Overview of Bugcrowd

Bugcrowd is an award-winning fully managed crowdsourced security platform. It connects the entire vulnerability management lifecycle, leveraging the expertise of elite white hat hackers to identify high-value vulnerabilities efficiently. By offering contextualized intelligence and security workflow automation, Bugcrowd helps organizations find and fix vulnerabilities faster, leading to better overall security.

Bugcrowd Platform

Bugcrowd's platform, Crowdcontrol, caters to both researchers and customers. It includes two main interfaces:

1. Researcher Side:

- Researchers use this interface to view bounty briefs, understand the scope of the programs, and submit their findings.

- They participate in both public and private programs to identify vulnerabilities.

- Researchers earn "kudos points" by finding vulnerabilities, which helps them become eligible for private programs.

2. Customer Side:

- Customers use this interface to manage their vulnerability reports, generate reports, and interact with Bugcrowd and the researchers.

- Bugcrowd assists customers by drafting program briefs that outline the rules of engagement, scope, and other essential details.

Public vs. Private Programs

- Public Programs:
  - Open to all researchers.
  - Researchers can join, test, and submit vulnerabilities for the listed companies.

- Private Programs:
  - Restricted access, only available to selected researchers who meet specific criteria.
  - Researchers are invited based on their performance in public programs and their kudos points.

Bounty Brief

The bounty brief is a critical document that outlines the details of a program. It includes:

- Targets: Specifies what researchers should test (e.g., websites, APIs, mobile applications, hardware, IOT devices).
- Scope: Defines what is in-scope and out-of-scope for testing.
- Focus Areas: Highlights areas of the application or system that require more attention.

- Out-of-Scope: Lists actions or vulnerabilities that researchers should avoid.

- Access Details: Provides information on how researchers can access the targets, including credentials if necessary.

Rewards and Vulnerability Rating

- Reward Ranges:

  - Researchers are informed about the potential payouts for vulnerabilities they find, based on the technical severity.

- Vulnerability Rating Taxonomy:

  - Bugcrowd categorizes vulnerabilities from P1 (most severe) to P5 (least severe).

  - Customers can customize these categories based on their priorities and risk assessments.

Customization and Collaboration

Bugcrowd collaborates with each customer to customize the bounty brief according to their specific needs. This includes defining what vulnerabilities are of high priority, which ones are less critical, and any specific tools or areas researchers should avoid. This ensures that the testing aligns with the customer’s security goals and requirements.

Conclusion

Bugcrowd’s Crowdcontrol platform streamlines the vulnerability management process by connecting businesses with skilled security researchers. This approach not only enhances the security posture of organizations but also fosters a collaborative environment where researchers and companies work together to improve overall cybersecurity.

Bugcrowd Program Briefs and Submission Process

Customizable Bounty Briefs

1. Vulnerability Rating:

- The bounty brief includes a customizable Vulnerability Rating Taxonomy (VRT) listing vulnerabilities from P1 (most severe) to P5 (least severe).

- Customers can specify the severity of particular vulnerabilities, affecting the payouts for researchers. For example, an external injection might be rated as a P2 instead of a P1, affecting the reward amount.

2. Scope and Rules:

- Details the scope of the program, including what is in-scope and out-of-scope, and specific areas of focus.

- Includes Bugcrowd's standard non-disclosure terms, which researchers must agree to when participating. Researchers are prohibited from disclosing details about the program, targets, or

vulnerabilities found without explicit written permission from the company.

3. Rewards:

- Lists the reward ranges based on the severity of the vulnerabilities. Most programs do not pay for P5 vulnerabilities, as these are often easily discoverable by automated tools and are of lesser concern.

Researcher Submission Process

1. Submission Form:

- Researchers submit vulnerabilities using a structured form that includes:

  - Target: Where the vulnerability was found.

  - Technical Severity: Selected category relevant to the found vulnerability (e.g., Remote Code Execution).

  - Description: Detailed explanation of the vulnerability, its impact, and reproduction steps.

  - Optional Fields: Post request body, attachments (e.g., screenshots, video files), and other relevant details.

2. Agreement:

- Researchers must agree to the program's non-disclosure terms each time they submit a vulnerability.

Bugcrowd’s Backend: Crowdcontrol

1. Overview Page:

- Provides a summary of recent activities and submission status for each program.

- Allows program owners to manage multiple programs from a single view.

