PHPit hacked? Never!

By Dennis Pallett

Update: The "hacker" responds! More at page 2.

It seems someone has managed to exploit a bug in my CMS code to allow himself access to the CMS. I already knew about this bug a few weeks ago, but I just never fixed it. Call it lazy, or no time, but it did mean there was a bug. I didn't worry about it too much, because very little can be done from the CMS. Only this website goes down (for a short while), and I get database backups every 24 hours (it's automatic!) so there is hardly any data loss.

Restoring PHPit didn't take very long either, and I had it back online within about 20 minutes. Of course, the bug has been fixed now, and no 'hacks' can occur anymore.

The hacker did claim to have "root access to my server", which is completely false. Heck, I don't even have root access myself, because I'm on a shared server. So the hacker definately didn't have root access, or any access at all to be honest. He/she could only access the CMS, which has very little power.

Of course the hacker had to slander me a bit. I don't know whether you read it, but the hacker claimed that I though I was a great PHP coder, and he seemed to disagree. If the hacker is reading this: I don't think I'm a fantastic PHP coder, but I'm not a bad one either. I'm still going through the learning process, and at the moment I'm really trying to get a grip of PHP patterns. At least I spend my time useful, instead of destroying other websites.

Having said that, now is probably a good time to point to some PHP Security articles:

- PHP: Security by example (Flash)
- PHP Security Mistakes
- ONLamp: PHP Security, Part 1
- ONLamp: Ten Security Checks for PHP, Part 1
- PHP Security Guide
- On the Security of PHP, Part 1

The "hacker" has contacted me. He had not real malicious intent, and he has told me about the bug. To be honest, I made a really stupid mistake, involving highlight_file(). To demonstrate code files in articles, I use a viewsource file (located at http://phpit.net/viewsource.php?url=*some path*.). I actually took counter-measures to prevent anyone from opening files that shouldn't be opened, but I missed one critical thing.

I restricted the script to only open files from the demo directory, using the following code:

```
if (substr($url, , strlen("/demo")) == "/demo") {
        highlight_file ($begin . $url);
```

```
 } else {
        die ("Security Alert! Breach has been logged for review (IP Address: " . $_SERVER['REMOTE_ADDR'] .
").");
 }
```

Who can spot the HUGE security bug in that one? I didn't, until the hacker showed me (and I can't believe I forgot about it).

The problem is that the path can include '..', which means go a directory up. Do something like http://phpit.net/viewsource.php?url=/demo/.../.../.../.../etc/passwd and it actually shows the .passwd file. Gasp! (it's fixed now, of course)

Thankfully, the hacker wasn't really a hacker, and contacted me through the contact form to show me my error. Heck, he even had a look at the viewsource.php file, to suggest a fix. So, to the hacker: no hard feelings, and thanks for pointing out my error. Don't worry about any legal action or nonsense like that. I haven't lost any money or time, so I'm not angry or mad.

Lesson learnt from this? Security is hard, *really* hard. I thought I had covered all my bases, but there was still a way in. In the near future, I will probably write a PHP security article that has a look at all kinds of different situations, with some good examples and code. Stay tuned!

About this PDF