Application Security - New Application Assessments - Template

There are a million questions that application / product security teams can ask developers before reviewing an application. Here's a few fundamental items that you may want to consider.

WHY THIS CHECKLIST?

- The use of "you" and "your" is meant to invoke a sense of responsibility. Security is merely a consultant for the risk owners – business and product engineering.
- The world of product security is huge.
    - This checklist attempts to quickly identify scope and priorities for all parties. If the application being deployed is internal only with no sensitive data, then the engagement should end early as needed.
    - Developers have context that security personnel will never have. Application security engineers should always ask, **"What's the worst that can happen? (Question 8)."**

HOW TO USE:

1. Modify the checklist below as needed to fit your company's specific needs.
2. Disseminate the checklist to all product engineering teams
3. Require that each development team requiring sign-off complete the checklist to the best of their ability before meeting with your team. They get bonus points if they can provide everything in advance.
4. Inquire regularly for feedback and changes to this checklist (from your product engineering teams especially). Changes should be accepted willingly to improve readability and effect positive outcomes.
5. See other questions to ask below.

App Name:	*Name and any other important identifiers?*
Repository URL:	*Location where the source code can be found?*
Test Environment URL:	*Test deployment location?*
Description:	*What does the application do? Feel free to provide a link to README or other documentation.*
Business Unit/Team Name:	*Which team owns the application?*
Product Owner:	*Besides your team who owns the risk?*

1. How sensitive is the application?

- ☐ *Is your application exposed to the public network specifically meaning is it accessible outside of the company network (ie. VPN)?*
- ☐ *Does your application send, receive or store sensitive, regulated data (ie. patient health information, insurance PII or PCI-DSS sensitive authentication data). If **YES**, see Step 5.*
- ☐ *How many humans would be affected? (ie. patient health records, user accounts, etc)*

2. Who will use your application?

- ☐ *Corporate clients and partners? If so, whom?*
- ☐ *Internal staff*
- ☐ *External users (ie. self-service)*

3. Have you completed a basic threat model or architecture diagram?

In my diagram, I have included the following:

- ☐ *The data that I need to protect such as PHI, PII, and sensitive business data.*
- ☐ *A list of my application's data flows including data stores and incoming/outgoing flows.*
- ☐ *A list of possible routes into my application including sign up/sign in forms, api endpoints, file upload forms, search boxes, privileged user roles, etc.*
- ☐ *A list of controls to protect my application and its data. This may include authentication, access control, user monitoring, rate limiting, etc.*

4. Does your application have basic security controls configured?

- ☐ *My application has unit tests in place.*
- ☐ *My application has key security tools configured in CI/CD*
  - ☐ *<Insert static analysis tool>*
  - ☐ *<Insert patch-level verification or software composition analysis tool>*
  - ☐ *<Insert dynamic scanning tool>*
- ☐ *I have checked that all security tools have run successfully.*
- ☐ *All identified issues have been fixed and/or exceptions have been documented.*
  - ☐ *Exceptions are listed here: (ie. JIRA-123)*
- ☐ *My team has reviewed all pertinent security guidance and/or secure code checklists. <Insert link here>*

5. Regulatory guidance

- ☐ *Please follow specific guidance for regulated data.*
  - *<ADD GUIDANCE HERE FOR SPECIAL INSTRUCTIONS SUCH AS MANDATORY VULNERABILITY ANALYSES OR INVOLVEMENT FROM 3RD PARTIES SUCH AS LEGAL, COMPLIANCE OR AUDIT.>*

6. How will you detect bad user behavior?

- ☐ *Our logs contain the information needed to identify anomalous user behavior including:*
  - ☐ *All successful and unsuccessful authentication operations (ie. login, logoff, password reset)*

- ☐ *All successful and unsuccessful access control operations (ie. user creation, permissions changes, email changes)*
- ☐ *Create, read, update and destroy operations to sensitive data*
- ☐ *For more information: <add link to 'How to Log' instructions>*

☐ *We actively monitor our logs for anomalous activity via <insert tool here>*

7. What will you do if there is an incident or breach?

☐ *My team has a practiced security incident plan in place for this application.*

☐ *Our team can be contacted/paged here:*

8. What's the worst thing that can happen?

List any remaining concerns or risks that have been identified by your team but that have not been mitigated. Include your team's best guess that the risk may be realized and the impact it may have on the application, product or the company as a whole.

Description	Likelihood	Impact	Notes
Ex. "This unprotected endpoint is highly likely to be discovered and it will lead to a breach of more than 5 million records of regulated, sensitive user data.	*HIGH*	*CRITICAL*	

We're ready to deploy!

☐ *This application meets/exceeds our team's definition of done and quality of standards.*

☐ *This application has completed all required steps for deployment:*

- ☐ *Code review*
- ☐ *Risk and/or security review*
- ☐ *Engineering manager or designate sign-off*

☐ *The product team (product owner & development team) ACCEPTS all remaining unmitigated risks associated with the application.*

Notes for Application Security Team
☐ See A Simple Rubric for Application Security Engineers for possible checklist items ☐ Assessment meets or exceeds team's quality requirements? ○ Regulatory Security Requirements ○ Information Gathering & Reconnaissance ○ Authentication ○ Access Controls & Authorization ○ Application Logic ○ Session Management ○ Injection ○ Data Input Validation ○ Cross Site Scripting ○ Application Hosting ☐ Application needs vulnerability analysis or pentest before deployment?

Resources:

- Philippe De Ryck - AppSec is too hard?
- https://github.com/OWASP/ASVS/
- https://www.pcisecuritystandards.org/document_library
- https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
- https://www.hhs.gov/hipaa/for-professionals/security/nist-security-hipaa-crosswalk/index.html