**TECHNICAL ASSIGNMENT**

**TOAST.SWIFT**

Test case repository: <https://github.com/scalessec/Toast-Swift>

**Description:** Toast-Swift is a Swift extension that adds toast notifications to the UIView object class. It is intended to be simple, lightweight, and easy to use. Most toast notifications can be triggered with a single line of code. A library to show toasts / popup notifications inside iOS or MacOS applications in SwiftUI.

**1. Security Scanning**

|  |  |  |
| --- | --- | --- |
| **No.** | **Task** | **Result** |
| I | Use any open-source tool and setup scanning  Methodology used | 1. **Scanning tool**  |  |  |  | | --- | --- | --- | | **#** | **Tool** | **Methodology / Test Scope** | | 1 | Devskim | DevSkim is a security linter that highlights common security issues in source code.   * Built-in ruleset highlighting common security issues in source code * Support for scanning code contained in archives * Information and guidance provided for identified security issues * Broad language support including: C, C++, C#, Cobol, Go, Java, Javascript/Typescript, Python, and [more](https://github.com/Microsoft/DevSkim/wiki/Supported-Languages). | | 2 | Mayhem for API | An API Fuzzer that provides test coverage for APIs in the application portfolio.   * finds high-risk defects as OWASP ZAP * handles all REST verbs, and finds novel sequences of verbs to trigger previously unknown bugs. * testing valid, invalid and malicious requests. | | 3 | Detek | Static analysis on Android, JVM, JS, Native and multiplatform projects   * analyze code with multiple rule sets * flag the code that breaks any of its rules * detect potential bugs | | 4 | Mobsf | An automated, all-in-one mobile application (Android/iOS/Windows) pen-testing   * Static/dynamic analysis of applications: Android, Apple iOS, and Windows Phone * malware analysis | |  |  |  |   General methodology of scanning used in Github using the above tools as below: |
| Ii | Perform the security scanning on a test machine (with 5 security loopholes) | 1. **Findings** 2. **Vulnerabilities**   The results from the security scanning are listed below.   |  |  |  |  | | --- | --- | --- | --- | | **#** | **Vulnerability** | **Tool** | **Solution** | | 1 | Insecure URL | Devskim | enabling TLS (previously known as SSL) | | 2 | Do not store tokens or keys in source code. | Devskim | A token or key was found in source code. If this represents a secret, it should be moved somewhere else. | | 3 | The App logs information. Sensitive information should never be logged. | Mobsf (Mobile Security Framework) | One common solution is for an application to declare and use a custom log class, so that log output is automatically turned on/off. | | 4 |  |  |  | | 5 |  |  |  |  |  |  | | --- | --- | | 1 | **Insecure URL** | | 2 | **Do not store tokens or keys in source code** | | 3 | **The App logs information. Sensitive information should never be logged.** | | 4 |  | | 5 |  | |
| Iii | Prepare the scanning result and summary | 1. **Scanning result/Summary**   The results should not be interpreted as definitive measurement of the security posture of the application/code. Other elements used to assess the current security posture would include policy review, a review of internal security controls  and procedures, or internal red teaming/penetration testing.  Additional measure can also be used as control. Prefer to the sample list of NIST/OWASP code security practice. |
| iv | Present the findings and remediation required | **NIST , OWASP**  Other test case that can be used to check on the sample list of code security practice.   |  |  | | --- | --- | | **Test Case** | **is Vulnerable?** | | Site is partitioned into private and public URLs | Not Set | | Sensitive data is not hardcoded in configuration files | Not Set | |  |  | | Sensitive data is only transmitted over an SSL connection | Not Set | | User credentials are encrypted using framework/library using a stretching algorithm and uniquely salted | Not Set | |  | n/a | | Session cookies are encrypted and have a length of at least 128 bits, are complex | Not Set | | Session cookies are not persistent | Not Set | | Session cookies use cookie attributes httponly, secure, samesite | Not Set | | Strong passwords are enforced | Not Set | | Users are unable to login over GET, only POST | Not Set | | Block ciphers operate in CBC and IV values are not reused | Not Set | | Salts are unique per user, have over 64 bits of secure random data | Not Set | |  |  | | Sensitive transactions require re authentication | Not Set | | Authentication andAuthorization checks are done on each private request | Not Set | | Authorization checks are granular, per page / directory / action | Not Set | | Authorization checks are approriate for each HTTP Verb the application supports | Not Set | |  |  | | Session tokens are not passed in URLs | Not Set | | Session Cookies expire in a resonable amount of time | Not Set | | Logout will invalidate the session | Not Set | |  |  | |

