bugcrowd

CASE STUDY

PEN TESTING BUG BOUNTY

Catawiki maximizes security ROI with Bugcrowd Pen Test and Bug Bounty

catawiki

Industry Online auctions eCommerce

Founding Date 2008

Website catawiki.com

# of Employees 750

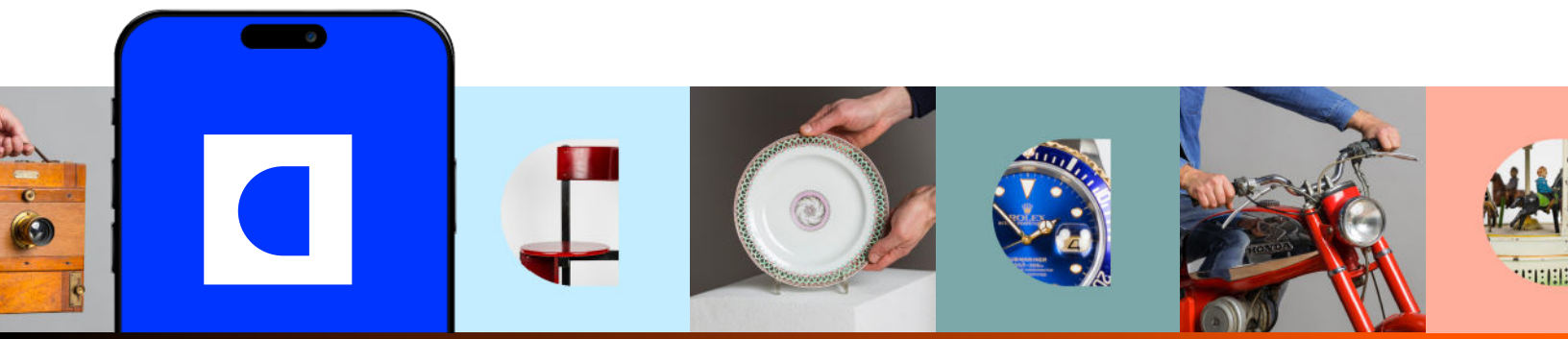
Headquarters Amsterdam, NL

How Europe's leading marketplace for special objects secured its platform and API with pen tests and bug bounties

The Situation

Catawiki runs Europe's leading marketplace for special objects. It has 10 million unique visitors every month and needs strong security measures in place to ensure that auctions and online sales work seamlessly and without interference to protect its users' trust. To secure its products and reputation, Catawiki focuses on its web platform, where the auctions are run, and its internal API.

The company and its leadership have long been believers in crowdsourced and offensive security, where the good actors probe for vulnerabilities before they become a problem. Catawiki set up pen tests and bug bounties with the goal of rooting out vulnerabilities. However, its previous bug bounties and pen tests were not delivering the results it needed, with no pen test vulnerabilities found in 2022.



The Challenge

Catawiki needed a better solution. Although it had other controls in place to catch vulnerabilities earlier, it wasn't confident that its previous providers had enough skilled ethical hackers to find the hidden vulnerabilities. Even when vulnerabilities were found, Catawiki felt they were basic and not directly impacting ones that an automated scanner could have picked up. During the tests themselves, prior pentesters weren't very communicative, and Catawiki didn't feel like it could focus the tests on the right areas of its product. Because of this lack of results, Catawiki found itself choosing different providers every year, burdening its security team with regular migration and onboarding work. Finally, after its last bug bounty provider found only two minor bugs and ended the bug bounty before Catawiki's funds were even used up, the company decided to switch to Bugcrowd.

The Bugcrowd Solution

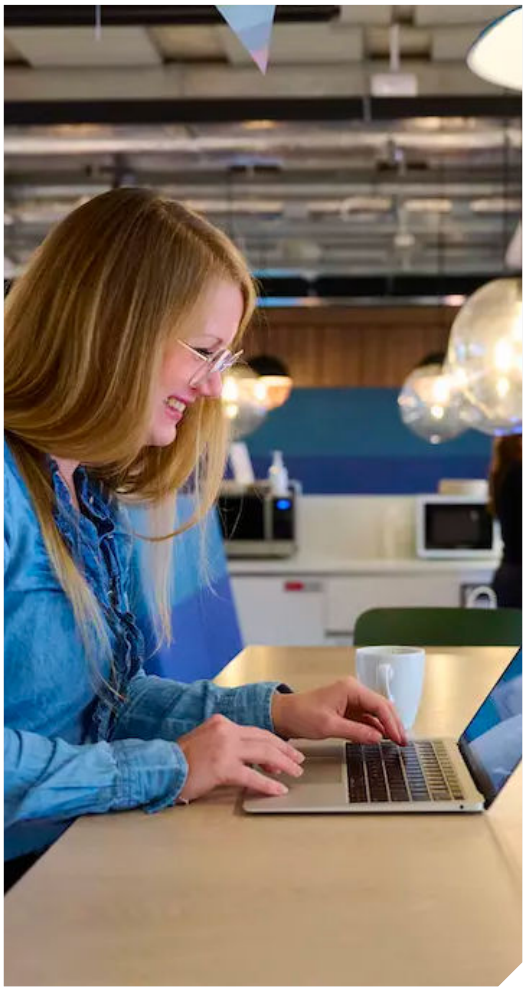
In considering its provider options, **Catawiki found that Bugcrowd stood out as a leader in the crowdsourced and offensive security market.** It ultimately chose Bugcrowd because it offers a well-unified bug bounty and pen testing platform—one place to do it all. Catawiki was excited by the prospect of using pen testing results to directly enhance the bug bounty program.

In the words of Aristide Bouix, Security Engineer at Catawiki, **"The bug bounty program provides added value beyond a pen test, but if it's run through the same platform, its value is doubled."** By choosing Bugcrowd, Catawiki stopped having to juggle multiple engagements with different pen test and bug bounty providers, and it no longer needed to port results from one provider to another. Furthermore, it could avoid the myriad onboarding and monitoring meetings that were part of its prior security efforts. Given these considerations and obstacles, Bugcrowd made the most sense.

Catawiki started with a Bugcrowd pen test. From the start, the process was transparent and controllable, which Catawiki felt had been missing with previous providers. Pentesters communicated frequently in Slack, detailing the surfaces they were going to test along with their methodology. There were also many pentesters available, allowing Catawiki to choose the right testers for its specific surfaces.

Bugcrowd's pentesters ultimately found four P2 vulnerabilities for Catawiki, including some that affected its API, which was a high-priority surface. **The pen test results directly helped Catawiki shape its security roadmap.** Aristide shared, "We were able to reuse the content of this pen test report to shape our internal product security program roadmap and prioritize initiatives that go beyond the simple findings, as part of our engineering effort."

- ✓ In the first 2 months of their engagement, Catawiki found 3x more vulnerabilities than the industry standard.



The Outcome

After the pen test, Catawiki transitioned to running a managed bug bounty with Bugcrowd. Running both programs through one platform with Bugcrowd let Catawiki use the pen test results to catch the low-hanging fruit so that the bug bounty can yield more elusive vulnerabilities. With the bug bounty, hackers caught 3X more vulnerabilities in the first two months of the engagement than the industry standard. Discovering more API bugs through the bounty also helped Catawiki develop its security roadmap even more effectively. In contrast to previous bug bounties, Bugcrowd's bug bounty uncovered novel vulnerabilities. "These vulnerabilities had not been identified in previous pen tests or responsible disclosures until they were discovered through Bugcrowd" Aristide says.

With new critical vulnerabilities found, Catawiki was able to make a security roadmap to fix its most critical issues and secure its platform and API. Reflecting on the process, Catawiki mentioned that major benefits included the breadth of expertise available on Bugcrowd, the strong communication, and the ability to run pen tests and bug bounties through the same platform. With its yearly pen test concluded, Catawiki will continue to run its bug bounty to keep ensuring its auctions and online sales are secure.

"Combining pen testing and bug bounty through Bugcrowd helps our team meet immediate security requirements while proactively reducing risk. It gives us the scale and agility to stay ahead of today's biggest threats and tomorrow's unknown challenges."

— **ARISTIDE BOUIX** Security Engineer • Catawiki