目录

一、题目

1、源码

```php
class TokenStorage {
    public function performAction($action, $data) {
        switch ($action) {
            case 'create':
                $this->createToken($data);
                break;
            case 'delete':
                $this->clearToken($data);
                break;
            default:
                throw new Exception('Unknown action');
        }
    }
    public function createToken($seed) {
        $token = md5($seed);
        file_put_contents('/tmp/tokens/' . $token, '...data');
    }
    public function clearToken($token) {
        $file = preg_replace("/[^a-z.-_]/", "", $token);
        unlink('/tmp/tokens/' . $file);
    }
}
$storage = new TokenStorage();
$storage->performAction($_GET['action'], $_GET['data']);
```

2、知识点

知识点	说明
file_put_contents()	把一个字符串写入文件中

3、解读

1）实例化TokenStorage()对象，调用该对象中的performAction()函数，接收GET方法传入的action和data作为参数。
2）第2行：action为'create'时，调用createToken()函数，并使用data的值作为参数。
3）第14行：createToken()函数中，通过md5对data的值进行加密，拼接到指定目录中生成文件。
4）第7行，action为'delete'时，调用clearToken()函数，并使用data的值作为参数。
5）第18行，clearToken()函数中，对data的进行过滤特殊字符，并使用unlink()函数删除该文件
6）第10行：如果action的值不是 'create'或者'delete'，就抛出异常提示

4、分析

1）第19行，preg_replace()函数对 a-z、.-_之间的字符进行限制
2）但是没有对目录穿越符../进行过滤，导致可以造成路径穿越，实现任意文件删除。

5、利用

```
action=delete&data=../../config.php
```

二、CMS

1、源码-WeEngine0.8

web/source/site/category.ctrl.php

```php
elseif ($do == 'delete') {
    load()->func('file');
    $id = intval($_GPC['id']);
    $category = pdo_fetch("SELECT id, parentid, nid FROM ".tablename('site_category')
                ." WHERE id = '$id'");
    if (empty($category)) {
        message('抱歉，分类不存在或是已经被删除！', url('site/category/display'), 'error');
    }
    $navs = pdo_fetchall("SELECT icon, id FROM ".tablename('site_nav')." WHERE id IN
            (SELECT nid FROM ".tablename('site_category')." WHERE id = {$id} OR
            parentid = '$id')", array(), 'id');
    if (!empty($navs)) {
        foreach ($navs as $row) {
            file_delete($row['icon']);
        }
        pdo_query("DELETE FROM ".tablename('site_nav')." WHERE id IN (".implode(',',
                array_keys($navs)).")");
    }
    pdo_delete('site_category', array('id' => $id, 'parentid' => $id), 'OR');
    message('分类删除成功！', url('site/category'), 'success');
}
```

framework/function/file.func.php

```php
function file_delete($file) {
    if (empty($file)) {
        return FALSE;
    }
    if (file_exists($file)) {
        @unlink($file);
    }
    if (file_exists(ATTACHMENT_ROOT . '/' . $file)) {
        @unlink(ATTACHMENT_ROOT . '/' . $file);
    }
    return TRUE;
}
```

web/source/site/category/ctrl.php

```php
if (!empty($navs)) {
    foreach ($navs as $row) {
        file_delete($row['icon']);
    }
    pdo_query("DELETE FROM ".tablename('site_nav')." WHERE id IN (".implode(',',
                array_keys($navs)).")");
}
```

```
$navs = pdo_fetchall("SELECT icon, id FROM ".tablename('site_nav')." WHERE id IN (SELECT nid FROM ".tablename('site_category')." WHERE id = {$id} OR parentid = '$id')", array(), 'id');
```

```php
if(!empty($nav_exist)) {
    pdo_update('site_nav', $nav,
                array('id' => $category['nid'], 'uniacid' => $_W['uniacid']));
} else {
    pdo_insert('site_nav', $nav);
    $nid = pdo_insertid();
    $data['nid'] = $nid;
}
```

```php
$data['icontype'] = intval($_GPC['icontype']);
......
$isnav = intval($_GPC['isnav']);
if($isnav) {
    $nav = array(
        'uniacid' => $_W['uniacid'],
        'categoryid' => $id,
        'displayorder' => $_GPC['displayorder'],
        'name' => $_GPC['cname'],
        'description' => $_GPC['description'],
        'url' =>
        "./index.php?c=site&a=site&cid={$category['id']}&i={$_W['uniacid']}",
        'status' => 1,
        'position' => 1,
        'multiid' => intval($_GPC['multiid']),
    );
    if ($data['icontype'] == 1) {
        ......
    } else {
        $nav['css'] = '';
        $nav['icon'] = $_GPC['iconfile'];
    }
```

2、知识点

知识点	说明
intval()	用于获取变量的整数值
implode()	返回一个由数组元素组合成的字符串
array_keys()	返回包含数组中所有键名的一个新数组

3、解读

1）图1，定义了一个文件删除的操作，判断是否存在需要删除的文件，如果存在，则进入12行的判断，调用函数`file_delete()`进行删除。

2）图2，跟进函数`file_delete()`到`file.func.php`中，可以看到这里的`file_delete()`函数对`$file`进行判断，存在即删除，但是这里没有并没有对`$file`的值进行过滤。

3）图3，通过`file_delete()`被调用的其他位置，跟进`$file`对应的值到`category.ctrl.php`中，可以看到这里`$file`对应数据库中就是`$row['icon']`的值，并且该值来自变量`$navs`。

4）代码块，在当前文件中跟进到变量`$navs`的定义，可以看到`$navs`变量是从数据库`site_nav`表中取出，包含了`icon`和`id`两个字段。

5）图4，在当前文件中跟进`'site_nav'`表，可以看到表中对应的数据来自变量`$nav`。

6）图5，第21行，可以看到`$nav['icon']`从`$_GPC['iconfile']`中得到。

4、分析

1）`$nav['icon']`变量的值可控。

2）程序没有对值进行控制，直接传入了`file_delete()`函数，导致文件删除漏洞。

5、利用

1) 访问 http://xxx.xxx.xxx.xxx/WeEngine/web/index.php?c=account&a=display，点击管理公众号。
2) 点击添加文章分类，输入要删除文件的路径 ../xx.txt 作为分类名。
3) 添加成功后，点击删除分类，该文件成功被删除。

6、修复方案

1) 过滤$row['icon']中../等目录穿越符号
2) 定义$row['icon']必须是文件名称，而非路径

7、参考链接

https://github.com/hongriSec/PHP-Audit-Labs/blob/master/Part1/Day6/files/README.md