HACKER-POWERED **PEN TESTS** AND THE POWER OF **MORE**

hackerone

Your Attack Surfaces Are Multifaceted. Your Security Should Be Too.

Traditional penetration testing is a common strategy for application security. But you're probably not always satisfied with the results. Standard pentests are often conducted by recently trained employees who deliver a report outlining lower severity vulnerabilities. Boutique firms promise more experience, but at an even higher cost.

With modern hacker-powered pen tests, you tap into more of the best talent, without a huge initial price tag. The hacker-powered model has been proven to deliver immense value, with customers reporting 6x returns.

Like traditional penetration testing, a hacker-powered pen test like the HackerOne Challenge program runs for a fixed time period. But it also brings to bear the skills of up to thousands of independent, trusted security researchers, ethical hackers who probe your web applications for vulnerabilities. These creative, talented hackers have more diverse skillsets than a comparable junior pen tester. They also find many more severe vulnerabilities than traditional pen testers, in part because **they are paid not for their time, but for results**.

> "Our developers are frequently blown away by the ingenuity of the researchers. Using HackerOne saves our security team a large amount of time, but more importantly it also saves our finance team a lot of trouble."
>
> - Neil Matatall, Security Engineer, GitHub

MORE PROS

MORE SKILL SETS

MORE TYPES OF BUGS FOUND

MORE SEVERE BUGS FOUND

MORE THAN JUST PCI AND SOC2 COMPLIANT

Traditional Pen Testing: The Good, The Bad And The Ugly.

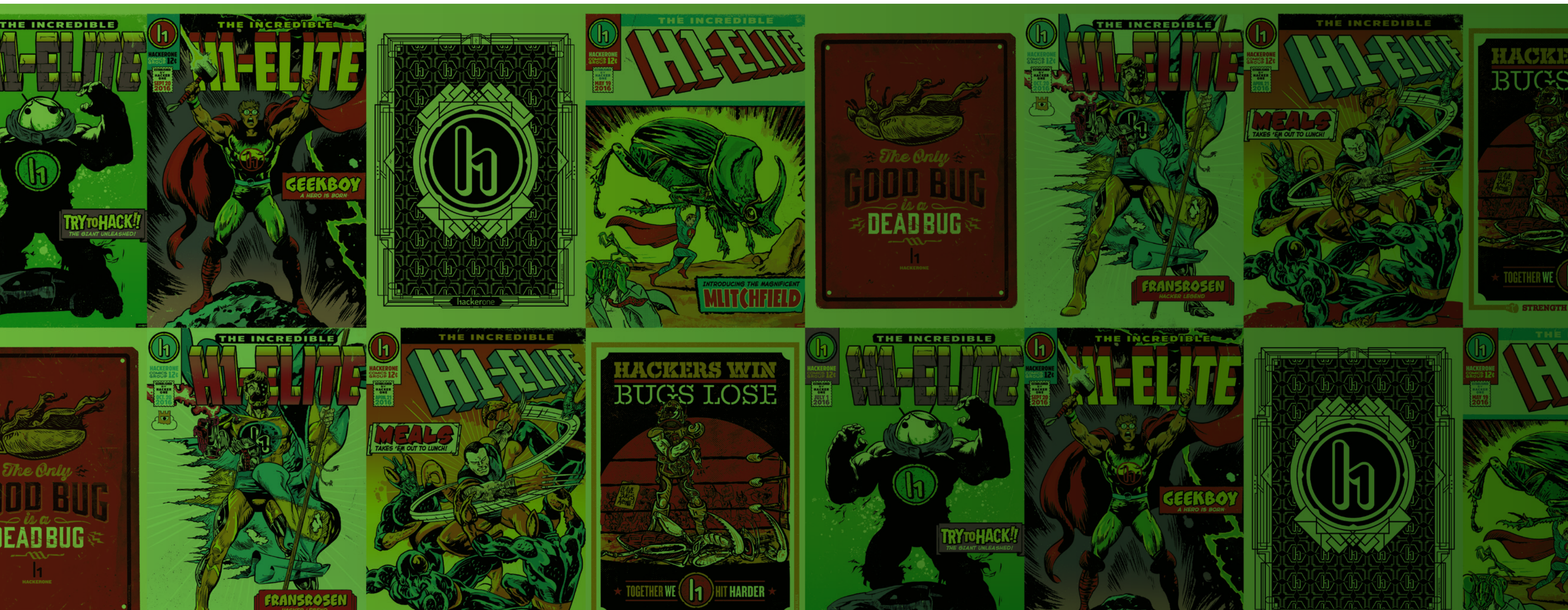
Traditional pen tests work well for testing on-site security and running crystal-box, insider tests.

