模拟缺陷报告&验证记录

【高危】评论模块存储型XSS漏洞（未过滤`<script>`标签）
复现步骤：

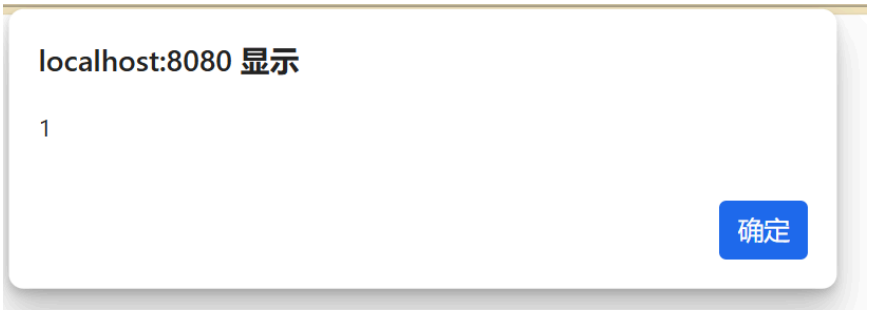
1. 登录WordPress后台
2. 进入任意文章页面
3. 评论框输入：`<script>alert(1)</script>`
4. 提交评论
5. 清除浏览器缓存或使用无痕模式访问该文章

预期结果：评论内容应作为纯文本显示，不应执行脚本

实际结果：页面加载后弹出警告框"1”

严重程度：高危（影响所有访问该文章的用户，可窃取Cookie）

截图证据：弹窗截图



浏览器开发者工具Console截图（显示执行了脚本）

```
<div class="wp-block-comment-content">
    <p>
        <script>
            alert(1)
        </script>
    </p>
</div>
```

环境信息：WordPress 6.4 + Docker + Edge（开发者工具）+MySQL8.0

2.模拟修复

安装WPcode插件，添加片段-自定义代码-PHP类型

```
add_filter('pre_comment_content', 'wp_kses_post');
```

3. 验证修复 （ Regression Testing ）

清除缓存:（WordPress缓存、浏览器缓存）

重新提交:同样的payload（`<script>alert(1)</script>`）

验证结果:评论显示为纯文本`<script>alert(1)</script>`，不再弹窗

检查数据库:phpMyAdmin查看wp_comments表，确认script标签被转义或过滤

回归测试:确保正常评论（无脚本）功能不受影响