ISSeG

Integrated Site Security for Grids

EU-FP6 Project 026745

Checklist for Developers

David Jackson, STFC

CHEP 07, Victoria BC, 4 September 2007

Integrated
Site
Security for
Grids

www.isseg.eu

Information Society and Media

Checklist

1. **Architecture**
2. **Design**
3. **Cryptography**
4. **Implementation**
5. **Coding**
6. **After Implementation**

Integrated
Site
Security for
Grids

www.isseg.eu

Information Society and Media

1. Architecture

- Divide the program into semi-independent parts, each part should work correctly even if others fail.
- Build multiple layers of defence.
- Simple solutions are usually the most secure.

2. Design

- Make security-sensitive parts of your code small.
- Don’t require more privileges than you need.
- Avoid standard default passwords.
- Deny by default.
- Limit resource consumption, to limit the likelihood or impact of a Denial of Service attack.
- Fail securely: e.g., if there is a runtime error when checking a user’s access rights, assume s/he has none.
- In distributed or web applications don’t trust the client.

3. Cryptography

- Use trusted, public algorithms, protocols and products.

4. Implementation

- Read and follow guidelines for your programming language and software type.
- Think of the security implications of what your code does.
- Reuse trusted code (libraries modules, etc.).
- Write good-quality readable and maintainable code (bad code won't ever be secure).

5. Coding

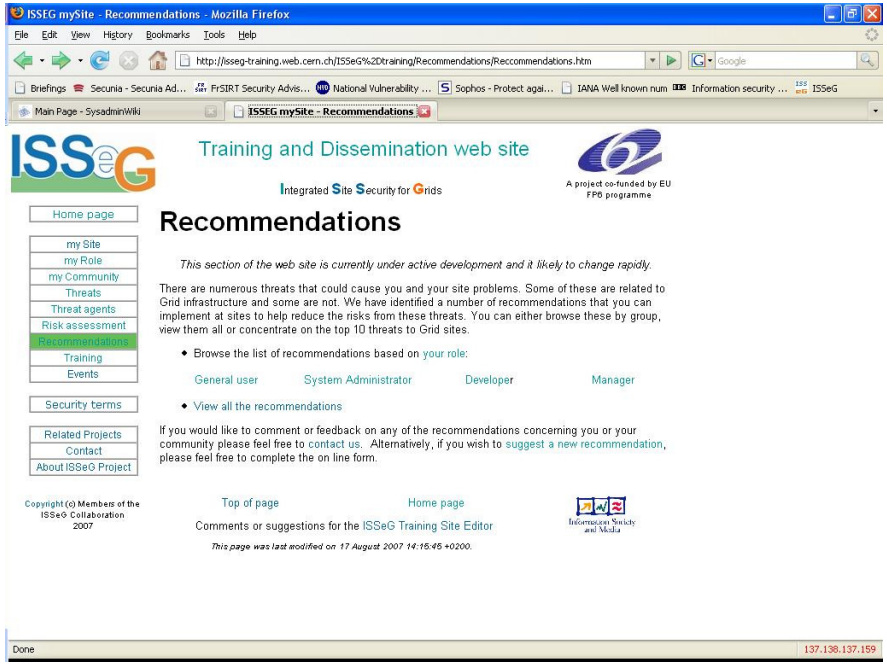
- Don't trust input data.
- Validate all input data.
- Don't make any assumptions about the environment.
- Beware of race conditions.
- Deal with errors and exceptions.
- Fail gracefully.
- Protect passwords and secret information.
- Be careful when handling files, especially temporary files: don't fall for the symbolic link attack
- Be careful with shell calls, eval functions etc.

6. After implementation

- Review your code and let others review it.
- When a (security) bug is found, search for similar ones.
- Use tools specific to your programming language:
  - bounds checkers,
  - memory testers,
  - bug finders etc.
- Turn on compiler / interpreter warnings and read them (Perl -w, gcc -Wall).
- Disable debugging information (strip command, javac -g:none, etc.)

Implementing the checklist

- The ISSeG project are developing a number of recommendations that will include links to practical advice on how to implement some or all of the above suggestions.



http://www.isseg.eu/

Integrated Site Security for Grids

www.isseg.eu

Information Society and Media