Dennis Chen
Comp116 Security

Risk Table
CTF

Risk ID	Technical Risk	Technical Risk Indicators	Impact Rating	Impact	Mitigation	Validation Steps
1	Code Injection	Script can be injected into input	H	Malicious code can be executed	Validate user input	Inject untrusted input into application that evaluates and executes code
2	SQL Injection	The function call constructs a dynamic SQL query using a variable derived from user-supplied input.	H	Attacker can exploit flaw to execute arbitrary SQL queries to manipulate database queries (to access/modify/delete data)	Validate user input. Avoid constructing SQL queries and use parameterized prepared statements. Normalize user supplied input	Construct dynamic SQL query
3	Credentials Management	Storing passwords in easily accessible locations.	M	User accounts and data compromised	Store passwords out of band from application code and avoid storing passwords hard-coded. Also can use cryptographic hashes	Look for hard-coded passwords or try to find MD5 hashes of passwords or just look in code
4	Cross Site Scripting (HTML Injection)	Attack can use web application to send	M	Attack can use XSS to manipulate/steal cookies, modify content, and	Sanitize output generated from user-	Try to input code by injecting script tags

		malicious code to different end user		compromise information	input, validate user input using positive filters. Disallow user to input HTML content in anything or be strict about tags. Also use contextual escaping!	
5	Information Leakage	Source code disclosure, browsable directories, log files accessible, unfiltered backend error messages, exception stack traces, server version information, transmission of sensitive data	L	Provides information about product/environment that attacker can use as building blocks to carry out more complicated attacks	Return generic error messages from servers and applications. Suppress stack traces from being displayed. Do not reveal backend issues. Removes files from web-accessible directories.	Try to get error messages and see if it is a possible leak of information.