South Dakota Application Security Vulnerabilities

The purpose of this document is to list existing and emerging threats that pose significant risk to State hosted applications and the critical information that is generated, processed, transmitted, and stored on the State's network. This document provides recommendations for multiple security issues common in web applications and distributed systems. Remediation requirements are based on the threat's potential to negatively impact our infrastructure. This is not an exhaustive list, and issues may be added to the list at any time.

Section A
Security issues that will NOT be allowed:

1. Unverified or non-validated input fields (Cross Site Scripting and SQL Injection)
2. Cross Frame Scripting
3. Broken Authentication and Session Management
4. Improper (non-encrypted, default settings) data transfer between client and application server (Refers to Insecure Direct Object References and Cross-Site Forgery)
5. Unsecured configuration files
6. Unrestricted upload of dangerous file types
7. Failure to restrict URL access (refers to open orphan urls in web applications and Path Traversal Vulnerabilities)
8. Un-validated redirects and forwards
9. Information Exposure through and Error Message
10. Buffer copy without checking size of input (Buffer Overflow)
11. Use of a Broken or Risky Cryptographic Algorithm (refers to the use of insecure data decryption keys)
12. Missing authentication for critical functions
13. Use of hard-coded credentials
14. Failure to use proper programmatic procedures for preventing automated form submissions, may that be through Captcha or other methods.

Section B
Security items that may/may not be allowed depending on the security level:

1. Allocation of resources without limits or throttling
2. Insufficient Transport Layer protection (refers to lack of use of SSL certificates when required)

Section C
Security items that are allowed but mitigation is recommended:

1. Applications which rely on outdated technologies (i.e. the app uses Java 6, but Java 7 has been released)
2. Lack of two-factor authentication