

hackerone

Hacker-Powered Security Report

INDUSTRY INSIGHTS '21



INTRODUCTION

Digital transformation and cloud migrations expand potential attack surfaces and internal security teams are stretched beyond measure.

The most innovative CISOs stay ahead of cybersecurity threats and mitigate vulnerabilities by augmenting internal teams and security testing tools with a skilled and engaged hacking community.

HackerOne's *Hacker-Powered Security Report: Industry Insights* leverages data from real-world vulnerability reports to provide insight into the fastest-growing vulnerability categories, how bounty prices are changing year over year, and which industries are fastest to fix.

Data will strengthen your security testing program. It will enable to you set the right bounty price, identify common vulnerabilities, and fix bugs faster and earlier.



In the 2021 Hacker-Powered Security Report: Industry Insights:

FIND OUT AT WHAT LEVEL YOUR PEERS ARE EMBRACING HACKER-POWERED SECURITY

FIND OUT WHICH HACKER-POWERED SECURITY PRODUCTS ARE GROWING IN POPULARITY AND EFFECTIVENESS

FIND OUT THE TOP TEN VULNERABILITIES IN YOUR INDUSTRY

FIND OUT THE AVERAGE BOUNTY PRICE YOU CAN EXPECT TO PAY FOR A CRITICAL VULNERABILITY

FIND OUT IF YOUR INDUSTRY IS KEEPING PACE WITH REMEDIATING VULNERABILITIES

ADOPTION

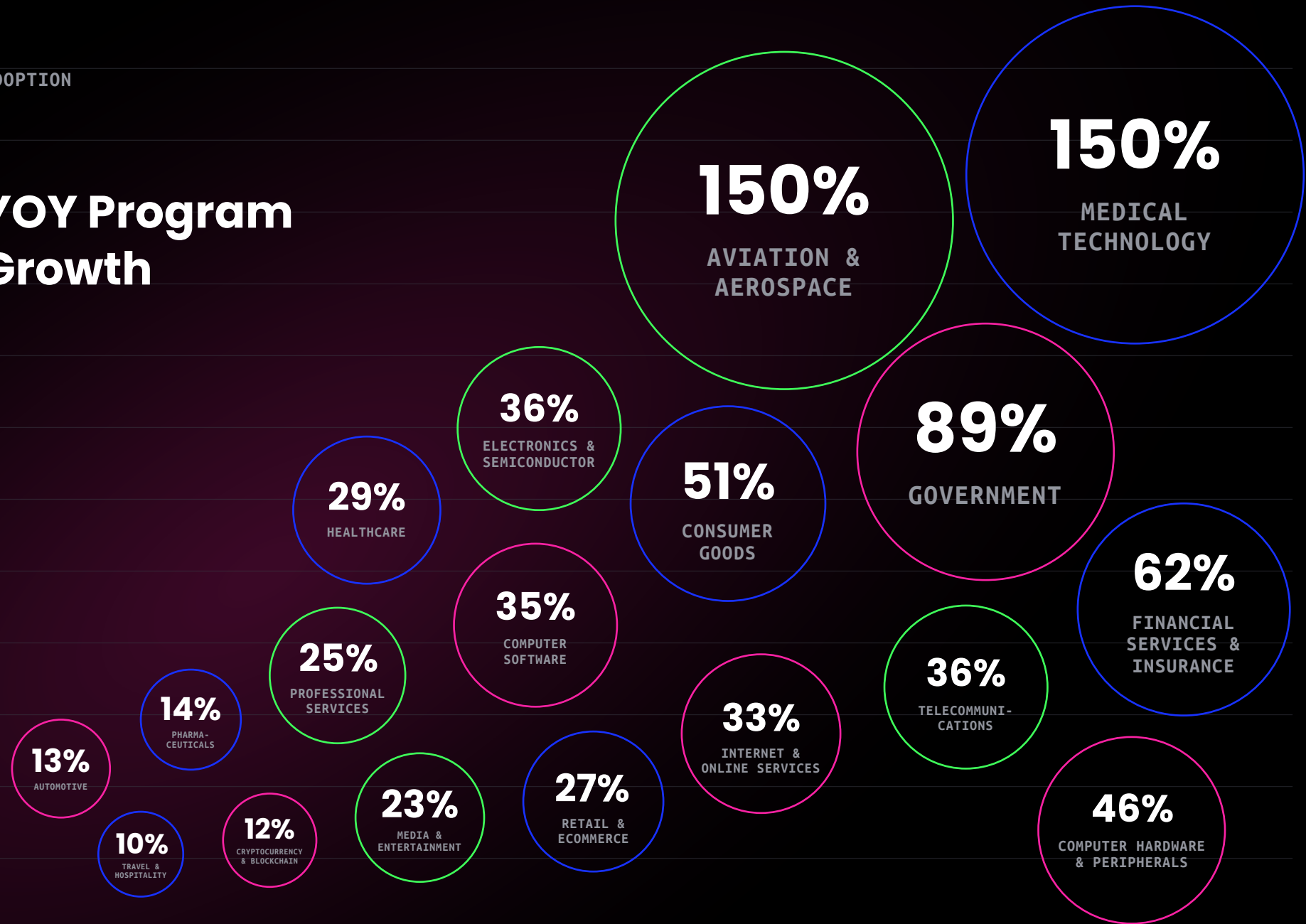
Adoption of hacker-powered security programs is growing across all industries, with the total number of hacker-powered customer programs increasing by **34% in 2021.**

34%

PROGRAM GROWTH

ADOPTION

YOY Program Growth



ADOPTION

We continue to see steady growth in Financial Services, which outside of core tech industries tends to lead the way with forward-thinking and agile security solutions.

62%

FINANCIAL SERVICES

We've seen significant growth in government programs with the UK's Ministry of Defense running the first of their bug bounty programs and Singapore's Govtech expanding their programs to deliver continuous security across the organization.

89%

GOVERNMENT

Industries that have seen significant cyber attacks and breaches, such as Aviation and Medical Technology, have seen particularly high growth, with a 150% increase in hacker-powered programs since 2020.

