bugcrowd

2018 STATE OF BUG BOUNTY

Bugcrowd's fourth annual report on the global crowdsourced security economy

VULNERABILITY EDITION

Table of Contents

Motivation

WannaCry, Petya, NotPetya, Meltdown, the Equifax Apache Struts bug — these are just a few examples of exploited vulnerabilities that hit headlines this past year, leaving many systems, users and companies devastated.

The global security threat outlook evolves with each coming year. There is a growing number of ways known vulnerabilities can be exploited to damage businesses and individuals. Attackers take advantage of different vulnerabilities for different reasons depending on the business model. And that is just accounting for the known vulnerabilities. But what about the unknown vulnerabilities?

Cyber attackers are always at play. The biggest difference between an unknown vulnerability and a known vulnerability, is the ability to take action on it. And depending on who gets ahold of the information first, you're either celebrating with a glass of champagne or cleaning up a PR nightmare. Because once a vulnerability is publicly known, the clock starts ticking, and it's just a matter of time until it hits users.

Defenders continuously face the challenge of making remediation decisions around vulnerabilities without access to all of the facts. For example, it may be difficult to find the exploits that actually impact your business, in an official vulnerability databases or even a vulnerability scanner. There's simply too much information out there.

Executive Summary

In the last few years, we've witnessed continued increase in the number of vulnerabilities. At the same time, CISOs are in a crisis for resources. **By 2020, there will be an estimated 1.5 million unfulfilled security positions.**

To stay ahead of these adversaries, organizations are depending more and more on the crowdsourced security model to bring light to the vast number of emerging vulnerabilities unknown to most scanners -- helping companies realize their own vulnerabilities before the bad guys do. Bug bounty and vulnerability disclosure programs have the ability to bring together tens of thousands of the brightest minds in security research, to uncover seven times more high priority vulnerabilities than traditional assessment methods. The growing number of organizations across industries adopting bug bounty and vulnerability disclosure programs in the past year has made it clear that the crowdsourced security model is here to stay.

In its fourth iteration, the **Bugcrowd State of Bug Bounty Report** provides an unparalleled, inside look into the trends in crowdsourced security, and for the first time, a deep dive into the most common and emerging vulnerabilities found over the past year.

Methodology

The Bugcrowd State of Bug Bounty Report analyzes proprietary platform data, collected from more than 700 managed crowdsourced security programs, segmenting for statistics around adoption, economics, the researcher community or The Crowd and vulnerabilities.

The data includes all Bugcrowd platform data from April 1, 2017 through March 31, 2018.

Key Findings

We've seen an overall increase of 40% in all programs launched during the past year. With 33% increase in private programs, 79% of all program launches last year were private.

In the past year, **the Crowd has grown by 71%**, represented by more than 100 countries around the world.

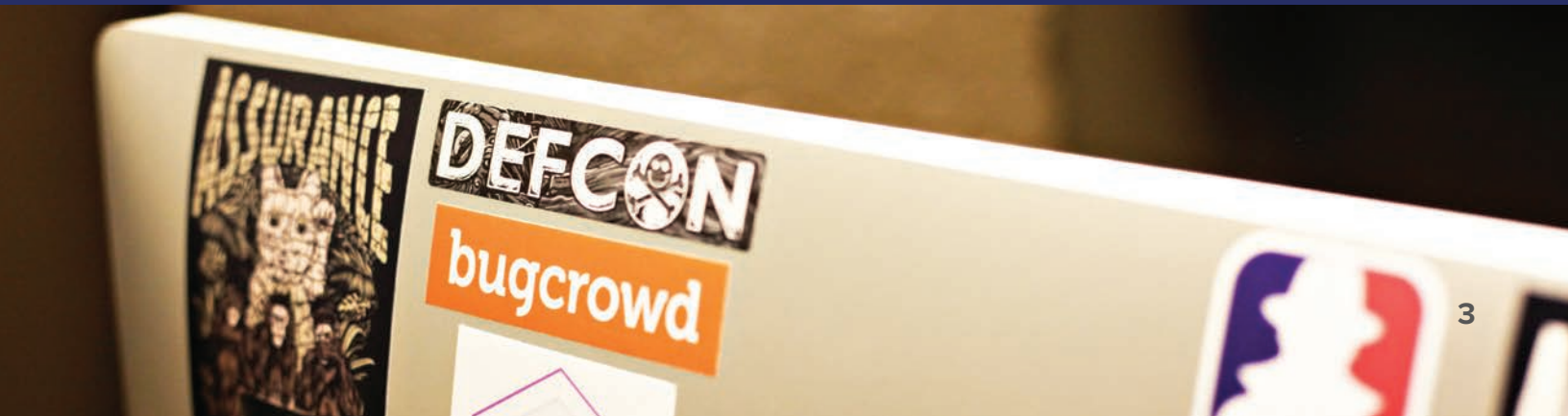
The average payout per vulnerability is $781, a 73% increase over last year. **75%** of all **P1** vulnerability payouts were above **$1,200**, up from **$926** last year.

The majority, **13% of all submissions paid out** last year were for vulnerabilities classified as **Cross-Site Scripting (XSS) Stored**.

The total number of vulnerabilities submitted via Crowdcontrol™ increased **21% from last year.**

The majority, **31% of total valid submissions** were classified as **P3 severity**, **26%** were classified as **P4**, **16.3%** were classified as **P5** and **13%** were **P2**. Just **7% of total valid vulnerabilities** were **P1 severity.** (6% were classified as "other")

Cross-Site Scripting (XSS) Reflected (P3), was the **top vulnerability submitted this year** via the Crowdcontrol™ platform.



