Dell Top Threats Cheat Sheet

	Cross-site scripting	Command Injection	Improper Authentication	Improper Authorization	Sensitive Data Exposure
The Threat	Occurs when uncontrolled input data is sent to a browser.	Occurs whenever untrusted data is sent to an interpreter.	Improperly verifies the identity ofa user.	Improperly grants permissions to resources or actions.	Occurs when sensitive data is not encrypted which may allow access to secure environments or proprietary to Dell.
The Impact	Can be leveraged to hijack users' browsers, deface websites redirect users or hijack the users' browser using malware, redirect to phishing sites as examples.	Can result in remote code execution, denial of service, sensitive information disclosure, data loss.	Gain unauthorized access to the product or application to gain access to sensitive information, run arbitrary code.	Result in information exposure, denial of service, and running arbitrary code execution.	Can violate data security and privacy laws, violate obligations to our customers, trigger regulatory actions and litigation, and spur further compromise.
Architectural considerations at the Design Phase					
Do Not Trust Any Input	✓	✓			
Defense in Depth	✓	✓			✓
Apply Least Privilege		✓		✓	
Ensure Proper Authentication			✓		
Establish Secure Defaults			✓		✓
Mitigate these threats in the Development Phase					
What to do	□ Validate input. □ Escaping. □ Setting extra flags on cookies.	□ SQL: Prepared Statements. (with parameterized queries) □ SQL: Stored Procedures. □ SQL: Input Sanitization. □ OS Command: Built-in functions v OS Command Invocation. □ OS Command: Parameterized with input validation. □ OS Command: Parameterization .	□ Integrate with an authentication mechanism. □ Password Management. □ Session Management. □ Transmit securely. □ Prevent Brute Force Attacks. □ Don't use Verbose Messages. □ Multi-factor Authentication.	□ Identify all privileged assets. □ Identify user roles. □ Enforce Authorization at the Server. □ Never use untrusted data to make authorization decisions. □ Deny by Default. □ Review Authorization Logic. □ Log and Alert. □ Implement Authorization Logic. □ Limit the execution of a script.	□ Classify Data. □ Use Proven Crypto. □ Transit. □ Store. □ Retrieval. □ Don't use Verbose Error Messages. □ Never post Dell intellectual property (source code) or sensitive information (hostnames, credentials, test code)on public repositories like GitHub or when using AI.

	Cross-site scripting	Injections	Improper Authentication	Improper Authorization	Sensitive Information Exposure
SDL Technical Controls (Check applicability criteria)	□ Prevent Cross-Site Scripting SDL Control □ Secure Headers or HTTP Security Headers □ Transmit secrets securely	□ Do not mix code and unvalidated data □ Prevent OS CommandInjection	□ Ensure Proper Authentication □ Protect Against Brute Force Attacks SDL Control □ Support Changeable Secrets or Rekey Ability SDLControl □ Follow best practices for cryptography and security protocols □ Support and encourage manufactured-unique or installation-unique secrets SDL Control	□ Limit and Document Service Access SDL Control □ Apply Least Privilege □ Secure handling of Errors, Logging and Auditing	□ Do Not Display Secrets in Plaintext SDL Control □ Store secrets secure SDLControl □ Transmit Secrets Securely SDLControl □ Follow best practices for cryptography and security protocols □ Secure Defaults and Configuration □ Ensure Data protection and Privacy
Maturity Model					
Verification Activities	COMPLIANT: □ Leverage Static Code Analysis Service STANDARD: □ Perform test for reflected cross-site scripting □ Perform test for stored cross-site scripting □ Testing for DOM-based cross-site scripting (OTG-CLIENT-001) LEADING-EDGE: • Coding conventions	COMPLIANT: □ Leverage Static Code Analysis Service STANDARD: □ Validate Apply Least Privileges through Perform Threat Modeling □ Testing for Command Injections □ Using BURP to validate Command Injection LEADING-EDGE: • Coding conventions	COMPLIANT: • Attest that all the above SDL Controls Requirements have been implemented. □ Leverage Static Code Analysis Service • Provide an inventory of passwords that include whether each is manufacturedor installation unique secrets. STANDARD: • Perform Threat Modeling to verify that the requirements of the technical control above have been implemented & validated through testing. LEADING-EDGE: • Manual code review of authentication logic.	COMPLIANT: □ Secure handling of Errors, Logging and Auditing STANDARD: • Perform Threat Modeling to verify that the technical controls requirements above have been implemented & validated through testing. • Validate all service access including accounts that have beendocumented in the security configuration guide or equivalent documents. LEADING-EDGE: • Manual code review of authorization logic.	COMPLIANT: • Attest that all the above SDL Controls Requirements have been implemented. • Provide a list of any and all-non approved crypto used in the software. • Network Vulnerability & STIG Scanning Service STANDARD: • Perform Threat Modeling to verify that the technical controls requirements above have been implemented & validated through testing.

Check out our Shift Security Left Community https://dell.sharepoint.com/sites/security-community