150%

AVIATION

51%

CONSUMER GOODS

150%

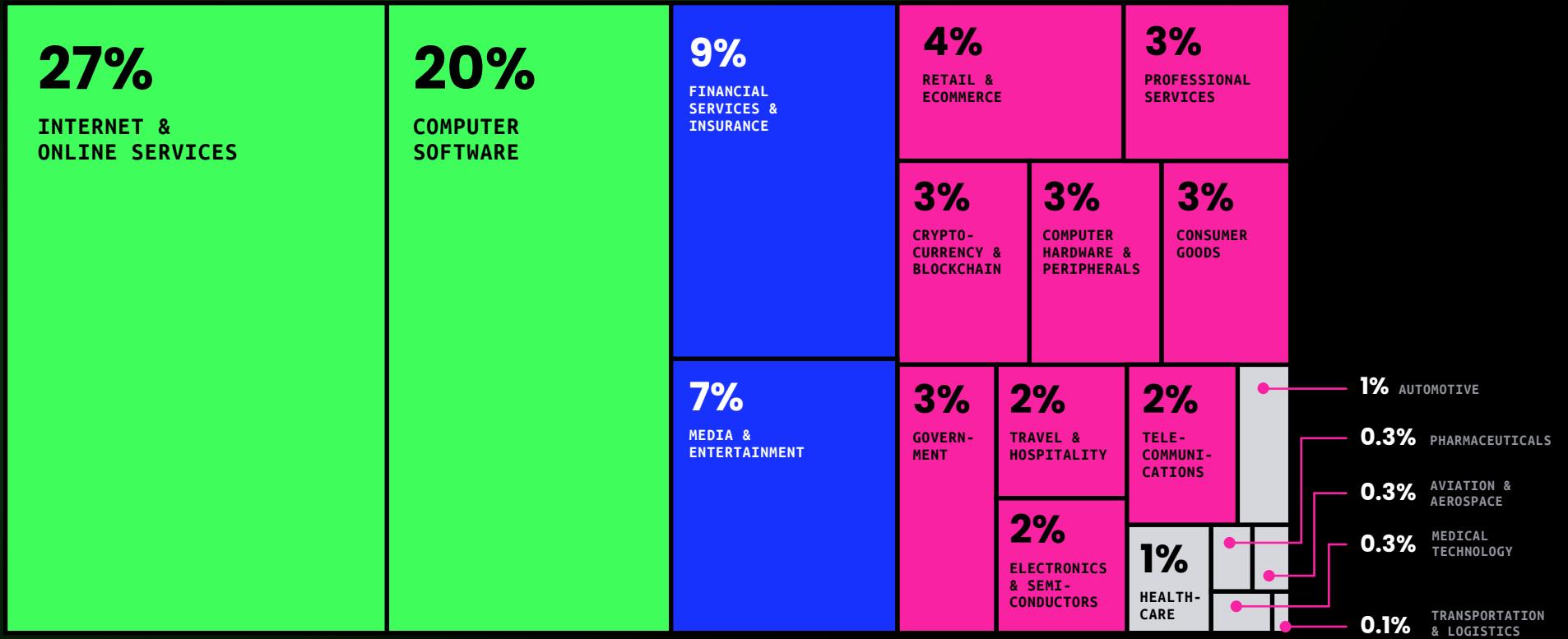
MEDICAL TECHNOLOGY

29%

HEALTHCARE

ADOPTION

Computer Software and Internet & Online Services continue to make up the bulk of hacker-powered security users. Financial Services is taking a more significant share with nearly 10% of customers falling into this vertical.



VULNERABILITY

Hackers reported **66,547** valid bugs in 2021—a **21% increase** from 2020.

66,547

VALID BUGS REPORTED

Total Bug Bounties

10%

YOY INCREASE IN
BUGS SUBMITTED

2020

38,863

VALID BUGS REPORTED 2020

2021

42,805

VALID BUGS REPORTED 2021

Public Bug Bounties

2%

YOY INCREASE IN
BUGS SUBMITTED

2020

17,151

VALID BUGS REPORTED 2020

2021

17,477

VALID BUGS REPORTED 2021

Private Bug Bounties

16%

YOY INCREASE IN
BUGS SUBMITTED

2020

21,701

VALID BUGS REPORTED 2020

2021

25,278

VALID BUGS REPORTED 2021

Private bug bounties resolve the most vulnerabilities. **Eighty percent of customers run private bug bounty programs but there are other reasons for the high vulnerability count.**

- Private programs are often a first step on the bug bounty journey and therefore are likely to yield higher results than a mature public program.
- There's less competition among hackers in a private program, meaning they will discover a greater number of valid findings and fewer duplicate findings.
- Hackers also spend more time with private programs where they are more likely to be rewarded. In public programs, they risk submitting duplicate vulnerabilities, and those don't qualify for rewards.

80%

OF CUSTOMERS RUN PRIVATE
BUG BOUNTY PROGRAMS



VULNERABILITY

Vulnerability Disclosure Programs

47%

YOY INCREASE IN
BUGS SUBMITTED

2020

14,054

VALID BUGS REPORTED 2020

2021

20,721

VALID BUGS REPORTED 2021

Pentests

264%

YOY INCREASE IN
BUGS SUBMITTED

2020

495

VALID BUGS REPORTED 2020

2021

1,804

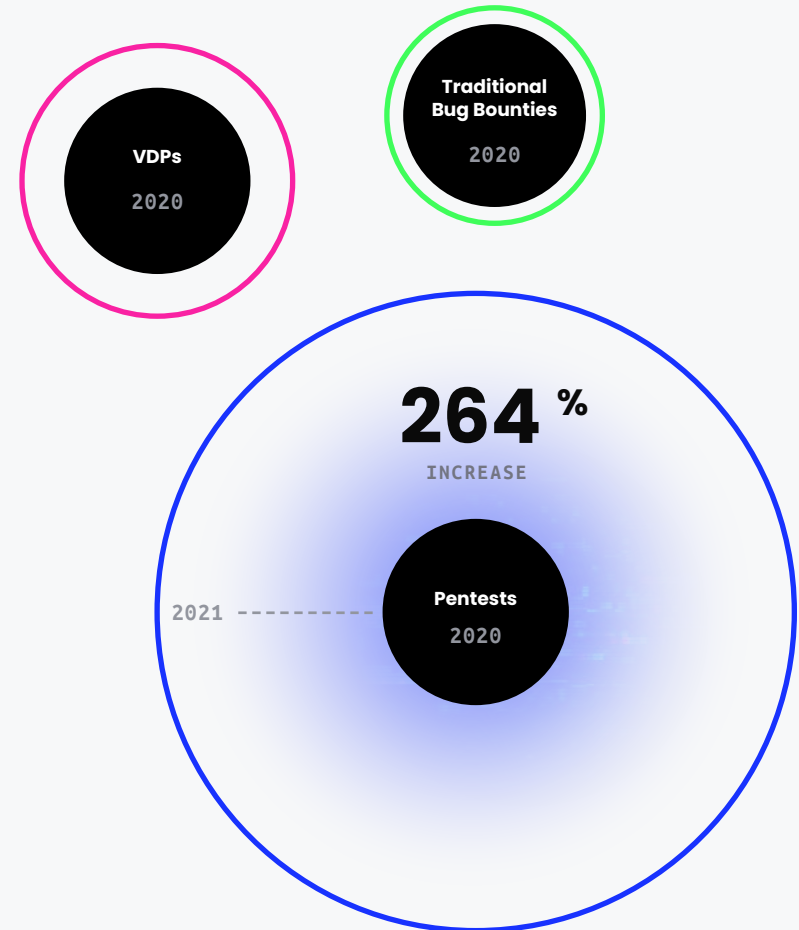
VALID BUGS REPORTED 2021

VULNERABILITY

While traditional bug bounties saw a **10%** increase in findings in the past 12 months, Vulnerability Disclosure Programs (VDPs) saw **47%** vulnerability growth, and hacker-powered pentests rose **264%**.

- We're seeing a significant increase in the percentage of vulnerabilities surfaced from VDPs and pentests. Pentest vulnerabilities made up 0.9% of all vulnerabilities in 2020. That has increased to 3% in the past 12 months.
- Significantly more customers launched pentests in 2021 than 2020. We've seen an enhanced customer focus on compliance with security regulations and standards, which is driving the requirement for pentests.
- We're also seeing customers bridging the security and development lifecycle with frequent assessments during product or feature releases. They're adding pentests to their existing continuous security testing programs.