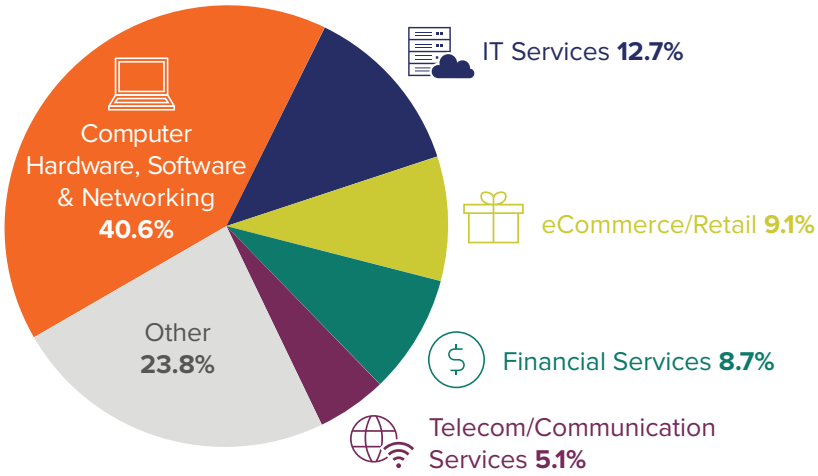
Adoption

Growth continues across industries and verticals. We've seen an overall increase of 40% in all programs launched during the past year. As the model becomes necessity, it's attracted more of the traditionally risk averse businesses that are feeling the impact of a growing attack surface and motivated adversaries.

This past year, the top 5 areas of adoption by industry are Computer Hardware, Software & Networking, IT Services, eCommerce / Retail, Financial Services, and Telecom / Communication Services.

Programs by Industry

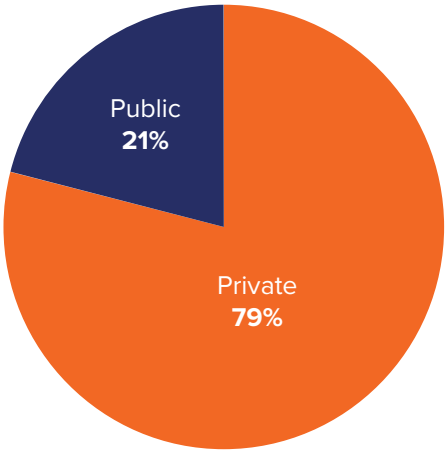
We've seen an overall increase of **40%** in all programs launched during the past year.



According to our **CISO survey**, more than 30% of CISOs plan on implementing crowdsourced security programs in the next year. With policies and standards in place such as NIST, The Department of Justice Framework, and the Data Security and Breach Notification Act, it's now incumbent on organizations to ensure they are setup to receive vulnerability data from external parties and is already becoming an adhered-to standard for major private organizations.

79% of all program launches in the last year were private. Private programs offer organizations the opportunity to utilize the power of the crowd – volume of testers, diversity of skills and methodologies – in a more controlled and stringent environment. Where public programs are open to all researchers, private programs and limited to vetted, ID verified and trusted researchers, giving companies the power to control what is tested and how it's tested.

Program Types



Private programs are a great entry point for anyone looking to start their first crowdsourced security testing program or introduce testing on a new asset — it offers significant breadth and depth of coverage without overwhelming your security and development teams.

Policies and Standards

Over the past few months, the widespread popularity and adoption of bug bounties and vulnerability disclosure has grabbed headlines. This rapid adoption paired with recent incidents like Equifax and Uber, have hastened the need to make sure things are defined clearly—specifically, the difference between a good hack versus a bad one. This has drawn the attention of the U.S. Senate and other legislative bodies, which ultimately is a good thing, important and expected.

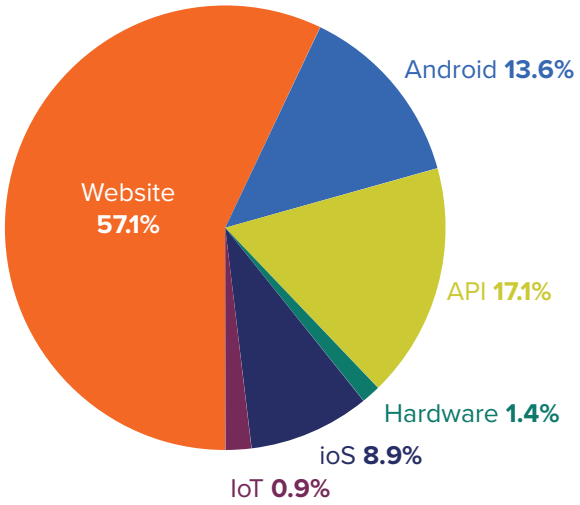
It's important to ensure the appropriate frameworks are created over time, while also working to avoid any chilling effect on the benefit that has been created by this model. Vulnerability exploitation is, like many things, a dual-use activity able to be exploited for both good and bad. Determining the intent of a hacker as good faith or malicious becomes more difficult at scale.

With the number of other policies and standards in place, it's only a matter of time before every organization has to implement VDP or bug bounty. Having a good partner will make it possible for more organizations to do this sooner, and more effectively.

“Our private bug bounty program allowed us to tap into the creativity and abilities of hundreds of researchers to find and report the most complex bugs — the ones application scanners just can’t uncover. Now we’re expanding our program for access to a bigger pool of researchers to improve our ability to find and fix vulnerabilities.”

Thibault Candebat, Information Security Manager, INTERCOM

57% of all programs launched in the past year primarily included website targets, **17%** API, **14%** Android and **9%** iOS.



