

How to protect your site

Actually, it has become a true sport for webservers to find flaws in a website and then exploit them. But every now and then, when opening new sites, we may find ourselves in front of an unknown index and a completely devastated website.

**What is « defaced » and « owned by »?**

This code means that your site has been defaced and added to a list of digital attacks.

A hacker has recovered information from a flaw and is now scanning the internet searching to exploit sites concerning this flaw.

The attack does not directly attack you or the site, but rather the security loophole.

**How can they do this ?**

By using these sites that webmasters use for website security and information on flaws, bugs and bad program configurations, explorers and databases like SQL. Ignoring or under estimating a problem often produces large hacker attacks. One of the most sought after is which shows details on : flaws, the means of exploitation, and most of all it shows the immediate solution or patch for fixing the problem.

**Admin.php**

NoHackAllowed :: the security problems on admin.php

**How to protect**

You must also consult other websites which distributes this type of information and gives you information specific to your site right away.

Protect the pages that are not designated or published with .htaccess. Do not choose easy to find/solve passwords and avoid calling your administration interface « admin.php ».

Unless you want your databases shut down and no longer available. If you use open source programs such as: phpnuke, xoops, and phpbb make sure you frequently and regularly check the site, the development team, and the forums. Inform yourself on updates and most of all on the informations which we send out regularly through the mailing lists.