As the adoption of hacker-powered solutions grows beyond bug bounty, they prove their value, not only for meeting regulatory standards but also for shoring up digital asset security.



Insight into vulnerabilities is the first step in mitigating against them.

The HackerOne Global Top 10 leverages our unique dataset giving customers insight into the most impactful weaknesses from a hacker perspective. These vulnerabilities are based on what hackers discover and are rewarded for on the platform.

How has the Top 10 changed in the past 12 months?

2020	2021	YoY % increase in valid reports
1 Cross-site Scripting (XSS)	1 Cross-site Scripting (XSS)	7%
2 Improper Access Control	2 Information Disclosure	58%
3 Information Disclosure	3 Improper Access Control	26%
4 Server-Side Request Forgery (SSRF)	4 Insecure Direct Object Reference (IDOR)	9%
5 Insecure Direct Object Reference (IDOR)	5 Privilege Escalation	55%
6 Privilege Escalation	6 Improper Authentication	18%
7 SQL Injection	7 Code Injection	12%
8 Improper Authentication	8 SQL Injection	-7%
9 Code Injection	9 Server-Side Request Forgery (SSRF)	-17%
10 Cross-Site Request Forgery (CSRF)	10 Business Logic Errors	67%

In the past 12 months, reports for Business Logic Errors increased by 67%, putting this vulnerability category on the Top 10 for the first time, replacing Cross-Site Request Forgery (CSRF) as number 10.

- Information disclosure rose from third to second place, with a 59% increase in reports, and code Injection saw a 13% increase in reports, increasing from 9th to 7th place.
- The most significant shift in the Top 10 is Server Side Request Forgery (SSRF) falling from 4th place to 9th. Improvements in cloud computing environments (AWS) have made that class of vulnerability easier to mitigate. Additionally, a number of high-profile breaches have been attributed to SSRF vulnerabilities, meaning security leaders are encouraging a focus on finding and fixing SSRF vulnerabilities across their networks.

67%
INCREASE

**Business
Logic Errors**

59%
INCREASE

**Information
Disclosure**

13%
INCREASE

**Code
Injection**

TOP 10 VULNERABILITIES

Bounties Total Financial Rewards Amount

\$36,925,156

TOTAL BOUNTIES FINANCIAL REWARDS AMOUNT


Top 10 Vulnerabilities














































Total bounty payouts 2021

1	Cross-site Scripting (XSS)	\$4,568,335
2	Information Disclosure	\$4,520,834
3	Improper Access Control	\$4,173,966
4	Insecure Direct Object Reference (IDOR)	\$2,678,161
5	Privilege Escalation	\$2,273,302
6	Improper Authentication	\$1,981,539
7	Code Injection	\$1,502,707
8	SQL Injection	\$1,440,657
9	Server-Side Request Forgery (SSRF)	\$1,420,749
10	Business Logic Errors	\$874,511

TOP 10 VULNERABILITIES


Check out how your industry compares against the HackerOne Top 10.


















































 % of total bounty spend

Top 10 Vulnerabilities	Automotive	Aviation & Aerospace	Computer Hardware & Peripherals	Computer Software	Consumer Goods
1. XSS	\$59,875  8%	\$10,700  33%	\$88,360  14%	\$781,361  9%	\$129,905  27%
2. Information Disclosure	\$131,250  18%	\$950  3%	\$70,280  11%	\$1,226,307  14%	\$58,625  12%
3. Improper Access Control	\$98,550  13%	\$650  2%	\$82,210  13%	\$1,765,475  20%	\$26,077  5%
4. Insecure Direct Object Reference (IDOR)	\$142,150  19%	\$0 0%	\$16,720  3%	\$377,986  4%	\$28,375  6%
5. Privilege Escalation	\$33,900  5%	\$250  1%	\$54,080  9%	\$712,767  8%	\$25,850  5%
6. Improper Authentication	\$36,300  5%	\$1,000  3%	\$26,760  4%	\$370,251  4%	\$29,730  6%
7. Code Injection	\$60,250  8%	\$0 0%	\$29,740  5%	\$411,619  5%	\$4,440  1%
8. SQL Injection	\$27,550  4%	\$2,000  6%	\$44,244  7%	\$328,022  4%	\$43,800  9%
9. Server-Side Request Forgery (SSRF)	\$1,275 0%	\$200  1%	\$12,740  2%	\$238,453  3%	\$11,600  2%
10. Business Logic Errors	\$2,700 0%	\$2,000  6%	\$2,600 0%	\$171,825  2%	\$9,650  2%
Total	\$730,150	\$32,825	\$630,349	\$8,730,891	\$479,887

TOP 10 VULNERABILITIES

Check out how your industry compares against the HackerOne Top 10.















































 % of total bounty spend

Top 10 Vulnerabilities	Cryptocurrency & Blockchain	Electronics & Semiconductor	Financial Services & Insurance	Government	Healthcare
1. XSS	\$34,945  7%	\$35,450  5%	\$272,162  11%	\$80,800  18%	\$33,300  22%
2. Information Disclosure	\$41,589  8%	\$30,150  4%	\$253,145  10%	\$38,050  8%	\$8,200  6%
3. Improper Access Control	\$51,434  10%	\$20,650  3%	\$253,245  10%	\$26,825  6%	\$28,450  19%
4. Insecure Direct Object Reference (IDOR)	\$2,800  1%	\$106,900  15%	\$234,354  10%	\$73,950  16%	\$14,150  10%
5. Privilege Escalation	\$38,026  7%	\$18,850  3%	\$155,760  6%	\$6,400  1%	\$3,200  2%
6. Improper Authentication	\$183,436  35%	\$10,700  1%	\$121,460  5%	\$28,050  6%	\$7,050  5%
7. Code Injection	\$500  0%	\$7,600  1%	\$79,410  3%	\$5,900  1%	\$8,000  5%
8. SQL Injection	\$16,500  3%	\$54,900  8%	\$118,350  5%	\$10,900  2%	\$14,000  9%
9. Server-Side Request Forgery (SSRF)	\$100  0%	\$14,000  2%	\$78,799  3%	\$61,400  14%	\$10,700  7%
10. Business Logic Errors	\$47,285  9%	\$29,200  4%	\$56,800  2%	\$2,500  1%	\$325  0%
Total	\$527,199	\$722,400	\$2,450,085	\$451,000	\$148,175

TOP 10 VULNERABILITIES


Check out how your industry compares against the HackerOne Top 10.

































