New issue

Jump to bottom

存储型XSS漏洞1 #34

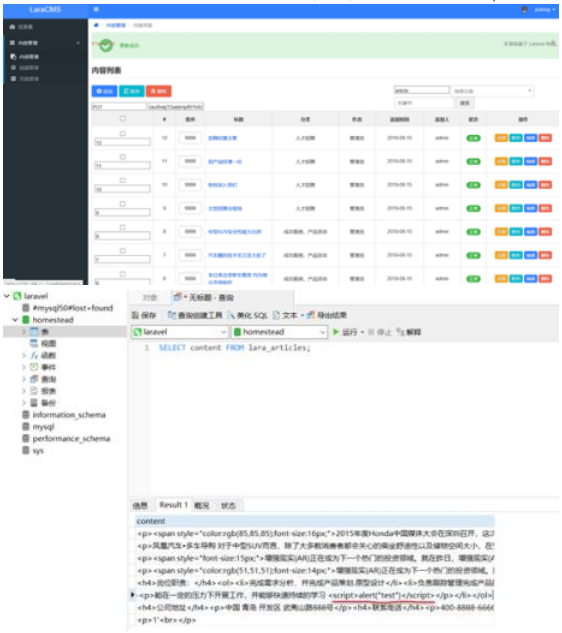
Open **Kinfedge** opened this issue on Aug 25, 2019 · 1 comment

Kinfedge commented on Aug 25, 2019

如图进入内容管理页面，查看内容列表，随意挑选一个内容进行编辑（测试中编辑“招聘结算主管”这一条）
在内容编辑处，输入任意脚本内容（测试输入alert("test")），同时选择输入内容点击插入链接，,并在链接处输入script，如上图。

然后完成编辑，点击提交按钮

使用相关工具，拦截提交的请求，并将提交的alert("test")的URL编码替换为<script>alert("test")</script>的URL编码



提交请求到服务器，此时对应脚本已写入数据库中。

任意用户访问该页面，都会执行插入的脚本，测试中则是弹出“test”提示框。
修复建议：对插入的超链接请求在服务器端也做编码和过滤。

wanglelecc commented on Aug 25, 2019 Owner

非常感谢提醒！

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants