hackerone

GET MORE FROM YOUR **PEN TEST** BUDGET

Your attack surfaces are multifacted,
your security should be too.

Use Hackers to Get More from Your Pen Test Budget

Don't just check the box on your annual pen test regimen. Check the box and get useful results to improve your overall security.

Every technology has vulnerabilities, and the role of an organization's security team is to both minimize them and discover them before they can be exploited by attackers. An important part of every security apparatus is an annual penetration test regimen, which puts researchers to work finding bugs and then delivering a final report. It fulfills a compliance requirement, and usually comes with a high price tag and only returns a list of low-severity bugs.

Instead of just completing an annual pen test and moving on, it's time to look at pen tests differently, and apply new, innovative, and dynamic techniques to protect your customers and your business. One of the most effective and efficient ways is by leveraging the support, expertise, and cleverness of white-hat hackers in a focused, time-bound bug bounty program (also known as a hacker-powered pen test or "Challenge").

Hackers Produce Better Results

CISOs across all industries are already discovering the benefits of bug bounty programs, where organizations offer cash rewards to hackers who find and report verifiable vulnerabilities. For forward-thinking security teams, bug bounty programs have become the fastest way to put trusted hackers and their skills to work testing for critical vulnerabilities.

With a hacker-powered pen test, security teams can utilize large pockets of the best talent, all without a huge initial cost. It brings more security professionals to the table—dozens or even hundreds—testing your attack surfaces. It expands the pool of skills available, putting diverse approaches to work to increase the likelihood of identifying more bugs, harder to find bugs, and more severe vulnerabilities.

Best of all, hacker-powered pen tests let you pay for results, not time. Payment is only made when vulnerabilities are validated, and the price is based on severity. It's a win-win model, since hackers are incented to find as many bugs of high severity as possible.

And, it's easy to integrate a hacker-powered pen test into your existing security apparatus.

A Better Pen Test with a Familiar Workflow

It's easy to fit bug bounties into any existing security program. From training to design and development to testing and deployment, the information gleaned from a hacker-powered pen test is valuable across all areas of the software development lifecycle. Here are a few things to consider as you put hackers to work for your next pen test.

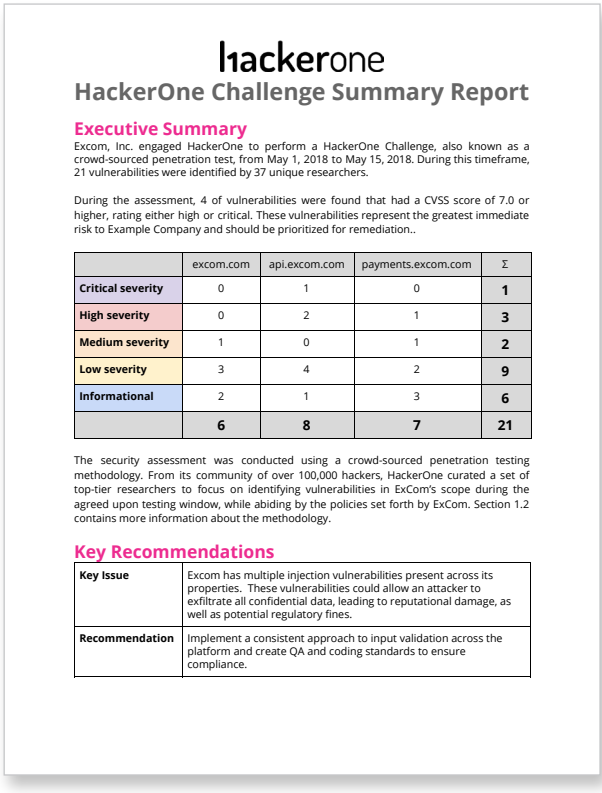
Good bug bounty platforms publish APIs that allow security teams to push and pull data from the bounty program into and out of their bug tracking, ticketing, project management, and security tools. They also provide dashboards and reports to open a strategic view of the types, numbers, and properties where vulnerabilities are found, allowing managers to identifying training issues, inform design and development cycles, and refocus testing efforts.

Bug bounty platforms can further add automation to categorize and route incoming reports, which helps teams effectively respond to critical reports while ignoring duplicates or out of scope reports. Some platform providers also offer triage services to supplement the efforts of security teams and ease the resource strain of an annual pen testing regimen.

