INDUSTRY REPORT

THE ADOPTION OF BUG BOUNTIES IN THE FINANCIAL SERVICES INDUSTRY

Bug bounties are fundamentally changing the way financial service organizations approach the security of the Internet—moving from the realm of novelty towards becoming best practice. While they have been used for over 20 years, widespread adoption by enterprise organizations has just begun to take off within the last few. Private and public bug bounty programs provide an opportunity to level the cybersecurity playing field—by arming complex organizations with the strength and expertise to combat constant external threats.

Within this financial services spotlight, we present how the financial services industry is now looking to bug bounty programs to augment their existing application security testing programs and better protect their customers. We also present real statistics that illustrate why financial organizations utilize bug bounty programs and the results of those programs.

This case study report also offers a perspective on how organizations have successfully implemented bug bounty programs, and some of the key factors to evaluate if your organization is considering a bug bounty program.

THE CURRENT STATE OF BUG BOUNTIES

Read our annual State of Bug Bounty Report to learn more about the current state of bug bounty programs.

This report delivers insights into the organizations running bug bounty programs, the hackers competing for their rewards, and the vulnerabilities being discovered.

Download the report >

bugcrowd

The Financial Services Industry Looks to the Crowd

As financial services organizations continue developing, deploying and managing highly-connected and distributed products, combating external threats continues to be a major challenge for several reasons:

- As attack surfaces become more complex, attackers are upping their intensity and resourcefulness to capitalize on security vulnerabilities.
- Hiring and training internal resources is more and more difficult as the cybersecurity job deficiency grows.
- Traditional security methods are falling short, as proof of major data breaches amongst financial services and banking companies in the past few years.

APPSEC SPENDING TRENDS

According to a study performed by SANS, companies within the financial services industry are set to spend up to $1M annually on IT, with 10-12% budgeted for information security programs.

Additionally, SANS showed that over 30% of the respondents claimed design and development as a key information security investment area. Thus it comes as no surprise that organizations are beginning to spend money on outsourced application security.

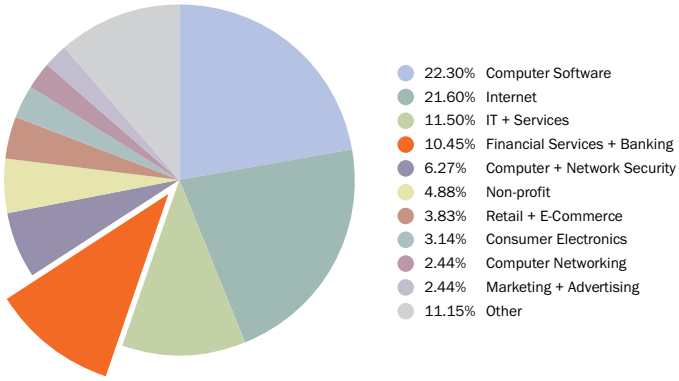
BUG BOUNTY TRENDS IN THE FINANCIAL SERVICES SECTOR

Bug bounty programs present financial services companies with the opportunity to address the aforementioned challenges of increasingly complex attack surfaces, resource scarcity and the need for improved testing methods. Financial service organizations are adopting crowdsourced cybersecurity programs more and more in order to strengthen the security of their products while cultivating a mutually-rewarding relationship with the security researcher community.

Out of nearly 300 public and private programs launched in the past three years, Bugcrowd has run bug bounty programs for organizations from nearly every industry.

Financial Services makes up the fourth largest portion of those programs at 11%. Learn more in our State of Bug Bounty Report.

This segment is among the first of more 'traditional' industries to adopt bug bounties and is among the fastest growing industries in the bounty space. The number of programs started by financial services organizations in 2015 has nearly doubled since 2014, with 400% growth since 2013.

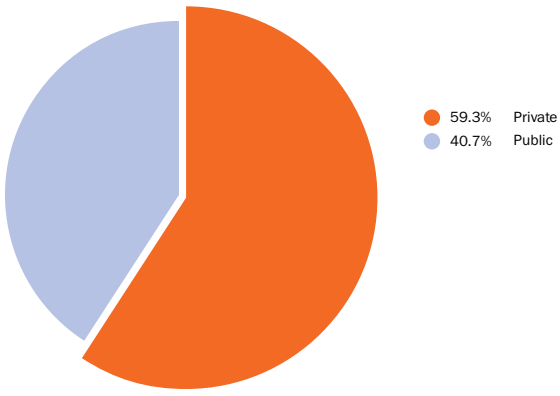


BUG BOUNTY SOLUTIONS FOR FINANCIAL SERVICES

Bugcrowd supports both public programs and private programs. Private programs include both on-demand and ongoing programs in which researchers must be invited to participate. Researchers that are invited to private programs are measured on four metrics: accuracy, impact, activity and trust.

