

Injection hack detection method - PHP Code

A good working Injection hack detection method provided by Ez via StopBadWare Forum

The script is brutally simple because we needed a quick fix. If the hacks recur I will make it smarter. Its only purpose is to tell me if a critical file (such as index.php) has changed size. I assume that injection hacks change the file size, as they did on our site.

A smarter script would compare file mod times with a database record. This would require a more complex script because it would have to store legitimate mod timestamps and depend on a human (unless more complex still, including the IP or http login etc.).

Operating scenario --

- 1.) Hacker injects code, increasing the file size.
- 2.) Next request to serve the home page (or other page of your choice) triggers the detector, which compares current file size with that for archived original.
- 3.) Detector sends email with file mod timestamp to webmaster.
- 4.) Script replaces hacked file with copy of an archived original, exits.

The webmaster needs to keep track of the most recent authorized file modifications (presumably by the webmaster). The email includes the timestamp of the over-size file's mod time. The system admin (or tech

support) uses this timestamp to trace the hack through the server log and identify the mode of entry.

To get fancier, you could scan all files in a directory for the mod time (example, using the PHP filemtime() function), comparing with a database record of legitimate mod timestamps.

Anyhow, here's the index file size script. I keep utility functions in a separate file named "func.inc" so it needs to load first. But this isn't necessary. Then the function compares the size of the file that usually gets hacked (such as index.php) and compares it with a reference copy (x_index.php) in a secure directory ("refz"). Of course, you can also loop through a list of filenames that are popular hack targets. The function can return the file write result, but I don't use it.

```
/* top of index.php, after DOCTYPE declaration */
```

```
function hackDet () {
```

```
$stst = "";
```

```
$gzt = "index.php";
```

```
$stat = stat($gzt);
$gzt2 = "refz/x_" . $gzt;
$rstat = stat($gzt2);
$ref = $rstat[size];
$rtim = $_SERVER['REQUEST_TIME'];
$rtim2 = date("F d Y H:i:s.", $rtim) . " Eastern";
$mtim = filemtime($gzt);
$mtim2 = date("F d Y H:i:s.", $mtim) . " Eastern";

if ($stat[size] <> $ref)
{
$fw = "index.php";
$hak = file_get_contents($fw);

$msg = "$gzt has $stat[size] bytes and not $ref as it should.\n\n";
$msg .= "FILE MOD TIME $mtim: $mtim2\n";
$msg .= "REQUEST_TIME $rtim: $rtim2\n\n";
$msg .= "=====\n\n";
$msg .= $hak;

$msg = wordwrap($msg, 70);
mail('yourn...@yourdomain.com', 'HACK ALERT', $msg);

$fr = "refz/x_index.php";
$str = file_get_contents($fr);
$stst = file_put_contents($fw, $str);
}
return $stst;
}

$stst = hackDet(); // calls the hack detection function

?>
```