hackerone

THE HACKER-POWERED SECURITY REPORT 2017

The Hacker-Powered Security Report examines the largest dataset of more than 800 hacker-powered security programs, compiles learnings from application security practitioners and the hackers who participate in bug bounty and vulnerability disclosure programs. The report also analyzed vulnerability disclosure data from the world's 2,000 biggest publicly traded companies according to Forbes. See the highlights here of some of the top findings. You can also download the full 27-page report packed with key learnings, graphs, and links to other helpful resources at https://www.hackerone.com/resources/hacker-powered-security-report

41%

While over half of bug bounty programs launched in 2016 are for technology companies, 41 percent are from other industries.

See Reports: http://www.hackerone.com/hacktivity

There has been a **46%** increase year over year in publicly disclosed vulnerability reports.

BUG BOUNTY PROGRAM GROWTH BY INDUSTRY

	2016 - 2017
TECHNOLOGY	59%
OTHER	9%
MEDIA & ENTERTAINMENT	10%
ECOMMERCE & RETAIL	6%
FINANCIAL & BANKING	10%
HEALTHCARE	3%
TRAVEL & HOSPITALITY	3%
TRANSPORTATION	2%
FOOD & BEVERAGE	2%
EDUCATION	1%
TELECOM	1%
GAMING	1%
GOVERNMENT	2%

Industries that launched programs from the overall share of programs, year over year.

Sample report header information from Hacktivity.

Sean Melia (meals) — 17050 Reputation · 2nd Rank · 5.46 Signal · 94th Percentile · 16.84 Impact · 87th Percentile

29 #141120 **Parameter Manipulation allowed for editing the shipping address for other user's teavana.com subscriptions.** Share:

State	Resolved (Closed)	Severity	No Rating (---)
Disclosed publicly	January 26, 2017 4:52pm -0700	Participants	
Reported To	Starbucks	Visibility	Public (Limited)
Scope			
Weakness	Improper Authentication - Generic		
Bounty	$4,000		

HACKERONE STATISTICS

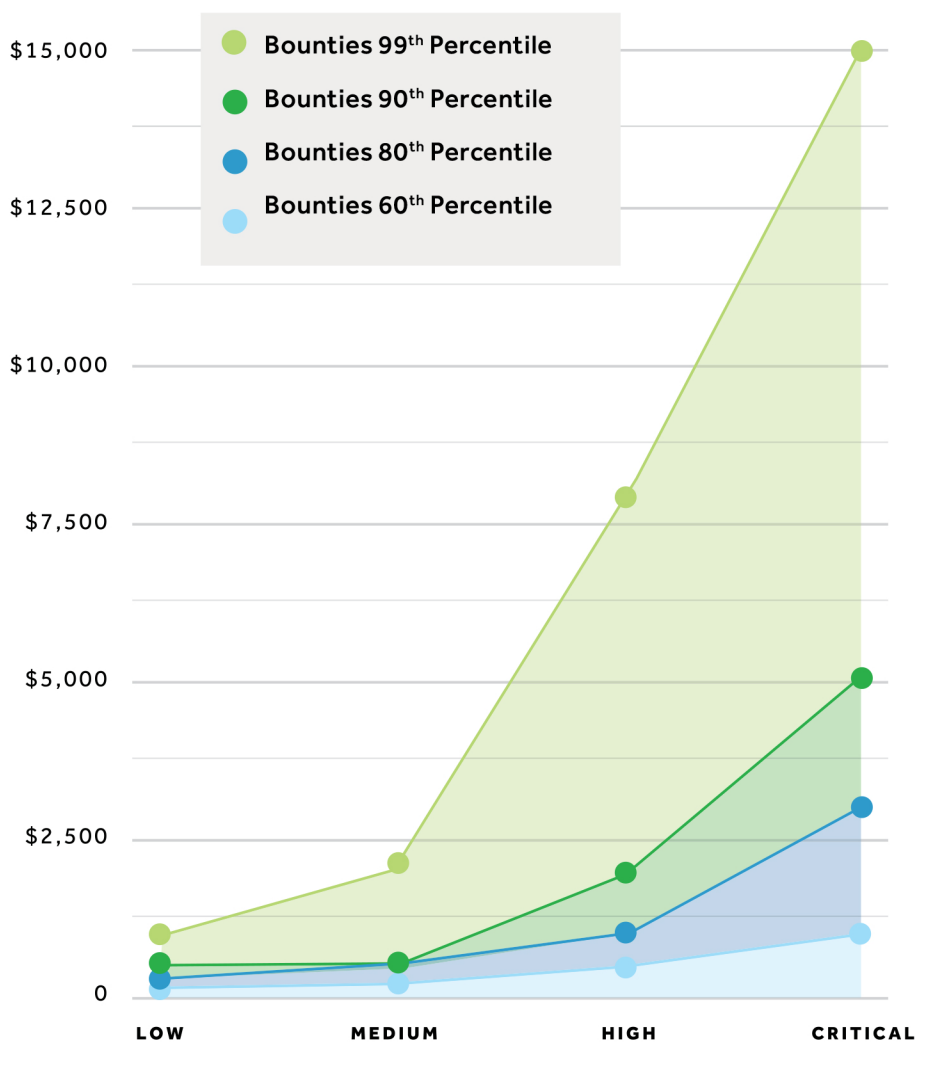
hackerone	Total Submissions	Valid Vulnerabilities	Hacker Community Size	Bounties Paid
	210,000	95,000	120,000	$18M