Of all programs started by financial services organizations, 59.3% of all programs launched were private. Private programs are popular amongst financial services organizations for the following reasons:

- Organizations looking to access the benefits of crowdsourcing with PII, complex technologies or environments benefit from a gated testing pool.
- These organizations pay higher bounties to attract and maintain interest from the top researcher talent.
- Financial services organizations utilize on-demand crowdsourced security testing to fulfill compliance obligations.
- In recent years, more organizations looking to start a public bug bounty program begin privately while they build their response capabilities and processes.



Why Are Financial Services Organizations Leveraging the Crowd?

In a recent Bugcrowd survey of financial service organizations, the top two areas of value that were pointed out were 1) the varied and unique skill sets and expertise of hackers and 2) paying for valid results.

THE DIVERSITY AND POWER OF THE CROWD

As of July 31, 2016, over **35,000 researchers** have signed up on the **Bugcrowd platform** with rapid community growth quarter over quarter. In addition to volume, however, the strength in the Bugcrowd community lies within its diversity in background, perspective and skill sets. They differ in demographics–age, education level, geographic region–as well as what their expertises and motivations are.

112

COUNTRIES REPRESENTED

Bugcrowd researchers hail from 112 different countries; with the vast majority of researcher, sign ups are from India (28.2%) and the United States (24.4%), followed by the United Kingdom (3.9%), Pakistan (3.5%) and Australia (2.4%). Activity and quality vary by region.

88%

HAVE 1+ YEAR OF COLLEGE

In a recent survey, 88% of researchers have at least one year of college under their belts, and all respondents had at least a high school degree. Additionally, 75% responded as being between the ages of 18 and 29 followed by the second largest group, aged 30 to 44, (19%).

15+

AREAS OF EXPERTISE

When asked which technologies they had intermediate to advanced skill in, 95% of respondents of our aforementioned survey felt they had intermediate or advanced knowledge of web application testing, 48% in Android, 28% in iOS and 15% in IoT.

Researchers are motivated by a range of incentives, extrinsic and intrinsic, from prestige or profit to philanthropy or professional development. As the community grows and we learn more about it, we leverage these motivations to assist this flourishing marketplace better. This community will be forever evolving and growing, and we will continue to analyze and report on the state of bug hunters and the security research economy. Look out for our upcoming report on the Bugcrowd community.

PAYING FOR VALID RESULTS

Bug bounties are often compared to traditional application security assessment methods. The most prominent advantages of bug bounty programs are the volume of testers involved, and the advantageous reward model. Bug bounties utilize a large quantity of researchers, as opposed to a select few penetration testers, and a pay-for-results reward model rather than for effort.

Bounty payout volume and average bug cost are correlated to the overall health of programs and the severity of vulnerabilities submitted. As the bug bounty space has matured, we have begun to standardize the market rate of security bugs based on organizational security maturity and criticality level. The financial services sector has exhibited favorable trends on this front:

- Over 12% of total bounty payouts have been made by financial services programs, accounting for more than the number of all Bugcrowd programs launched
- All time, the average payout per bug across financial services programs is $323.05, nearly 10% more than the average across all programs.

DEFENSIVE VULNERABILITY PRICING MODEL

According to our Defensive Vulnerability Pricing Model (DVPM), a P4 submitted to an organization on the 'basic' end of the security maturity scale should be rewarded $100, while a P1 submitted to an organization on the 'advanced' end of the security maturity scale should be rewarded $15,000.

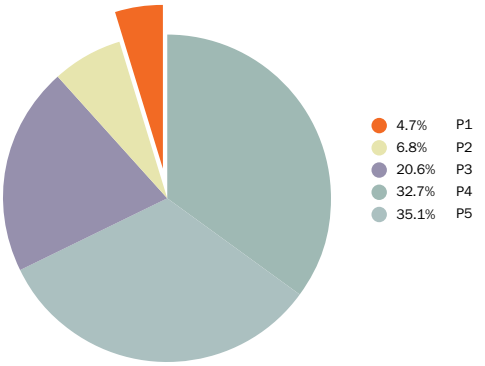
Read the full guide >

Results: Do Bug Bounty Programs Work for Financial Services?

To measure the success of the bug bounty programs, we utilize a few key performance indicators, including 1) vulnerability criticality and 2) bug classification.

