Builders vs Breakers

Aldo Salas
aldo.salas@owasp.org
Agenda

• Diff Between Builders and Breakers
• What’s the problem?
• What can we do to help.
What is Builder?

• Software developer.
• Application maintainer.
• Software architect.
• Person who codes.
• Etc.
What is Breaker?

- Security Engineer.
- Penetration Tester.
- Vulnerability Manager.
- Etc.
So what’s the problem?

• Different mindsets
  – Only wants to build
  vs
  – Only wants to break
Breaker’s bad practices

- Finds vulns just for fun.
- Only brags about vulnerabilities but doesn’t share with dev teams.
- Only shares details if they get paid.
- Doesn’t provide guidance to dev teams.
- Doesn’t care if vulns are not fixed.

[OWASP logo]
Builder’s bad practices

• Doesn’t care about reported vulnerabilities.
• Vulns are not fixed unless issue is escalated.
• Agrees with everything but doesn’t actually fix it.
• Argues about validity of vulnerability.
• Complains about risk classification.
This is wrong.
Breaker’s bad advise

• “Just update everything!”
Let’s start working on this
What can testers do better?

• Help, not mock.
• Provide guidance.
• Help, not brag.
• Share - It's not useful finding 100+ and not disclosing them.
What can coders do better?

• Be open to receive feedback.
• Learn about new (and old) vulnerabilities.
• Fix reported vulnerabilities.
• Push business to prioritize secure development.
Other limitations
Limitations for builders:

• It’s not intentional.
• Lack of awareness.
• Not within budget/planning.
• Not a business priority.
• It’s a business requirement.
• Management needs to get involved.
Real life example:

• Missing account lockout.
Takeaways
What can we actually do?

• Understand we are not enemies.
• We’re on this together.
  – Different teams on same company.
  – Independent researchers.
  – Consultants.
Comments/Questions?
Thanks!

aldo.salas@owasp.org