bugcrowd

DATA SHEET

PEN TEST AS A SERVICE

API Penetration Testing

Find hidden vulnerabilities with specialized talent

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.

While regular testing can help, organizations face significant trade-offs in available options: Scanners are fast, but typically, they only surface low-hanging fruit and are almost always more noisy than useful. Traditional pen test providers leverage critical human creativity, but they do so as cumbersome consulting engagements that take too long and leave you in the dark about results.

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
- 24/7 visibility into timelines, findings, and pentester progress through their checklist via a rich dashboard
- 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
- Detailed auditor report

Key Points of Value

Start testing faster

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

Expert testers are matched to your requirements

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

See results in real time

Leave opaque pentesting behind. Instead, view prioritized findings as they're reported, and flow them into your SDLC for fast remediation.

Testing can be customized to suit individual testing needs--including expedited launches, re-testing, and special pentester requirements.

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.

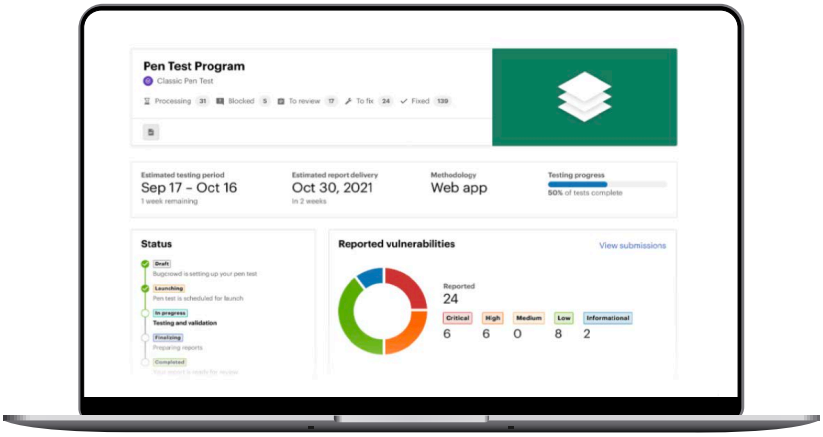
Exploitation and Documentation

Verify security weaknesses and collect results

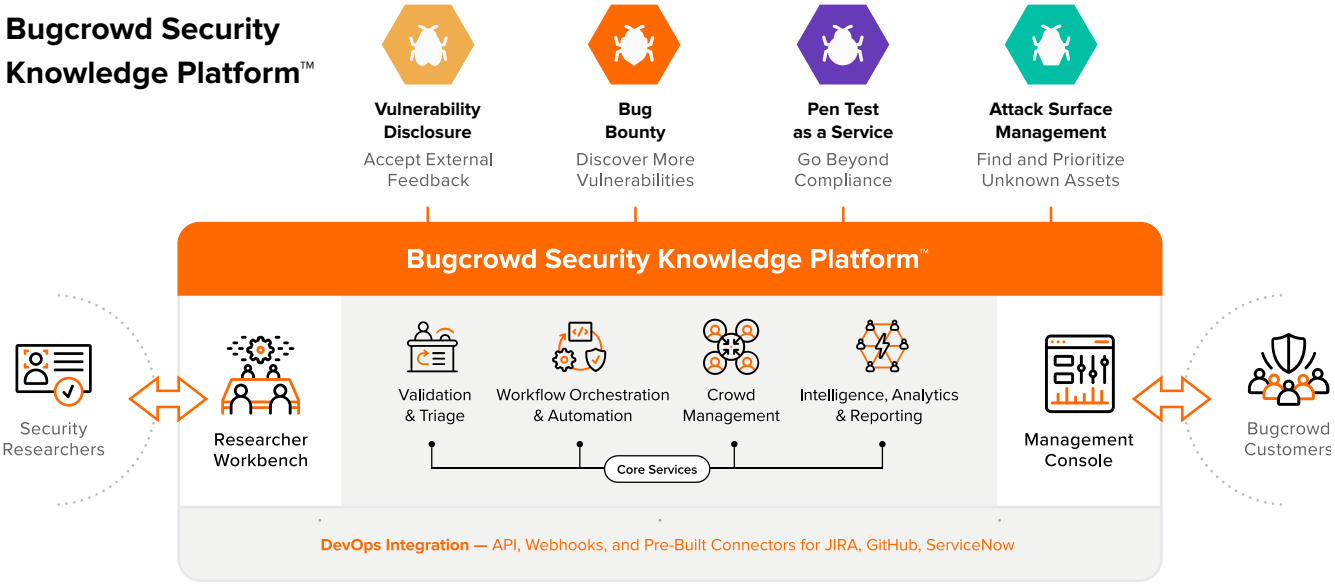
- Review endpoints to determine if any are exposing sensitive information.
- Test authentication flow for logic errors that may result in bypasses.
- Test session mechanism for weaknesses or configuration mistakes.
- Test for access control issues between user roles.
- Check for service misconfigurations 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)

How It Works

The ugcrowd Security nowledge latform makes it easy to configure and launch pen tests for any asset. fter building a pentester team per your e act needs, we'll launch your pen test within days and give you 24/7 access to prioritized results, along with test status and progress, in a rich dashboard. When your test is complete, you can download a detailed report for compliance directly inside your dashboard.



Bugcrowd Security Knowledge Platform™



Right Crowd, Right Time

Need special skills? We match the right trusted hackers to your needs and environment across hundreds of dimensions using AI (CrowdMatch™).

Engineered Triage at Scale

sing an advanced toolbo in our the platform, our global team rapidly validates and triages submissions, with s often handled within hours.

Insights From Security Knowledge Graph

We apply knowledge developed over a decade of e perience across thousands of customer programs to help you make continuous improvements.

Works With Your Existing Processes

The platform integrates with your e isting tools and processes to ensure that applications and ls are continuously tested before they ship.