AVERAGE VULNERABILITY CRITICALITY

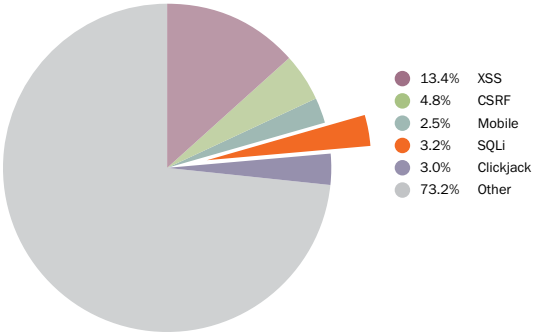
The criticality scale for a submission ranges from Priority 1 (P1) to Priority 5 (P5), 1 being the most critical, 5 being the least critical. This scale provides researchers and organizations a baseline for prioritization of a fix and potential reward amount. Our Vulnerability Rating Taxonomy reviews the priority of vulnerabilities by type.



Across programs run by financial services organizations, 4.7% of all valid submissions are classified by the organization as P1 submissions, the most critical vulnerabilities. This value is 167% more than the number of P1 submissions submitted across all other programs.

BUG CLASSIFICATION

Bug bounty programs receive many of the common bugs listed in top-ten lists such as OWASP top ten, with Cross-Site Scripting (XSS) and Cross-Site Request Forgery (CSRF) topping our charts. In addition to these vulnerabilities, bug bounty programs frequently find unique vulnerabilities, which accounts for the large unclassified category of submissions.



The types of bugs found in financial services programs are more varied, with a bigger 'other' category than represented across all programs. Additionally, these programs find 53% fewer XSS bugs and 43% more SQLi bugs.

Considerations For Financial Services Organizations

Running a bug bounty program can seem difficult to launch, resource intensive, and even scary. We support our customers from discovery and program scoping to program execution and iteration to overcome some common considerations:

- **Internal buy-in:** As bug bounties become more commonplace, the perceived risk of running them has decreased, making it easier to implement them quickly and realize long term success.
- **Resources:** Bug bounty programs can be hard and expensive. Bugcrowd makes them easy by delivering only valid, actionable results, providing a secure vulnerability disclosure platform, and facilitating seamless communication with researchers.
- **Unknown Results:** From guiding our customers through setting up bounty briefs to regulating researcher engagement and activity, Bugcrowd mitigates this concern by ensuring all programs launch seamlessly, run smoothly and provide actionable results.

Bugcrowd's solutions provide customers with the combination of a robust platform and comprehensive support from a team of experts, making running a bug bounty easy, efficient, and valuable. Here are a few of those customers in the financial services industry...

THE WESTERN UNION BUG BOUNTY

LAUNCHING A PRIVATE BUG BOUNTY PROGRAM:

As one of the oldest financial institutions in the United States, servicing 144 countries and transferring millions of dollars daily, Western Union has a robust security portfolio across many departments and applications. After recognizing the need for a channel to connect with the security researcher community to find critical vulnerabilities quicker and more efficiently, the company launched its private bug bounty program with Bugcrowd in 2014.

"A bug bounty program really provides an additional layer to help protect our customers." - David Levin, Western Union

MOVING TO A PUBLIC PROGRAM:

On March 11, 2015, Western Union expanded that program, launching the first-ever bug bounty program for a publicly-traded financial institution. The continuous testing from Bugcrowd's community of thousands of security researchers provides the Western Union team with valuable vulnerabilities on a large scale. By leveraging the management and triage services provided by Bugcrowd, the Western Union security and development teams can focus on implementing fixes quickly and seamlessly.

"It really puts things in perspective when you have a channel to collect this information and when you have a partner like Bugcrowd you really reduce some of those false positives and noise." - David Levin, Western Union

WESTERN UNION

BOUNTY PROGRAM DETAILS

Scope: Western Union web properties
Rewards: $100 to $5,000
Requires explicit permission to disclose the results of a submission

BOUNTY PROGRAM ACTIVITY

2,000+ submissions
600+ submitting researchers
800+ valid bugs
80+ critical bugs

Western Union's program page is available here.

Getting the Most from Your Bug Bounty Program

Financial services organizations are successfully utilizing bug bounty programs to augment their existing solutions and securing their products. These statistics illustrate why financial services organizations use bug bounty programs, how financial services organizations have successfully implemented and deployed bug bounty programs, and the impactful results of those programs.

ADDITIONAL RESOURCES:

- For more detailed information on the latest vulnerability trends in bug bounties, be sure to check out our 2016 State of Bug Bounty Report.
- Learn more about the A to Z process of setting up running, iterating and learning from your program, download our Lifecycle of Bug Bounties Infographic.
- For a comprehensive guide to writing your bounty brief, download our Anatomy of a Bounty Brief.