

Your AppSec Program Training Course

From SheHacksPurple.dev

Assignment #2: AppSec Activities

Your Name:

Choosing activities to reach your goals. Below is the list of activities we discussed in class. Which ones will help you reach the goals you identified in the previous chapter? Which ones will help you reach your goals the most quickly? The least-expensive? The most reliably? Which ones require the most time or manual toil?

- Vulnerability (VA) Scans and Assessments *
- Threat Modeling *
- Secure Code Reviews (Static Application Security Testing)
- Software Composition Analysis (SCA)
- Penetration Tests (PenTests) *
- Responsible Disclosure & Bug Bounties
- Developer Education and Advocacy Programs
- Helpful Policies, Guidelines and Standards
- Giving Developers Security Tools
- Secure Coding Library/ Templates
- Security Reference Materials (including hardening guides) *
- 'The Partnership Model' for projects *
- Creating Custom Tools
- Gathering Metrics/ Measurement *
- Targeting an Entire Bug Classes
- Security Regression Testing (with unit tests)
- Red Teaming *
- CTFs
- Adding Security to a Pipeline
- Creating an asynchronous sec pipeline
- Adding shield for your app (WAF/RASP) * (WAF only)
- Chaos Engineering *
- Security Sprints
- Forcing secure coding with IDE tooling
- Forcing use of secure packages with proxying to secure package management tools

* These apply to both Custom Apps and COTS (Configurable Off The Shelf software)

1)
AppSec Program Goal #1

AppSec Activities that could help you reach this goal:

2)
AppSec Program Goal #2

AppSec Activities that could help you reach this goal:

3)
AppSec Program Goal #3

AppSec Activities that could help you reach this goal:



