SAFECode
Software Assurance Forum for Excellence in Code
Driving Security and Integrity

Reference table from Section 2a of
Practical Security Stories and Security Tasks for Agile Development Environments
www.safecode.org/publications/SAFECode_Agile_Dev_Security0712.pdf

Security-focused Stories and Associated Security Tasks

No.	Security-focused story	Backlog task(s)	SAFECode Fundamental Practice(s)	CWE-ID
1	As a(n) architect/developer, I want to ensure **AND** as QA, I want to verify allocation of resources within limits or throttling	**[A]** Clearly identify resources. A few examples: • Number of simultaneous connections to an application on a web server from same user or from different users • File size that can be uploaded • Maximum number of files that can be uploaded to a file system folder **[A/D]** Define limits on resource allocation. **[T]** Conduct performance/stress testing to ensure that the numbers chosen are realistic (i.e. backed by data). **[A/D/T]** Define and test system behavior for correctness when limits are exceeded. A few examples: • Rejecting new connection requests • Preventing simultaneous connection requests from the same user/IP, etc. • Preventing users from uploading files greater than a specific size, e.g., 2 MB • Archiving data in file upload folder when a specific limit is reached to prevent file system exhaustion	• Validate Input and Output to Mitigate Common Vulnerabilities • Perform Fuzz/Robustness Testing	CWE-770

No.	Security-focused story	Backlog task(s)	SAFECode Fundamental Practice(s)	CWE-ID
2	As a(n) architect/ developer, I want to ensure **AND** as QA, I want to verify application of appropriate encoding for output context	**[A]** Clearly identify all types of output context. A few examples: • Output is rendered only as HTML • Output is rendered as HTML attributes • Output is rendered as a URL **[D]** Adhere to SAFECode's Fundamental Practices for Secure Software Development for proper encoding of output context. Prefer use of language-specific in-built APIs such as HTMLEncode() (for C#) for encoding purpose. If that's not feasible, use well-known encoding frameworks/controls such as ESAPI encoder. Also, do canonicalization of user input to prevent bypass of encoding filters that have been applied. **[T]** Use a combination of manual test cases and automated means (web vulnerability scanners) in order to verify the strength of encoding filter applied.	• Use Anti-Cross Site Scripting (XSS) Libraries • Validate Input and Output to Mitigate Common Vulnerabilities	CWE-838
3	As a(n) architect/ developer, I want to ensure **AND** as QA, I want to verify application of or access within index boundaries of buffers and arrays	**[A/D]** Define where buffer operations (on dynamic buffers) occur. Define data types and bounds for buffer operations. **[D]** Adhere to SAFECode's Fundamental Practices for Secure Software Development for prevention of buffer overflows. **[D]** Scan source code for such violations using static code analyzer tools, e.g., Coverity. **[A/D]** Conduct false positive analysis of flagged issues. **[D]** Fix buffer overflow issues analyzed as confirmed. **[T]** Use fuzz testing tools to verify that no process/system crashes/hangs exist. If they do, fix them and re-run the tool.	• Minimize Use of Unsafe String and Buffer Functions • Use a Current Compiler Toolset • Use Static Analysis Tools	CWE-120 CWE-131 CWE-805

No.	Security-focused story	Backlog task(s)	SAFECode Fundamental Practice(s)	CWE-ID
4	As a(n) architect/developer, I want to ensure **AND** as QA, I want to verify graceful handling of all exceptions	**[A/D]** Application should have provisions to catch all exceptions. **[A/D]** Application exception codes should be clearly defined. **[A/D/T]** Unknown exceptions should be tied to a generic error code. **[A/D/T]** Any exception condition in the application should not throw stack trace (or similar information) to the end-user.	• Perform Fuzz/Robustness Testing • Use a Current Compiler Toolset • Use Static Analysis Tools	CWE-754
5	As a(n) architect/developer, I want to ensure **AND** as QA, I want to verify concurrent execution using shared resources with proper synchronization	**[D]** Scan source code for race condition violations using static code analyzer tools, e.g., Coverity. **[A/D]** Conduct false positive analysis of flagged issues. **[D]** Fix race condition issues analyzed as confirmed. **[T]** Use fuzz testing tools to verify that process/system crashes/hangs don't exist. If they do, get them fixed and re-run to verify.	• Perform Fuzz/Robustness Testing • Use Static Analysis Tools	CWE-362
6	As a(n) architect/developer, I want to ensure **AND** as QA, I want to verify use of controlled format string	**[D]** Adhere to SAFECode's Fundamental Practices for Secure Software Development for preventing format string issues. **[D]** Scan source code for such violations using code analyzer tools, e.g., Coverity. **[A/D]** Conduct false positive analysis of flagged issues. **[D]** Fix format string issues analyzed as confirmed. **[T]** Use fuzz testing tool to verify that no process/system crashes/hangs exist. If they do, fix them and re-run the tool.	• Minimize Use of Unsafe String and Buffer Functions • Use Canonical Data Formats • Use Static Analysis Tools • Perform Fuzz/Robustness Testing	CWE-134