**2. Code scanning**

|  |  |  |
| --- | --- | --- |
| **No.** | **Task** | **Result** |
| I | Use any open-source tool and setup scanning  Methodology used | 1. **Scanning tool**  |  |  |  | | --- | --- | --- | | **#** | **Tool** | **Methodology** | | 1 | Swiftlint | Identify and flag parts of the code that may not be following the stylistic rules | |  |  |  | |
| Ii | Perform the security scanning on a test machine (with 5 security loopholes)  Present the findings and remediation required | 1. **Findings**    * 1. **Vulnerabilities**   The results from the security scanning are listed below.   |  |  |  |  | | --- | --- | --- | --- | | **#** | **Vulnerability** | **Tool** | **Solution** | | 1 | Lines should not have trailing whitespace. | Swiftlint | White spaces do not affect coding function, but removing them definitely makes the code much cleaner and avoids unwanted small mistakes. | | 2 |  |  |  | | 4 |  |  |  | | 5 |  |  |  |  |  |  | | --- | --- | | **1** | **Lines should not have trailing whitespace.** | |  |  | |  |  | |  |  | |
| Iii | Prepare the scanning result and summary | The results should not be interpreted as definitive measurement of the security posture of the application/code. Other elements used to assess the current security posture would include policy review, a review of internal security controls and procedures, or internal red teaming/penetration testing.  Additional measure can also be used as control. Prefer to the sample list of code security practice. |

Other reference :

