arbitrary file read vulnerability #15

Open destinypwd opened this issue on Jan 10 · 0 comments

destinypwd commented on Jan 10

analysis

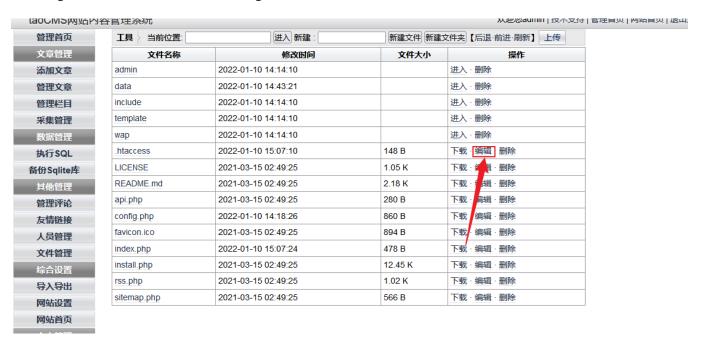
The location of the vulnerability is line 55 in \taocms\include\Model\File.php and we can see that the path parameter is passed directly to file_get_contents function without filtering

```
◄ ▶ admin.php
                                                 × Article.php
                                                                                                             × Config.php
                                                                                             × Template.php
 FOLDERS
 <?php
  ▼ admin
                                        class File{
                                            public $table;
   template
     admin.php
                                            public $tpl;
     index.php
                                            public $path;
  ▶ 🛅 data
                                            public $realpath
   ▼ 🚞 include
                                            function __construct($table,$id=0){
                                                 $this->table=$table;
    ▶ 🛅 Db
                                    8
                                                 $this->path=$_REQUEST['path'];
    ▼ 🚞 Model
                                   10
                                                 $this->realpath=SYS_ROOT.$this->path;
      Admin.php
                                   11
                                                 $this->tpl=new Template();
       Api.php
                                   12
       Article.php
                                   13
      Base.php
                                                 if($size > 1073741824) {
                                   14
       Category.php
                                   15
                                                     $size = round($size / 1073741824 * 100) / 100 . ' G';
       Cms.php
                                                 } elseif($size > 1048576) {
                                   16
       Comment.php
                                   17
                                                     $size = round($size / 1048576 * 100) / 100 . ' M';
       Config.php
                                                 } elseif($size > 1024) {
                                   18
       Datastore.php
                                                     $size = round($size / 1024 * 100) / 100 . ' K';
                                   19
      File.php
                                   20
                                                 } else {
       Frame.php
                                   21
                                                     $size = $size . ' B';
       ☐ Index.php
       Link.php
                                   23
                                                 return $size;
       ☐ Memcached.php
                                   24
       C Spider.php
                                   25
       Sql.php
                                   26
                                                 $path=$this->path?str_replace('//','/',$this->path.'/'):'';
       ☐ Template.php
                                   27
                                                 $fhandle = opendir($this->realpath);
       Upload.php
■ 17 characters selected
```

```
× Article.php
                                                                                    File.php
                                                                                                                × Config.php
 FOLDERS
 ▼ 🖮 taocms-3.0.2
                                    46
  ▼ 📄 admin
                                    47
    ▶ 🔳 template
                                                  unset($dirdb);
                                    48
                                    49
                                                  unset($filedb);
      admin.php
                                                  closedir($fhandle);
     index.php
                                    50
                                                  sort($dirdata);
  ▶ 🔳 data
                                    51
                                                  sort($filedata);
                                    52
   ▼ include
                                    53
    ▶ Db
                                    54
    ▼ 🖳 Model
                                    55
                                             function edit(){
       Admin.php
                                    56
                                                  $path=$this->path;
       Api.php
                                    57
                                                  $filedata=file_get_contents($this->realpath);
       Article.php
                                    58
                                                  include($this->tpl->myTpl('edit'.$this->table));
       Base.php
                                    59
       Category.php
                                    60
       Cms.php
                                    61
                                                  $path=$this->realpath;
                                                                                                      权限');
       Comment.php
                                    62
                                                  if(!is_writable($path))Base::showmessage('无册
       Config.php
                                    63
                                                  if(is_dir($path)){
       Datastore.php
                                    64
                                                      if(count(scandir(\$path))>2)
       🕒 File.php
                                                          Base::showmessage('目录非空, 不能删除');
                                    65
       Frame.php
                                                      rmdir($path);
                                    66
       Index.php
                                    67
                                                  }else{
       Link.php
                                                      unlink($path);
                                    68
       ☐ Memcached.php
                                    69
                                                  $info=pathinfo($this->path);
       Spider.php
                                    70
                                                  Base::showmessage('删除成功','admin.php?action=file&ctrl=lists&path='.$info['
       Sql.php
                                    71
       Template.php
                                                      dirname']);
                                    72
       Upload.php
Line 60, Column 20
```

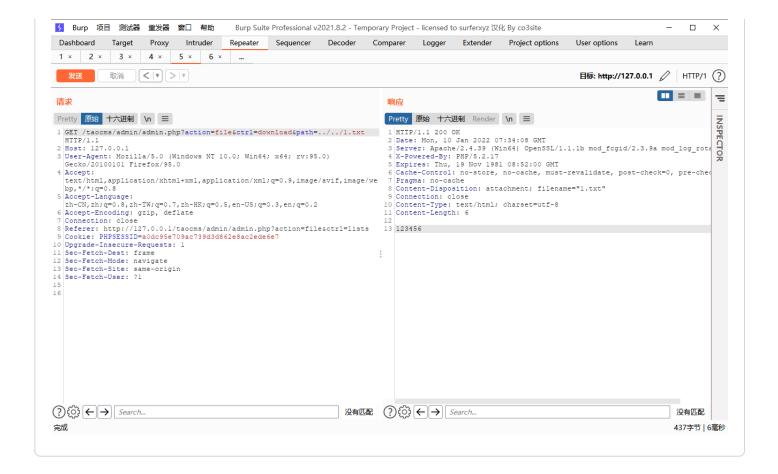
poc

After login as admin, Enter the file management interface and edit function



Get packets using brup

Any file can be read after changing the path parameter



Ass	11	nr	٦Δ	00	۰
മാ	11	41	10	C	į

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