No.	Security-focused story	Backlog task(s)	SAFECode Fundamental Practice(s)	CWE-ID
7	As a(n) architect/developer, I want to ensure **AND** as QA, I want to verify use of controlled integer bounds	**[D]** Adhere to SAFECode's Fundamental Practices for Secure Software Development for preventing integer overflows. **[D]** Scan source code for such violations using code analyzer tools, e.g., Coverity. **[A/D]** Conduct false positive analysis of flagged issues. **[D]** Fix integer overflow issues analyzed as confirmed. **[T]** Use fuzz testing tools to verify that no process/system crashes/hangs exist. If they do, fix them and re-run the tool.	• Use Robust Integer Operations for Dynamic Memory Allocations and Array Offsets • Use Static Analysis Tools • Perform Fuzz/Robustness Testing	CWE-190
8	As a(n) architect/developer, I want to ensure **AND** as QA, I want to verify that users have access to the specific resources they require which they are authorized to use	**[A]** Create a detailed authorization matrix that specifies which user groups/users have access to which resources (folders, files, UI, etc.). **[D]** Ensure that your application's authorization mechanism complies with the matrix created in step (for example, if role-based access control [RBAC] is used, ensure it corresponds to the authorization matrix created). **[T]** Test effectiveness by using a combination of manual and automated means.	• Use Least Privilege	CWE-862 CWE-863
9	As a(n) architect/developer, I want to ensure **AND** as QA, I want to verify correct conversion between numeric types	**[D]** Adhere to SAFECode's Fundamental Practices for Secure Software Development for preventing type conversion errors. **[D]** Scan source code for such violations using code analyzer tools, e.g., Coverity. **[A/D]** Conduct false positive analysis of flagged issues. **[D]** Fix incorrect numeric type issues analyzed as confirmed. **[T]** Use fuzz testing tool to verify that no process/system crashes/hangs exist. If they do, fix them and re-run the tool.	• Use Robust Integer Operations for Dynamic Memory Allocations and Array Offsets • Use Static Analysis Tools • Perform Fuzz/Robustness Testing	CWE-681

No.	Security-focused story	Backlog task(s)	SAFECode Fundamental Practice(s)	CWE-ID
10	As a(n) architect/developer, I want to ensure **AND** as QA, I want to verify correct permission assignment and maintenance for all critical resources	**[D/T]** When a critical resource is defined or accessed, make sure that the access permissions (programmatic and systemic) to it are left in their most restrictive but useful possible setting. **[D]** Describe correct permissions for the resource in the security configuration guide.	• Use Least Privilege	CWE-732
11	As a(n) architect/developer, I want to ensure **AND** as QA, I want to verify that sensitive data is kept restricted to actors authorized to access it	[**A/D/T]** When sensitive data (either user data that's considered sensitive or system data that may lead to insecure outcomes if leaked) is transferred by any channels across a trust boundary (for example, internal IP addresses as part of an HTTP or SMTP header, or a full internal filename with path is exposed in a GUI), be sure to remove the sensitive part. **[A]** Clearly specify which data produced by the system is to be considered sensitive and socialize that status across the development team and QA. **[D/T]** When handling sensitive data, have your code fail gracefully so that sensitive data does not leak. **[D/T]** Make sure that sensitive information is not leaked in error messages and stack traces.	• Use Least Privilege	CWE-212
12	As a(n) architect/developer, I want to ensure **AND** as QA, I want to verify that the same steps are followed in the same order to perform an action, without possible deviation on purpose or not	**[A/D/T]** When creating and verifying the business logic of multiple-step actions in the system, ensure that the action cannot suffer from missing steps, that steps cannot be performed in an arbitrary order, and that there is a timeout in each step that invalidates the whole operation. **[D/T]** In case of timeout or user-cancelation of the action, be sure that all initiated changes are rolled back to the state they were in before the action started. **[D/T]** Be sure that all database commits and system state changes are only affected after the business logic has been validated and the action has been completed.	• Threat Modeling	CWE-841

