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

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

Images from flaticon.com
Bug bounty programs

• Crowd-sourced vulnerability discovery systems
Bug bounty programs

- Crowd-sourced vulnerability discovery systems
- Bug bounty hunters find vulns.
Bug bounty programs

• Crowd-sourced vulnerability discovery systems
  • Bug bounty hunters find vulns.
  • Companies learn vulnerabilities.
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 programs

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

Images from flaticon.com
Bug bounty platforms
Bug bounty platforms

Images from flaticon.com
Bug bounty platforms

- Platforms that help connect bug bounty programs with bug bounty hunters
Bug bounty platforms

- Platforms that help connect bug bounty programs with bug bounty hunters
- Can help standardize the hunter-manager process

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

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

Images from flaticon.com
Why care about bug bounties?

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

- Works great for organizations!
Why care about bug bounties?

- Works great for organizations!
  - Cheaper to run than in house team

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

- Works great for organizations!
- Cheaper to run than in house team
- Access to diverse skills
Why care about bug bounties?

• Works great for organizations!
  • Cheaper to run than in house team
  • Access to diverse skills
  • 400K+ valid vulns foun
Why care about bug bounties?

• Works great for organizations!
• Cheaper to run than in-house team
• Access diverse skill pool
• 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 vulnerabilities found

What about the hunters? Their experience?

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

✔ What are the benefits?
The hunters’ perspective

✔ What are the benefits?

❓ Factors in choosing programs?
The hunters’ perspective

✔️ What are the benefits?
❓ Factors in choosing programs?
❌ What are the challenges?
The hunters’ perspective

✔ What are the benefits?

❓ Factors in choosing programs?

⚠️ What are the challenges?

➡️ Which platform utilities are useful?

<table>
<thead>
<tr>
<th>Program</th>
<th>Launch date</th>
<th>Reports received</th>
<th>Bounties received</th>
<th>Bounties average</th>
</tr>
</thead>
<tbody>
<tr>
<td>U.S. Dept Of Defense</td>
<td>11/2016</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Verizon Media</td>
<td>02/2014</td>
<td>6398</td>
<td>$50</td>
<td>$400-$500</td>
</tr>
<tr>
<td>Ali.ru</td>
<td>04/2014</td>
<td>3618</td>
<td>$100</td>
<td>$250-$300</td>
</tr>
<tr>
<td>AT&amp;T</td>
<td>07/2019</td>
<td>2985</td>
<td>$100</td>
<td>$500</td>
</tr>
<tr>
<td>Adobe</td>
<td>02/2015</td>
<td>2628</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>IBM</td>
<td>07/2018</td>
<td>2067</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Ford</td>
<td>01/2019</td>
<td>1893</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Uber</td>
<td>12/2014</td>
<td>1513</td>
<td>$50</td>
<td>$500-$750</td>
</tr>
<tr>
<td>Twitter</td>
<td>05/2014</td>
<td>1194</td>
<td>$140</td>
<td>$420-$560</td>
</tr>
<tr>
<td>Sony</td>
<td>10/2017</td>
<td>1168</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Magento</td>
<td>01/2019</td>
<td>1092</td>
<td>$100</td>
<td>$290-$690</td>
</tr>
<tr>
<td>Slack</td>
<td>02/2014</td>
<td>1073</td>
<td>$100</td>
<td>$500</td>
</tr>
<tr>
<td>Ubiquiti Inc</td>
<td>01/2015</td>
<td>1002</td>
<td>$150</td>
<td>$175-$250</td>
</tr>
<tr>
<td>Starbucks</td>
<td>05/2016</td>
<td>999</td>
<td>$100</td>
<td>$250-$375</td>
</tr>
</tbody>
</table>
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
Our multi-pronged approach

Factor free listing (n=56)
Our multi-pronged approach

Factor free listing (n=56) → Qual coding
Our multi-pronged approach

Factor free listing (n=56) → Qual coding
Our multi-pronged approach

Factor free listing (n=56) → Qual coding
Our multi-pronged approach

Factor free listing (n=56)

