bugcrowd

DATA SHEET

PENETRATION TESTING

API Penetration Testing

Bugcrowd Penetration Testing-as-a-Service Solution

Summary

APIs have opened a new world of opportunity for engineers and data analysts, but they're equally useful for teachers, pilots, and baristas alike. They connect people and systems to data that matters, whenever, and wherever needed. Often, they're the target of attackers looking for such data. Unfortunately, APIs are commonly neglected in application security. This is especially problematic considering that 90% of web-enabled applications have more surface area for attack in the form of exposed APIs rather than the UI itself. Regular testing can help, but organizations face significant trade-offs in available options. Scanners can be implemented quickly, but carry excessive noise. Traditional pen tests leverage necessary human creativity, but in limited capacity, or at the cost of significant scheduling delays.

Specialized Pen Testing for APIs

A thorough discovery of flaws in APIs requires specialized knowledge, skills, and experience. Bugcrowd API Pen Testing brings the talents of a global community of security researchers, precise crowd matching via our CrowdMatch™ ML technology, rapid validation and triage, and the vast reservoir of vulnerability knowledge residing in the Bugcrowd Security Knowledge Platform to bear on every pen test engagement.

Every assessment includes:

- Dedicated, vetted pentesters matched by skill, experience, and performance
- Strict adherence to Bugcrowd's BugHunter Methodology™ including best practices from the OWASP Testing Guide, SANS Top 25, CREST, WASC, PTES, and more
- In-depth reconnaissance, scanning, and exploitation measures for thorough network analysis
- Validation and prioritization according to Bugcrowd's Vulnerability Rating Taxonomy (VRT)
- End-to-end program management with the industry's highest signal-to-noise ratio
- QSAC-Assessed compliance report

Key Points of Value

Start testing faster

Use the power of the Bugcrowd Platform and the Crowd to rapidly start your testing in as little as 72 hours.

Expert testers are matched to your requirements

CrowdMatch™ ML technology helps rapidly align the right skills and experience for the engagement.

Get real-time results

Vulnerabilities are triaged, validated, and then made available in real time via the Bugcrowd Platform and in your integrated tools of choice to enable rapid remediation.

Packages can be modified and expanded to suit individual testing needs; indeed, they may include expedited report delivery, executive reporting, vulnerability re-testing, and even options to incentivize greater vulnerability discovery.

API Testing Methodology

Bugcrowd API Pen Test includes a testing methodology that blends key organizational and operational best practices of leading industry standards to drive both risk reduction and compliance for customers with varying priorities. Bugcrowd API Pen Test is executed through four critical phases: Reconnaissance, Enumeration, Documentation, and Exploitation. Each phase is executed in a cyclical manner allowing penetration testers to build upon findings and potentially uncover significant risk. A blend of organizational and operational best practices provides coverage as well as meaningful results.

Reconnaissance and Enumeration

This phase is sometimes necessary if adequate API documentation is not provided to the pentesters

It includes but is not limited to:

- Use brute force methods to probe the directory and/or endpoint.
- Searching public code repositories for instances where the API may be used.
- Use search engines to discover documentation or Swagger UI endpoints that may be viewed publicly

Scanning

If allowed, use industry-standard scanning tools to test for various vulnerabilities against all user input

- Enumerate and document all in-scope services and version numbers.
- Check for unencrypted services.
- Check for misconfigured services or DNS records allowing for subdomain takeovers or similar attacks.
- Analyze returned error codes and stack traces for additional information.
- Check for server misconfigurations that may result in security issues such as missing/incorrect headers, bad CORS implementations, etc.