No.	Security-focused story	Backlog task(s)	SAFECode Fundamental Practice(s)	CWE-ID
13	As a(n) architect/developer, I want to ensure **AND** as QA, I want to verify that the damage incurred to the system and its data is limited if an unauthorized actor is able to take control of a process or otherwise influence its behavior in unpredicted ways	**[A]** Make sure distinct processes that need to communicate can do so in a way that only requires the minimum set of permissions (for example, don't run two processes as root just because they both need to access the same resource in a Unix environment). **[D]** Make sure any process that needs to have privileged access has it only for the minimum amount of time necessary and is able to drop the privileges as soon as they are not needed (for example, a network service opening a port lower than 1024 and dropping the elevated privileges necessary to do so right after the port is successfully opened). **[D]** Make sure that privileges are dropped correctly as part of privileged operations exception handling. **[A/D/T]** Make use of operating systems facilities like dedicated users, operating system capabilities matrices, jails and sandboxes to limit the exposure of the system to exploitation of a given process. **[T]** Make sure when testing that the system can operate in a security-hardened environment (more restrictive in terms of privilege handling).	• Implement Sandboxing • Threat Modeling • Determine Attack Surface	CWE-250

No.	Security-focused story	Backlog task(s)	SAFECode Fundamental Practice(s)	CWE-ID
14	As a(n) architect/developer, I want to ensure **AND** as QA, I want to verify that every resource and system that I access as part of operating my own system is providing me with verified services and content, and that content I provide gives my customer protection and verification against substitution and tampering in-transit	**[D/T]** When relying on the content of remote systems for the correct operation of your system, verify both the identity of the remote system (by using DNS and reverse-DNS queries and/or SSL certificates) and the integrity and authenticity of the content acquired (by using signatures and hashes). **[A/D/T]** Make use of code-signing technologies like Authenticode, jar signing, etc., as appropriate per content when consuming, and provide when producing. **[D/T]** Make sure to perform all necessary checks to validate the object being checked depending on the technology used (certificate chain of trust, for example). **[A/D]** Make proper use of cryptography tools to ensure integrity of a given value between its inception and its use. **[A/D]** Store all sensitive information used for security decisions on the server only—do not rely on client-side security decisions. **[A/D]** Use session management frameworks over stateless protocols to maintain security-decision values. **[A/D/T]** Understand the data flows of your application and identify those where information used for security decisions can be intercepted and tampered with and armor those channels.	• Eliminate Weak Cryptography • Threat Modeling	CWE-494

No.	Security-focused story	Backlog task(s)	SAFECode Fundamental Practice(s)	CWE-ID
15	As a(n) architect/developer, I want to ensure **AND** as QA, I want to verify that the system does not import functionality from sources that are not under the system's control	**[D]** Do not include the capability to refer to code that is defined, stored and controlled in an external location outside the control mechanisms of your system and that can interact with the system and its components. [**D/T**] If you absolutely must import functionality from external sources, make sure that relevant server-side checks are applied to all content generated by the imported code. Do not trust the imported functionality "as is." **[A]** Use an application-level firewall that can guard against this kind of vulnerability.	• Threat Modeling	CWE-829
16	As a(n) architect/developer, I want to ensure **AND** as QA, I want to verify limitation of a pathname to a restricted directory ('Path Traversal')	**[D/T]** When accepting external input that will be used to construct a file path, remove or invalidate special constructs like ".", "..", "\" and "/", including their many representations in alternate character sets. **[D/T]** Filter data repeatedly until all findings are exhausted to prevent nested constructs. **[D/T]** Only after cleaning up the input for extraneous characters, make sure that the full path received falls inside of the permitted area by using a whitelist of possible path locations. **[D]** Perform checks as close to the operation as possible, as content may change in transit. **[D]** Use language or operating system-provided functions to create a canonical form of the path and check it against your whitelist. **[A/D]** Prefer mappings and indexed menus instead of free-form input when choosing paths. **[D]** Examine relevant findings from static code analysis tools.	• Use Canonical Data Formats • Validate Input and Output to Mitigate Common Vulnerabilities	CWE-22