2. Submission Queues:

- Processing Queue: New submissions first enter this queue for triage and validation.

- Bugcrowd’s application security engineers review each submission, validating the details and determining its severity.

3. Validation Process:

- Engineers examine the submission, verifying the vulnerability and assessing its impact.

- Submissions with insufficient information may require additional details or clarification from the researcher.

Conclusion

Bugcrowd’s platform effectively connects businesses with skilled security researchers through well-defined bounty programs. The structured submission process, coupled with customizable bounty briefs and a robust backend system, ensures a streamlined and efficient vulnerability management lifecycle. This approach not only

enhances security for the businesses but also provides a clear and rewarding path for researchers to contribute their expertise.

Detailed Walkthrough of Bugcrowd's Platform and Process

Submission and Validation Process

1. Submission Review:

- When a researcher submits a potential vulnerability, it lands in the "Processing Queue".

- Bugcrowd's application security engineers review the submission to validate its authenticity and severity.

- If the submission lacks sufficient details, engineers request additional information from the researcher via the platform's communication tools.

2. Handling Incomplete Information:

- If a submission is unclear or incomplete (e.g., a provided URL doesn’t show the vulnerability as expected), Bugcrowd engineers reach out to the researcher for more details.

- Engineers use the platform’s messaging system to request specific information or clarification.

3. State Management:

- New: Initial state when a submission is first made.

- Triage: Once validated by Bugcrowd engineers, the submission is marked as "Triage", notifying the customer.

- Out of Scope: Marked if the submission targets areas outside the defined program scope.

- Not Reproducible: Used when a vulnerability cannot be reproduced after several attempts and researcher follow-ups.

- Won't Fix: Chosen if the customer decides not to address a specific vulnerability, accepting the associated risk.

- Not Applicable: A catch-all for issues that don’t fit other categories.

- Duplicate: Applied when the vulnerability has already been reported or discovered by other means.

Customer Actions

1. Review and Accept:

- Customers review validated submissions in the "Triage" state.

- If accepted as valid, the customer moves the submission to the "Unresolved" state, confirming it as a valid issue to be fixed.

2. Final Payout Control:

- Upon marking a submission as "Unresolved", the customer determines the final payout.

- The payout is based on the agreed reward range from the bounty brief, with the option to adjust the amount and provide feedback to the researcher.

- If the payout is lower than expected, an explanation is required to help the researcher understand the rationale.

3. Post-Validation Workflow:

- Unresolved State: Indicates an accepted vulnerability that will be fixed.

- To Fix Bucket: Contains all unresolved issues that are scheduled to be addressed.

- Fixed Bucket: For vulnerabilities that have been resolved and verified as fixed.

Communication and Transparency

1. Researcher Interaction:

- Bugcrowd encourages customers to communicate with researchers, although it's optional.

- Engineers and customers can converse with researchers directly through the platform to clarify issues, request additional details, and provide feedback.

2. Blockers and Notifications:

- Submissions with pending information requests are marked with blockers, providing visibility into why certain submissions are delayed.

- Researchers receive notifications when additional information is requested or when there are updates on their submissions.

3. Issue Importer:

- Allows customers to import internally discovered issues to prevent duplicate payouts.

- These imported issues are used by Bugcrowd engineers to cross-check and ensure unique discoveries by researchers.

Conclusion

Bugcrowd’s platform provides a comprehensive and structured process for handling security vulnerabilities, from initial submission to final resolution. The system emphasizes clarity, communication, and customizable workflows to align with each customer’s security needs and priorities. This ensures efficient management of vulnerabilities while maintaining a rewarding and transparent process for researchers.

Detailed Walkthrough of Bugcrowd's Platform and Process (Continued)

Submission and Validation Process (Continued)

1. Transparency with Customers:

- Bugcrowd maintains full transparency with customers about the submission and triage processes.

- Customers can monitor the status of submissions and understand what Bugcrowd is working on at any given time.

2. Submission Details:

- Each submission includes details entered by the researcher, such as the nature of the vulnerability and steps to reproduce it.

- Bugcrowd provides remediation advice tailored to developers, including reference links to authoritative sources like the OWASP Top 10, CVEs, and CWEs.

3. Researcher Interaction:

- Conversations between researchers and Bugcrowd or customers are logged within the platform, promoting clear communication and effective resolution of queries.

