Secure Coding

If you are a developer, please make an effort to become aware of how to avoid introducing new vulnerabilities and how to write secure code

Validate input Don't trust user input, it could be malicious. This should include input from clients you have written, as they can be modified to allow malicious input.

Check File permissions Any file or directory with world write permission could be modified with malicious content

Learn about secure programming Tutorials have been given at various Grid conferences and texts are available on how to avoid writing vulnerable code.

Top 25 Most dangerous programming errors

The Sans Institute provides a list of the Top 25 most dangerous programming errors Although these are not Grid specific, many of the vulnerabilities found by or reported to the previous EGEE GSVG in Grid Middleware fall into these categories.

University of Wisconsin Tutorials and secure coding practices

The University of Wisconsin have developed a two-part tutorial to help train analysts and developers in their vulnerability assessment techniques and in secure programming. These are available at their tutorials page.

They have also developed a library for safely opening files, where the ownership and permissions of directories that comprise a path in the file system are tested to make sure an attacker can not manipulate them. This is known as the safefile library and its adoption is being considered by the EMI project.