TIME TO RESOLUTION

	How quickly issues are solved per industry	Average time between bug filed and bounty awarded
Ecommerce & Retail	31	32
Education	33	30
Media & Entertainment	34	29
Technology	36	37
Financial & Banking	37	27
Travel & Hospitality	42	18
Food & Beverage	43	19
Healthcare	47	48
Transportation	49	39
Gaming	53	27
Government	63	61
Telecom	90	22

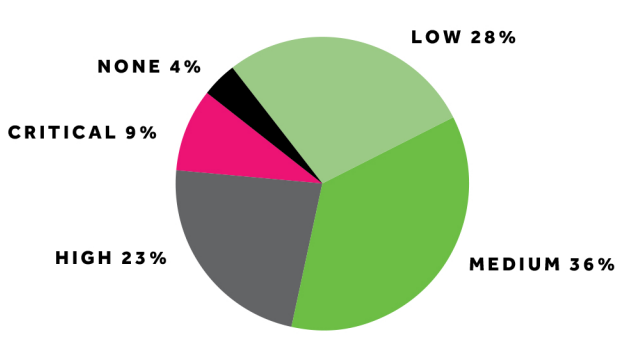
Average number of days to resolution and to reward, measured from Jan 1, 2016 to May 31, 2017.

AVERAGE BOUNTY PAYOUT BY VULNERABILITY SEVERITY



Bug bounty reward competitiveness for critical vulnerabilities from January 2016 to 2017. Organizations in the 99th percentile, rewarding $15,000 on average, are rewarding bounties higher on average than 99 percent of the programs on HackerOne.

VULNERABILITIES BY SEVERITY



Percentage of vulnerability type by severity Jan 2016 to May 2017.

AVERAGE BOUNTY PAYOUT PER INDUSTRY FOR CRITICAL VULNERABILITIES

Transportation	$4,491
Gaming	$3,583
eCommerce & Retail	$3,471
Other	$2,431
Technology	$2,015
HackerOne Platform Average	***$1,923***
Media & Entertainment	$1,017
Food & Beverage	$918
Travel & Hospitality	$647
Financial & Banking	$646
Healthcare	$643
Telecom	$383
Education	$317

Average bounty payouts per industry for critical vulnerabilities from 2013 to May 2017.