BOTTOM LINE:

You pay the pen testing firm the same fee, regardless of results.

You invite pen testers into your company and give them passwords. They go beyond your firewalls and work with your engineering team. You can check anything from employee vulnerabilities to social engineering and even phishing attacks. But traditional pen testing firms can't do the whole job.

You may have very different priorities from a traditional pen tester using an automated approach or working from a playbook. The results from a traditional pen test may be limited in scope and severity, finding mainly non-critical vulnerabilities.



Traditional Pen Testing Versus Hacker-Powered Pen Testing

	TRADITIONAL PENETRATION TESTS	HACKERONE CHALLENGE
On-Demand	No	Yes
Access to Skilled Hackers / Testers	Shallow talent pool means a limited ability to match finder with scope.	The world's largest community of elite security talent, which includes world-class penetration test veterans, provide superior matching capabilities based on your program needs.
# of Researchers / Hackers per Challenge	2-4	Customizable (1, 5, 10, 500, ...)
Hacker Matching & Secure Collaboration Tools	No	Yes
Notice of Findings	Once at the end of test	In Real-Time; On-Demand
Severity of Findings	Common; Low Impact	Rare and Complex; High-Critical
Find Complex Vulnerability Chains	Rare	Common
Includes Retesting	Varies	Available
Point-in-Time or Continuous	Point-in-Time Only	Customizable (Bundles Also Available)
Dedicated Program Specialist	Yes	Yes
Managed, End-to-End Program Support	Yes	Yes
SDLC Integrations (ie, JIRA, Slack, ServiceNow, others)	No	Yes
Methodology-driven Engagements Assessments	Yes	Yes
Technical Reporting	PDF at end of testing period	Accessible In-Platform + Integrated into SDLC for easy access
Executive Summary Report	Yes	Yes (PDF)
Meet Compliance Needs (ie, PCI, HIPAA, SOC2)	Yes	Yes

Integrating Hacker-Powered Pen Testing Into Your Annual Pen Testing Regimen

A hacker-powered pen test, or **HackerOne Challenge**, is a fixed cost, time-bound complement or alternative to traditional pen testing.

A Challenge can help direct your next traditional pen test by focusing on a certain application to identify vulnerabilities and components in need of additional hardening. A Challenge can determine if a traditional pen testing firm has uncovered all problem areas.

As independent security researchers, hackers think like outsiders because they are outsiders. Adding a hacker-powered pen test to your rotation of traditional pen tests enables you to do true black box testing.

"SUCH A SUCCESS"

A multinational financial services firm ran a Challenge, focusing on applications that had been tested multiple times by top-tier pen testing firms. In the brief timespan of the Challenge, hackers found more than 50 vulnerabilities, with several critical reports filed.

Quarter 1	Quarter 2	Quarter 3	Quarter 4
CHALLENGE	TRADITIONAL	CHALLENGE	TRADITIONAL
Uncover weaknesses and remediate	Focus efforts where most needed	Find vulnerabilities, broad scope	Address insider threats

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.

Advantages of HackerOne Challenge

MORE SECURITY PROS TESTING YOUR ATTACK SURFACES

MORE DIVERSE SKILLSETS

MORE BANG FOR YOUR BUCK

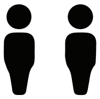
MORE SEVERE VULNERABILITIES SURFACED

MORE THAN JUST PCI AND SOC2 COMPLIANT

More Security Pros

Traditional Pen Testing

With a traditional pen test, you get one to three experts testing your security.



VS

Hacker-Powered Pen Testing

With a Challenge, you get dozens, hundreds or even thousands of independent security researchers testing your attack surfaces.

More Diverse and Deep Skills

While your contract for pen testing may be with a big-name security firm, the actual pen testers are often entry level employees with limited experience. They're learning on the job.

A Challenge ensures your hackers have many years of experience and a variety of skills. Your hacker-powered team will conduct testing with a diverse set of approaches, increasing the likelihood of finding hidden, severe vulnerabilities.