Today’s Critical Attack Surfaces

Web Front-End

API

x86 Server/Cloud

Mobile

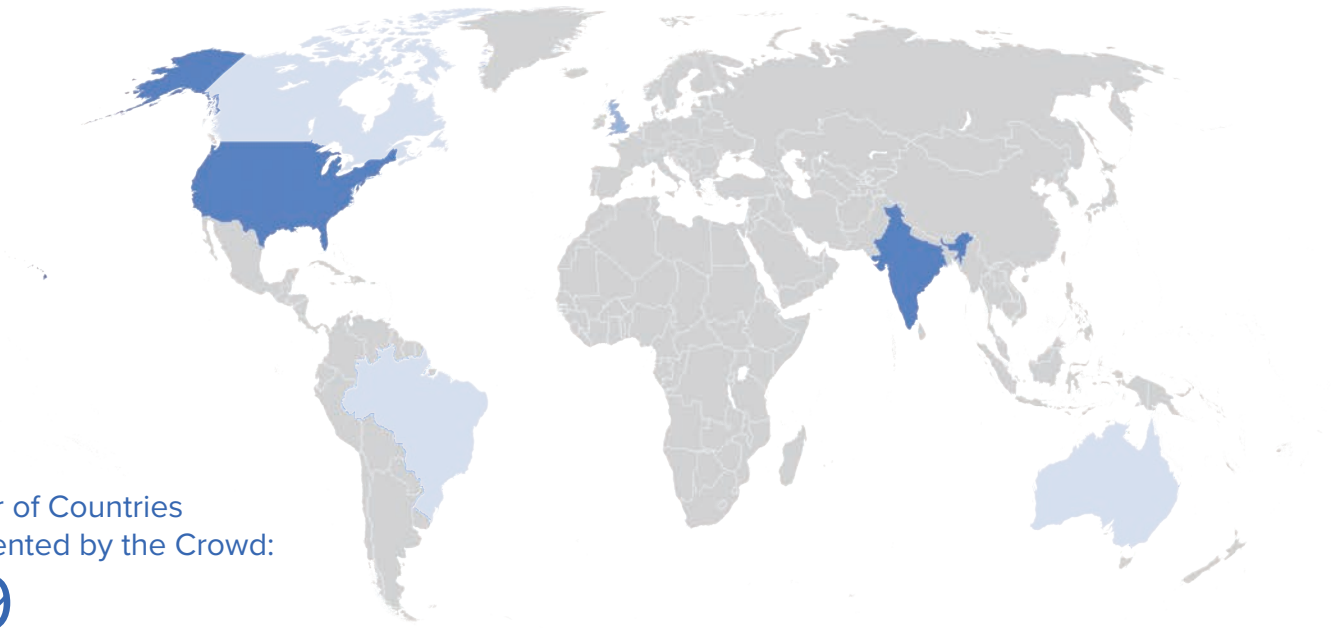
IoT

Crowdsourced Security supports today's key attack surfaces, as well as "the unknown". As organizations move to cloud architectures and applications, the biggest concerns are web application front ends and APIs, which may be deployed on IoT devices, mobile apps, or on-prem/cloud. All of these can be evaluated for risk by Crowdsourced Security. Furthermore, a public crowd program can uncover risk in areas unknown to the security organization, such as shadow IT applications or exposed perimeter interfaces.

The Crowd

Over the past year, we have continued to cultivate and invest in our security researcher community, watching it grow into the vibrant, self-educating group of talented and passionate experts that it is today. In the past year, the Crowd has grown by 71%, represented by more than 100 countries around the world.

> "We are able to extend our security team with thousands of researchers with skills and time not available to us internally. We get better results with the right, trusted researchers for our program."
>
> **Ron White, VP of Engineering, ibotta**



Number of Countries Represented by the Crowd:

109

0 1.1K

We have a crowd of more than 80K researchers, with nearly 4K unique ID verified researchers, half of which are private crowd qualified. **Growing every day, we have nearly 7K researchers who have submitted unique, valid vulnerabilities.**

According to our **Inside the Mind of the Hacker 2.0 Report**, Bugcrowd security researchers have expertise in many technologies — providing direct access to hard-to-find resources and skill sets. Bug hunters are young, ambitious, and always looking to expand their knowledge and build on their skill set through the challenge of the hunt. 71% of bug hunters are between 18-29 years old, up from 60% last year, indicating more hackers are getting an earlier start.

Our Crowd ranks "the challenge" as a top motivation. 62% reinvest earnings from bug hunting back into their craft, spending it on security tools and training. Their top skill sets include web application testing, web API assessment, network pentesting, social engineering, and source code analysis.

Economics

Across all programs and industries, the average payout per vulnerability is $781, a 73% increase over last year. We are seeing a 2X uplift in the average payout year-on-year. 75% of all P1 vulnerability payouts were above $1,200, up from $926 last year.

Who can participate in private bug bounty programs?

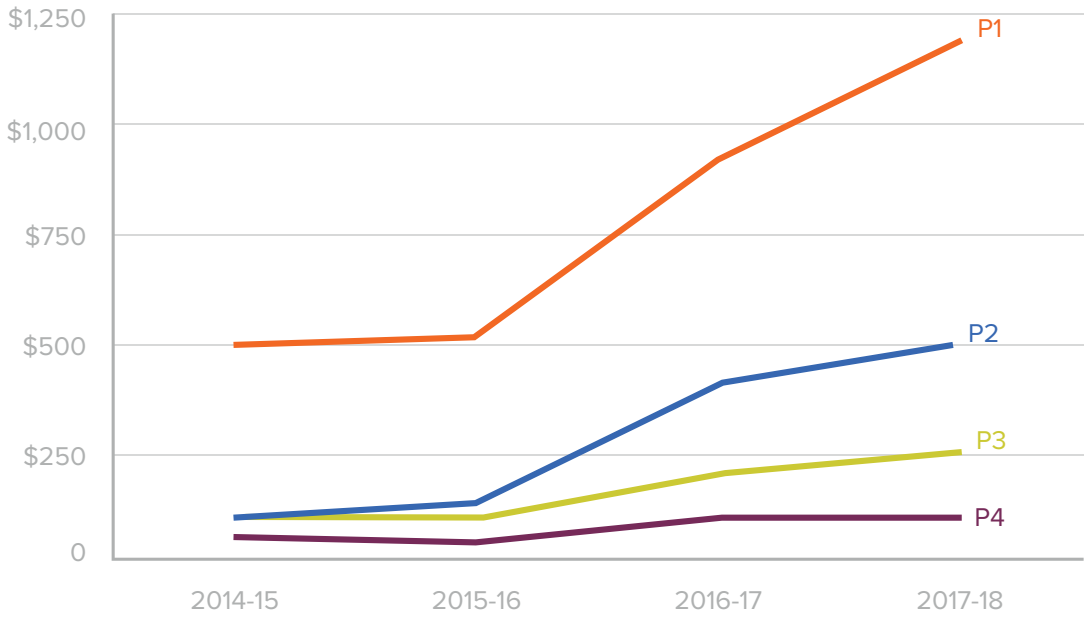
Bugcrowd has a large, skilled crowd of global security researchers coming from all walks of life, and varying degrees of experience in security research and bug hunting. Anyone can sign up to become a Bugcrowd researcher to participate in public bug bounty programs.

