Nicolas Sempere

Capture the Flag Website, Fall 2015:
A Technical Risk Analysis

VC - A marking of “VC” indicates credit being given to Veracode’s diagnostic reporting.
CWE - Indicates credit due to the relevant CWE entry.

Risk ID	1
Technical Risk	User inputs are susceptible to XSS injection (VC)
Indicators	Multiple locations where input is taken and handled without any form of sanitization.
Related CVE, CWE, or OSVDB IDs	CWE-80
Impact Rating	Medium
Impact	Could result in the sabotage of web assets or in denial of service
Mitigation	Include filtering for input containing html entities (<, >, etc.)
Validation Steps	Implemented sanitization for user-generated input before further handling of data, thus preventing injection of any more code.

Risk ID	2
Technical Risk	Improper neutralization of SQL injection (VC)
Indicators	Multiple locations where SQL queries are made with unfiltered user input.
Related CVE, CWE, or OSVDB IDs	CWE-89
Impact Rating	High
Impact	Potential for leaks of sensitive data; May create an access point for attackers to gain elevated privileges. (VC)
Mitigation	Filter user input that will be queried for special SQL

	characters like “ ‘ ”
Validation Steps	Included screening for user-defined queries that do not comply with intended format (irrelevant/suspicious characters).

Risk ID	3
Technical Risk	Vulnerability to PHP injections and remote file inclusion through dynamically evaluated input. (VC)
Indicators	Visible in numerous WordPress scripts (VC) - ● plugins.php ● template.php
Related CVE, CWE, or OSVDB IDs	CWE-98
Impact Rating	Very High
Impact	Potential entry-point for remote code execution; attackers can upload files with malicious code that could steal information or damage system infrastructure.
Mitigation	Verify that all user input conforms to the desired format before passing it to functions like include() or require() (VC).
Validation Steps	Added input sanitization as an initial step before handling user-provided data in any other way.

Risk ID	4
Technical Risk	Error Logs are too verbose
Indicators	Template sentences detailing information about errors and about the database in question (board.php:19)
Related CVE, CWE, or OSVDB IDs	CWE-209
Impact Rating	Low

Impact	User input that causes a SQL error will return detailed information about what went wrong, allowing user to learn more about the database than in necessary or secure.
Mitigation	Shorten error messages and only point out information that is absolutely vital to the user's understanding of what went wrong.
Validation Steps	Modified error messages; no longer send dynamically evaluated information.

Risk ID	5
Technical Risk	Directory listings in enabled
Indicators	Site exposes list up recent uploads
Related CVE, CWE, or OSVDB IDs	CWE-548
Impact Rating	Low
Impact	Gives away unnecessary information about how this tool's files are laid out; makes a potential attack easier to conduct.
Mitigation	Disable automatic directory listing and require authorization for what directory information is still mad available. (CWE)
Validation Steps	Removed directory listing page from group of client-accessible assets.

Risk ID	6 (VC)
Technical Risk	Passwords stored in plaintext
Indicators	board.php:15, dblib.php:4, index.php:33
Related CVE, CWE, or OSVDB IDs	CWE-259
Impact Rating	High
Impact	Dramatically increases the danger of compromising all accounts/authorizations that the password is

	linked to.
Mitigation	Ensure that any passwords that are set are done so outside of the jurisdiction of PHP scripts, and that authentication establishment is done in an encrypted form.
Validation Steps	Removed plaintext password interactions.

Risk ID	7
Technical Risk	Use of Unreliable Encryption Algorithm
Indicators	SHA1 password encryption (dblib.php:24)
Related CVE, CWE, or OSVDB IDs	CWE-327
Impact Rating	Known collisions mean this algorithm lacks the strength to protect passwords stored in the database. SHA1 is also a very fast algorithm, designed for file signatures rather than password hashing; brute-force attacks are easier.
Impact	Medium
Mitigation	Replace with a stronger, slower hashing algorithm.
Validation Steps	Replaced SHA1 hash with bcrypt hash, a specialized algorithm for password storage.

Risk ID	8
Technical Risk	Lack of tokenized sessions allows CSRF attacks
Indicators	Sessions are created but do not initiate any sort of challenge token
Related CVE, CWE, or OSVDB IDs	CWE-352, CWE-384
Impact Rating	Medium
Impact	Authenticated users can unintentionally make requests for information they should not have access to.

Mitigation	Include some sort of tokenized ID with each new session created, or with each new request made. Only legitimate requests will be able to use these tokens.
Validation Steps	Implemented tokenized session storage with timeouts.

Risk ID	9
Technical Risk	Cookie contents are unencrypted
Indicators	main.php:21
Related CVE, CWE, or OSVDB IDs	CWE-312, CWE-472,CWE-565
Impact Rating	Medium
Impact	Plaintext information on the contents of a cookie gives away information unnecessarily and allows users to tamper with that information, potentially causing more information leakage.
Mitigation	encrypt the information being used in the cookie, thereby making it difficult for users to tamper with information in a meaningful way.
Validation Steps	Serialized and encrypted cookie information before seeding it in client browsers.

Risk ID	10
Technical Risk	Unnecessary service running
Indicators	See class-ftp.php
Related CVE, CWE, or OSVDB IDs	-
Impact Rating	Medium
Impact	With FTP running as a service in the background, the server unnecessarily exposes another entry point that can leak information.
Mitigation	Do not run this service.

Validation Steps	Disabled script that initializes/configures FTP service.