Other test case that can be used to check on the code security practice.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Test Type** | **Test Area** | **Test Case** | **Test Result  (No Issue, Finding, NA, Not Set )** | **Remark** |
| Code Security Test | Application Output | All header output is URL encoded | Not Set |  |
| Code Security Test | Application Output | All page output is properly encoded | Not Set |  |
| Code Security Test | Application Output | Cache headers are properly set on sensitive data | Not Set |  |
| Code Security Test | Application Output | Error messages aren't user controllable | Not Set |  |
| Code Security Test | Application Output | Error messages don’t reveal sensitive information | Not Set |  |
| Code Security Test | Application Output | Security headers are properly set on the application | Not Set |  |
| Code Security Test | Application Output | Sensitive Application information is not revealed to the user | Not Set |  |
| Code Security Test | Authentication | Passwords are encrypted using a framework / library | Not Set |  |
| Code Security Test | Authentication | Strong password policy in effect | Not Set |  |
| Code Security Test | Authentication | Test for user enumeration | Not Set |  |
| Code Security Test | Authentication | User credentials are encrypted using framework/library | Not Set |  |
| Code Security Test | Authentication | Users are unable to login over GET, only POST | Not Set |  |
| Code Security Test | Authorization | Authentication and Authorization checks are done on each private request | Not Set |  |
| Code Security Test | Authorization | Authorization checks are appropriate for each HTTP Verb the application supports | Not Set |  |
| Code Security Test | Authorization | Authorization checks are granular, per page / directory / action | Not Set |  |
| Code Security Test | Authorization | Sensitive transactions require re authentication | Not Set |  |
| Code Security Test | Configuration | Dependencies are up to date | Not Set |  |
| Code Security Test | Configuration | Develop and test code are properly segregated from production | Not Set |  |
| Code Security Test | Configuration | Sensitive data is not hard-coded in configuration files | Not Set |  |
| Code Security Test | Cryptography | Block ciphers operate in CBC and IV values are not reused | Not Set |  |
| Code Security Test | Cryptography | Check for known bad ciphers (RC4), cryptographic hash functions (MD5) and insecure random number generation | Not Set |  |
| Code Security Test | Cryptography | Salts are unique per user, have over 64 bits of secure random data | Not Set |  |
| Code Security Test | Cryptography | User passwords are encrypted using a stretching algorithm and uniquely salted | Not Set |  |
| Code Security Test | Data Validation | All user input is validated for proper type, length, format and range | Not Set |  |
| Code Security Test | Data Validation | Does invalid input trigger handled exceptions | Not Set |  |
| Code Security Test | Data Validation | Special characters are sanitized before being used in external systems, like databases | Not Set |  |
| Code Security Test | Data Validation | Uploaded files are validated for content type, size, file type and filename | Not Set |  |
| Code Security Test | Data Validation | Validation on user input is done server side | Not Set |  |
| Code Security Test | Log Management | All sensitive system actions are logged with the following: Where, What, When, Who, How answered | Not Set |  |
| Code Security Test | Log Management | All sensitive user actions are logged with the following: Where, What, When, Who, How answered | Not Set |  |
| Code Security Test | Log Management | Sensitive info is not logged | Not Set |  |
| Code Security Test | Log Management | User input is sanitized and validated before being placed in application logs | Not Set |  |
| Code Security Test | Secure Transmission | Sensitive data doesn’t leak to non private channels | Not Set |  |
| Code Security Test | Secure Transmission | Sensitive data has been secured in memory, storage and transit | Not Set |  |
| Code Security Test | Secure Transmission | Sensitive data is only transmitted over an SSL connection | Not Set |  |
| Code Security Test | Secure Transmission | Site is partitioned into private and public URLs | Not Set |  |
| Code Security Test | Session Management | Establish how session management is handled in the application | Not Set |  |
| Code Security Test | Session Management | Logout will invalidate the session | Not Set |  |
| Code Security Test | Session Management | Session cookies are encrypted and have a length of at least 128 bits and are complex | Not Set |  |
| Code Security Test | Session Management | Session cookies are not persistent | Not Set |  |
| Code Security Test | Session Management | Session Cookies expire in a reasonable amount of time | Not Set |  |
| Code Security Test | Session Management | Session cookies use cookie attributes httponly, secure, samesite | Not Set |  |
| Code Security Test | Session Management | Session tokens are not passed in URLs | Not Set |  |
| Mobile Apps Test | App permissions | Behavior when the user grants/revokes certain permissions | Not Set |  |
| Mobile Apps Test | [App permissions](https://github.com/gaurav-singh/testing-checklists/blob/master/mobile_testing.md#app-permissions) | Does the app require correct level of permissions and the behavior around those | Not Set |  |
| Mobile Apps Test | App permissions | Only necessary permissions are requested | Not Set |  |
| Mobile Apps Test | [App upgrades](https://github.com/gaurav-singh/testing-checklists/blob/master/mobile_testing.md#app-upgrades) | Can user proceed with any in-flight flows after app upgrades? | Not Set |  |