 % of total bounty spend

Top 10 Vulnerabilities	Internet & Online Services	Media & Entertainment	Medical Technology	Pharmaceuticals	Professional Services
1. XSS	\$2,023,071  13%	\$412,520  19%	\$1,850  3%	\$3,650  2%	\$72,030  16%
2. Information Disclosure	\$1,891,526  13%	\$312,216  14%	\$4,900  8%	\$21,750  14%	\$35,935  8%
3. Improper Access Control	\$1,181,746  8%	\$236,834  11%	\$5,750  9%	\$33,150  22%	\$34,945  8%
4. Insecure Direct Object Reference (IDOR)	\$1,158,547  8%	\$112,360  5%	\$16,800  27%	\$14,500  10%	\$43,762  10%
5. Privilege Escalation	\$792,253  5%	\$112,363  5%	\$2,400  4%	\$7,550  5%	\$90,650  20%
6. Improper Authentication	\$638,337  4%	\$82,622  4%	\$6,850  11%	\$24,750  16%	\$22,960  5%
7. Code Injection	\$696,400  5%	\$88,455  4%	— —	\$1,650  1%	\$5,563  1%
8. SQL Injection	\$407,550  3%	\$103,587  5%	— —	\$8,100  5%	\$18,300  4%
9. Server-Side Request Forgery (SSRF)	\$843,342  6%	\$47,450  2%	\$0 0%	\$3,475  2%	\$6,950  2%
10. Business Logic Errors	\$349,246  2%	\$111,359  5%	\$250 0%	\$2,450  2%	\$5,220  1%
Total	\$9,982,018	\$2,213,422	\$62,600	\$151,925	\$442,825

TOP 10 VULNERABILITIES

Check out how your industry compares against the HackerOne Top 10.

 % of total bounty spend

Top 10 Vulnerabilities	Retail & eCommerce	Telecommunications	Transportation & Logistics	Travel & Hospitality
1. XSS	\$136,824  14%	\$206,792  10%	\$0 0%	\$107,669  16%
2. Information Disclosure	\$104,445  11%	\$140,792  7%	\$200  12%	\$80,662  12%
3. Improper Access Control	\$95,955  10%	\$106,291  5%	\$0 0%	\$94,232  14%
4. Insecure Direct Object Reference (IDOR)	\$125,765  13%	\$93,560  5%	\$1,200  71%	\$81,157  12%
5. Privilege Escalation	\$34,020  3%	\$141,955  7%	\$0 0%	\$24,427  4%
6. Improper Authentication	\$38,760  4%	\$283,723  14%	\$0 0%	\$47,178  7%
7. Code Injection	\$30,600  3%	\$58,600  3%	— —	\$9,518  0.01%
8. SQL Injection	\$75,010  8%	\$122,294  6%	— —	\$43,000  0.06%
9. Server-Side Request Forgery (SSRF)	\$22,450  2%	\$20,170  1%	— —	\$14,123  0.02%
10. Business Logic Errors	\$35,881  4%	\$22,200  1%	\$0 0%	\$12,559  2%
Total	\$986,592	\$2,041,653	\$1,700	\$685,615

TOP 10 VULNERABILITIES

Check out what the Top 10 Vulnerabilities are in your industry.

Automotive

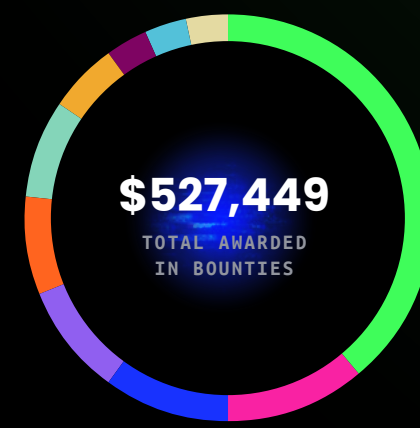
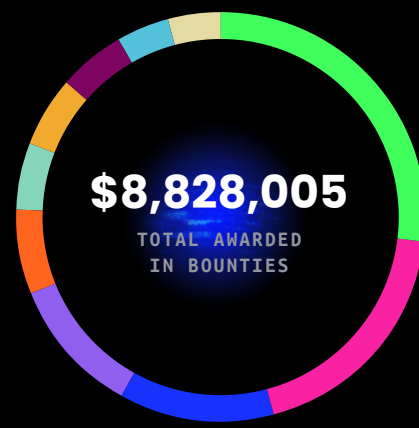
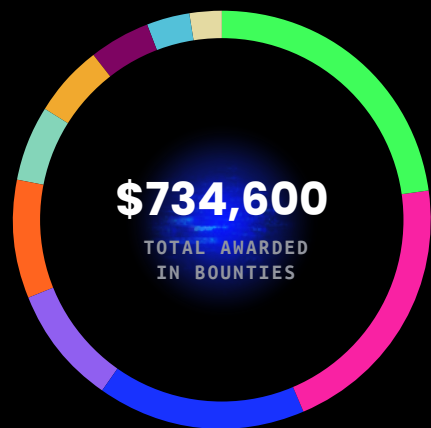
- 1. Insecure Direct Object Reference (IDOR) — **\$143,650**
- 2. Information Disclosure — **\$131,300**
- 3. Improper Access Control - Generic — **\$99,550**
- 4. XSS — **\$60,625**
- 5. Code Injection — **\$60,250**
- 6. Improper Authentication - Generic — **\$36,300**
- 7. Privilege Escalation — **\$34,400**
- 8. SQL Injection — **\$27,550**
- 9. Cleartext Storage of Sensitive Information — **\$20,200**
- 10. Insecure Storage of Sensitive Information — **\$12,000**

Computer Software

- 1. Improper Access Control - Generic — **\$1,784,833**
- 2. Information Disclosure — **\$1,229,207**
- 3. XSS — **\$804,991**
- 4. Privilege Escalation — **\$715,417**
- 5. Code Injection — **\$414,719**
- 6. Insecure Direct Object Reference (IDOR) — **\$379,736**
- 7. Improper Authentication - Generic — **\$373,043**
- 8. SQL Injection — **\$328,072**
- 9. Server-Side Request Forgery (SSRF) — **\$244,203**
- 10. Improper Authorization — **\$230,301**

Crypto & Blockchain

- 1. Improper Authentication - Generic — **\$183,436**
- 2. Improper Access Control - Generic — **\$51,434**
- 3. Business Logic Errors — **\$47,285**
- 4. Information Disclosure — **\$41,589**
- 5. Privilege Escalation — **\$38,026**
- 6. XSS — **\$34,945**
- 7. Denial of Service — **\$26,384**
- 8. SQL Injection — **\$16,500**
- 9. Deserialization of Untrusted Data — **\$15,500**
- 10. External Control of Critical State Data — **\$15,000**



TOP 10 VULNERABILITIES

Check out what the Top 10 Vulnerabilities are in your industry.