Researcher Management

1. Researcher Profiles:

- Customers can view participating researchers' profiles, including their accuracy rate and overall performance across programs.

- Researchers with public profiles can have their statistics and performance history viewed in detail.

2. Customizing Researcher Access:

- Customers can restrict program access based on specific criteria, such as expertise in certain types of vulnerabilities (e.g., SQL injection) or geographic location.

- Researchers can request ID verification and background checks to participate in private programs, ensuring a vetted and reliable researcher pool.

Rewards and Insights

1. Reward Management:

- Customers have control over the final payout amount for each validated vulnerability.

- If the reward is lower than the recommended range, an explanation is required to help researchers understand the decision.

2. Insight and Analytics:

- The platform provides detailed metrics and analytics, monitored by assigned account managers.

- Metrics include the number of submissions, severity of vulnerabilities, response times, and payout amounts.

- Performance over time can be tracked to ensure the program is running smoothly and efficiently.

Program Management

1. Crawl-Walk-Run Approach:

- Bugcrowd adopts a gradual approach to program expansion, starting with a smaller number of researchers and scope, and expanding as customers get accustomed to managing submissions and interacting with researchers.

- The approach ensures that development teams can handle the incoming workload and fix vulnerabilities in a timely manner.

2. Training and Improvement:

- Insights from the platform can highlight areas where development teams may need additional training, such as common types of vulnerabilities being reported.

- Regular monitoring and recommendations help customers improve their security posture continuously.

3. Statistical Breakdown:

- The platform breaks down vulnerabilities by target, severity, and category, providing customers with a clear view of their security landscape.

- Performance metrics track how long it takes to accept, fix, and triage vulnerabilities, helping to optimize the process.

4. Payouts and Rewards:

- The platform provides detailed information on payouts, allowing customers to see how much is being spent on resolving vulnerabilities and the distribution of rewards among researchers.

Additional Features

- Remediation Advice and Reference Links: Tailored advice and links to authoritative sources help developers understand and fix vulnerabilities.

- Detailed Researcher Information: Access to researcher profiles and performance statistics.

- Customization of Researcher Participation: Ability to restrict program access based on various criteria.

- Comprehensive Metrics and Analytics: Detailed insights into program performance, helping to ensure effective vulnerability management.

Conclusion

Bugcrowd’s platform offers a structured and transparent process for managing security vulnerabilities, emphasizing clear communication, detailed analytics, and customizable workflows to align with each customer's needs. The gradual approach to program expansion, combined with comprehensive insights and researcher management, ensures a robust and effective vulnerability management process.

Summary of Bugcrowd Platform Features and Settings

Insights and Reports

1. Exportable Data:

   - All data on the insights page can be exported as a PDF report or CSV file.

   - Options for generating full program reports are available, including detailed submission indexes and program details.

2. Report Generation:

   - Reports resemble traditional penetration test reports, including executive summaries, program descriptions, and scope details.

   - Findings tables provide high-level overviews of vulnerabilities, with full details available further in the report.

Program Settings and Management

1. Transparency and Customization:

- Customers can edit program briefs, scope, and targets.

- Known issues can be imported to help mark duplicate submissions and inform researchers of existing vulnerabilities.

2. Integration Options:

- Bugcrowd integrates with tools like JIRA, Slack, GitHub, and ServiceNow for streamlined issue tracking and management.

- The JIRA integration supports bi-directional updates, automatically pushing issues from Bugcrowd to JIRA and marking them as resolved in both platforms.

3. Credential Management:

- Credentials required by researchers to access certain areas of applications can be securely managed and provisioned within the platform.

4. Team Management:

- Various user roles are available, such as organization owner, admin, analyst, and viewer.

- Unlimited seats for team members can be assigned without additional costs.

Additional Features

1. Custom Fields and CVSS Scoring:

- Custom fields can be added for specific program needs.

- CVSS scoring can be toggled on, enabling Bugcrowd to calculate vulnerability scores based on the CVSS calculator.

2. Remediation Advice and Retesting:

- Remediation advice tailored to developers can be toggled on to help understand and fix vulnerabilities.

- Retesting is available as an add-on service, allowing verified fixes to be confirmed.

Conclusion

Bugcrowd's platform offers comprehensive tools for managing bug bounty programs, including detailed reporting, integration with development tools, credential management, and customizable settings. The platform supports transparency and flexibility, ensuring customers can effectively oversee and manage their security vulnerabilities.