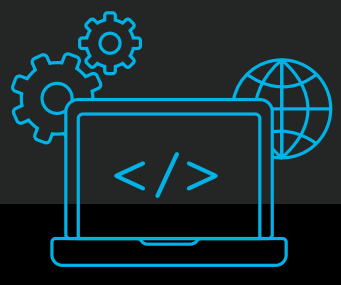
VERACODE

Tips to Follow on Your AppSec Journey

In AppSec, and most other areas of life, there are the best practices and then there are the practicalities of what you can actually achieve today.

01



BEST PRACTICE

Use multiple AppSec testing types.

PRACTICAL FIRST STEP

Based on your risk tolerance, release cadence, and programming languages, start by implementing the AppSec test that will have the most impact, in the shortest amount of time, for the least amount of money. Then expand to other testing types over time.

2 of 5 Top vulnerability categories found during dynamic testing weren't among the top five found by static.[1]

02

BEST PRACTICE

Shift security testing left.

PRACTICAL FIRST STEP

Help the security and development teams understand each other's roles to ensure that security testing can be integrated into the development cycle organically.

50% higher profit growth is seen in companies that integrate security tests into their development process.[2]

03

BEST PRACTICE

Find flaws and fix them fast.

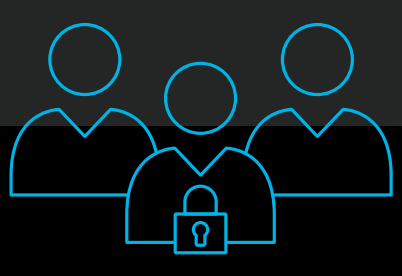
PRACTICAL FIRST STEP

A practical first step in remediation is to revisit your AppSec policy and make sure it includes guidance on prioritizing flaws — consider not only the criticality of the application, but also the exploitability of a vulnerability.

THE LARGEST AMOUNT OF DEBT ACROSS APPLICATIONS COMES FROM:

1. Cross-site Scripting (XSS)
2. Injection
3. Authentication
4. Misconfiguration flaws[3]

04



BEST PRACTICE

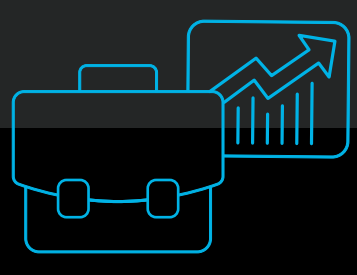
Have security champions on every development team.

76% of developers were not required to take security courses in college.[4]

PRACTICAL FIRST STEP

Building a team of security champions takes time. Concentrate on getting everyone on board with the concept and help the security and development teams build a relationship.

05



BEST PRACTICE

Measure and report on the success of your AppSec program.

PRACTICAL FIRST STEP

Bringing too many metrics to your executives early on can be overwhelming. Start by presenting one metric: how your AppSec program is complying with your internal AppSec policy.

Want to learn more about the steps you can take when starting an AppSec program?

DOWNLOAD OUR RECENT GUIDE

AppSec Best Practices vs. Practicality

VERACODE

[1] AppSec: What Not to Do: The Top 6 Application Security Mistakes; [2] Integrating Security into the DNA of Your Software Lifecycle, Freeform Dynamics and CA Technologies, 2018; [3] State of Software Security, Volume 10, By the Numbers, Veracode, 2019; [4] DevOps Global Skills Survey Report, Veracode, 2017