Financial Services

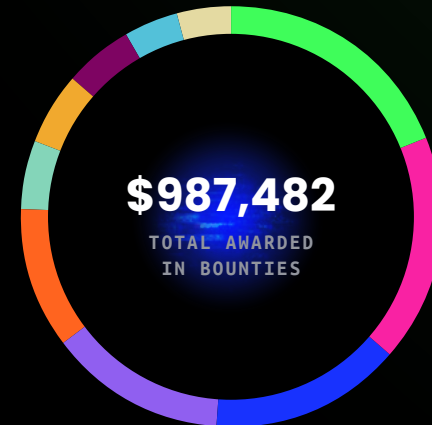
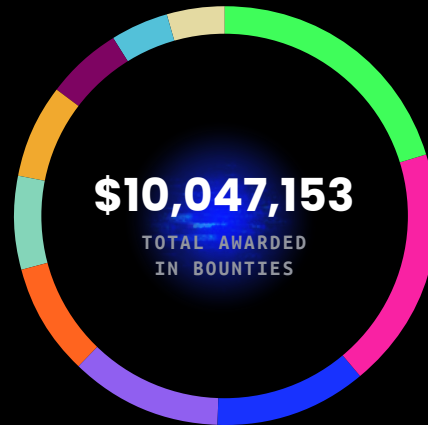
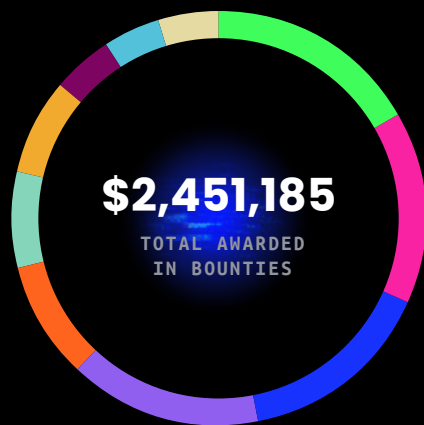
- 1. XSS — \$272,512
- 2. Improper Access Control - Generic — \$253,795
- 3. Information Disclosure — \$253,145
- 4. Insecure Direct Object Reference (IDOR) — \$234,354
- 5. Privilege Escalation — \$155,760
- 6. Improper Authentication - Generic — \$121,510
- 7. SQL Injection — \$118,350
- 8. Code Injection — \$79,410
- 9. Server-Side Request Forgery (SSRF) — \$78,799
- 10. Path Traversal — \$67,305

Internet and Online Services

- 1. XSS — \$2,046,524
- 2. Information Disclosure — \$1,898,726
- 3. Improper Access Control - Generic — \$1,195,146
- 4. Insecure Direct Object Reference (IDOR) — \$1,159,047
- 5. Server-Side Request Forgery (SSRF) — \$828,735
- 6. Privilege Escalation — \$794,498
- 7. Code Injection — \$696,400
- 8. Improper Authentication - Generic — \$641,687
- 9. SQL Injection — \$407,550
- 10. Incorrect Authorization — \$378,840

Retail & eCommerce

- 1. XSS — \$136,824
- 2. Insecure Direct Object Reference (IDOR) — \$125,765
- 3. Information Disclosure — \$104,445
- 4. Improper Access Control - Generic — \$95,955
- 5. SQL Injection — \$75,010
- 6. Misconfiguration — \$39,900
- 7. Improper Authentication - Generic — \$38,760
- 8. Business Logic Errors — \$36,131
- 9. Privilege Escalation — \$34,020
- 10. Code Injection — \$30,600



TOP 10 VULNERABILITIES

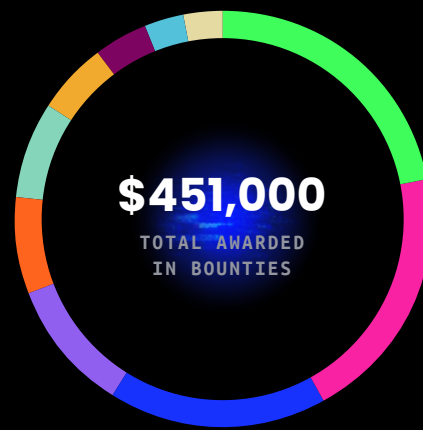
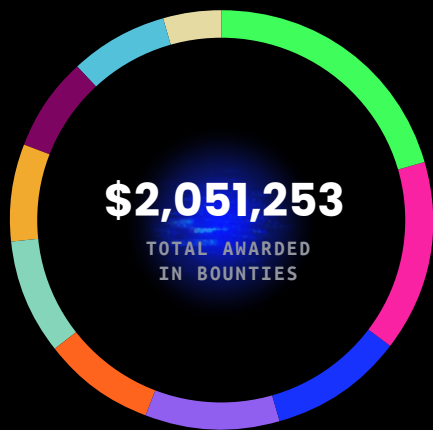
Check out what the Top 10 Vulnerabilities are in your industry.

Telecoms

- 1. Improper Authentication - Generic — **\$284,573**
- 2. XSS — **\$207,192**
- 3. Information Disclosure — **\$142,792**
- 4. Privilege Escalation — **\$141,955**
- 5. Authentication Bypass Using Alt. Path — **\$133,000**
- 6. SQL Injection — **\$122,294**
- 7. Improper Access Control - Generic — **\$109,041**
- 8. Improper Authorization — **\$95,150**
- 9. Insecure Direct Object Reference (IDOR) — **\$93,860**
- 10. Incorrect Authorization — **\$67,250**

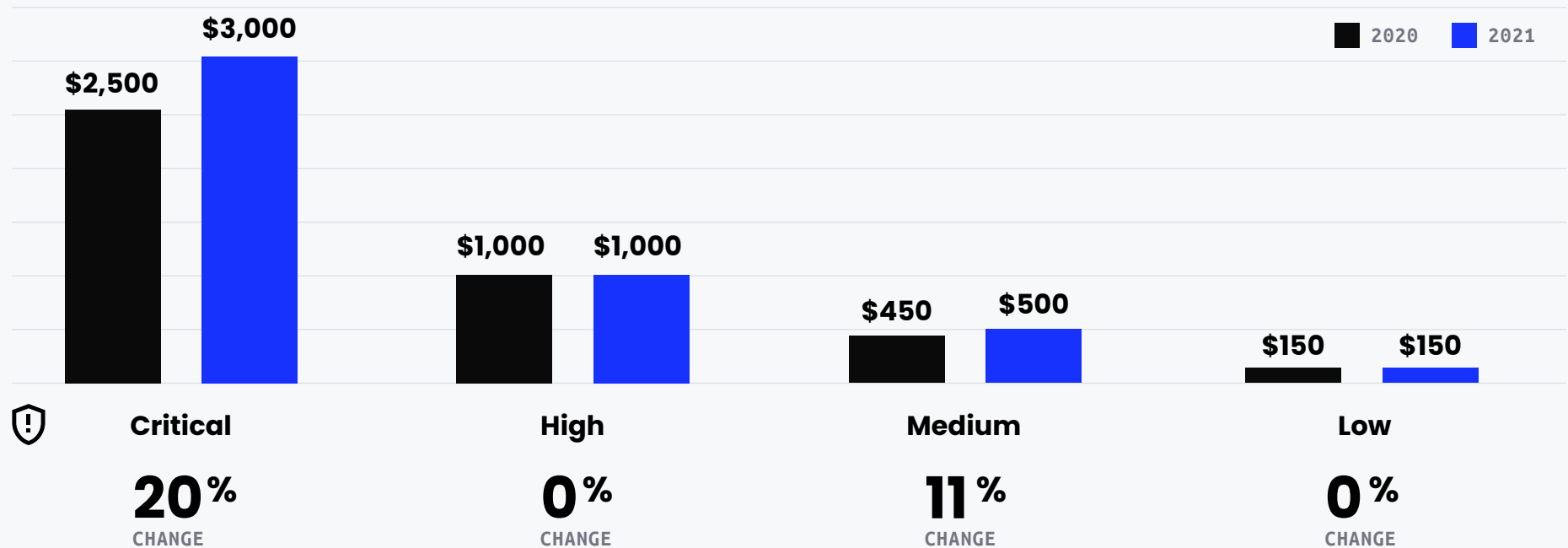
Government

- 1. XSS — **\$80,800**
- 2. Insecure Direct Object Reference (IDOR) — **\$73,950**
- 3. Server-Side Request Forgery (SSRF) — **\$61,400**
- 4. Information Disclosure — **\$38,050**
- 5. Improper Authentication - Generic — **\$28,050**
- 6. Improper Access Control - Generic — **\$26,825**
- 7. XML External Entities (XXE) — **\$20,425**
- 8. Path Traversal — **\$16,050**
- 9. SQL Injection — **\$10,900**
- 10. Denial of Service — **\$10,500**



How much can you expect to pay for a bug? The median price of a critical bug rose from \$2500 in 2020 to **\$3000 in 2021**.