Platform flexibility adapts a bug bounty program to a security team's unique needs. Programs can be public and open to all available hackers, or private and run as an invitation-only program.

Hackers can also be limited based on skills or past experience, background checks, or other eligibility requirements.

Most importantly, the findings from a pen test must be clear, concise, and compliant. Program metrics should be easily accessible from any bug bounty platform to ease reporting, expand the learning opportunities, and provide insights that are not usually available using traditional pen testing methods. And a formal report with detailed results and recommendations should be provided.



hackerone

HackerOne Challenge Summary Report

Executive Summary

Excom, Inc. engaged HackerOne to perform a HackerOne Challenge, also known as a crowd-sourced penetration test, from May 1, 2018 to May 15, 2018. During this timeframe, 21 vulnerabilities were identified by 37 unique researchers.

During the assessment, 4 of vulnerabilities were found that had a CVSS score of 7.0 or higher, rating either high or critical. These vulnerabilities represent the greatest immediate risk to Example Company and should be prioritized for remediation..

	excom.com	api.excom.com	payments.excom.com	Σ
Critical severity	0	1	0	**1**
High severity	0	2	1	**3**
Medium severity	1	0	1	**2**
Low severity	3	4	2	**9**
Informational	2	1	3	**6**
	6	**8**	**7**	**21**

The security assessment was conducted using a crowd-sourced penetration testing methodology. From its community of over 100,000 hackers, HackerOne curated a set of top-tier researchers to focus on identifying vulnerabilities in ExCom's scope during the agreed upon testing window, while abiding by the policies set forth by ExCom. Section 1.2 contains more information about the methodology.

Key Recommendations

Key Issue	Excom has multiple injection vulnerabilities present across its properties. These vulnerabilities could allow an attacker to exfiltrate all confidential data, leading to reputational damage, as well as potential regulatory fines.
Recommendation	Implement a consistent approach to input validation across the platform and create QA and coding standards to ensure compliance.

Example of HackerOne Challenge Summary Report

HackerOne Challenge: The Hacker-Powered Pen Test

HOW IT WORKS

Week 1

Meet with client.
Explain process.
Define scope and goals.
Invite prescreened hackers.

Week 2 - 3

Hackers report vulnerabilities.
HackerOne manages process,
validates and triages bugs.
Provides payout to hackers.

Week 4

Deliver summary report.
Review results.
Discuss options.

HackerOne Challenge: A Turnkey Pen Test

HackerOne Challenge brings all of the benefits of HackerOne and our community of expert white-hat hackers, but in a fixed cost, time-bound approach to replace or augment a traditional annual pen testing regimen. HackerOne Challenge is compliant, results-driven security testing that has been proven to outperform traditional pen tests.

Hackers think like outsiders because they are outsiders. They add true black box testing to your rotation of traditional pen tests, and put many more experts, with more diverse skills, to work searching for vulnerabilities faster than ever and with incredible cleverness. Combined, it provides a bang for the security buck that cannot be matched by traditional pen tests.

HackerOne Challenge can also be used to supplement a traditional pen testing regimen, providing insights to direct subsequent pen tests and identify areas for additional focus in the future. It can also determine if previous pen tests have thoroughly identified vulnerabilities in a specific application or component.

HackerOne Challenge is a turnkey method for elevating any security apparatus. It provides better results, allows more flexibility, and produces more critical vulnerabilities to result in a higher ROI and better security outcomes.

Learn more about HackerOne Challenge or download "Hacker-Powered Pen Tests and the Power of More" to dig deeper into the ways hackers can replace or augment traditional pen test regimens.

READ MORE

hackerone

ABOUT US

HackerOne is the #1 hacker-powered security platform, helping organizations receive and resolve critical vulnerabilities before they can be exploited. More Fortune 500 and Forbes Global 1000 companies trust HackerOne than any other hacker-powered security partner. Organizations, including the U.S. Department of Defense, U.S. General Service Administration, General Motors, Google, Twitter, GitHub, Nintendo, Lufthansa, Panasonic Avionics, Qualcomm, Starbucks, Dropbox, Intel, and the CERT Coordination Center trust HackerOne to find critical software vulnerabilities. HackerOne customers have resolved over 70,000 vulnerabilities and awarded over $28M in bug bounties. HackerOne is headquartered in San Francisco with offices in London, New York, and the Netherlands.

Contact us to get started.