As a bug hunter submits bugs, climbs the ranks within the community, and proves his/her trustworthiness, they may gain access to private programs.

Bugcrowd researchers are vetted and measured in four areas — activity, quality, impact and trust.

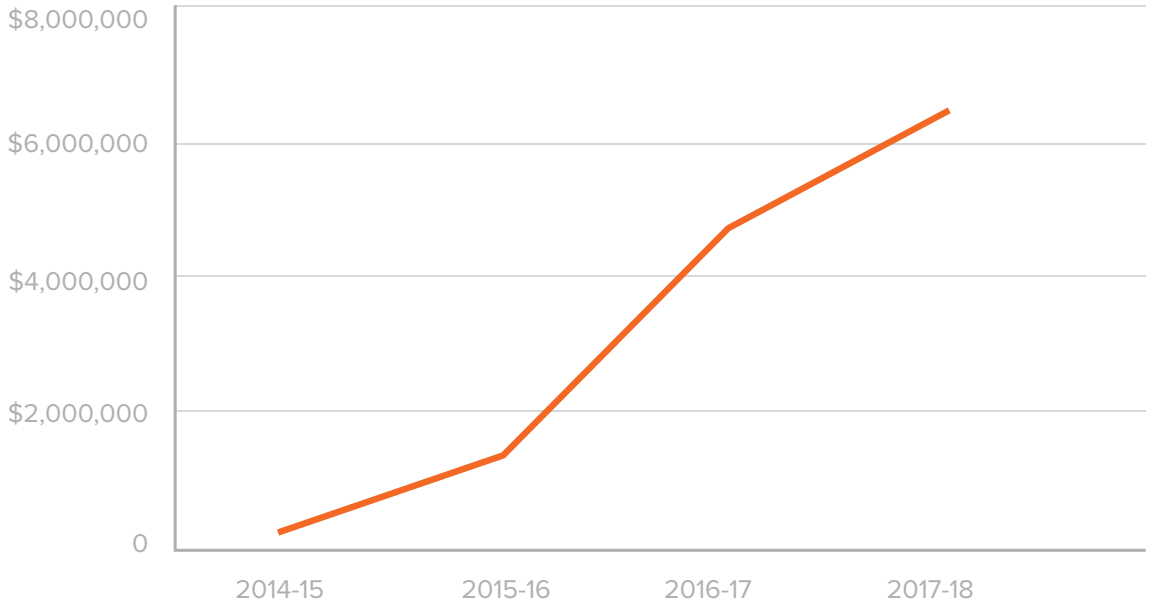
Only the top performers who have proven their skill and trustworthiness receive invitations to private programs.

75% of all **P1** vulnerability payouts were above **$1,200**, up from **$926** last year.

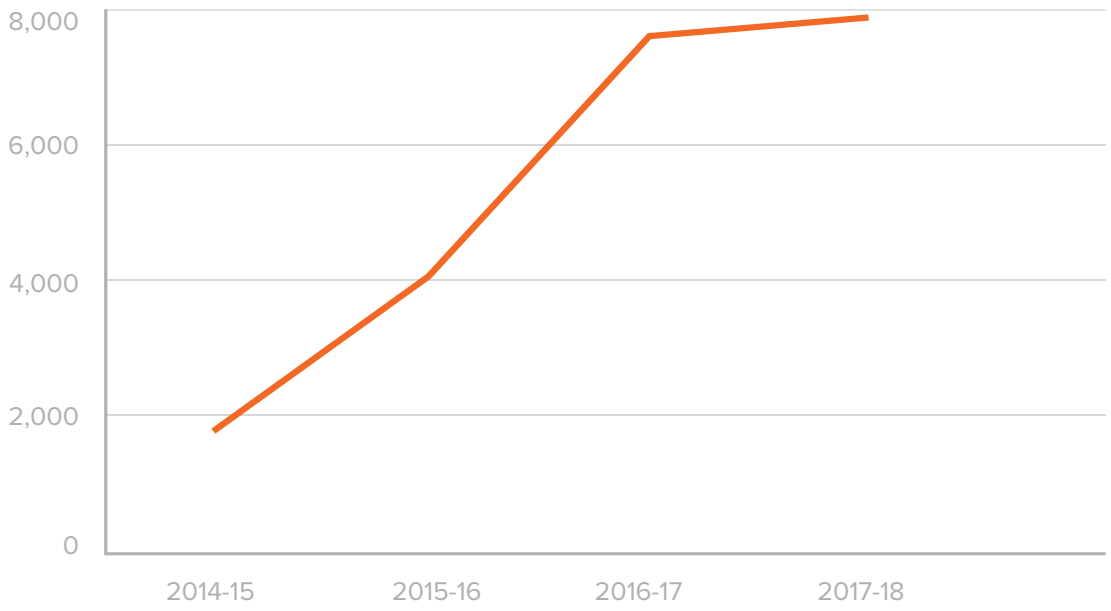


Organizations continue to add complex targets to their scope, at the same time adding more value to securing their assets via their bounty offering. The more complex a target and the more critical a vulnerability, the higher the price tag.

Our **total payouts** have increased **36%** from last year.



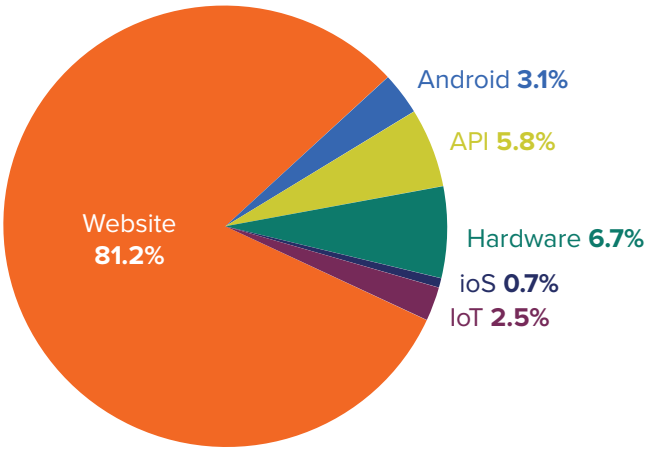
The **total number of submissions paid** has increased **4%** from last year.