No.	Security-focused story	Backlog task(s)	SAFECode Fundamental Practice(s)	CWE-ID
17	As a(n) architect/ developer, I want to ensure **AND** as QA, I want to verify that cross-site scripting attacks are prevented	**[D]** Consider all input as malicious and filter according to the context. **[D/T]** When generating dynamic web pages, filter the input for any browser-executable content that is not intended (for example, from user-originated fields in a database). Consider all forms of input of content that might eventually be presented to and consumed by a browser, like events generated outside the system, log messages, arguments in a URL, form field values, etc. Perform this filtering at server-side, close to use. **[D]** When generating dynamic web pages, encode the output to the needed character set and explicitly declare it as part of the page. **[D]** When generating dynamic web pages, sanitize the output by properly escaping and quoting the dynamic content in a way to properly enforce separation of code and data according to the environment in use. **[D]** Use automated scanning tools in a credentialed mode with maximum coverage of the application interface to test for this vulnerability. **[D]** Use one of the many available libraries that takes cross-site scripting into account; create and enforce a single way of filtering input for cross-site scripting injection. **[D]** Always use cookies (authentication/session) with HttpOnly attribute.	• Use Anti-Cross Site Scripting (XSS) Libraries • Validate Input and Output to Mitigate Common Vulnerabilities	CWE-79

No.	Security-focused story	Backlog task(s)	SAFECode Fundamental Practice(s)	CWE-ID
18	As a(n) architect/developer, I want to ensure **AND** as QA, I want to verify that cross-site request forgery attacks are prevented	**[D]** Use one of the many available libraries and frameworks that takes CSRF into account. **[D]** Defend against cross-site scripting (see Story 17). **[A/D]** Add business logic and workflow steps to critical processes in the system, and make them out-of-band: send an email in case of password change, send a text message when changing a critical value. **[D/T]** Log critical operations and the details of their initiation and arguments. **[A/D]** Do not use HTTP GET for any method that effects a change in system state.	• Use Anti-Cross Site Scripting (XSS) Libraries • Validate Input and Output to Mitigate Common Vulnerabilities • Use Logging and Tracing	CWE-352
19	As a(n) architect/developer, I want to ensure **AND** as QA, I want to verify proper neutralization of Special Elements used in an OS Command ('OS Command Injection')	**[D]** Consider all input as malicious and filter according to the context. **[D]** Check all arguments to functions like exec() or system() for the expected format before executing. **[D]** Limit the use of external processes; prefer library calls. **[D]** Use static code analysis tools. **[D]** Consider the use of command shells [system()] as opposed to directly calling an executable [exec()] and its implications in command line arguments, like shell expansion. **[A/D]** Reduce the attack surface by adopting the backlog items of "Execution with Unnecessary Privileges."	• Validate Input and Output to Mitigate Common Vulnerabilities • Use Static Analysis Tools • Use Least Privilege	CWE-78