3,000
MEDIAN BOUNTY PRICE



Prices for medium and lower-impact bugs are falling. This suggests focus is shifting to high-value findings, as organizations rely on hackers to find the vulnerabilities that traditional scanning solutions miss.

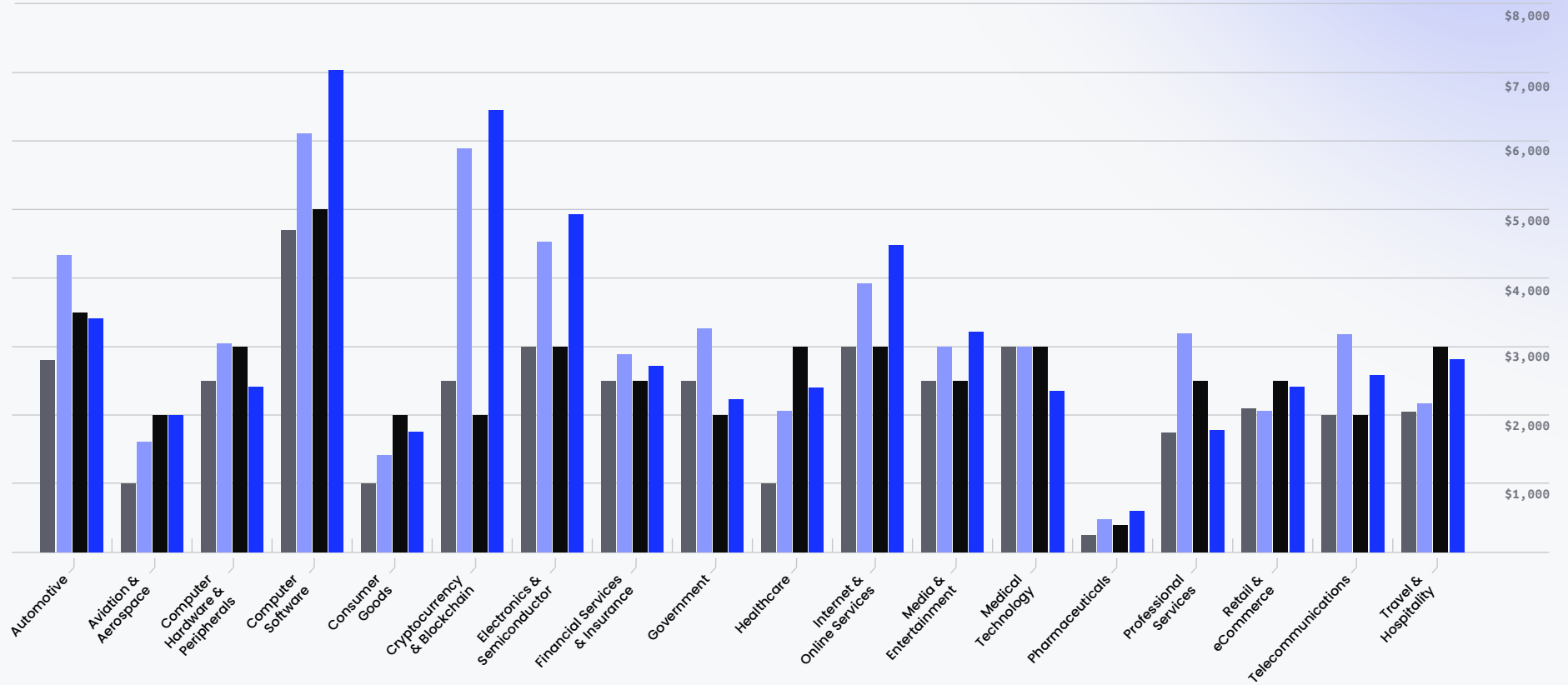
- The top tier of hackers are in high demand as organizations trust them to find bugs with the most severe impact, or to have the creativity to chain multiple low-severity bugs into one finding. The primary way customer programs bid for the time and effort of these top-tier hackers is to increase the reward for the highest-impact bugs.
- Medium and low-severity bugs are much easier to find, and typically don't represent the same risk to organizations as critical or high severity vulnerabilities. Therefore, there's less need for customers to bid higher rewards for them.



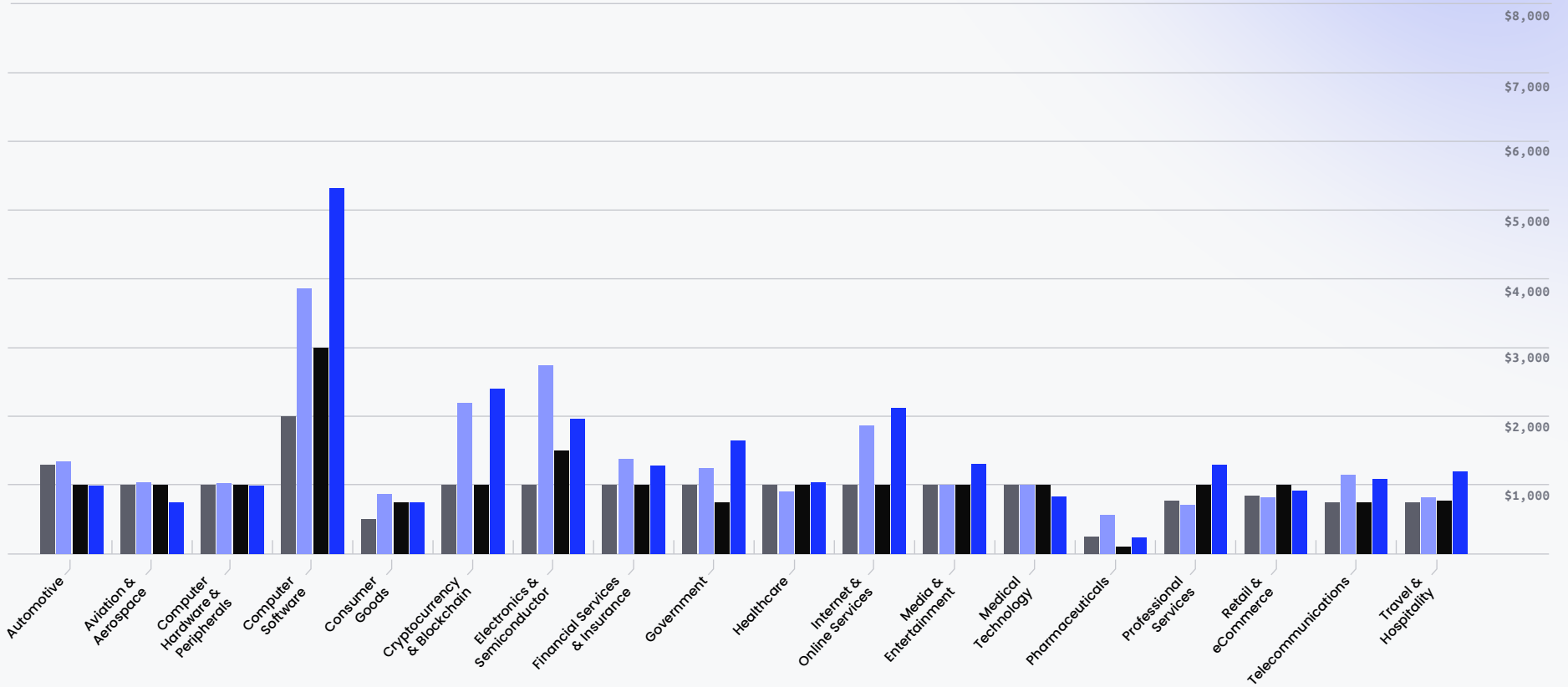
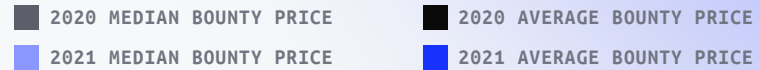
Check out the median and average bounty price in your industry