| Mobile Apps Test | [App upgrades](https://github.com/gaurav-singh/testing-checklists/blob/master/mobile_testing.md#app-upgrades) | Does app work when upgraded to a new version? | Not Set |  |
| Mobile Apps Test | Backend responses and conditions | 2XX (Success) | Not Set |  |
| Mobile Apps Test | Backend responses and conditions | 3XX (Redirects) | Not Set |  |
| Mobile Apps Test | Backend responses and conditions | 4XX (Client side errors - Bad requests) | Not Set |  |
| Mobile Apps Test | Backend responses and conditions | 5XX (Server side errors) | Not Set |  |
| Mobile Apps Test | Backend responses and conditions | Does the app block the user from proceeding when waiting for an API when not needed? | Not Set |  |
| Mobile Apps Test | Backend responses and conditions | Does the app engage user while waiting for an API response (with an animation/loader) | Not Set |  |
| Mobile Apps Test | Backend responses and conditions | How the app handles cases when server is undergoing deployments? | Not Set |  |
| Mobile Apps Test | Backend responses and conditions | How the app handles when the API times out? | Not Set |  |
| Mobile Apps Test | [Backend responses and conditions](https://github.com/gaurav-singh/testing-checklists/blob/master/mobile_testing.md#backend-responses-and-conditions) | Status codes check | Not Set |  |
| Mobile Apps Test | [Boundary values](https://github.com/gaurav-singh/testing-checklists/blob/master/mobile_testing.md#boundary-values) | Check for value/length as per below: | Not Set |  |
| Mobile Apps Test | Boundary values | max | Not Set |  |
| Mobile Apps Test | Boundary values | max + 1 | Not Set |  |
| Mobile Apps Test | Boundary values | min | Not Set |  |
| Mobile Apps Test | Boundary values | min - 1 | Not Set |  |
| Mobile Apps Test | Date and Times | Different datetime formats | Not Set |  |
| Mobile Apps Test | [Date and Times](https://github.com/gaurav-singh/testing-checklists/blob/master/mobile_testing.md#date-and-times) | Future datetimes | Not Set |  |
| Mobile Apps Test | Date and Times | Holidays | Not Set |  |
| Mobile Apps Test | Date and Times | Invalid datetimes (32 days, 13 month, 25 hours, 61 minutes, 61 second) | Not Set |  |
| Mobile Apps Test | Date and Times | Leap days | Not Set |  |
| Mobile Apps Test | Date and Times | Past datetimes | Not Set |  |
| Mobile Apps Test | Date and Times | Timezones | Not Set |  |
| Mobile Apps Test | Date and Times | Weekends | Not Set |  |
| Mobile Apps Test | [Error conditions](https://github.com/gaurav-singh/testing-checklists/blob/master/mobile_testing.md#error-conditions) | Correct error messages are displayed in different conditions | Not Set |  |
| Mobile Apps Test | [Error conditions](https://github.com/gaurav-singh/testing-checklists/blob/master/mobile_testing.md#error-conditions) | CTA (Call to action) should be as per the application flow (e.g. Do not ask user to retry in case of any terminal state in the app) | Not Set |  |
| Mobile Apps Test | Feature Toggles | Any data created with old/new app should be compatible and should not lead to app crashes | Not Set |  |
| Mobile Apps Test | Feature Toggles | Feature turned OFF | Not Set |  |
| Mobile Apps Test | Feature Toggles | Feature turned ON | Not Set |  |
| Mobile Apps Test | [Feature Toggles](https://github.com/gaurav-singh/testing-checklists/blob/master/mobile_testing.md#feature-toggles) | How does the app respond to future toggles | Not Set |  |
| Mobile Apps Test | Inputs | Copy paste values | Not Set |  |
| Mobile Apps Test | Inputs | Leading or trailing whitespaces | Not Set |  |
| Mobile Apps Test | Inputs | Line breaks | Not Set |  |
| Mobile Apps Test | Inputs | Non ASCII characters (Swedish/Russian) | Not Set |  |
| Mobile Apps Test | Inputs | Null/Empty/Blank | Not Set |  |
| Mobile Apps Test | Inputs | Numeric separators (1000, 1.000, 1,000) | Not Set |  |
| Mobile Apps Test | [Inputs](https://github.com/gaurav-singh/testing-checklists/blob/master/mobile_testing.md#inputs) | Overflow values (Enter value > max allowed value for a given data type of the field) | Not Set |  |
| Mobile Apps Test | Inputs | Special Chars (!@#$%^&\*()) | Not Set |  |
| Mobile Apps Test | Inputs | String characters (If numeric) and numeric (If String) | Not Set |  |
| Mobile Apps Test | [Interruptions](https://github.com/gaurav-singh/testing-checklists/blob/master/mobile_testing.md#interruptions) | How does the app respond to any interruptions while use? | Not Set |  |
| Mobile Apps Test | Interruptions | If Incoming call, message, PN causes the user to switch context | Not Set |  |
| Mobile Apps Test | Interruptions | If killed and restarted | Not Set |  |
| Mobile Apps Test | Interruptions | If put in background and resumed | Not Set |  |
| Mobile Apps Test | [Navigations](https://github.com/gaurav-singh/testing-checklists/blob/master/mobile_testing.md#navigations) | Back button | Not Set |  |
| Mobile Apps Test | Navigations | Pagination (Move forward on last or move backward on first) | Not Set |  |
| Mobile Apps Test | Navigations | Sortnig on columns (In case of a list/table control) | Not Set |  |
| Mobile Apps Test | Onboarding flows | Check different user personas | Not Set |  |
| Mobile Apps Test | Onboarding flows | How do we introduce user to new features in the product? Ease of comprehension | Not Set |  |
| Mobile Apps Test | Onboarding flows | These flows should be shown only a certain no of times | Not Set |  |
| Mobile Apps Test | [Onboarding flows](https://github.com/gaurav-singh/testing-checklists/blob/master/mobile_testing.md#onboarding-flows) | UX when a first time user engages with the app (Introduction flows) | Not Set |  |