The number of **researchers paid** has increased **13%** over the past year.

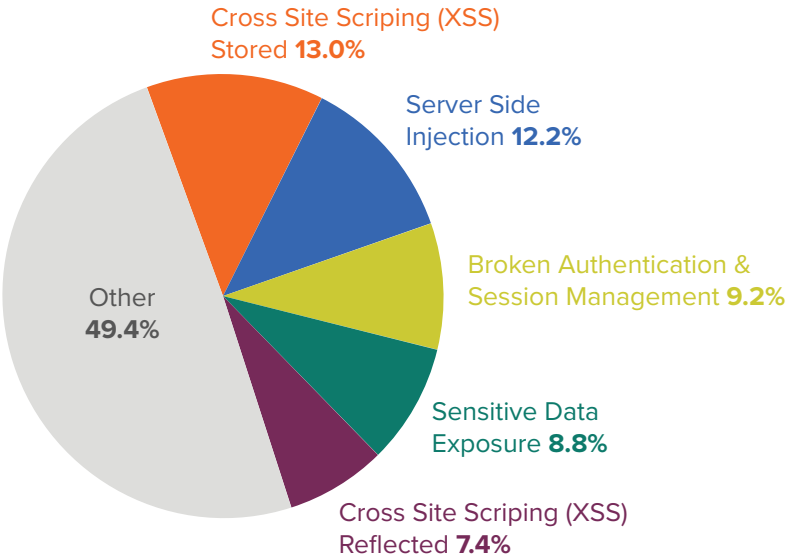
In the past year, the largest amount paid out (81%) was for vulnerabilities categorized as website. The web is still the largest attack surface out there, but others are gaining traction quickly with more user adoption and hacker sophistication. 7% was paid out for hardware and 6% was paid out for API.

Amount Paid by Target



The majority, 13% of all submissions paid out last year were for vulnerabilities classified as cross site scripting XSS stored. 12% were classified as server side injection and 9% were classified as broken authentication and session management.

Amount Paid by VRT Classification



Bugcrowd's VRT provides a resource outlining Bugcrowd's baseline priority rating P1 being the most severe and P5 being the least, including certain edge cases, for vulnerabilities that we see often. To arrive at this baseline priority, Bugcrowd's security engineers started with generally accepted industry impact and further considered the average acceptance rate, average priority, and commonly requested program-specific exclusions (based on business use cases) across all of Bugcrowd's programs. The VRT maps to both the CVSS rating system and CVE vulnerability database.

Vulnerabilities

According to the **CVE**, 2017 saw 14,713 published vulnerabilities, an increase of more than 128% from last year. For 2018, the CVE has already seen more than 5K published vulnerabilities so we should see the upward trajectory continue.

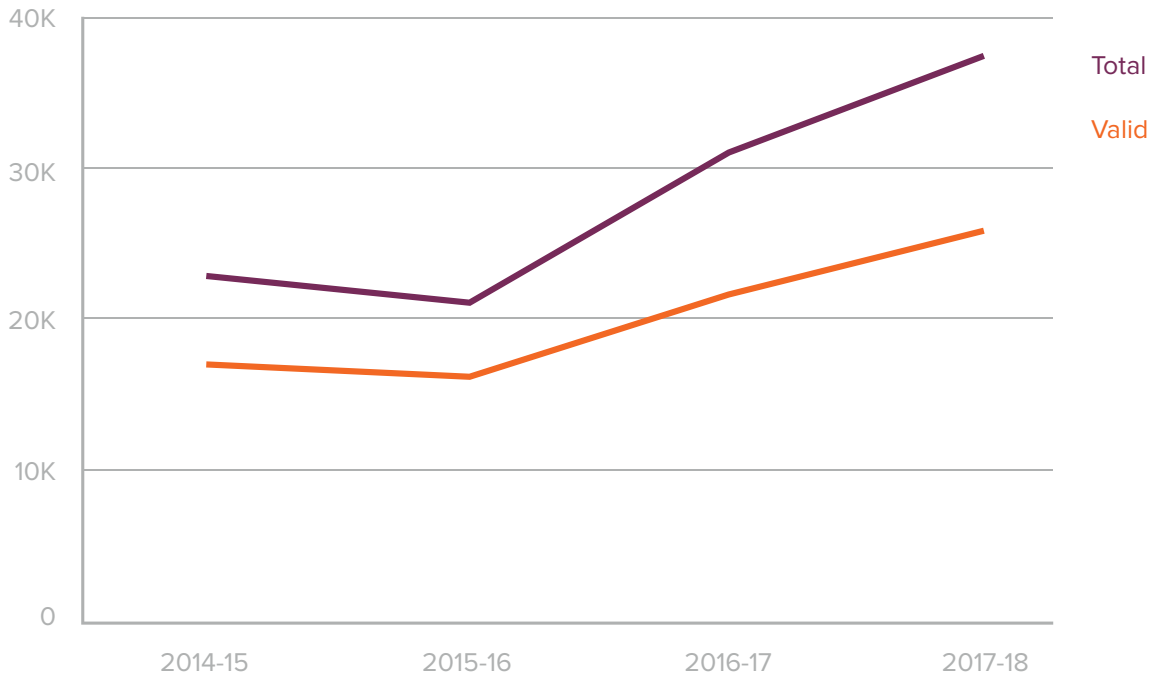
This past year was a year for the books. The **Equifax breach**, the **third Yahoo! breach**, the **Uber breach** — today nearly every American has been impacted by the loss of personally identifiable information (PII) data. And the threat continues to rise. Companies, healthcare systems, governmental and educational entities have started to realize how real the threat is but resources are scarce and dwindling. The number of vulnerabilities out in the wild is outpacing the ability to find and fix them.

Crowdcontrol intakes hundreds of vulnerability submissions a day. Over the past year, we saw a total of more than 37K submissions, 69% of which are valid. This is 21% increase in total vulnerabilities from last year.