Exploitation and Documentation

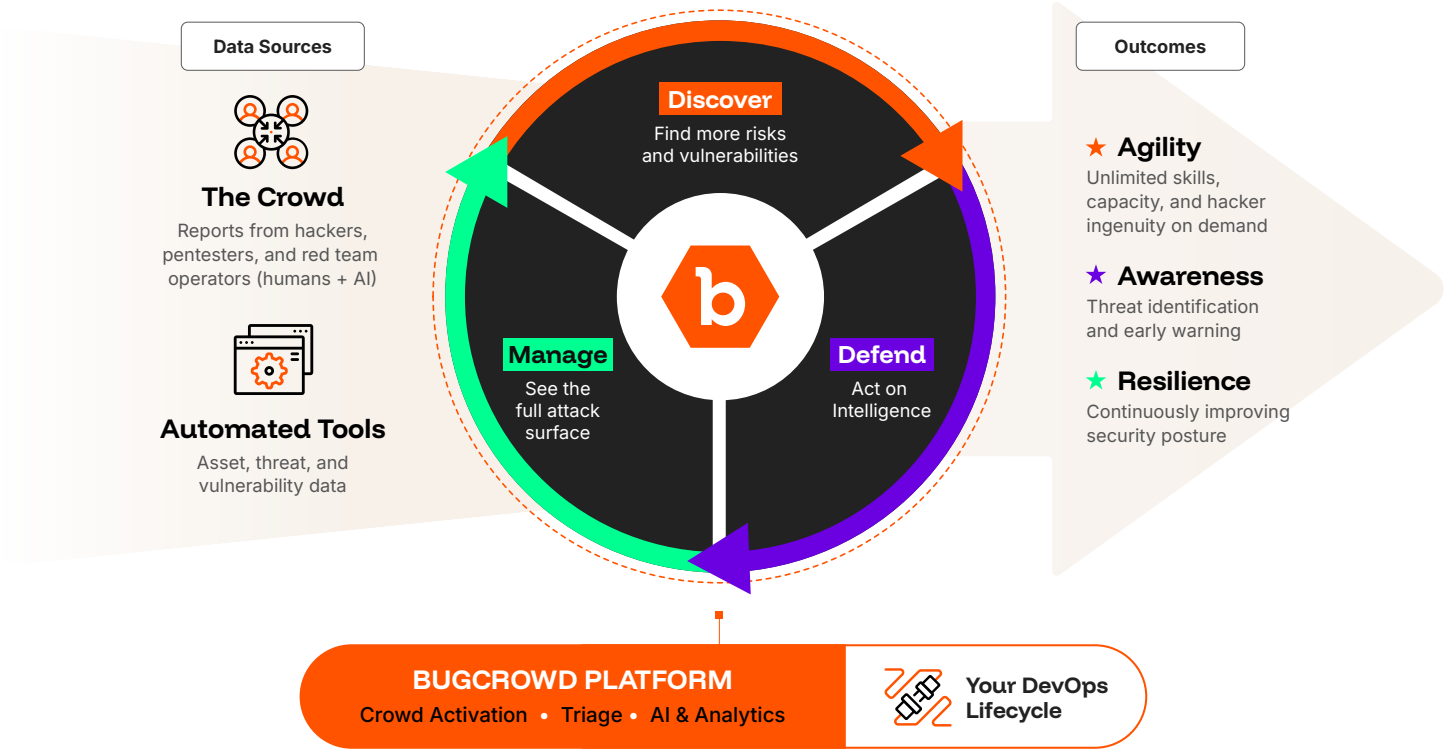
Verify security weaknesses and collect results

- Review endpoints to determine if any are exposing sensitive information.
- Test authentication flow for logic errors that may result in bypasses.
- Test session mechanism for weaknesses or configuration mistakes.
- Test for access control issues between user roles.
- Check for service misconfigurations and deployment mistakes.
- Attempt to discover exposed files with sensitive information (database backups, open git repositories, etc.)
- Check for default/weak credentials
- Check for weak encryption (SSL/TLS ciphers, older protocols, etc.)
- Check for known/public exploits on discovered services by cross-referencing software version numbers against public vulnerability databases.
- Test all user input for vulnerabilities, including but not limited to:
  - → SQL Injection (SQLi)
  - → Remote Code Execution (RCE)
  - → XML Entity Injection (XXE)
  - → Server-side request forgery (SSRF)
  - → File inclusion (LFI/RFI/AFI)
  - → Cross-Site Request Forgery (CSRF)

BUGCROWD

DATA SHEET

Bugcrowd Platform



The Bugcrowd Platform fuses AI with real-time, crowdsourced intelligence from the world's top ethical hackers, pentesters, and red teamers (aka The Crowd), as well as from automated tools that generate asset, threat, and vulnerability data. The powerful combination of human creativity and automation empowers you to continuously:

Agility

Augment Your Team On Demand

- Attacker mindset on tap for vulnerability discovery, pen testing, and red teaming
- 350+ skill sets and certifications available
- Crowd curation and activation guided by data and AI

Awareness

See and Prioritize Emerging Threats

- Continuous vulnerability intake, validation, and triage at scale
- 24/7 triage coverage with same-day response for P1s
- Early warning of emerging vulnerabilities

Resilience

Continuously Improve Security Posture

- Actionable reporting, benchmarking, and recommendations
- Directly integrates with existing tools for change at DevOps speed
- Deep bench of solution & support specialists at your side for quick wins and long-term ROI

mastercard indeed credit karma Pinterest NASA ATLASSIAN

Unleash Human Creativity for Proactive Security

TRY BUGCROWD