| Mobile Apps Test | Performance | Extremely high load from concurrent users | Not Set |  |
| Mobile Apps Test | [Performance](https://github.com/gaurav-singh/testing-checklists/blob/master/mobile_testing.md#performance) | How responsive is the app when: | Not Set |  |
| Mobile Apps Test | Performance | Normal load | Not Set |  |
| Mobile Apps Test | Performance | When app is used in low memory configs/devices | Not Set |  |
| Mobile Apps Test | Performance | When too many apps are open | Not Set |  |
| Mobile Apps Test | Performance | X times normal load | Not Set |  |
| Mobile Apps Test | Push notifications | Correct text for different app states? | Not Set |  |
| Mobile Apps Test | [Push notifications](https://github.com/gaurav-singh/testing-checklists/blob/master/mobile_testing.md#push-notifications) | Does the app generate and handle push notifications correctly? | Not Set |  |
| Mobile Apps Test | Push notifications | Tap on PN to redirect user to correct screen | Not Set |  |
| Mobile Apps Test | Security | App should handle different user roles and ensure correct information is displayed to the user with his role/priviledges | Not Set |  |
| Mobile Apps Test | Security | App should never show sensitive db, server informations | Not Set |  |
| Mobile Apps Test | Security | Local storage should not show sensitive information | Not Set |  |
| Mobile Apps Test | [Security](https://github.com/gaurav-singh/testing-checklists/blob/master/mobile_testing.md#security) | SQL Injections | Not Set |  |
| Mobile Apps Test | [User Input](https://github.com/gaurav-singh/testing-checklists/blob/master/mobile_testing.md#user-input) | Does the app handle different types of inputs and allows user to enter invalid inputs? | Not Set |  |
| Web Application Test | Cryptography | Check for proper use of salting | Not Set |  |
| Web Application Test | Cryptography | Check for randomness functions | Not Set |  |
| Web Application Test | Cryptography | Check for weak algorithms usage | Not Set |  |
| Web Application Test | Cryptography | Check for wrong algorithms usage depending on context | Not Set |  |
| Web Application Test | Cryptography | Check if data which should be encrypted is not | Not Set |  |
| Web Application Test | Cryptography | Risky Functionality - File Uploads | Not Set |  |
| Web Application Test | Cryptography | Test that acceptable file types are whitelisted | Not Set |  |
| Web Application Test | Cryptography | Test that all file uploads have Anti-Virus scanning in-place. | Not Set |  |
| Web Application Test | Cryptography | Test that file contents match the defined file type | Not Set |  |
| Web Application Test | Cryptography | Test that file size limits, upload frequency and total file counts are defined and are enforced | Not Set |  |
| Web Application Test | Cryptography | Test that files and other media are integrated with the authentication and authorisation schemas | Not Set |  |
| Web Application Test | Cryptography | Test that unsafe filenames are sanitised | Not Set |  |
| Web Application Test | Cryptography | Test that uploaded files are not directly accessible within the web root | Not Set |  |
| Web Application Test | Cryptography | Test that uploaded files are not served on the same hostname/port | Not Set |  |
| Web Application Test | Data Validation | Compare client-side and server-side validation rules | Not Set |  |
| Web Application Test | Data Validation | Test for auto-binding | Not Set |  |
| Web Application Test | Data Validation | Test for Code Injection | Not Set |  |
| Web Application Test | Data Validation | Test for Command Injection | Not Set |  |
| Web Application Test | Data Validation | Test for Cross Site Flashing | Not Set |  |
| Web Application Test | Data Validation | Test for DOM based Cross Site Scripting | Not Set |  |
| Web Application Test | Data Validation | Test for Expression Language Injection | Not Set |  |
| Web Application Test | Data Validation | Test for Format String | Not Set |  |
| Web Application Test | Data Validation | Test for HTML Injection | Not Set |  |
| Web Application Test | Data Validation | Test for HTTP parameter pollution | Not Set |  |
| Web Application Test | Data Validation | Test for HTTP Splitting/Smuggling | Not Set |  |
| Web Application Test | Data Validation | Test for HTTP Verb Tampering | Not Set |  |
| Web Application Test | Data Validation | Test for IMAP/SMTP Injection | Not Set |  |
| Web Application Test | Data Validation | Test for incubated vulnerabilities | Not Set |  |
| Web Application Test | Data Validation | Test for LDAP Injection | Not Set |  |
| Web Application Test | Data Validation | Test for Local File Inclusion | Not Set |  |
| Web Application Test | Data Validation | Test for Mass Assignment | Not Set |  |
| Web Application Test | Data Validation | Test for NoSQL injection | Not Set |  |
| Web Application Test | Data Validation | Test for NULL/Invalid Session Cookie | Not Set |  |
| Web Application Test | Data Validation | Test for Open Redirection | Not Set |  |
| Web Application Test | Data Validation | Test for ORM Injection | Not Set |  |
| Web Application Test | Data Validation | Test for Overflow (Stack, Heap and Integer) | Not Set |  |
| Web Application Test | Data Validation | Test for Reflected Cross Site Scripting | Not Set |  |
| Web Application Test | Data Validation | Test for Remote File Inclusion | Not Set |  |
| Web Application Test | Data Validation | Test for SQL Injection | Not Set |  |
| Web Application Test | Data Validation | Test for SSI Injection | Not Set |  |
| Web Application Test | Data Validation | Test for Stored Cross Site Scripting | Not Set |  |