No.	Security-focused story	Backlog task(s)	SAFECode Fundamental Practice(s)	CWE-ID
20	As an architect/ developer I want to ensure **AND** as QA I want to verify that database queries function as expected by separating the data from the query	**[D]** Follow best practices defined in SAFECode's Fundamental Practices for Secure Software Development: "Avoid String Concatenation for Dynamic SQL Statements." **[A/D]** Utilize common frameworks or libraries (such as OWASP ESAPI) that provide a secure database query functionality, as defined below. **[A/D]** Use prepared statements with bind variables (parameterized queries) that automatically enforce the separation between data and code. **[A/D]** Deploy the database user accounts with minimal access rights (least privilege) required to perform the database action. Use separate accounts for different access roles (read only, read and update, etc.). **[A/D]** Validate all input to ensure only allowed (whitelisted) set of characters is processed. **[A/D]** If dynamic SQL or stored procedures with user-supplied data is required, escape all parameters carefully using a database-specific escaping routine. **[A/D/T]** Comparable techniques apply also to XPath, NoSQL and other database queries. **[T]** Test all database queries created or used by the application to ensure they conform to the actual intent and structure, and cannot be manipulated by user input. **[T]** Utilize common SQL injection payloads and static/dynamic code analysis to ensure database access works as designed. **[T]** Ensure only pre-defined set of characters (whitelist) is processed by the system.	• Avoid String Concatenation for Dynamic SQL Statements • Validate Input and Output to Mitigate Common Vulnerabilities • Use Least Privilege	CWE-89

No.	Security-focused story	Backlog task(s)	SAFECode Fundamental Practice(s)	CWE-ID
21	As an architect/developer I do not want to store **AND** as QA I want to verify that the system does not store hard-coded sensitive information	**[A/D]** Store all sensitive credentials outside of the code in an encrypted, access-restricted configuration file or database accessible to a very limited number of users. **[A/D]** If possible, use hashes or keys instead of passwords. **[A/D]** Develop the application so that the credentials can be changed regularly. **[A/D]** All access to the credentials shall be logged on a separate storage. **[T]** Verify the credentials are protected and access is logged. **[T]** Apply black box methods, system-call tracing, and static/dynamic analysis to detect hard-coding weaknesses.	• Use Least Privilege • Eliminate Weak Cryptography • Use Static Analysis Tools	CWE-798
22	As a(n) architect/developer, I want to ensure **AND** as QA, I want to verify that pointer-related checks are in place	**[D]** Check the results of all functions that return a pointer value and verify that the value is valid (e.g., not NULL and in range). **[T]** Use testing methods such as fuzzing and automated static code analysis tools to detect this flaw.	• Perform Fuzz/Robustness Testing	CWE-822 CWE-825 CWE-476

No.	Security-focused story	Backlog task(s)	SAFECode Fundamental Practice(s)	CWE-ID
23	As an architect/ developer I want to prevent **AND** as QA I want to verify there is no information exposure through error messages	**[A/D]** Ensure error messages only contain the minimal understandable details the user needs to know about the error. Do not return and display details such as stack traces, path names, or database query details in the response. **[A/D]** Do not use the client to hide server-side error details. The client should not make any other changes to the message other than apply formatting (style). **[T]** Systematically cause both in-the-system and application errors, and verify only approved information is returned and displayed back to the user. Ensure that not only web server errors (e.g., 404 page not found) are generic, but also that errors returned from the backend, such as the application or database server, do not contain any sensitive information (e.g., stack traces). **[T]** Use techniques such as fuzzing, static code analysis and fault injection to cause errors.	• Validate Input and Output to Mitigate Common Vulnerabilities	CWE-209

No.	Security-focused story	Backlog task(s)	SAFECode Fundamental Practice(s)	CWE-ID
24	As an architect/ developer I want to ensure **AND** as QA I want to verify URL redirection to un-trusted sites is not possible	**[A]** Define a strict whitelist of accepted redirection destinations. If this is not possible, ensure only valid URLs are accepted. **[A]** Deny access to all other destinations. **[A]** Consider whether the user should separately be warned/notified about the redirection ("Leaving our site"). **[A]** Consider verifying on the server side that the destination URL shall not redirect the user to a different destination. While sometimes this may serve a legitimate purpose, it is often used to fool the user, e.g., by using URL shortening services or open redirectors on other sites to hide the real destination. Follow all detected redirects (up to a predefined count) and display a warning if any/too many are detected. **[A/D]** If possible, use mapping to ensure the destination URL is retrieved from a safe repository, such as having "destination=123" to correspond with a certain predefined URL. **[A/D]** If displaying the URL back to the user, ensure it is sanitized via input validation and cross-site scripting prevention mechanisms (see Story 17), as defined in this document and other common best practices. **[T]** Verify redirection can only take the user to approved destinations. **[T]** If there is no approved list, ensure no cross-site scripting attacks can take place (see Story 17) by testing with malicious URLs (e.g., containing JavaScript or malformed payload).	• Validate Input and Output to Mitigate Common Vulnerabilities • Use Anti-Cross Site Scripting (XSS) Libraries	CWE-601

