

## Application Security Standards

Version: 1 Date: 08-24-2010

- Encrypt Web.Config connection string for internet apps (both internet/intranet are preferable). CROMERR connection string hashing is also acceptable.
- Ensure Web.Config Custom Error Mode = "On" with custom error page to prevent server displays of any internal server info on the page when an application crashes.
- Avoid SQL injection attack: No in-line SQL in codes. Developers should review the old applications for this vulnerability when there is a chance to work on these applications. The in-line SQL codes need to be converted to stored procedure or Linq2SQL.
- Dynamic SQL inside stored procedure present the same risk an in-line SQL. The dynamic SQL is acceptable only as long as it is executed using the built-in procedure sp\_executeSQL **and** with Parameterized query.
- Avoid Cross-Site attack:
  - In the web-config: Set Validate Request = True
  - Using HttpUtility.HtmlEncode utility for string input data from users. Example: <http://dotnetperls.com/httputility-1>
  - Using RangeValidator, RegularExpressionValidator control, and or a regular expression to validate input.
- Avoid file upload attack:
  - Limit the size of upload to reduce the impact of the DoS attacks.
  - Store the file in separate partition with anti-virus software in place to scan the file immediately.
  - Limit the file types being uploaded to approved types.
- Avoid using filenames in URLs . Use an index or other method to not allow users access to your files.

**Tool to reduce application security risks:**

- Anti-Xss (anti-cross-site) library
  - [Training Demo](#)
  - [Anti-Xss library tools](#)
- CAT.NET: scan and identify application flaws in cross-site attack, SQL injection attack. [Download location](#). (After download, please rename CATNETx32.ms to CATNETx32.msi and double click for installation)
- WACA: scan servers for security configuration issues. This tool is for server administrator. [Download location](#). (After download, please rename WACAV10.ms to WACAV10.msi and double click for installation)

## Document History

Date	Version	Editor	Change
08-05-2010	1 <sup>st</sup> Draft	Son Tran	creator
08-07-2010	2 <sup>nd</sup> Draft	Miles Neale	Editing and added new elements
08-13-2010	2 <sup>nd</sup> Draft	SAT	SAT first review and comment
08-24-2010	1.0		SAT officially approved.