Risk ID	1	2	3	4	5
Technical Risk	XSS (Reflected in case of id parameter, and Persistent in case of posts)	Files exposed by common names (subject to URL fuzzing with wordlist)	SQL Injection	Hard-coded password	Information exposure through an error message
Technical Risk Indicators	Evidence that it happened: HTTP requests in web server log (or database entries in MySQL) containing scripts within them Evidence in the code: For persistent XSS, unsanitized usage of stored user input at ctf/board.php: lines 44, 59, 64; for reflected XSS, unsanitized usage of id parameters at lines 43, 50, 58	Evidence that it happened: HTTP requests in web server log with sensitive filenames at end of URL Evidence in the code: Sensitive file names match common words (ctf/flag.txt, ctf/logout.php)	Evidence that it happened: HTTP requests containing SQL keywords; Database log shows queries with conditions that are always true (like '1=1') Evidence in the code: Unsanitized, dynamically created queries like those at ctf/board.php lines	Evidence in the code: Initializing a password variable in the application code and using that variable as parameter for DB login (board.php, lines 15 and 18; includes/dblib.php lines 3 and 6; scoreboard/index.php lines 31, 34, 111, 114)	Evidence that it happened: outbound HTTP traffic (in logs) containing revealing error messages Evidence in the code: Calls to "mysql_error", which gives the direct error from the DB, are part of the error message string (board.php line 18, includes/dblib.php lines 8 and 27, scoreboard/index.php lines 34 and 114
Related CVE, CWE, or OSVDB IDs	CWE-79	N/A	CWE-89	CWE-259	CWE-209
Impact Rating	Medium	Medium	High	Medium	Low

Impact	Cookie stealing or tampering; defacing; redirection to other sites	Sensitive information about business or web server can be obtained, which may be inherently valuable (like the CTF key) or may be used for other exploits	Read or modify application data; bypass authentication system	Developers of the software can get inappropriate access to live customer implementations because they know password; software must be patched if password becomes known to public	Can help guide an attacker even if their initial attempt fails (e.g. showing malformed SQL queries which might reveal underlying logic, or revealing file directory information)
Mitigation	Sanitize inputs; check input against a white list; do not allow embedding of HTML tags in posts	Configure web server not to serve specific files or specific file types (httpd.conf or .htaccess controls this in Apache)	Sanitize inputs; check input against white list; use prepared SQL statements; use stored procedures with parameter restrictions	Outsource password strings to properties or config files; store strings as cryptographic hash digests	Publish generic error messages which reveal nothing about the system

Validation Steps	Insert script for a JavaScript alert into form for post, or in the id parameter of the URL. Save it and reload page. Pop up should not appear.	Run URL fuzzer tool (https://pentest-tools.com/website-vulnerability-scanning/discover-hidden-directories-and-files) and verify that no sensitive files are found	Insert SQL code (against known table) as URL parameter or in forms. Check database logs to make sure no request was made.	Search application code for the password. Verify it cannot be found.	Run a fuzz tool to intentionally trigger errors and verify that all returned messages are generic

6	7	8	9
Directory Traversal	Cookie Tampering	Weak password / weak hashing? (for Bobo)	Weak cryptography
Evidence that it happened: Web server log shows requests to non-existent locations, followed immediately by downloads of files Evidence in the code: apache2.conf or .htaccess files have Indexs option activated			
CWE-548			
High			

Access to listed files, which themselves may be sensitive; possible access to source code which can reveal more weaknesses

Turn directory listing off by default; allow accounts access to files on "need to know" basis

Enter URL to access non-existent file in an existing directory, and verify that no listing appears