Factor rating (n=159)

Qual coding
Our multi-pronged approach

Factor free listing (n=56)

Factor rating (n=159)

Qual coding

Quant Analysis
Our multi-pronged approach

Factor free listing (n=56) → Qual coding

Factor rating (n=159) → Quant Analysis
Our multi-pronged approach

Factor free listing (n=56)

Factor rating (n=159)

Qual coding

Quant Analysis
Our multi-pronged approach

Interviews (n=24)

Factor free listing (n=56)

Factor rating (n=159)

Qual coding

Quant Analysis
Our participants
Our participants

• Wide range of participants
Our participants

- Wide range of participants
- Across the globe
Our participants

• Wide range of participants
• Across the globe
• Weekly hours
Our participants

• Wide range of participants
  • Across the globe
  • Weekly hours
  • # of bugs found
Our participants

• Wide range of participants
  • Across the globe
  • Weekly hours
  • # of bugs found
  • Years of experience
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?

Images from flaticon.com
What are the factors?

✔ What are the benefits?
What are the factors?

✔ What are the benefits?

❓ Factors in choosing programs?
What are the factors?

✔️ What are the benefits?

❓ Factors in choosing programs?

❌ What are the challenges?

Images from flaticon.com
What are the factors?

✔️ What are the benefits?
❓ Factors in choosing programs?
💥 What are the challenges?
(IT) Which platform utilities are useful?
What are the factors that influence your choice of transportation platform?

- Factors in choosing the platform
- Which platform?

Images from flaticon.com
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?

Images from [hackerone.com](http://hackerone.com), [bugcrowd.com](http://bugcrowd.com), and [flaticon.com](http://flaticon.com)
Benefits of bug-bounty?

✔ Monetary rewards (#1)
Benefits of bug-bounty?

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

Images from hackerone.com, bugcrowd.com, and 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)

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?

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

✔ Scope (#1)

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

Communication and disputes

Screenshots form hackerone.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)
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

Some images from flaticon.com
Potential troubling outcomes

• From interviews:
Potential troubling outcomes

• From interviews:
  • Hunters quit/get deplatformed
Potential troubling outcomes

• From interviews:
  • Hunters quit/get deplatformed
  • Fixed but unacknowledged bugs
Potential troubling outcomes

• From interviews:
  • Hunters quit/get deplatformed
  • Fixed but unacknowledged bugs
  • Not reporting found bugs
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?
What to do?

• Bug bounty programs
What to do?

• Bug bounty programs

• Look into impact of increased scope and rewards
What to do?

- Bug bounty programs
- Look into impact of increased scope and rewards
- Avoid common communication pitfalls
What to do?

• Bug bounty programs

• Look into impact of increased scope and rewards

• Avoid common communication pitfalls

• Bug bounty platforms

Images from flaticon.com
What to do?

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

• Bug bounty platforms
  • Perceptions of mediation
What to do?

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

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

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
Takeaways

Bug bounty programs work well for companies.
Takeaways

Bug bounty programs work well for companies. What about the hunters?
Takeaways

Bug bounty programs work well for companies.

What about the hunters?

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

Bug bounty programs work well for companies.

What about the hunters?

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

Scope is most important when choosing a program.

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

Bug bounty programs work well for companies.

What about the hunters?

Rewards and learning are big motivators, reputation isn’t

Scope is most important when choosing a program.

Communication issues/disputes are top challenges
Takeaways

Bug bounty programs work well for companies.

What about the hunters?

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

Scope is most important when choosing a program.

Communication issues/disputes are top challenges.

Questions?

akgul@umd.edu
@oakgul
Takeaways

Bug bounty programs work well for companies.

$ € £ ₺

Scope is most important when choosing a program.

What about the hunters?

Rewards and learning are big motivators, reputation isn’t

Questions?

Questions?

akgul@umd.edu

What about the hunters?

Rewards and learning are big motivators, reputation isn’t

https://hackerone.com

https://api.hackerone.com

Communication issues/disputes are top challenges