Application Security Rubric

If your ASE's have the responsibility of performing new application or feature reviews, it can be difficult for new members of an application security team to gain the confidence to assess an application, especially with engineers and product leadership urging them to "sign-off" on an application before a production deployment.

This guide is by no means meant to be exhaustive but a starting point for discussion with your technical SME's to make the world of assessing an application smaller.

GRADING:

- **PASS:** Findings are medium-to-low risk and must be documented in an issue tracker per regulatory guidelines.
  - Team may proceed to production.

- **FAIL:** A failing attribute does not necessarily fail the app/feature as a whole. For instance, a public, static site may not meet the logging standard. However, some failures will fail the app/feature such as not having access control around sensitive operations.
  - Unmitigated risks must be documented in team's issue tracker
  - Critical and high risks will be tracked via risk management for follow-up per policy
  - Compensating controls will be required before the team proceeds to production.

- **CONCERNING:** Product or feature may require additional testing, information gathering or compensating controls before production deployment.

ASCERTAINING IMPACT AND LIKELIHOOD?

1. **Impact** - Can we quantify it in dollars roughly? Encourage your team to always communicate impact in dollars when engaging product or engineering leaders. See "Impacting Growth" and "Creating a high-growth app-sec program" for more information.

   a. Will the vulnerability impact product revenue?
   b. How many sensitive data records will be affected? If we know the number of records we can utilize our revenue per affected record to identify a total cost.
   c. How many users will be affected?
      i. External users (Self-enrollment)
      ii. Enterprise users

2. **Likelihood** - How easy is it to exploit the vulnerability?
   a. Layperson = Expected

b. Script kiddie = Likely/Possible
c. Experienced hacker / criminal group = Likely/Possible
d. Nation-state level resources needed = Remote

	PASS	FAIL	CONCERNING
Financial Impact *As identified by leadership (ex. “Don’t bother me about this unless it’s going to cost us $50m)*	< minimum risk exposure in dollars	> minimum risk exposure in dollars	N/A
Public Access	Application is internal	Application is external	N/A
Sensitive Data	< minimum # of unencrypted, sensitive data records requiring notification (ie. 500 in the case of HIPAA)	> minimum # of unencrypted, sensitive data records resulting in catastrophic loss in the case of a breach	> minimum # of unencrypted, sensitive data records requiring notification
Authentication	Has strong, well-tested authentication measures that protect sensitive data	Lacks authentication or has vulnerability where this is a high likelihood that authentication can be subverted trivially	N/A
Access Control	Has well-designed access controls mechanism where there is little to no risk of vertical or horizontal privilege escalation	Lacks access control. Users are able to read, update or delete others sensitive data	N/A
Encryption	Meets industry and company standards.	Does NOT meet industry and company standards.	N/A
Security Checklist *A technical checklist and/or secure coding guidelines for engineering teams to review.*	Has completed new application or feature checklist	Has NOT completed new application or feature checklist	N/A
Threat Model	Has documented threat model; recently created or updated within ***<time period>***	Does NOT have threat model	N/A
Audit Controls	Meets **Logging Standard**	Does NOT meet **Logging Standard**	N/A

OWASP ASVS https://owasp.org/www-project-application-security-verification-standard/	Meets appropriate ASVS recommendations	Does NOT meet appropriate ASVS recommendations	N/A
Regulatory Gap Analysis	Meets appropriate regulatory requirements	Does NOT meet appropriate regulatory requirements	N/A

Likelihood		Description	Probability
5	Expected	Is expected to occur in most circumstances	>85%
4	Likely	Will probably occur in most circumstances	60-85%
3	Possible	Might occur in some circumstances	30-60%
2	Unlikely	Could occur in some circumstances	10-30%
1	Remote	Could occur but only in exceptional circumstances	<10%

Impact	Category	Description
5	Critical	Potentially irrecoverable losses; complete inability to continue operations
4	Significant	Significant impact to the business and/or financial losses; recoverable in the long run though sustained losses in stakeholder groups
3	Moderate	Significant impact to the business and/or financial losses; recoverable in the long run though sustained losses in stakeholder groups
2	Minor	Minor impact to the overall business; temporary disruption to

		the organization
1	Insignificant	Minimal impact to the business with losses limited to distinct business units