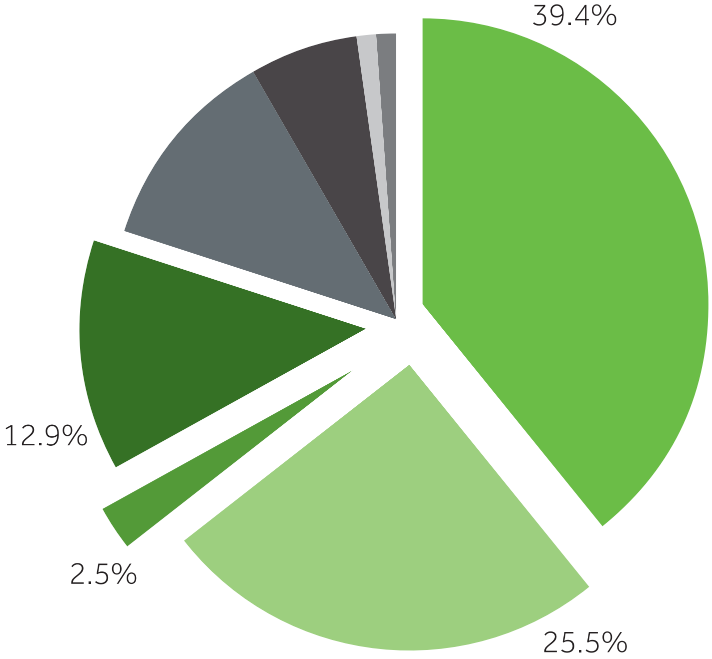
Some may be experts at finding database vulnerabilities, like SQL injection. Some may specialize in testing particular software frameworks like .NET. Others will be wizards at cross-site scripting issues.

Working with the hacker community also provides a unique perspective on your web application security. Ethical hackers in a Challenge program approach your surfaces as true outsiders. They test surfaces with creativity and persistence, using tricks from testing and probing other web applications with similar components.

A Challenge harnesses the power of more hackers with more diverse approaches, increasing the likelihood of finding hidden, severe vulnerabilities.

The Strength And Dedication Of The HackerOne Community

By profession



🟩 39.4% IT/Software/Hardware

🟩 25.5% Student

🟩 2.5% Unemployed

🟩 12.9% Consulting

Source: HackerOne

By motivation and dedication

- **14.3%** hack to earn money.
- **13.5%** hack for fun.
- **13.5%** hack to be challenged.
- **12.7%** hack to advance their careers..
- **9.3%** hack to do good in the world.
- **14.4%** hack more than 40 hours a week.

READ MORE

THE POWER OF MORE

Pay For Results: More ROI

Traditional pen testers are paid by the hour or paid a set fee per engagement.

Pen testers are incentivized to complete the assignment and bill the hours. It's a typical IT consulting model.

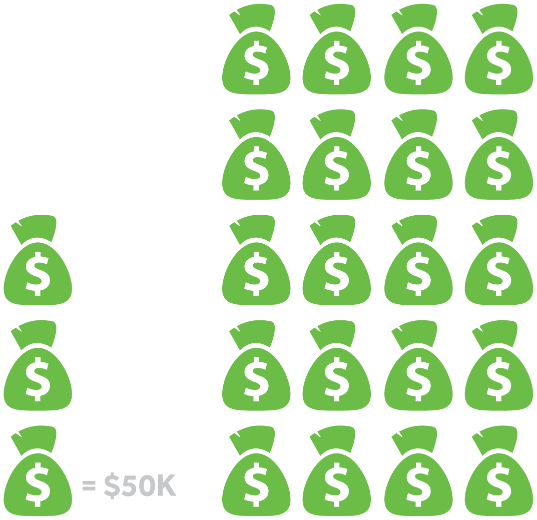
Hackers conducting pen tests are paid only if they find a vulnerability. You're in control. You incentivize discovery of critical vulnerabilities because you control how much more hackers are paid to find bugs you care about. You align your hackers' priorities with your business priorities.

Paying for results is a far cry from checking the box when it comes to compliance. It's a cost effective means to find as many vulnerabilities as possible, quickly, at the lowest possible cost.

Hack the Pentagon ran for four weeks and, in the end, the DoD concluded the return on investment was exceptional.

With a Challenge, hackers are incentivized to find results, especially the results you care about.