■ 2020 MEDIAN BOUNTY PRICE ■ 2020 AVERAGE BOUNTY PRICE
■ 2021 MEDIAN BOUNTY PRICE ■ 2021 AVERAGE BOUNTY PRICE



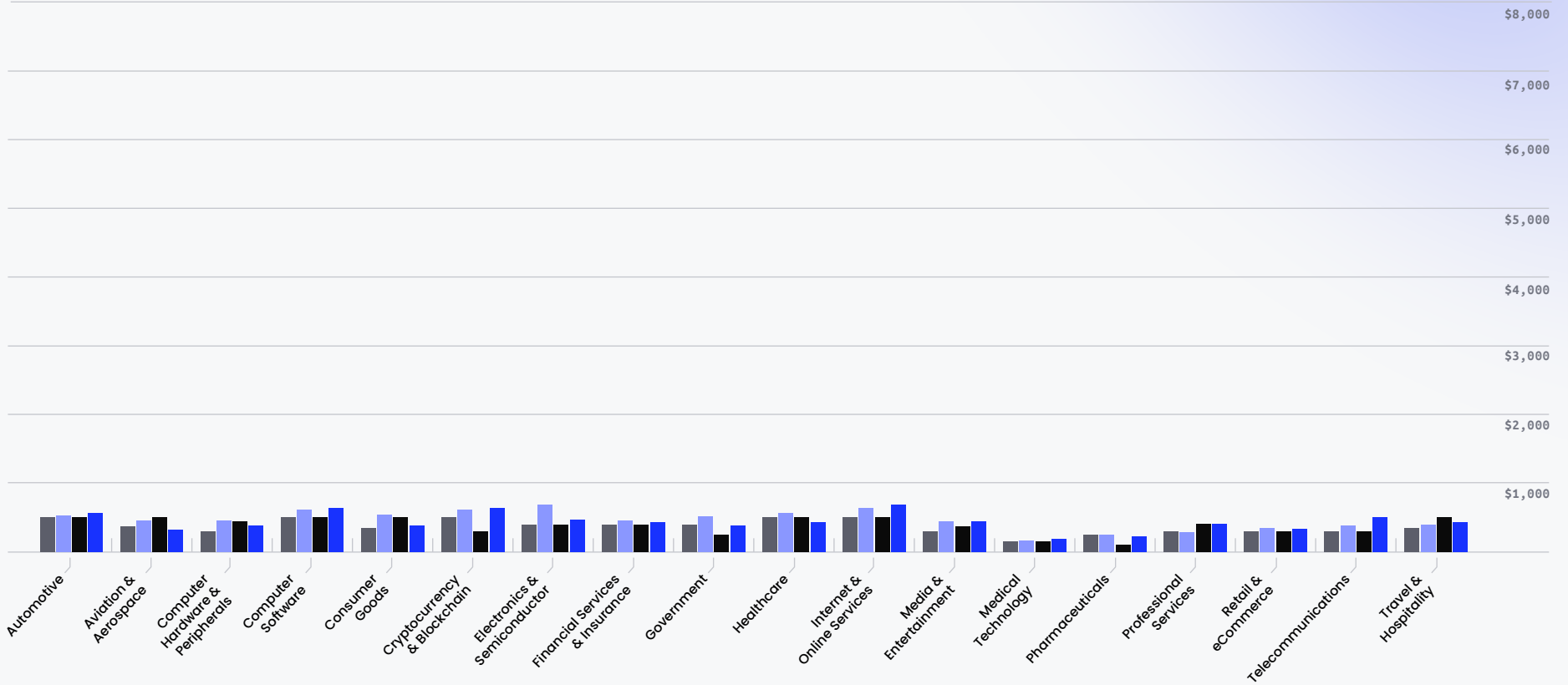
Check out the median and average bounty price in your industry



Check out the median and average bounty price in your industry

Medium

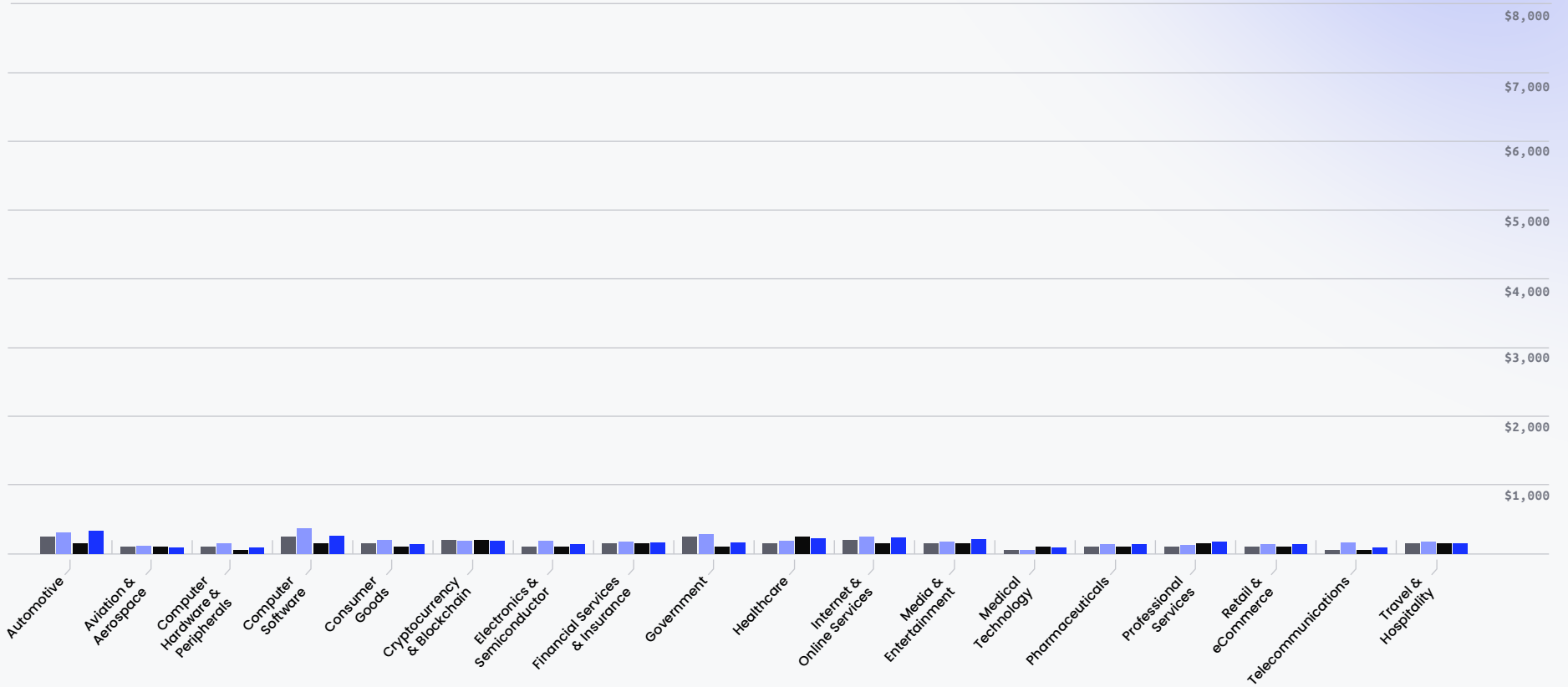
■ 2020 MEDIAN BOUNTY PRICE ■ 2020 AVERAGE BOUNTY PRICE
■ 2021 MEDIAN BOUNTY PRICE ■ 2021 AVERAGE BOUNTY PRICE



