

# HOW TO SECURE YOUR



Author: Viska Agasi a.k.a vhyVizz

Contact: vizz91agasi@gmail.com

Home: <http://www.facebook.com/vizkaaa> & <http://www.twitter.com/vhyVizz>

History:

- Introduce
- Analysis The c0de
- Patching / securing
- Reference
- Great and Thanks

## 0x01: INTRODUCE

What is FCKEditor ? FCKEditor is a browser based WYSIWYG editor, which brings to the Web common editing features found on desktop editing applications. It's fully accessible, semantics and standards aware.

## 0x02: Analysis The c0de

Mungkin semua sudah pada mengenal dan mengetahui Jenis dan type kelemahan or lobang keamanan pada web aplikasi yg satu ini.. Ya, FCKeditor Memiliki Vulnerability atau kelemahan atau bug pada session upload nya.

Vulnerability ini pertama sekali di temukan oleh rgod dari altavista melalui tehnic RCE (Remote Command Execution), Dan Belakangan lebih di populer kan oleh eidelweiss dan team security yg di kenal dengan sebutan `pentesters.ir` dengan eksploitasi remote file/ shell upload nya.

## Letak kesalahan atau vulnerability c0de nya bias kita lihat pada configuration file nya:

```
/filemanager/connectors/php/config.php

global $Config ;

// SECURITY: You must explicitly enable this "connector". (Set it to "true").
// WARNING: don't just set "$Config['Enabled'] = true ;", you must be sure
that only authenticated users can access this file or use some kind of
session checking.
$Config['Enabled'] = true ; // <= 1

---

// Path to user files relative to the document root.
$Config['UserFilesPath'] = '/userfiles/' ; // <= here is the path of
attacker file or shell backdoor will be placed.

// following setting enabled.
$Config['ForceSingleExtension'] = true ; //

$Config['AllowedExtensions']['File'] = array('7z', 'aiff', 'asf', 'avi',
'bmp', 'csv', 'doc', 'fla', 'flv', 'gif', 'gz', 'gzip', 'jpeg', 'jpg', 'mid',
'mov', 'mp3', 'mp4', 'mpc', 'mpeg', 'mpg', 'ods', 'odt', 'pdf', 'png', 'ppt',
'pxd', 'qt', 'ram', 'rar', 'rm', 'rmi', 'rmvb', 'rtf', 'sdc', 'sitd', 'swf',
'sxc', 'sxw', 'tar', 'tgz', 'tif', 'tiff', 'txt', 'vsd', 'wav', 'wma', 'wmv',
'xls', 'xml', 'zip') ; // <= 3
```

**Seperti yg kita lihat Dengan konfigurasi default or standart seperti di atas , an attacker might be able to upload arbitrary files containing malicious PHP code due to multiple file extensions isn't properly checked. Dan vulnerability c0de lain dapat kita temukan pada file**

```
/filemanager/connectors/upload.php

*/

require('./config.php');
require('./util.php');
require('./io.php');
require('./commands.php');
require('./phpcompat.php');

function SendError( $number, $text )
{
```

```

SendUploadResults( $number, " ", $text );
}

// Check if this uploader has been enabled.
if ( !$Config['Enabled'] )
SendUploadResults( '1', " ", 'This file uploader is disabled. Please check the
"editor/filemanager/connectors/php/config.php" file' );

$SqlCommand = 'QuickUpload' ;

// The file type (from the QueryString, by default 'File').
$styleType = isset( $_GET['Type'] ) ? $_GET['Type'] : 'File' ;

$CurrentFolder = GetCurrentFolder() ;

// Is enabled the upload?
if ( !IsAllowedCommand( $SqlCommand ) )
SendUploadResults( '1', " ", 'The "" . $SqlCommand . "" command isn\'t allowed' );

// Check if it is an allowed type.
if ( !IsAllowedType( $styleType ) )
SendUploadResults( 1, " ", 'Invalid type specified' );

FileUpload( $styleType, $CurrentFolder, $SqlCommand )

?>

```

**Seperti yg kita lihat, tidak ada nya session yg mengharuskan kita untuk login or mempunyai access untuk dapat melakukan upload file ke pada server.**

**Banyak cara yg bisa di lakukan untuk melakukan eksploitasi dengan vulnerability ini.Salah satu nya ialah FCKEditor Menyediakan sebuah file untuk melakukan test upload dan langsung menyimpan ke dalam server tanpa melakukan verifikasi atau pengecekan jenis file yg di upload terlebih dahulu.**

**File yg saya maksud di sini ialah pada link berikut:**

`/fckeditor/editor/filemanager/connectors/uploadtest.html`

`/fckeditor/editor/filemanager/connectors/test.html`

Seorang Attacker bisa langsung melakukan penetrasi dengan mengupload sebuah file baik itu sebuah text atau file html dan tidak menutup kemungkinan untuk mengupload file image yg di ijinan oleh pengaturan `$Config['AllowedExtensions']['File']`.

Dan tanpa di sadari file images tersebut bisa berisikan file script shell php, Atau Para Attacker juga bisa menggunakan Trick dengan mengupload sebuah file .htaccess terlebih dahulu untuk dapat langsung mengupload file php seperti berikut:

```
<FilesMatch "_php.gif">
SetHandler application/x-httpd-php
</FilesMatch>
```

Banyak Cara lain yg bisa di lakukan untuk mengesekusi or mengexploitasi vulnerability pada FCKeditor ini. Salah Satu nya yg sangat Familiar ilah dengan menggunakan Metode Remote Comment Execution or Remote Shell Upload Yg Di populer kan oleh eidelweiss .

<http://www.exploit-db.com/exploits/12506>

<http://www.exploit-db.com/exploits/12376/>

### **0x03: Patching / Securing**

Setelah Kita Menganalisis c0de or Vulnerability nya lantas pasti kita akan bertanya Bagaimana cara Pengamanan nya ?

Yach, Pastinya Setiap Ada Kelemahan or lubang harus di perbaiki , di cegah atau pun di tambal (Bukan Tambal Ban loch :D). Berikut Ada Beberapa Tips and Trick Bagaimana untuk Mencegah Vulnerability Pada FCKEditor.

#### **1. Delete default uploader tester file on fckeditor**

```
/fckeditor/editor/filemanager/connectors/uploadtest.html
```

```
/fckeditor/editor/filemanager/connectors/test.html
```

#### **2. Creat Session authentication or user session based auth at the top of your upload.php**

example:

```
session_start();
$level=$_SESSION['level'];
if($level!="admin") { die();}
```

### 3. Change the c0de in configuration.php of your fckeditor file

```
global $Config ;

// SECURITY: You must explicitly enable this "connector". (Set it to "true").
// WARNING: don't just set "$Config['Enabled'] = true ;", you must be sure
that only
//      authenticated users can access this file or use some kind of session
checking.
$Config['Enabled'] = true ; // <= 1 This one(Change to False)
```

**Menjadi :** \$Config['Enabled'] = false ;

#### 0x04: Reference

- [www.google.com](http://www.google.com)
- <http://en.wikipedia.org/wiki/CKEditor>
- <http://www.exploit-db.com/exploits/12506>
- <http://www.exploit-db.com/exploits/17644/>

#### 0x05: Regards and Thanks

- Randy Arios a.k.a eidelweiss
- Devilz0de Forum