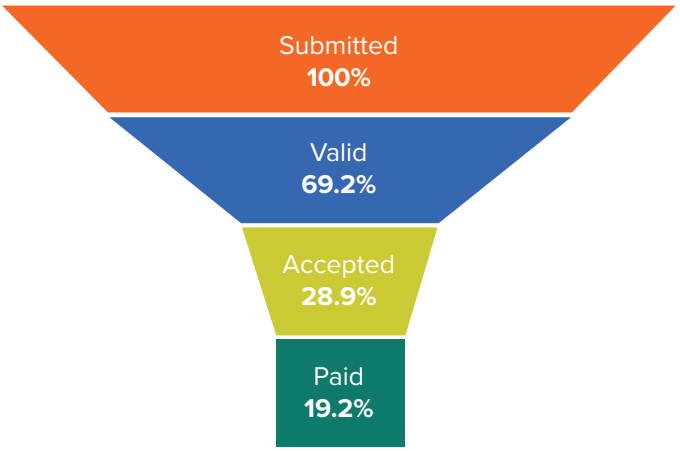
Common Vulnerabilities and Exposures (CVE) is a database of known security threats. The database is sponsored by the United States Department of Homeland Security (DHS), and threats are divided into two categories: vulnerabilities and exposures.

The database's main goal is to standardize identification of known vulnerabilities or exposures. This is important because standard IDs allow security administrators to quickly access technical information about a specific threat across multiple CVE-compatible information sources.

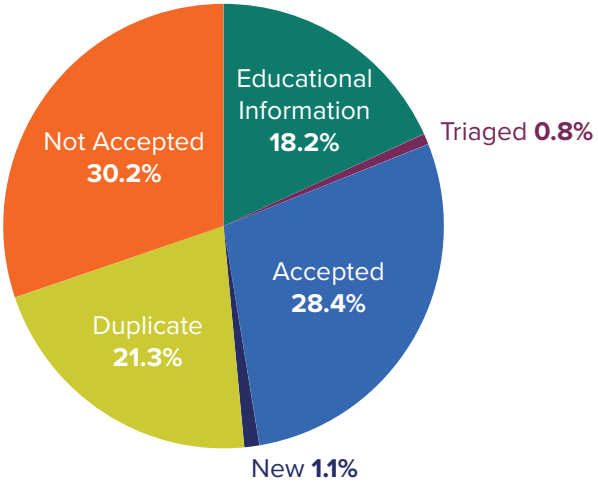
Vulnerability Submissions Over Time



Submissions



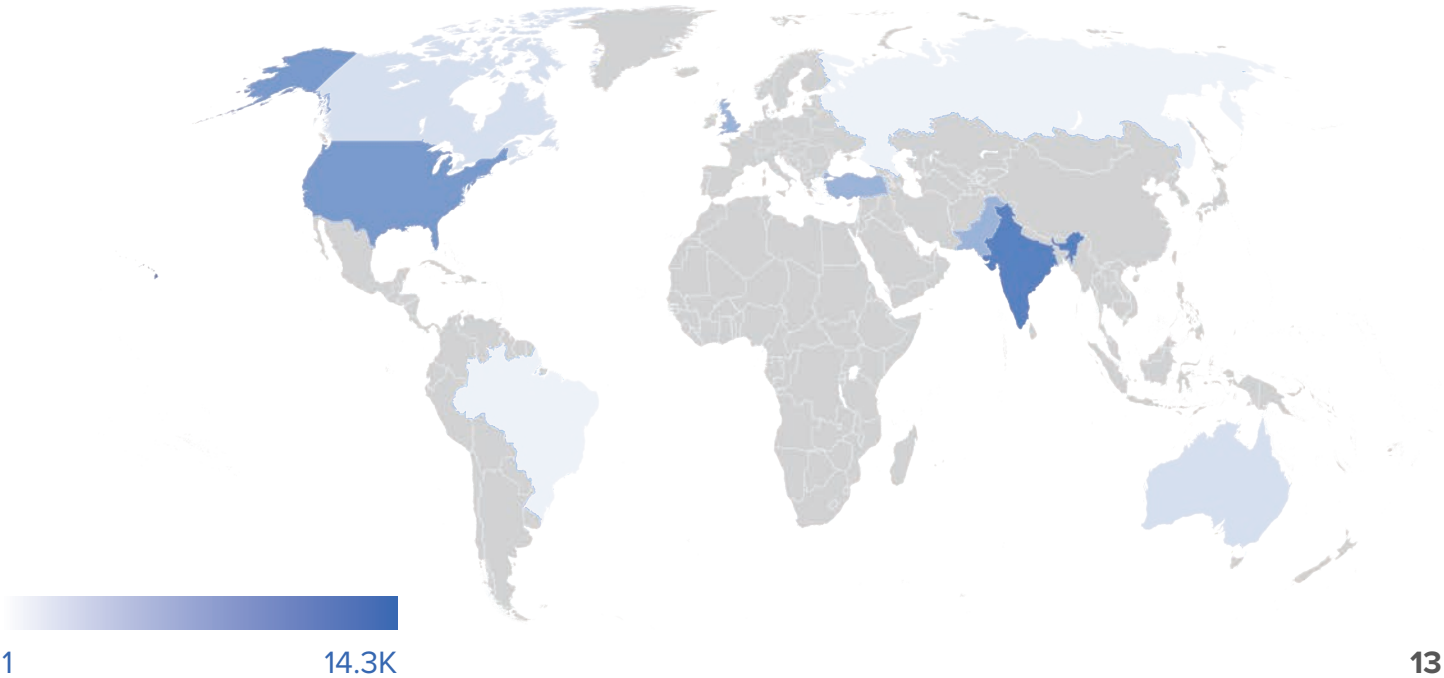
Submissions by Stage



Each and every vulnerability submitted through the Crowdcontrol platform is evaluated by our team of experts and is moved through different stages of triage and evaluation. Depending on the stage, Bugcrowd's security operations team prioritizes them for customers based on their business needs and scope of the program. As of March 31, 2018, 30% were not accepted given the scope, 28% are accepted, 21% are duplicate, 18% are educational information due to priority of business. The bottom line, is Bugcrowd sifts through this noise and delivers the only results that really matter.

