

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**



```
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

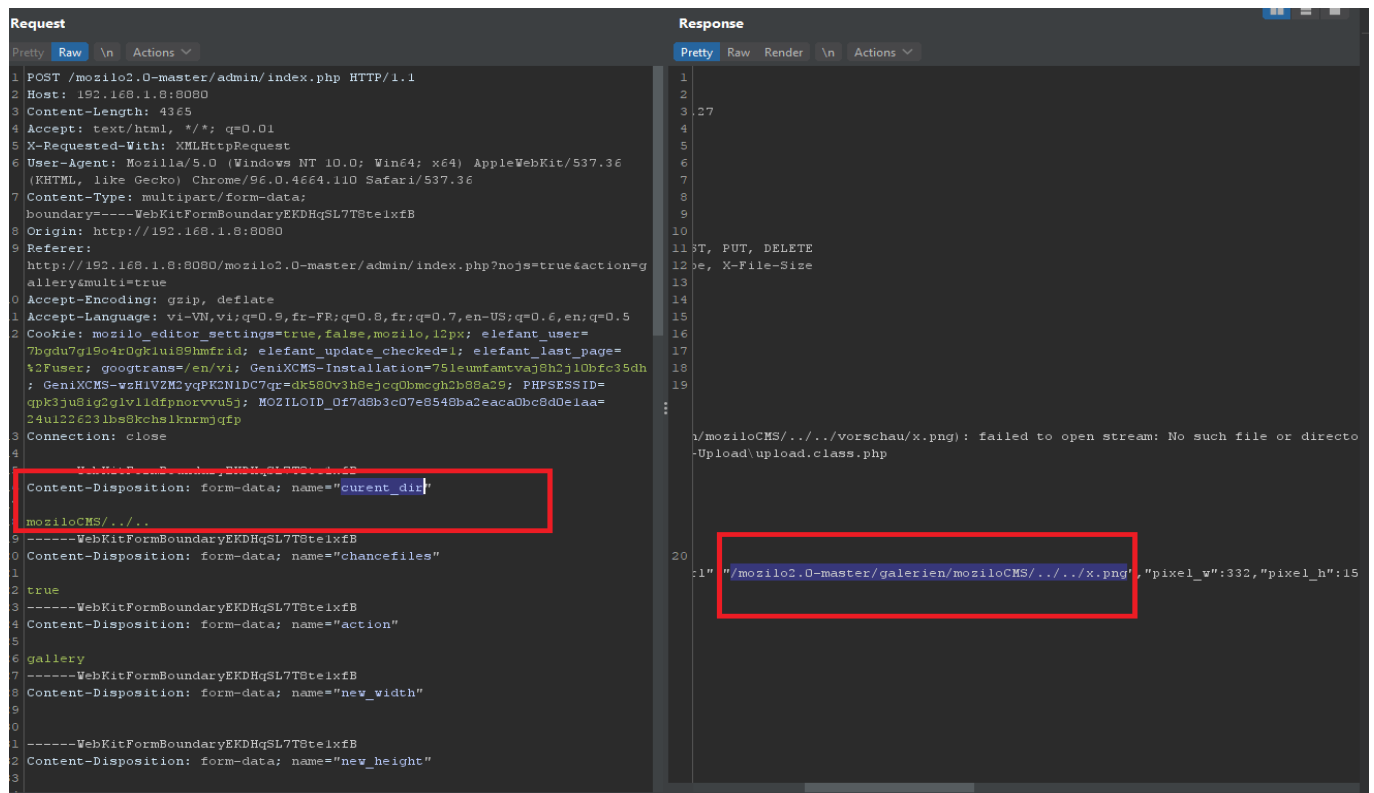
```
https://github.com/moziloDasEinsteigerCMS/mozilo2.0/blob/master/cms/DefaultFunc.php#L88L112
CourseSite - D... pentest web B Download Free Onli... Lập Trình Không Kh... Programming and... - Quản trị effbot.org F19_CỘNG ĐỒNG F...

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 B 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 % a
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 }
```



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			
Js	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		
	install.php	1/6/2022 4:20 PM	PHP File	42 KB		
is	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		
Js	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		
	update.php	1/6/2022 4:20 PM	PHP File	28 KB		
c (C:)	x.png	1/9/2022 12:28 AM	PNG File	4 KB		
c (E:)						