> "If we had gone through the normal process of hiring an outside firm to do a security audit and vulnerability assessment, which is what we usually do, it would have cost us more than $1 million."
>
> - Ash Carter,
> Secretary of Defense.



$150K
Total cost of the entire Hack the Pentagon

$1 Million
Hiring an outside contractor to conduct similar security test

More Vulnerabilities and More Severe Vulnerabilities

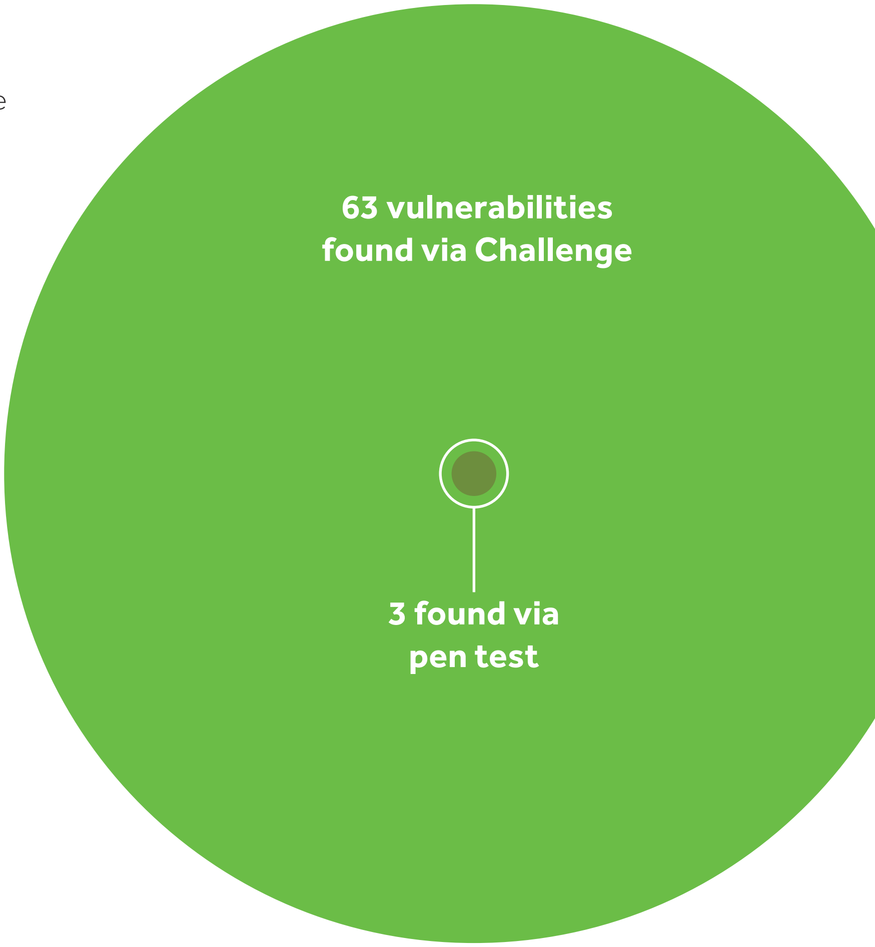
Higher severity vulnerabilities are extremely valuable. But you may not get them from a traditional pen test.

Incentives and goals are different for traditional pen testers compared to hacker-powered pen tests.

A traditional pen test firm may be hired with the goal of providing a clean bill of security health, above all. They may also be incentivized to provide that report as early as possible.

In contrast, the goal of a hacker-powered Challenge is to find all existing vulnerabilities, especially severe vulnerabilities, in a short amount of time. Since they're true outsiders, Challenge hackers work differently—like outsiders. Because a large group of hackers also is more diverse, motivated, creative and passionate than one to three pen testers, the hacker community uncovers more bugs and more severe vulnerabilities.

> In one comparison of a traditional pen test to a Challenge, pen testing found three vulnerabilities in the client organization. The Challenge found those three... plus 60 others



Challenge Results at a Client Site

U.S. Department Of Defense: The Power Of More In Action

The goal: Explore new approaches to security and adopt best practices based on results. Mission accomplished.

