Understanding Mistakes Developers Make: Qualitative Analysis from Build It, Break It, Fix It

Daniel Votipka, Kelsey R. Fulton, James Parker, Matthew Hou, Michelle L. Mazurek, and Michael Hicks

Research Questions
What types of vulnerabilities do developers introduce?
How severe and exploitable are they?

Build It, Break It, Fix It

Build It
Break It
Website: builditbreakit.org

Problems

Secure Log
Secure Comms
Multiuser Database

Vulnerabilities Introduced

Intuitive
Unintuitive
Bad Choice
Conceptual Error

Mistake

Most related to misunderstanding security concepts

Exploitability

Hard to exploit
Easy to find

Deep Insight
Source
Execution

Hard to find and exploit

Disabled automatic integrity checks

Examples

Conceptual Error

Mistake

Recommendations

1. API improvement
   - Make unintuitive requirements transparent
   - Document security assumptions and risks of non-default use

2. Security education
   - Cover all assumptions of security requirements
   - Highlight importance of implementation decisions through practice and feedback

3. Vulnerability analysis tools
   - Further work is needed to address design-level, conceptual issues