Alex Tong
Comp 116

Risk ID	Technical Risk	Technical Risk Indicators	Impact Rating	Impact	Mitigation	Validation Steps
1	Code Injection--PHP Remote File Inclusion (RFI) CWE-98	Remote files included in /wp-admin/plugins.php /wp-admin/update.php /www/wp-settings.php	H	Remote code execution if user specifies remote file location	Validate all user input	Validate input, then use whitebox static scan to determine vulnerability
2	SQL Injection CWE-89	Non-validated user SQL query in /www/board/php /includes/dblib.php /scoreboard/index.php /Cache/MySQL.php /wp-db.php	H	Access and change permissions to sensitive data stored in SQL database	Validate all user input for special characters especially ‘ or use prepared statements	Use static scan or dynamic SQL injection tools
3	Credentials Management – Hard coded passwords CWE-259	Passwords stored in plaintext in /www/board/php /includes/dblib.php /scoreboard/index.php /network/site-new.php	M	If discovered through some other vulnerability then could compromise admin credentials	Don’t store passwords in application zone, especially in plain text	Use static scan to determine vulnerability
4	Cross Site Scripting	Embed working javascript into page /www/board.php However many other pages are caught by veracode scan (30+)	M	Malicious content can be embedded on page	Escape all untrusted data in the correct way for the context of use	Static scan for any un-escaped user input
5	Cryptographic Issues—Missing Encryption of Sensitive Data	Game not global thermal nuclear war has access to sensitive data stored as a local variable	M	Access to sensitive data	Encrypt all sensitive data	Require authentication to access pages containing

	Security through obscurity CWE-311					sensitive data regardless of encryption
6	Use of Broken Cryptographic Algorithm CWE-327	Veracode static scan detects faulty cryptographic algorithm usage	M	Access to sensitive information	Use better encryption scheme for sensitive data	Centralize sensitive data to manage risk
7	Directory Traversal – External control of file path CWE-73	Access of files like flag.txt which are not accessible through normal navigation of site	M	Access to unauthorized files	Validate all user input	Check access to all sensitive files, especially of known name
8	Information Leakage CWE-209	Error messages generate sensitive stack information for other exploits, i.e. directory traversal	L	File location data	Ensure generic error messages	Static scan for generated error messages
9	Untrusted Initialization CWE-454	Application trusts outside variables	L	Variables may be used for a buffer overflow attack	Limit sizes of buffers	Use buffer length validation