Hackers vs Testers: A Comparison of Software Vulnerability Discovery Processes

Daniel Votipka, Rock A. Stevens, Elissa M. Redmiles, Jeremy Hu, and Michelle L. Mazurek
VULNERABILITY DISCOVERY
VULNERABILITY DISCOVERY

Testers:
• Functionality
• Performance
• Security

Generalists
VULNERABILITY DISCOVERY

Hackers:
• Security Team
• Contracted Review
• Bug Bounty

Experts
CHALLENGES

• Timeliness
• Cognitive Diversity
• Communication
RESEARCH QUESTIONS

1. How do testers and hackers search for vulnerabilities?
2. What are the differences between testers and hackers?

Interview study:
• Task Analysis
• Tools, Skills, and Communities
RECRUITMENT

Hacker Groups:
• Bug Bounty Programs
• Top Hacking Teams

Tester Groups:
• Meetup and LinkedIn
• IEEE and AST
• Ministry of Testing

106 total groups
### PARTICIPANTS

<table>
<thead>
<tr>
<th></th>
<th>10</th>
<th>15</th>
</tr>
</thead>
<tbody>
<tr>
<td>Participants</td>
<td>0-3</td>
<td>26-50</td>
</tr>
<tr>
<td>Vulnerabilities Found</td>
<td>5-10 hrs/w</td>
<td>10-20 hrs/w</td>
</tr>
<tr>
<td>Vulnerability Finding Time</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
RESEARCH QUESTIONS

1. How do testers and hackers search for vulnerabilities?
2. What are the differences between testers and hackers?
RESEARCH QUESTIONS

1. How do testers and hackers search for vulnerabilities?
2. What are the differences between testers and hackers?
HACKER AND TESTER PROCESS

- Info Gathering
- Program Understanding
- Attack Surface
- Exploration
- Vulnerability Recognition
- Reporting
Information Gathering

• Build context prior to reading or executing code
• Example actions:
  • Identifying libraries
  • Update history
  • Previous bug reports

“There were…other functional issues, so I figured that was probably where there was most likely to be security issues as well. Bugs tend to cluster.”
Program Understanding

- Determine how the program operates
  - Interaction between components
  - Interaction with the environment

“You’re touching a little bit everything, and then you are organizing that into a structure in your head.”
Attack Surface

- Identify how user interacts with program
- Direct and indirect inputs
Exploration

- Possible inputs to the attack surface
- Example actions:
  - Fuzzing
  - Reading code
Vulnerability Recognition

- Notice a problem when exploring
- Typically described as intuition-based
You do have to [convince] someone that there’s a risk. …It’s quite timely [time consuming], running a ticket.”

**Reporting**

- Tell developers about the problem
- Advocate for remediation
- Critical aspects:
  - Make report understandable
  - Importance of fixing
RESEARCH QUESTIONS

1. How do testers and hackers search for vulnerabilities?

2. What are the differences between testers and hackers?
Vulnerability Discovery Experience

Underlying System Knowledge

Access to Development Process

Motivation

Info Gathering

Program Understanding

Attack Surface

Exploration

Vulnerability Recognition

Reporting
As soon as I found the LinkedIn problem, I made sure to test [FB and Twitter input] to make sure [they were processed correctly]. And if we did allow login with another 3rd party in the future, I would check that too.
AMOUNT OF EXPERIENCE

- Employment
- Hacking Exercises
- Community
- Bug Reports

Vulnerability Discovery Experience
“It’s hard to ignore certain details once you know about certain areas already.”

**Internal**
- Communicate with developers
- Documentation

**External**
- Reverse engineering
- Develop exploits

“You can give feedback to your developers. . . .You’re coming back with information, and then they react on it.”
RECOMMENDATIONS

- Provide training in known contexts
  - Hire hackers into the testing team
  - Bug report-based exercises

- Improve hacker communication
  - Single point of contact
**SUMMARY**

- Similar processes
- Impacted by:
  - Vulnerability Discovery Experience
  - Underlying System Knowledge,
  - Access to the Development Process
  - Motivation
- Biggest difference in **amount of experience and relationship with the developers**

**Questions:**

dvotipka@cs.umd.edu
vulnstudy.cs.umd.edu

**Recommendations:**

- Training in a known context
- Hacker/company communication