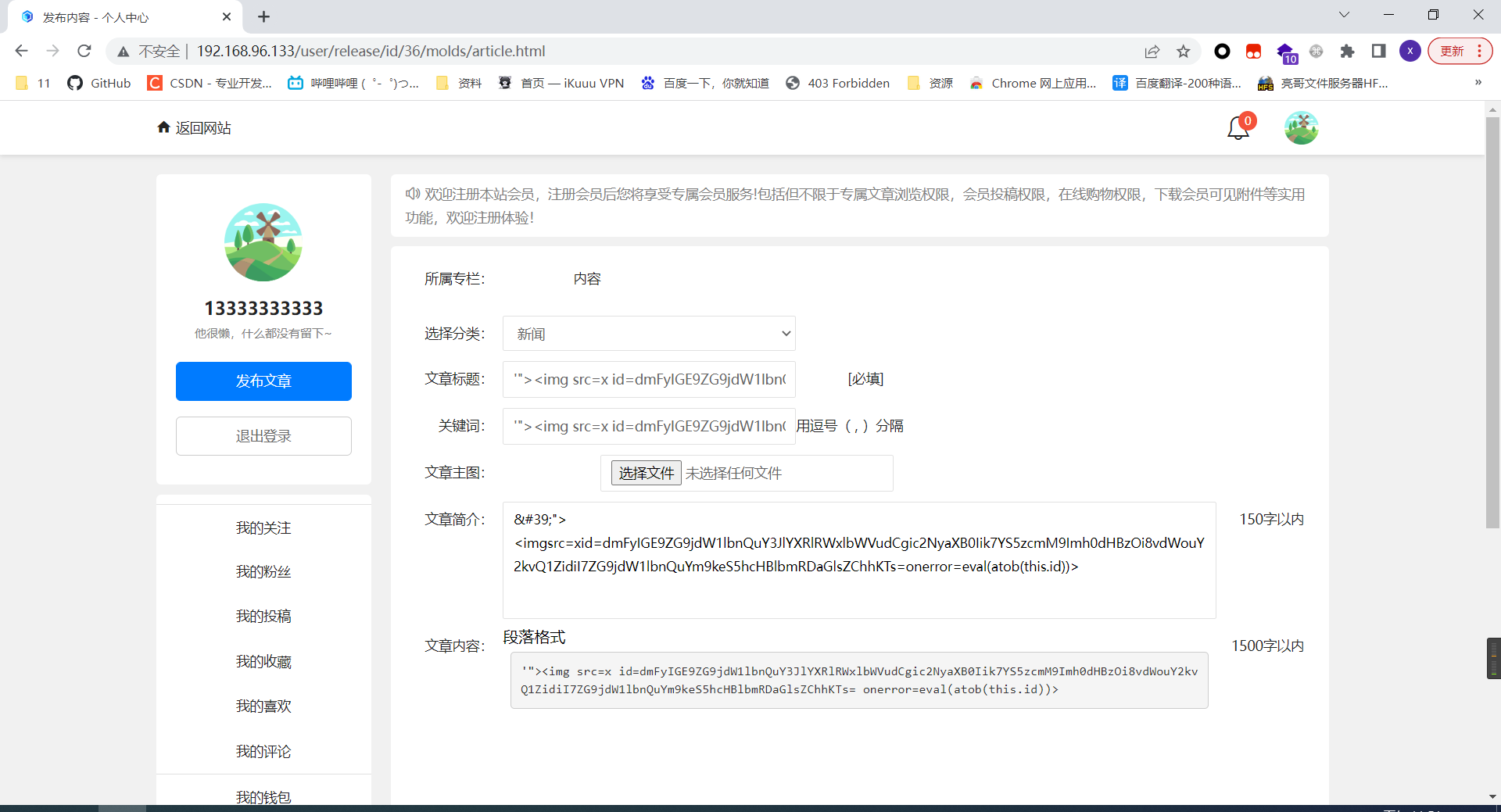
猜测可能存在存储型XSS，存储型XSS不需要闭合前后的标签或属性，因为一般都是输在p标签或者div或者h标签内，url除外（个人猜测），直接写入数据库，只需要判断是否有过滤即可

尝试直接写一个alert(1)

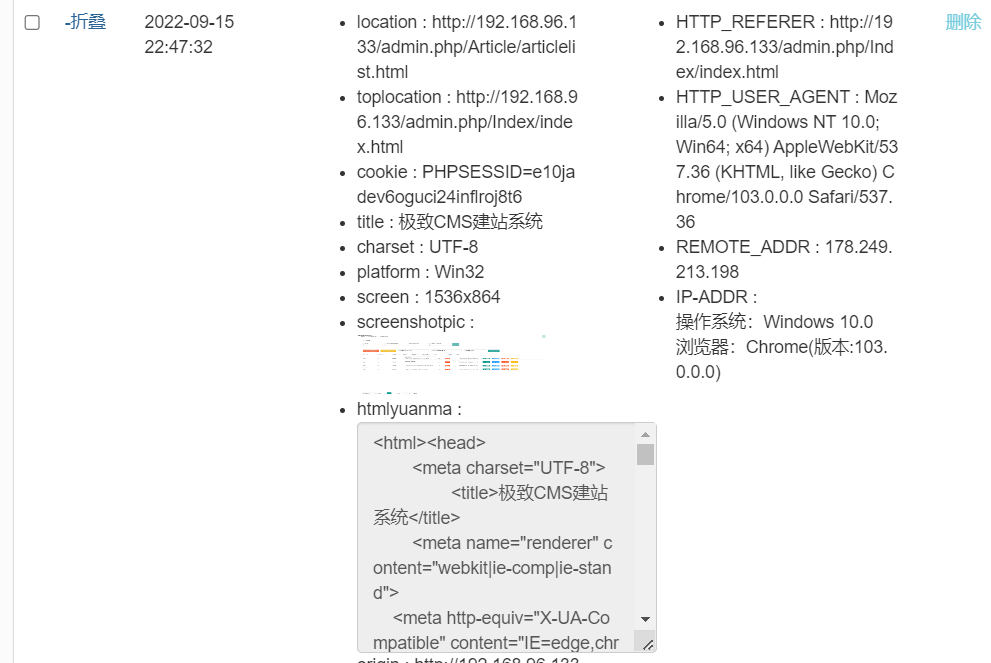


查看后台审核处，发现可以执行，确定为存储型XSS

直接传xss平台代码



后台管理员审核帖子后，成功拿到cookie



存在的问题：alert（）可以稳定触发，但是xss平台不能稳定收到cookie，每个浏览器访问后台审核后都可以收到一次，但是后面的审核就不会再收到，正在研究原因