ISO/IEC JTC 1/SC 22/OWGV N 0193

Suggested changes to outline for language-dependent annexes proposed by workshop at 2009 Ada Europe conference

Date	2009-06-22
Contributed by	John Benito
Original file name	Annex F Outline.doc
Notes	This version replaces a previous posting which was incorrect.

Annex Outline

Annex \<Language Name\>
(informative)

Language Specific Vulnerability Template

\<Language Name\>. Skeleton template for use in proposing language specific information for vulnerabilities

Every vulnerability description of Clause 6 of the main document should be addressed in the annex in the same order even if there is simply a notation that it is not relevant to the language in question.

\<Language Name\>.1 Identification of standards

This section should list the relevant language standards.

\<Language Name\>.2 General terminology and concepts

This section should provide an overview of general terminology and concepts that are utilized throughout the annex.

\<Language Name\>.3

\<Language Name\>.3.\<x\> \<short title\>\<unique immutable identifier\>

The "short title" and "unique immutable identifier" are copied from 6.x

\<Language Name\>.3.\<x\>.0 Status and history

The header will be removed before publication.
This temporary section will hold the edit history and status for this language specific vulnerability. [The following descriptions should assume that the reader has read the corresponding material in the main body of the document. They should explain differences in terminology and how the general concepts relate to the specific language but should not repeat the general material The text should be the minimum necessary to describe the relationship to the language, supplemented with examples.]

\<Language Name\>.3.\<x\>.1 Language-specific terminology and features

This sub-section should deal with terminology differences between the body of the document and the terminology used in the language standard. *This sub-section may also explain language specific features and terminology that are applicable to the subsequent sub-sections.*

\<Language Name\>.3.*\<x\>*.2 Description of application vulnerability

Replace this with a brief description and examples of how the general description relates to the language. The description should describe why the language is susceptible and provide

examples of the vulnerability in the language if possible. Or, demonstrates why the language is not susceptible to the vulnerability.
Susceptibilities and examples

\<Language Name\>.3.\<*x*\>.3 Mechanism of failure

Replace this with a section describing the mechanism of failure in terms relevant to the language being described.
Consequences

\<Language Name\>.3.\<*x*\>.4 Avoiding the vulnerability or mitigating its effects in \<language\>

This vulnerability can be avoided or mitigated in \<language\> in the following ways:
Replace this with a bullet list summarizing the ways in which the vulnerability can be avoided or mitigated in \<language\>. The bullet points should only apply to \<language\>. This is the spot for usage guidelines.
What the programmer can do to avoid or mitigate the vulnerability.

\<Language Name\>.3.\<*x*\>.5 Implications for standardization ~~in \<language\>~~

Optionally, replace with a bullet list summarizing various ways that standardization for \<language\> has assisted in mitigating the vulnerability. This is the opportunity to talk about actions that the language committee has already taken, such as deprecating features or providing alternatives. There is also the possibility of talking about future plans.
Future plans

\<Language Name\>.3.\<*x*\>.6 Bibliography

Insert numbered references for other documents specific to \<language\>. These will eventually be collected into an overall bibliography for the TR. So, please make the references complete. Someone will eventually have to reformat the references into an ISO-required format, so please err on the side of providing too much information rather than too little. Here [1] is an example of a reference:

[1] Greg Hoglund, Gary McGraw, Exploiting Software: How to Break Code, ISBN-0-201-78695-8, Pearson Education, Boston, MA, 2004