No.	Security-focused story	Backlog task(s)	SAFECode Fundamental Practice(s)	CWE-ID
25	As an architect/ developer I want to release a resource **AND** as QA I want to ensure resources are released after effective lifetime	**[A]** If possible, use a language that automatically handles garbage collection for de-allocated objects. **[D]** Consistently free all resources that have been reserved after they are no longer needed. **[D/T]** Verify that any failure in resource allocation places the system into a safe and recoverable posture and all throttling mechanisms function as intended. **[D]** Deploy built-in resource allocation limits in frameworks and platforms. [**T**] Test various parts of the system to ensure it is robust throughout. **[T]** Use methodologies such as static code analysis, load testing and fuzzing to identify unreleased resources.	• Use a Current Compiler Toolset • Use Static Analysis Tools • Perform Fuzz/ Robustness Testing	CWE-772
26	As a(n) architect/ developer, I want to ensure **AND** as QA, I want to verify that resources are initialized where necessary	**[A]** Consider using languages/frameworks that avoid these issues. [**A/D**] Ensure variables are properly initialized, especially when utilizing data from un-trusted sources. **[T]** Search for improperly initialized resources causing unusual error conditions in the system, using, for example, a static analysis tool, stress-testing, fuzzing, fault injection, and/or appropriate compiler settings.	• Use a Current Compiler Toolset • Use Static Analysis Tools • Perform Fuzz/ Robustness Testing	CWE-456

No.	Security-focused story	Backlog task(s)	SAFECode Fundamental Practice(s)	CWE-ID
27	As an architect/ developer I want to prevent **AND** as QA I want to verify controls against unauthorized access to user accounts by password guessing	**[A]** Ensure access restrictions are imposed after a predetermined number of unsuccessful login attempts. **[A/D]** Prompt the offending user with additional challenges, such as CAPTCHA or other intensive tasks before allowing to try again. If the attempts continue, shorten the cycle and increase the computational cost and complexity. **[A/D]** Increase the subsequent response times to slow down the attack. **[A/D]** Raise an alarm to the system administration team. **[A/D]** Lock the targeted account. **[A/D]** Potentially release the account lock after a defined time, or require further action to re-enable the account. **[A/D]** Disable access by the violating user at the appropriate level: IP blocking (may cause denial of service to legitimate users), page redirection or session termination. **[A/D]** Log the failed login attempt, account locking and reopening of an account with sufficient detail. **[A]** Consider also alternative misuse cases, e.g., where a single password is tested against multiple accounts. **[T]** Verify the implemented controls function as designed. Think of/test new ways of bypassing them.	• Use Logging and Tracing • Threat Modeling	CWE-307

No.	Security-focused story	Backlog task(s)	SAFECode Fundamental Practice(s)	CWE-ID
28	As an architect/ developer I want to ensure **AND** as QA I want to verify the user is protected by robust authentication and session management	**[A]** Define which areas of the application require authentication and authorization. **[A]** Utilize, as much as possible, common, robust authentication and session management solutions provided by platforms or frameworks. **[A/D]** Ensure credentials and sensitive session information is always transported over a secure channel such as the latest available version of TLS. **[A/D]** Prevent guessing or testing for existing usernames. If you must have this functionality, impose, e.g., throttling limits to prevent mass-harvesting of usernames. **[A/D]** Ensure, in cases of failed authentication attempts, the information returned to the user does not give away sensitive information such as whether the user account exists or not. **[A/D]** Ensure no channels exist to the system that have a weaker protection level than the rest of the channels. For example, if a service can be accessed from both the web browser and a native mobile application, they both should utilize a similar level of authentication and session management. **[A/D]** Ensure password or username brute force protection is built in as specified in Story 27 or other common best practices. **[A/D]** Ensure authentication and session management is enforced at all times (where needed). **[A/D]** Impose session expiration. **[A/D]** Follow best practices (e.g., OWASP Session Management Cheat Sheet) to prevent session management attacks. **[A]** Provide users convenient access to logout. ***continued on next page***	• Use Least Privilege • Threat Modeling	CWE-306

