Bug Hunters’ Perspectives on the Challenges and Benefits of the Bug Bounty Ecosystem

Omer Akgul · Taha Eghtesad · Amit Elazari · Omprakash Gnawali · Jens Grossklags
Michelle Mazeek · Daniel Votipka · Aron Laszka
Bug bounty programs

- Crowd-sourced vulnerability discovery systems
  - Bug bounty hunters find vulns.
  - Companies learn vulnerabilities.
  - Hunters get recognition/compensation

Images from flaticon.com
Bug bounty platforms

• Platforms that help connect bug bounty programs with bug bounty hunters
• Can help standardize the hunter-manager process
Why care about bug bounties?

• Works great for organizations!
  • Cheaper to run than in house team
  • Access to diverse skills
  • 400K+ valid vulns found

Images from flaticon.com and hackerone.com
Why care about bug bounties?

- Works great for organizations!
- Cheaper to run than in-house team
- Access diverse skill pool
- 400K+ valid vulns found

What about the hunters?

Images from flaticon.com and hackerone.com
Why care about bug bounties?

• Works great for organizations!
• Cheaper to run than in-house team
• Access diverse skill pool
• 400K+ valid vulnerabilities

What about the hunters?

Their experience?

Images from flaticon.com and hackerone.com
The hunters’ perspective

✔ What are the benefits?
❓ Factors in choosing programs?
_REGS What are the challenges?
嗲 Which platform utilities are useful?
The hunters’ perspective

✔ What are the benefits?

❓ Factors in choosing programs?

❎ Which platform utilities are useful?

Which factors are most important?
Our multi-pronged approach

- Interviews (n=24)
- Factor free listing (n=56)
- Factor rating (n=159)

10

Qual coding

Quant Analysis
Our participants

• Wide range of participants
  • Across the globe
  • Weekly hours
• # of bugs found
• Years of experience
• Similar to bug bounty platform reports.
What are the factors?

✔ What are the benefits?

❓ Factors in choosing programs?

❌ What are the challenges?

婵 Which platform utilities are useful?
What are the factors?

✔ What are the benefits?

❓ Factors in choosing programs?

✗ What are the challenges?

🛠️ Which platform utilities are useful?

Images from flaticon.com
Benefits of bug-bounty?

✔ Monetary rewards (#1)
✔ Learning/improving skills (#2)
✔ Fun! (#3)

Images from hackerone.com, bugcrowd.com, and flaticon.com
Benefits of bug-bounty?

✔ Monetary rewards (#1)
✔ Learning/improving skills (#2)
✔ Fun! (#3)
✔ Legal safe harbor (#4)
✔ Flexibility (#5)

Images from hackerone.com, bugcrowd.com, and flaticon.com
Benefits of bug-bounty?

✔ Monetary rewards (#1)
✔ Learning/improving skills (#2)
✔ Fun! (#3)
✔ Legal safe harbor (#4)
✔ Flexibility (#5)

❌ Reputation scoring (#9/10)

Images from hackerone.com, bugcrowd.com, and flaticon.com
Which program to work on?

✔ Scope (#1)

<table>
<thead>
<tr>
<th>In Scope</th>
<th>Critical</th>
<th>Eligible</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Domain</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Amazon DynamoDB</td>
<td>Amazon Web Services</td>
<td></td>
</tr>
<tr>
<td>GraphQL</td>
<td>JavaScript</td>
<td>PostgresSQL</td>
</tr>
<tr>
<td>Rails</td>
<td>React</td>
<td>Redis</td>
</tr>
</tbody>
</table>

| Domain | | |
|--------| | |
| Amazon Web Services | GraphQL |
| PostgresSQL | Rails | Redis | Ruby |

Screenshots from [hackerone.com](https://hackerone.com) and [bugcrowd.com](https://bugcrowd.com)
Which program to work on?

✔ Scope (#1)

✔ Tech familiarity (#4)

Screenshots from hackerone.com and bugcrowd.com
Which program to work on?

✔ Scope (#1)
✔ Tech familiarity (#4)
✔ Reward (#2)

Screenshots from hackerone.com and bugcrowd.com
Which program to work on?

✔ Scope (#1)
✔ Tech familiarity (#4)
✔ Reward (#2)
✔ Bounty table (#3)

Screenshots from hackerone.com and bugcrowd.com
Which program to work on?

✔ Scope (#1)
✔ Tech familiarity (#4)
✔ Reward (#2)
✔ Bounty table (#3)
✔ Legal safe harbor (#5)

Screenshots from hackerone.com and bugcrowd.com
What are the problems?

- Communication and disputes
- Responsiveness (#1)

Screenshots from hackerone.com
What are the problems?

⚠️ Communication and disputes

⚠️ Responsiveness (#1)

⚠️ Dissatisfaction with responses (#2)

Screenshots from hackerone.com
What are the problems?

❖ Communication and disputes
❖ Responsiveness (#1)
❖ Dissatisfaction with responses (#2)
❖ Scoping issues (#3)
❖ Mediation dissatisfaction (#4)

Screenshots form hackerone.com
Potential troubling outcomes

• From interviews:
  • Hunters quit/get deplatformed
  • Fixed but unacknowledged bugs
  • Not reporting found bugs
  • Exploiting for fun & profit.

Some images from flaticon.com
What to do?

• Bug bounty programs
  • Look into impact of increased scope and rewards
  • Avoid common communication pitfalls

Policy makers?

• Bug bounty platforms
  • Perceptions of mediation
  • Focus on learning resources*

Takeaways

Bug bounty programs work well for companies.

$ € £ ₺

Scope is most important when choosing a program.

Rewards and learning are big motivators, reputation isn’t.

What about the hunters?

Communication issues/disputes are top challenges.

https://hackerone.com  Critical $ Eligible
https://api.hackerone.com  Critical $ Eligible

Questions? akgul@umd.edu @_oakgul