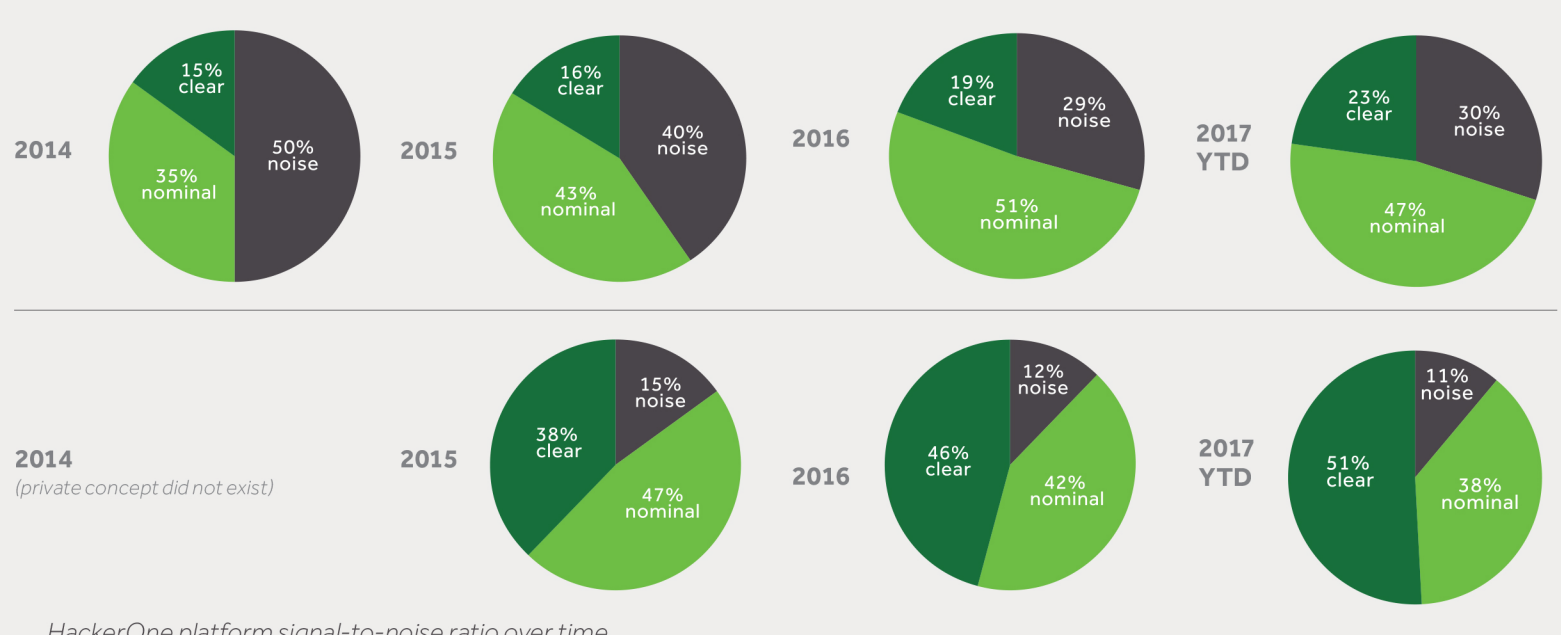
BOUNTIES BY GEOGRAPHY

	WHERE HACKERS ARE EARNING BOUNTIES	LOCATION OF COMPANY PAYING BOUNTIES
United States of America	**$2,435,169**	**$6,945,487**
India	**$1,814,578**	$50
Australia	**$1,065,095**	**$24,801**
Russia	**$723,778**	**$137,634**
Sweden	**$633,701**	**$25,230**
United Kingdom	**$539,946**	**$159,306**
Argentina	**$506,672**	$0
Hong Kong	**$415,210**	$950
Germany	**$377,621**	**$116,811**
Pakistan	**$365,885**	$0
Canada	**$355,014**	**$662,915**
Morocco	**$273,688**	$0
Philippines	**$261,248**	$3,340
Netherlands	**$249,256**	**$167,745**
China	**$227,137**	$3,340
Luxembourg	$167,745	**$116,765**
Finland	$81,034	**$103,424**
Japan	$63,246	**$28,757**
Singapore	$48,964	**$47,761**
Switzerland	$23,004	**$89,473**
United Arab Emirates	$16,560	**$33,135**
Mexico	$2,700	**$9,920**

Where hackers are earning the most dollars in total bounties, from April 2016 to April 2017. Where organizations are paying hackers the most dollars in total, from April 2016 to April 2017.

PUBLIC BUG BOUNTY PROGRAMS RESOLVE 4X AS MANY VULNERABILITIES AS PRIVATE PROGRAMS.

HackerOne has the highest published Signal-To-Noise Ratio (SNR) in the industry. To read more, see "Improving Signal Over 10K bugs"



HackerOne platform signal-to-noise ratio over time.

VULNERABILITY DISCLOSURE POLICY STATISTICS

Based on the 2017 Forbes Global 2000 list of the largest publicly traded companies in the world, our research team searched the Internet looking for ways a friendly hacker could contact a company to disclose a vulnerability.

94%
of the **Forbes Global 2000** do not have known vulnerability disclosure policies.

1
Starbucks is the only restaurant on the list with a vulnerability disclosure or bug bounty program.

14%
Five of 36 conglomerates have vulnerability disclosure programs, including **General Electric**, **Siemens**, **Honeywell International**, **ABB**, and **Philips**.

54%
of the top software/programming companies, 54% have programs: **Microsoft**, **Oracle**, **SAP**, **VMware**, **Adobe Systems**, **Symantec**, **Salesforce.com**, and **Intuit** (13 of 24).

8%
Two out of 24 airlines, **United Airlines** and **Lufthansa**, have vulnerability disclosure policies.

15%
Three out of 20 consumer financial services, including **Visa**, **MasterCard** and **PayPal** have programs.

10%
Three out of 31 auto and truck manufacturers have policies. They are **General Motors**, **Tesla** and **Fiat Chrysler Automobiles**.

9%
Six out 64 Major Banks have vulnerability disclosure policies: only **JPMorgan Chase**, **Citigroup**, **ING Group**, **Danske Bank**, **Swedbank**, and **Royal Bank of Scotland**.

GLOSSARY

VULNERABILITY DISCLOSURE POLICY (VDP):
an organization's formalized method for receiving vulnerability submissions from the outside world. This often takes the form of a "security@" email address. The practice is defined in ISO standard 29147.

BUG BOUNTY PROGRAM:
an open program any hackers can participate in for a chance at a bounty reward.

PRIVATE BUG BOUNTY PROGRAM:
a limited access program that select hackers are invited to participate in for a chance at a bounty reward.

TIME-BOUND BUG BOUNTY:
a program with a limited time frame. In most cases hackers will register or be invited.

TRUSTED GLOBALLY

GM · Lufthansa · Starbucks Coffee · Twitter · Spotify · Department of Defense · airbnb · LendingClub · Nintendo · WordPress · UBER · shopify · BLOCKCHAIN · Snapchat · CYLANCE