No.	Security-focused story	Backlog task(s)	SAFECode Fundamental Practice(s)	CWE-ID
		continued from previous page **[A]** Ensure sessions are terminated on the server side once they expire or the user logs out. **[A]** Provide a secure method for recovering forgotten usernames or passwords. Do not display whether a particular username exists in the system. **[A]** If using email as username, consider providing a nickname in cases where the username is publicly used to identify the user. Examples are discussion forums or software feedback/ratings pages. **[A]** Utilize CAPTCHA or similar complex methods to slow down repeated attack attempts. **[A/D]** For sensitive transactions, consider requiring re-authentication. **[A/D]** For administrative functionality, consider using strong (multi-factor) authentication and separate, private channels. Consider providing security-conscious normal users a stronger authentication mechanism utilizing, e.g., another channel such as text messages. **[A/D]** Consider preventing the browser to cache, e.g., the password and/or username. **[A/D]** If providing a "remember me" functionality, make that optional for the user (opt-in) and use a separate secure cookie. Use expiration for this option that balances security and user convenience. **[T]** Test all of the defined features by using static code analysis, manual methods (complemented with the help from security experts), and web application scanners. For more complete explanation of issues and test cases, please refer, e.g., to OWASP's Testing Project, Authentication Cheat Sheet and Session Management Cheat Sheet.		

No.	Security-focused story	Backlog task(s)	SAFECode Fundamental Practice(s)	CWE-ID
29	As a(n) architect/developer, I want to ensure **AND** as QA, I want to verify that strong encryption is used for sensitive information	**[A]** Identify data that should be classified as "sensitive." Some examples of sensitive data include (but are not limited to): • Login credentials and tokens • Cryptographic private keys • Financial data such as credit card or bank account numbers, balances, or loan applications • Personal health data and medical records • Sensitive personally identifiable information (PII) including government identification numbers (such as Social Security numbers) **[A/D/T]** Use secure channels (such as SSL/TLS or IPsec) to transmit sensitive data across trust boundaries. **[A/D/T]** Encrypt sensitive data when "at rest," i.e., when persisted to a file or other data store. **[A/D/T]** Control access to decryption keys. **[A/D]** Do not hardcode keys into application code. **[A/D/T]** Use strong cryptographic algorithms to encrypt data, use cryptographically strong random number generators to generate initialization vectors for encryption routines. **[A/D]** Use strong key derivation functions (such as PBKDF) when generating encryption keys from user-provided passwords. **[A/D/T]** Tokenize sensitive data whenever possible.	• Eliminate Weak Cryptography	CWE-311

No.	Security-focused story	Backlog task(s)	SAFECode Fundamental Practice(s)	CWE-ID
30	As a(n) architect/developer, I want to ensure **AND** as QA, I want to verify that sufficient transport layer protection exists	**[A]** Always use secure channels (such as SSL/TLS) to transmit authentication credentials. Always use secure channels to transmit authentication tokens, including HTTP authentication cookies. All resources served to an authenticated user should be performed over a secure channel. **[A/D/T]** As a defense-in-depth measure, apply the "secure" attribute to HTTP authentication cookies to help prevent them from being sent over non-SSL/TLS connections.	• Eliminate Weak Cryptography • Threat Modeling	CWE-759
31	As a(n) architect/developer, I want to ensure **AND** as QA, I want to verify that hashing uses a random salt	**[A/D/T]** When designing code to compare stored hashes to computed hashes (for example, when verifying a user's password in an authentication attempt), always store and append a per-hash unique, random salt value in order to hamper rainbow table attacks.	• Eliminate Weak Cryptography	CWE-327
32	As a(n) architect/developer, I want to ensure **AND** as QA, I want to verify that the cryptographic algorithm used is not broken or risky	**[A]** Always use vetted, industry-standard cryptographic algorithms to protect data. Do not attempt to develop your own algorithms. **[A]** Avoid using cryptographic algorithms with known weaknesses (such as MD) or that are beginning to show weakness (such as SHA-), whenever possible. **[A/D]** Take advantage of any cryptographic agility features supported by your application platform and language. **[A/D]** Avoid hard-coding particular algorithms into the application code. **[A/D]** Use abstract algorithm types and instantiate them from configuration files/stores.	• Eliminate Weak Cryptography	CWE-330

