

DAILY LIFE OF AN APPLICATION SECURITY ENGINEER AT BUGCROWD

by Bugcrowd PH Team

bugcrowd

WHAT WE DO?

KEEP IN MIND

HOW NOT TO
BUG BOUNTY?

Q & A

AGENDA

WHAT WE DO?

- We are responsible for the ongoing triage and validation services of Bugcrowd managed programs.

Hacking into the database to find out who's a good boy



WHAT WE DO?

- We are responsible for the ongoing triage and validation services of Bugcrowd managed programs.

<https://bugcrowd.com/programs>

Hacking into the database to find out who's a good boy



<p>Waitlisted</p> <p>Mesh Wifi ecosystem and mobile application Complete System: IoT Router, mesh repeaters, corresponding mo...</p> <p>\$35,000 reward pool Partial safe harbor Managed by Bugcrowd</p> <p>View details ☆</p>	<p>Unilever Vulnerability Disclosure Program At Unilever we meet everyday needs for nutrition, hygiene and...</p> <p>Points per vulnerability Partial safe harbor Managed by Bugcrowd</p> <p>Submit report ☆</p>	<p>Seeking specialists We're looking for researchers to work on select private progr...</p> <p>Learn more</p>	<p>Waitlisted</p> <p>Leading Video Game Company Experience with testing video games for security vulnerabil...</p> <p>\$100 – \$2,400 per vulnerability Partial safe harbor Managed by Bugcrowd</p> <p>View details ☆</p>	<p>Waitlisted</p> <p>3 Easy payments Pay in installments, get rewarded in lump sums.</p> <p>\$150 – \$2,500 per vulnerability Partial safe harbor Managed by Bugcrowd</p> <p>View details ☆</p>	<p>Waitlisted</p> <p>A payroll company is looking to the crowd to help maintain its security posture A payroll company is looking to the crowd to help maintain it...</p> <p>\$200 – \$4,500 per vulnerability Partial safe harbor Managed by Bugcrowd</p> <p>View details ☆</p>
<p>Waitlisted</p> <p>Customer Feedback Platform Help secure our main web platform</p> <p>Points – \$5,000 per vulnerability Safe harbor Managed by Bugcrowd</p> <p>View details ☆</p>	<p>Waitlisted</p> <p>Online Survey Software tool Help secure our web and API assets</p> <p>Points – \$5,000 per vulnerability Safe harbor Managed by Bugcrowd</p> <p>View details ☆</p>	<p>Waitlisted</p> <p>Web app testing for this privacy company's ongoing private bug bounty program. Help keep personal data private!</p> <p>\$100 – \$2,500 per vulnerability Partial safe harbor Managed by Bugcrowd</p> <p>View details ☆</p>	<p>TransferWise TransferWise is an online account that lets you send money, g...</p> <p>\$100 – \$4,000 per vulnerability Up to \$6,000 maximum reward Safe harbor Managed by Bugcrowd</p> <p>Submit report ☆</p>	<p>Waitlisted</p> <p>Automatic, Systematic Get into the flow, the automated flow!</p> <p>\$100 – \$1,500 per vulnerability Partial safe harbor Managed by Bugcrowd</p> <p>View details ☆</p>	<p>Takeaway.com Takeaway</p> <p>\$100 – \$2,500 per vulnerability Safe harbor Managed by Bugcrowd</p> <p>Submit report ☆</p>

WHAT WE DO?

- We are responsible for the ongoing triage and validation services of Bugcrowd managed programs.
- Take incoming submission data and curate it for validity, accuracy, and severity as well as communicate directly with Bugcrowd's clients and/or researchers when additional information is required.

WHAT WE DO?

- Take incoming submission data and curate it for validity, accuracy, and severity as well as communicate directly with Bugcrowd's clients and/or researchers when additional information is required.



Hacking into the database to find out who's a good boy



WHAT WE DO?

- We are responsible for the ongoing triage and validation services of Bugcrowd managed programs.
- Take incoming submission data and curate it for validity, accuracy, and severity as well as communicate directly with Bugcrowd's clients and/or researchers when additional information is required.
- Handle Incident Response – escalating and communicating about the highest severity bugs to clients.

KEEP IN MIND

- Read the program R&R
 - Scope (domain, sub-domains, mobile apps, etc.)
 - Exclusions (non-qualifying bug types, services, etc.)
 - Requirements (age, country, verified, etc.)
 - Rewards/Payout
 - Disclosure Policy
- Validate your bug
- Prepare a well-written report (Proof of Concept / POC)
- Be a good guy
 - Respect the program, owners and their decisions
 - Respect other researchers
 - Respect privacy
 - Have patience



HOW NOT TO BUG BOUNTY?

- Don't beg (not a Beg Bounty)
- Don't lie
- Don't test without permission
- Don't use Automated Scanners/Tools!
- Don't use foul/obscene languages in POC!



