Luca Carettoni
Application Security Recipes for Fast-Paced Environments
About Me

• AppSec since 2004
• Doyensec Co-founder
• Former AppSec Manager (LinkedIn), Director of Security (Addepar), Senior Security Researcher (Matasano), ....
• Warsaw ←→ San Francisco
Fast-Paced Environments
For software development

- New code is quickly created and deployed
  - e.g. Startups, Agile SDLC shops, ...
- Facebook’s “Move Fast and Break Things”
Good Application Security is all about

PEOPLE
PROCESSES
TECHNOLOGY
Good Application Security in fast-paced environments is all about

MANY TALENTED PEOPLE
EFFICIENT PROCESSES
STATE-OF-THE-ART TECHNOLOGY
PEOPLE
Security Talent Shortage

• 189,000 LinkedIn members in InfoSec roles
• 10 countries make up 75% of the talent poll
• Employer demand
  • US 4:3
  • Singapore 5:1
  • ...
  • Italy 50:1
• https://engineering.linkedin.com/security/exploring-information-security-talent-pool
How many?

• Rule of 2% works for small companies only
• In practice, you’re lucky if you have budget and you can hire 1%
PEOPLE - Take away

• Talented security professionals are difficult to find, hire, engage and retain
• Schools, universities won't catch up soon
• They’re your most precious asset
PROCESSES
Waterfall
DevOps

- Code
- Build
- Test
- Plan
- Release
- Monitor
- Deploy
- Operate
Divide et impera
Risk matrix to drive testing effort

![Risk Matrix Diagram](image-url)
Likelihood

• Service exposure
• Software maturity
• Use of modern web frameworks with built-in security mechanisms
• Confidence around your detection mechanisms and incident response
Impact

• Value of protected assets
• Bug classes
  • Focus on game-over bugs only
  • Focus on mitigations
• Prefer code coverage vs attack coverage
Home-field advantage

• Bugs tend to cluster. Spend time doing extra clean-up
• Always combine dynamic testing with source code reviews (*graybox* testing)
• Invest in framework-level protections
Translate security in numbers

• Build your own security metrics
  • # bugs discovered before prod
  • # bugs discovered by external parties
  • # bugs fixed
  • # incidents
  • # bug bounty payouts
  • ...

• Include those metrics in your reports to both developers and exec
PROCESSES - Take away

• Releasing more code requires continuous AND focused testing
• Forget the “once-a-year pentest" approach
• Use likelihood and impact to drive your testing effort
• Maximize your home-field advantage
• Share your numbers with the rest of the organization
True fact

- No security boxes with blinking lights that you can plug-in and walk away from
(Most) security tools are expensive

• Not just talking about $$$
• Evaluating, installing, tuning a security tool take time and resources
• Also, you need knowledgable people to properly install, use and maintain
One step at a time

• Don’t aim at the top from day one
• Instead, improve overtime

• E.g. Fortify SCA vs RepoGuard vs $grep
Automation

• Take more risk today, and invest in security automation for tomorrow
• “If it can be automated, it should be automated”
A few examples 1/2

• Continuous port-scanning with a $0 solution based on NMAP
  • Add NSE scripts and you get basic vulnerability scanning
• AWS/Azure/<yourFavouriteCloud> APIs for enumeration and services discovery
• SSH key provisioning service for temporary access to servers
A few examples 2/2

- Full web scanning automation
TECHNOLOGY - Take away

• Devote resources to security automation
• Having a big budget won’t necessarily solve your security problems
• People and tools are complementary
• If you need to choose, invest in a good security engineer
Thanks!

- luca@doyensec.com
- @lucacarettoni
Images

• https://thenypost.files.wordpress.com/2014/01/business-woman.jpg?quality=90&strip=all&w=664&h=441&crop=1
• https://qph.ec.quoracdn.net/main-qimg-4a656858b49a971c2464ba7b1ef062f7
• http://www.mbxdesign.com/images/11.png
• https://duncan.codes/assets/images/posts/cucumber-testing-diagram.png
30-31 MARCA 2017, PGE NARODOWY, WARSZAWA

SECURITY MANAGEMENT AUDIT FORUM

SEMAFOR

X FORUM BEZPIECZEŃSTWA I AUDYTU IT

W OBICZU KRYZYSU BEZPIECZEŃSTWA IT