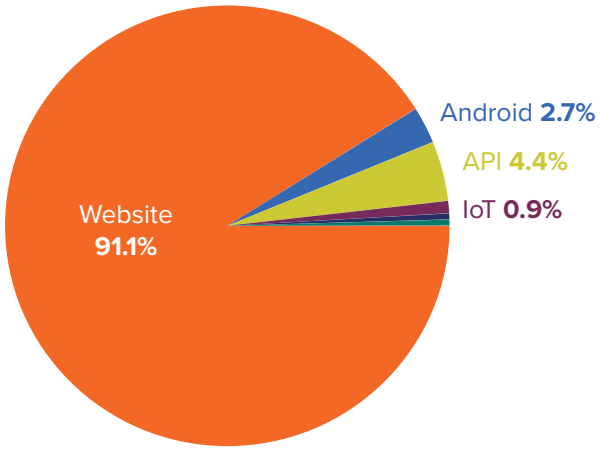
While the largest payment amount went to the US, the majority of total vulnerability submissions (30%) came from India, suggesting that younger bug hunters are emerging there, learning and growing their skills finding lower priority bugs.

Submissions by Geography

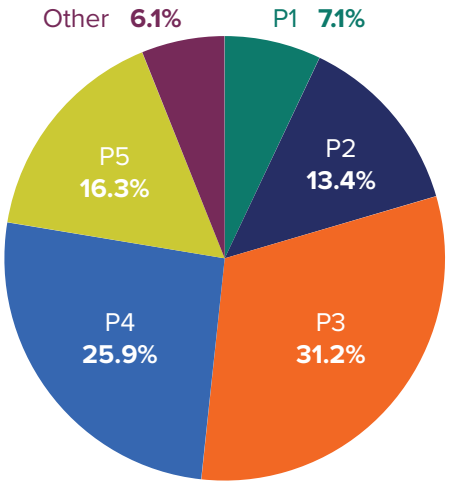


More than 91% of all vulnerability submissions were web vulnerabilities, and only 4% were API vulnerabilities. Organizations are understanding that attack surfaces are expanding so they continue to add new and complex targets to their scope.

Submissions by Target Type



Submissions by Severity



Over the past year, 20% of all valid vulnerabilities were classified as critical (P1 or P2). Of these 7% were P1, the most critical -- a 10% increase over the previous year.

31% of all valid submissions were classified as P3 severity, a 10% increase over last year. 26% were classified as P4, 16% were classified as P5 and 13% were P2.

Bug Spotlight - Apache Struts CVE-2017-5638 (The Equifax Vuln)

It's important to note upfront that every vulnerability is unique, and its severity depends on the nature of the flaw and the environment in which it exists.

The vulnerability that attackers exploited to access Equifax's system in March 2017 was in the Apache Struts Web-application software, a widely used enterprise platform. Apache Struts is a framework for building Web applications. If successfully exploited an attacker can execute arbitrary code in the context of the affected application.

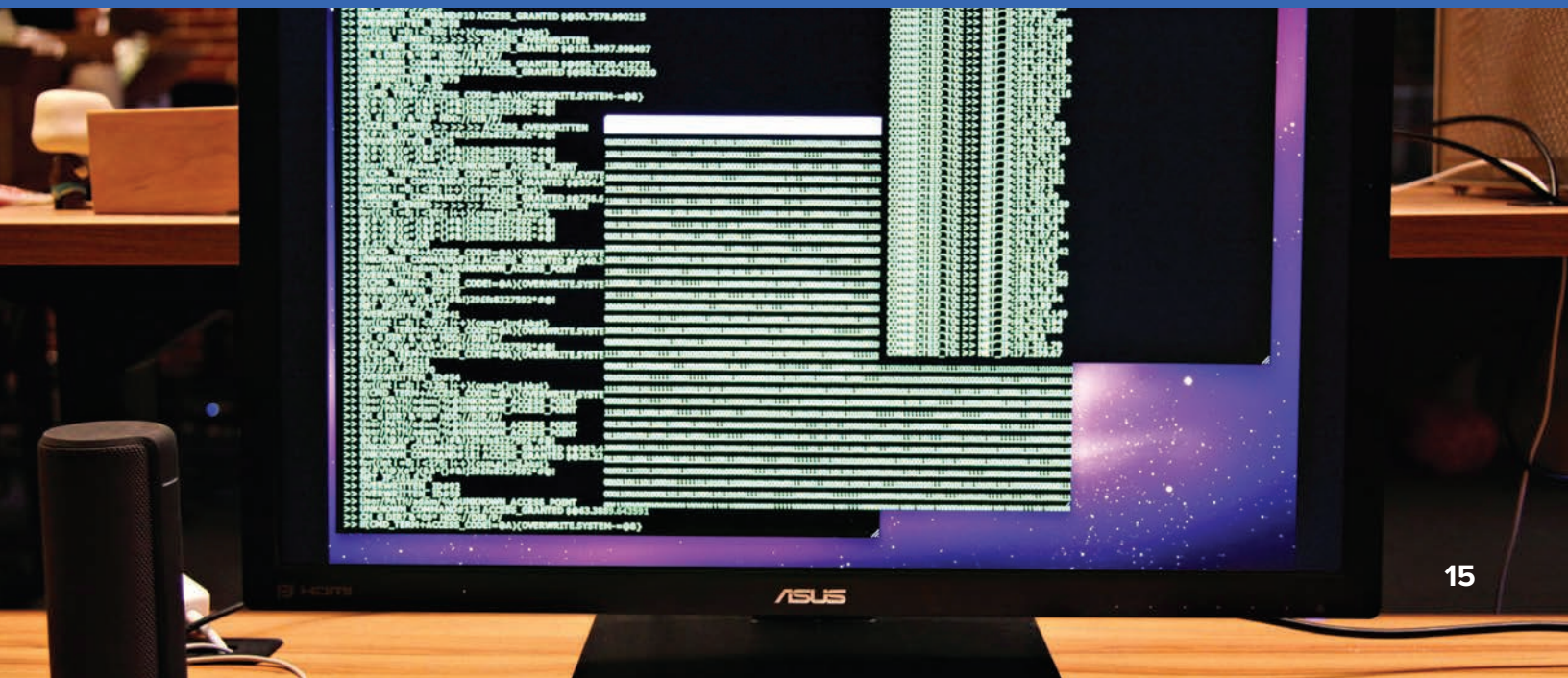
For Equifax, the severity was much higher than many other large-scale breaches due to the sensitivity of data that was leaked - data used to secure other types of accounts. This means the long term effects are more significant.