Hack the Pentagon was

6x Cheaper

than traditional pen testing

Hack the Air Force included

~300

vetted individuals

A single hacker made

30 Discoveries

during a Challenge

The Air Force security Challenge team found and addressed

207

real vulnerabilities

> "Adversaries are constantly attempting to attack our websites, so we welcome a second opinion—and in this case, hundreds of second opinions—on the health and security of our online infrastructure. By allowing the good guys to help us, we can better level the playing field and get ahead of the problem instead of just playing defense."
>
> - Peter Kim, U.S. Air Force Chief Information Security Officer

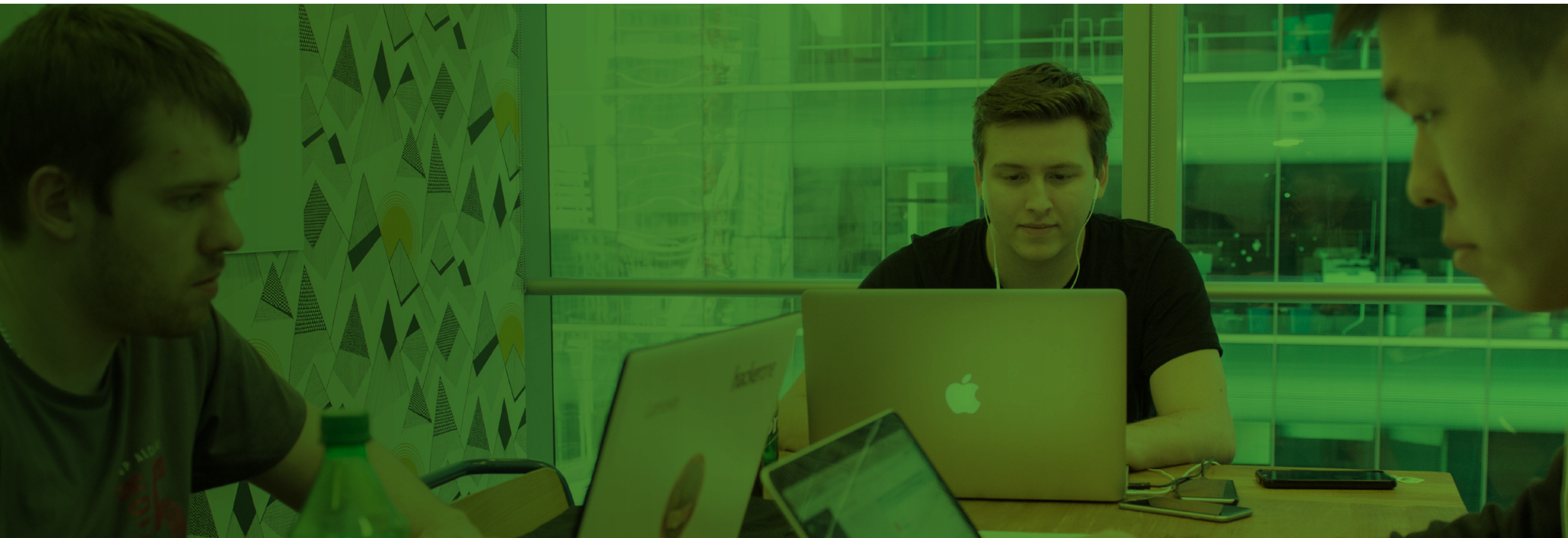
Making HackerOne Challenge Part Of Your Appsec Strategy

A Challenge can prepare for a pen test, or highlight areas that require more in-depth testing.

Challenges produce better results by tapping into a diverse, creative, and incentivized community of talented security researchers.

Challenges produce more critical vulnerabilities and provide stronger ROI.

Companies often rotate pen test vendors. Challenges can be added to that rotation as a cost-effective means to improve your security.



hackerone

ABOUT US

HackerOne is the #1 hacker-powered security platform, helping organizations find and fix critical vulnerabilities before they can be exploited. More Fortune 500 and Forbes Global 1000 companies trust HackerOne than any other hacker-powered security alternative. The U.S. Department of Defense, General Motors, Google, Twitter, GitHub, Nintendo, Lufthansa, Microsoft, MINDEF Singapore, Panasonic Avionics, Qualcomm, Starbucks, Dropbox, Intel, the CERT Coordination Center and over 1,300 other organizations have partnered with HackerOne to find over 120,000 vulnerabilities and award over $50M in bug bounties. HackerOne is headquartered in San Francisco with offices in London, New York, the Netherlands, and Singapore.

Contact us to get started.