Check out the median and average bounty price in your industry



2020 MEDIAN BOUNTY PRICE 2020 AVERAGE BOUNTY PRICE
2021 MEDIAN BOUNTY PRICE 2021 AVERAGE BOUNTY PRICE



Speed is cited as a key measurement in showing how effectively security teams stay on top of threats.

In the past year, the industry-wide median time to resolution fell by 19% from 33 days to 26.7, with some industries such as retail and e-commerce seeing time-to-remediation dropping by more than 50%. This is due to a number of factors. First, we're seeing better governance models across the industries, with CISOs having increased authority and power to take action.

Customers are focusing their investments in tooling and staff to provide greater insight into vulnerability management and to improve time-to-remediation. Finally, with high-profile ransomware attacks demonstrating an existential threat, there has been increased attention on vulnerability management practices.

19%

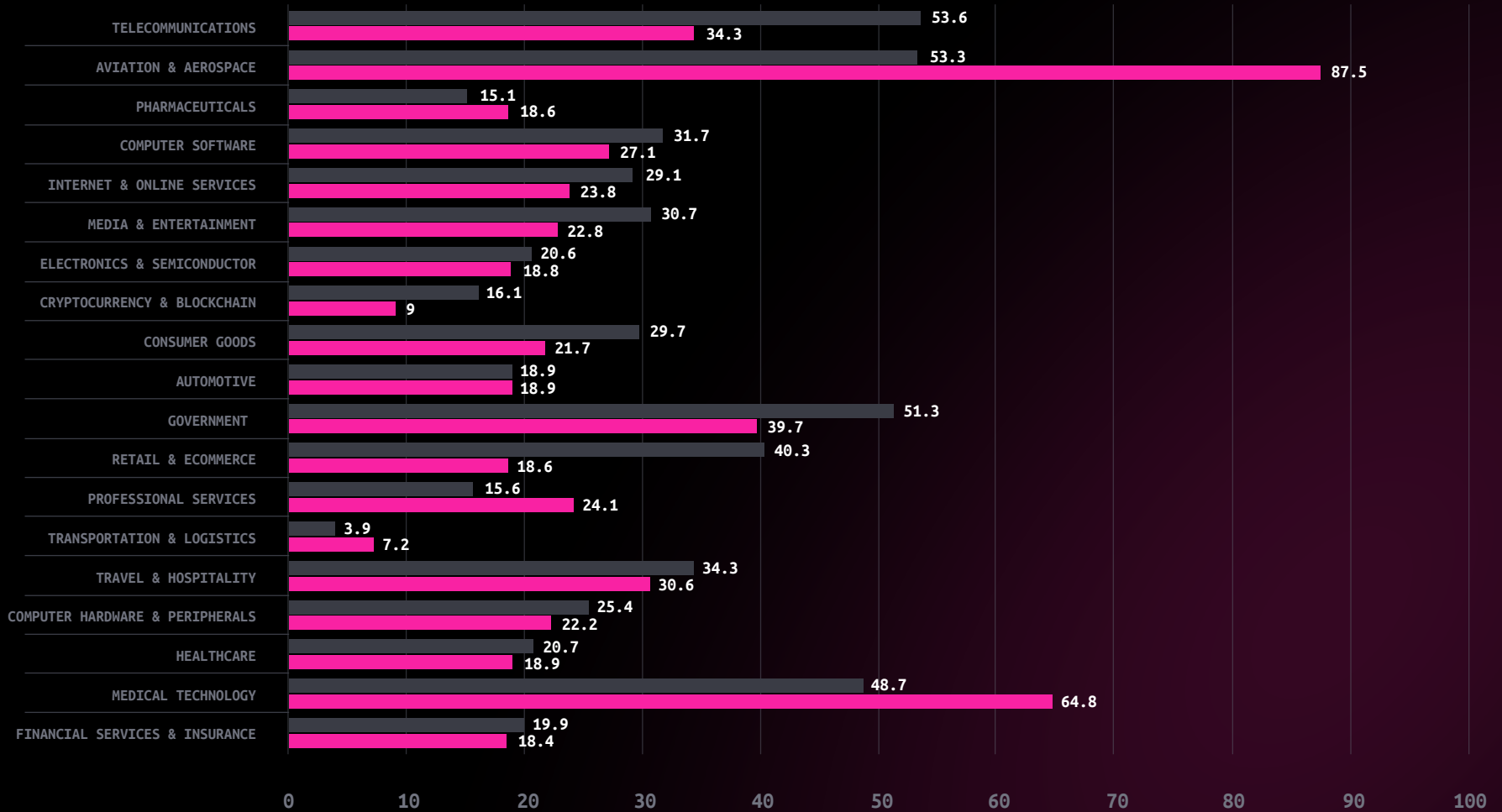
AVERAGE DROP IN
RESPONSE TIME

26.7 days

AVERAGE TIME
TO RESOLUTION

Average Days to Remediation

■ 2020 MEDIAN TIME TO REMEDIATE (BUSINESS DAYS)
 ■ 2021 MEDIAN TIME TO REMEDIATE (BUSINESS DAYS)



Hacker-powered security has gone beyond simply paying a hacker for a bug they found on a one-off basis.

Today's leading CISOs and security teams are leveraging the skills and expertise of a professional, committed community of hackers as a core piece of their overall security testing strategy. The data and vulnerability insights organizations gain from their bug bounty, VDPs, and pentests are enabling them to better identify where problems are originating and where resources and training need to be directed.

Knowing what vulnerabilities your peers are prioritizing, how they're fixing them, and what value they ascribe them, can help you build or enhance your own security testing program.



hackerone

**For more information
on what hackers can do
for your organization,
contact HackerOne.**

[Contact HackerOne](#)

hackerone

www.hackerone.com / sales@hackerone.com