Because given that the attack vector was an HTTP header, in most cases, this flaw would have been discoverable via automated scans. That said, there are certainly cases where automated scans wouldn't have found it, such as when the struts component of an application was behind authentication.

This is exactly the type of vulnerability that the Crowd should have, and would have, found easily. In fact, our Crowd did identify the same vulnerability for one of our Fortune 500 financial services customers, creating a far shorter exposure window and averting a similar outcome for them.

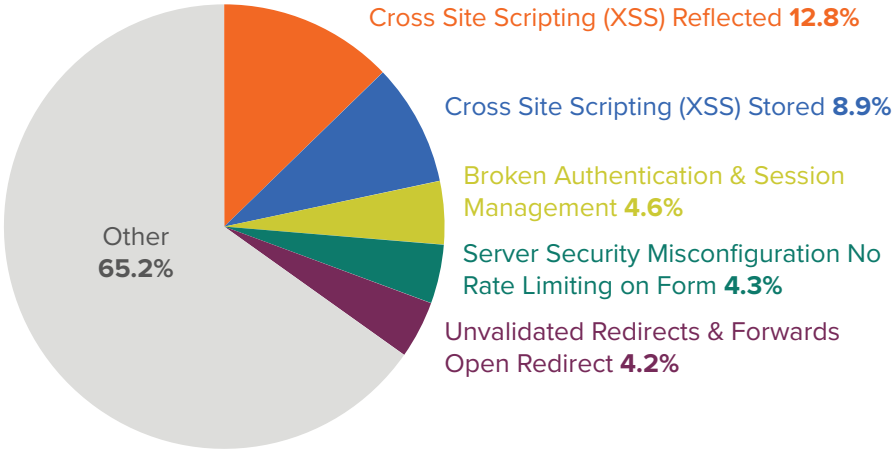
The security research community has long played an important role in discovering and reporting security flaws. In our platform, Crowdcontrol, we see multiple examples of vulnerabilities identified in customers' applications (on the public internet). These customers could have easily been in Equifax's position without the help of the security research community.

Vulnerabilities happen - Humans write code and humans make errors. Things get missed, no matter how good your internal processes. Crowdsourced security helps organizations mitigate the risk that these will be discovered by threat actors.



Top Valid Vulnerability Submissions by VRT Classification

Cross-Site Scripting (XSS) Reflected (P3), was the top vulnerability submitted this year via the Crowdcontrol platform.



The Top 5 vulnerabilities submitted this past year are:

Cross-Site Scripting (XSS) Reflected (P3)
According to **OWASP**, reflected cross-site scripting occurs when user input is immediately returned by a web application in an error message, search result, or any other response that includes some or all of the input provided by the user as part of the request, without that data being made safe to render in the browser, and without permanently storing the user provided data.

Cross-Site Scripting (XSS) Stored Admin (P3)
Stored XSS generally occurs when user input is stored on the target server, such as in a database, in a message forum, visitor log, comment field, etc. And then an attacker is able to retrieve the stored data from the web application without that data being made safe to render in the browser.

Broken Authentication and Session Management Failure to Invalidate Session (P4)
These types of weaknesses can allow an attacker to either capture or bypass the authentication methods that are used by a web application. Session value does not timeout or does not get invalidated after logout.

Broken Authentication and Session Management Weak Login Function Over HTTP (P3)
Application functions related to authentication and session management are not implemented correctly, allowing attackers to compromise passwords, keys, session tokens, or to exploit other implementation flaws to assume other users' identities.

Server Security Misconfiguration No Rate Limiting On Form (P4)
This occurs when a component is susceptible to attack due to an insecure configuration. This is considered the same vulnerability regardless of whether the misconfiguration occurs in the web server, database or in custom code.

You can find more definitions and terminology of vulnerabilities that cross our platform in our Glossary.

Implications

There has been a steady increase in new and uncategorized vulnerabilities discovered over the past few years, as well as the amount paid out for them. We saw a total of more than 37K submissions over the past year, a 21% increase in total vulnerabilities from last year. 75% of all P1 vulnerability payouts were above $1,200, up from $926 last year. Organizations continue to add complex targets to their scope, at the same time adding more value to securing their assets via their bounty offering. The more complex a target and the more critical a vulnerability, the higher the price tag.

Security professionals are beginning to realize that better awareness and information about disclosed vulnerabilities is critical to their operational success. Along with this, comes the realization that their organizations cannot rely on scanners or other traditional methods alone to assess risk.

The biggest issue is that traditional assessments are usually performed by one or two people using a routine, standardized methodology. Given the vast number of vulnerabilities, adversaries and their diverse skill sets and creativity, it is unrealistic to expect that this type of approach will reliably find the most serious application vulnerabilities.

Crowdsourced security breaks that mold with the goal to find high risk vulnerabilities, and not to complete a simplistic set of tests that do not reflect the way advanced attacks actually work. Services such as bug bounty and vulnerability disclosure programs leverage human intelligence at scale to deliver rapid discovery of high-risk vulnerabilities across attack surfaces.

With crowdsourced security, each vulnerability submission is verified and risk-rated, and can include advice that aids remediation and developer security best practices training. Organizations can get the coverage necessary in today's modern software development lifecycle.

Bugcrowd offers Vulnerability Disclosure and Bug Bounty Programs to meet all crowdsourced security requirements. When run in conjunction, they maximize the scale of creativity and coverage unmatched by any other vulnerability assessment solution.

Want to learn more about how your organization can start discovering and fixing high-value vulnerabilities missed by traditional security testing? Bugcrowd helps organizations leverage the crowdsourced security testing model through a full line of solutions. Visit **www.bugcrowd.com/get-started** to learn more.