No.	Security-focused story	Backlog task(s)	SAFECode Fundamental Practice(s)	CWE-ID
33	As a(n) architect/developer, I want to ensure **AND** as QA, I want to verify use of sufficiently random values to prevent sensitive information from being seen by unauthorized people	**[A/D/T]** Use cryptographically-strong random number generators whenever you need to protect a resource by making its name, identifier, or other property difficult to guess. Some examples of this include: • Session or authentication identifier tokens • Initialization vectors for cryptographic keys • Temporary file or directory names • Temporary or initial user passwords **[A]** Consider using a hardware-based random number generator for situations where randomness is critical.	• Eliminate Weak Cryptography	CWE-129
34	As a(n) architect/developer, I want to ensure **AND** as QA, I want to verify proper validation of array index	**[A]** When possible, prefer developing in a language with automatic array boundary checking. **[A/D/T]** For languages without automatic array boundary checking (such as C/C++): • Periodically test the application with a static analysis tool designed to detect potential array index violations. Ideally this testing would be performed against the source code repository either on a daily or as-checked-in basis. • Periodically test the application interfaces (including file and network parsing code) with a fuzz testing tool; investigate any crashes the fuzzer generates. • If the language supports a function parameter annotation language, use it to both clarify parameter meaning for human readers and to assist static analysis tools. • Compile and link your application with available automatic memory protection options such as address space layout randomization (ASLR) and NX (No eXecute)-bit support.	• Use a Current Compiler Toolset • Use Robust Integer Operations for Dynamic Memory Allocations and Array Offsets • Use Static Analysis Tools • Perform Fuzz/Robustness Testing	CWE-434

No.	Security-focused story	Backlog task(s)	SAFECode Fundamental Practice(s)	CWE-ID
35	As a(n) architect/developer, I want to ensure **AND** as QA, I want to verify that the system does not permit unrestricted upload of files with dangerous type	**[A]** Ensure antivirus software is deployed to test all user-uploaded files. **[A/D/T]** Avoid storing user-supplied files in file form on web servers; instead, store them as binary objects in a data store. • When this design choice is infeasible, store the user-supplied files in a directory structure outside of the application webroot so that users cannot directly request them. • When possible, change the name of the uploaded file to a random value such as a GUID. Do not reveal this filename to the client. **[A/D/T]** Define a "whitelist" of allowed file types and reject any attempts to upload files of other types. **[D/T]** Review the configuration of the web server before deploying a web application and disable any unnecessary interpreters.	• Implement Sandboxing • Threat Modeling	CWE-676

No.	Security-focused story	Backlog task(s)	SAFECode Fundamental Practice(s)	CWE-ID
36	As a(n) architect/developer, I want to ensure **AND** as QA, I want to verify that the system does not allow use of potentially dangerous functions	**[D/T]** Periodically test the application with a static analysis tool designed to detect dangerous or risky functions for the particular language in which the application is written. Replace any detected dangerous functions with their safe equivalents. Some examples of dangerous functions include (but are not limited to): • C/C++: § strcpy § memcpy • PHP: § eval § exec • JavaScript: § eval **[T]** Periodically test the application interfaces (including file and network parsing code) with a fuzz testing tool; investigate any crashes the fuzzer generates. **[A/D/T]** If they are available, compile and link your application with any automatic memory protection options such as address space layout randomization (ASLR) and NX (No eXecute)-bit support.	• Minimize Use of Unsafe String and Buffer Functions • Use a Current Compiler Toolset • Use Static Analysis Tools • Perform Fuzz/Robustness Testing	CWE-676

For more information, please visit www.safecode.org.

SAFECode
Software Assurance Forum for Excellence in Code
(p) +1 781-876-8833 (f) +1 781-224-1239
feedback@safecode.org
www.safecode.org
Twitter: @SAFECodeForum
Facebook: www.facebook.com/SAFECode