



Computer experts from more than 30 organizations worldwide have released a consensus list of the 25 most dangerous programming errors that lead to security breaches and that enable cyber espionage and cyber crime.

The impact of these errors is far reaching. Just two of them led to more than 1.5 million web site security breaches during 2008

Secure Hosting

The security of the hosting environment for all Ninja Hosting customers is very, very important to us.

Ninja Hosting was set up to provide a 'premium' hosting environment for clients who wanted much more than the 'Unlimited' space/bandwidth hosting offers. We're not promising something we can't deliver. Hosting in those types of environments is often not optimised for Joomla and other CMS systems and can be plainly insecure.

The Ninja Hosting server environment has a number of measures in place to promote security; from an effective firewall to anti-virus scanning of incoming e-mail.

Improved Security and Client Freedom

Implementing higher security in a hosting server environment does not mean more restrictions on the user, in fact the opposite is the case. File and directory permissions are optimised for security which means that none of our Joomla customers, for instance, will experience problems with the 'permission errors' that are common on other hosts.

Similarly 'shell' access is a great benefit to a serious web site developer because it is a very

powerful tool **but** it could possibly cause huge security problems for other users. Ninja Hosting uses 'jailed shell' to allow users access to the shell environment while at the same time restricting those users access to *just their own files and folders.*

Security Updates

Security was also the main reason we brought the Installatron script management system to Ninja Hosting. Other such systems are available but Installatron consistently publishes updates and especially security update in a timely manner meaning that once a vulnerability is discovered our customers are amongst the first to be able to plug those holes!

Read more of the original article [here](#)