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:

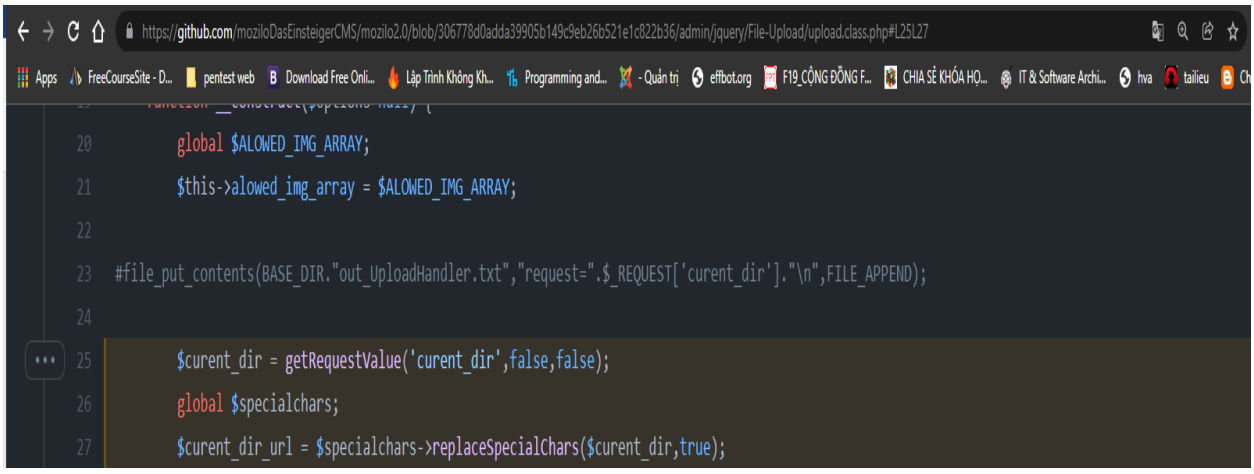
+ /admin/jquery/File-Upload/upload.class.php

+ / cms/DefaultFunc.php

+ /cms/SpecialChars.php

+ Proof of concept (POC):

+ Upload.class.php



+ **DefaultFunc.php**

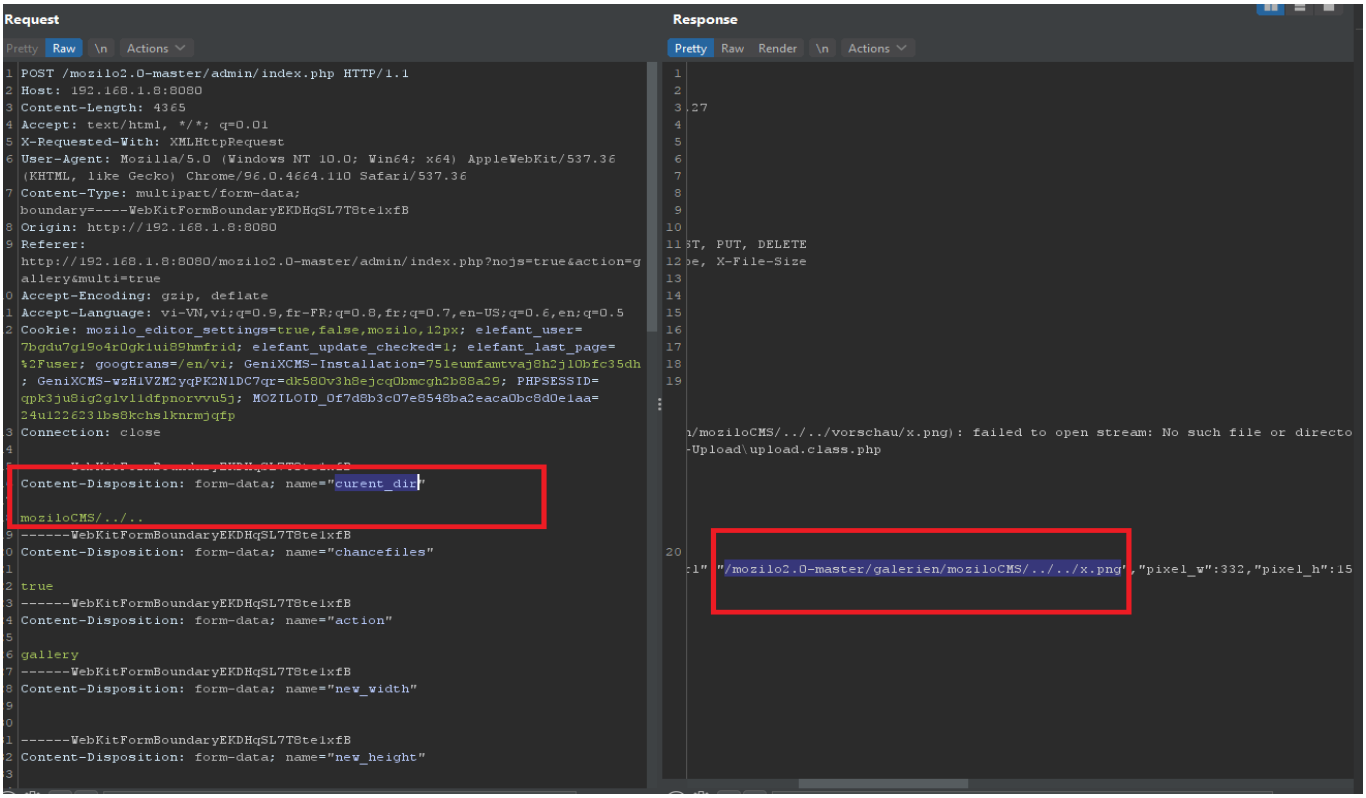
https://github.com/moziloDasEinsteigerCMS/mozilo2.0/blob/master/cms/DefaultFunc.php#L88L112

```php
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

```php
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