**Configuration Weakness Vulnerabilities**

Web server and application server configurations play a key role in the security of a web application. These servers are responsible for serving content and invoking applications that generate content. In addition, many application servers provide a number of services that web applications can use, including data storage, directory services, mail, messaging, and more. Failure to manage the proper configuration of your servers can lead to a wide variety of security problems.

Frequently, the web development group is separate from the group operating the site. In fact, there is often a wide gap between those who write the application and those responsible for the operations environment. Web application security concerns often span this gap and require members from both sides of the project to properly ensure the security of a site’s application.

There are a wide variety of server configuration problems that can plague the security of a site. These include:

* Unpatched security flaws in the server software
* Server software flaws or misconfigurations that permit directory listing and directory traversal attacks
* Unnecessary default, backup, or sample files, including scripts, applications, configuration files, and web pages
* Improper file and directory permissions
* Unnecessary services enabled, including content management and remote administration
* Default accounts with their default passwords
* Administrative or debugging functions that are enabled or accessible
* Overly informative error messages
* Misconfigured SSL certificates and encryption settings
* Use of self-signed certificates to achieve authentication and man-in-the-middle protection
* Use of default certificates
* Improper authentication with external systems

Some of these problems can be detected with readily available security scanning tools. Once detected, these problems can be easily exploited and result in total compromise of a website. Successful attacks can also result in the compromise of backend systems including databases and corporate networks. Having secure software and a secure configuration are both required in order to have a secure site.

**Environments Affected**

All web servers, application servers, and web application environments are susceptible to misconfiguration.

## How to Determine If You Are Vulnerable

If you have not made a concerted effort to lock down your web and application servers you are most likely vulnerable. Few, if any, server products are secure out of the box. A secure configuration for your platform should be documented and updated frequently. A manual review of the configuration guide should be performed regularly to ensure that it has been kept up to date and is consistent. A comparison to the actual deployed systems is also recommended.

In addition, there are a number of scanning products available that will externally scan a web or application server for known vulnerabilities, including Nessus and Nikto. You should run these tools on a regular basis, at least monthly, to find problems as soon as possible. The tools should be run both internally and externally. External scans should be run from a host located external to the server’s network. Internal scans should be run from the same network as the target servers.

**How to Protect Yourself**

The first step is to create a hardening guideline for your particular web server and application server configuration. This configuration should be used on all hosts running the application and in the development environment as well. We recommend starting with any existing guidance you can find from your vendor or those available from the various existing security organizations such as OWASP, CERT, and SANS and then tailoring them for your particular needs. The hardening guideline should include the following topics:

* Configuring all security mechanisms
* Turning off all unused services
* Setting up roles, permissions, and accounts, including disabling all default accounts or changing their passwords
* Logging and alerts

Once your guideline has been established, use it to configure and maintain your servers. If you have a large number of servers to configure, consider semi-automating or completely automating the configuration process. Use an existing configuration tool or develop your own. A number of such tools already exist. You can also use disk replication tools such as Ghost to take an image of an existing hardened server, and then replicate that image to new servers. Such a process may or may not work for you given your particular environment.

Keeping the server configuration secure requires vigilance. You should be sure that the responsibility for keeping the server configuration up to date is assigned to an individual or team. The maintenance process should include:

* Monitoring the latest security vulnerabilities published
* Applying the latest security patches
* Updating the security configuration guideline
* Regular vulnerability scanning from both internal and external perspectives
* Regular internal reviews of the server’s security configuration as compared to your configuration guide
* Regular status reports to upper management documenting overall security posture