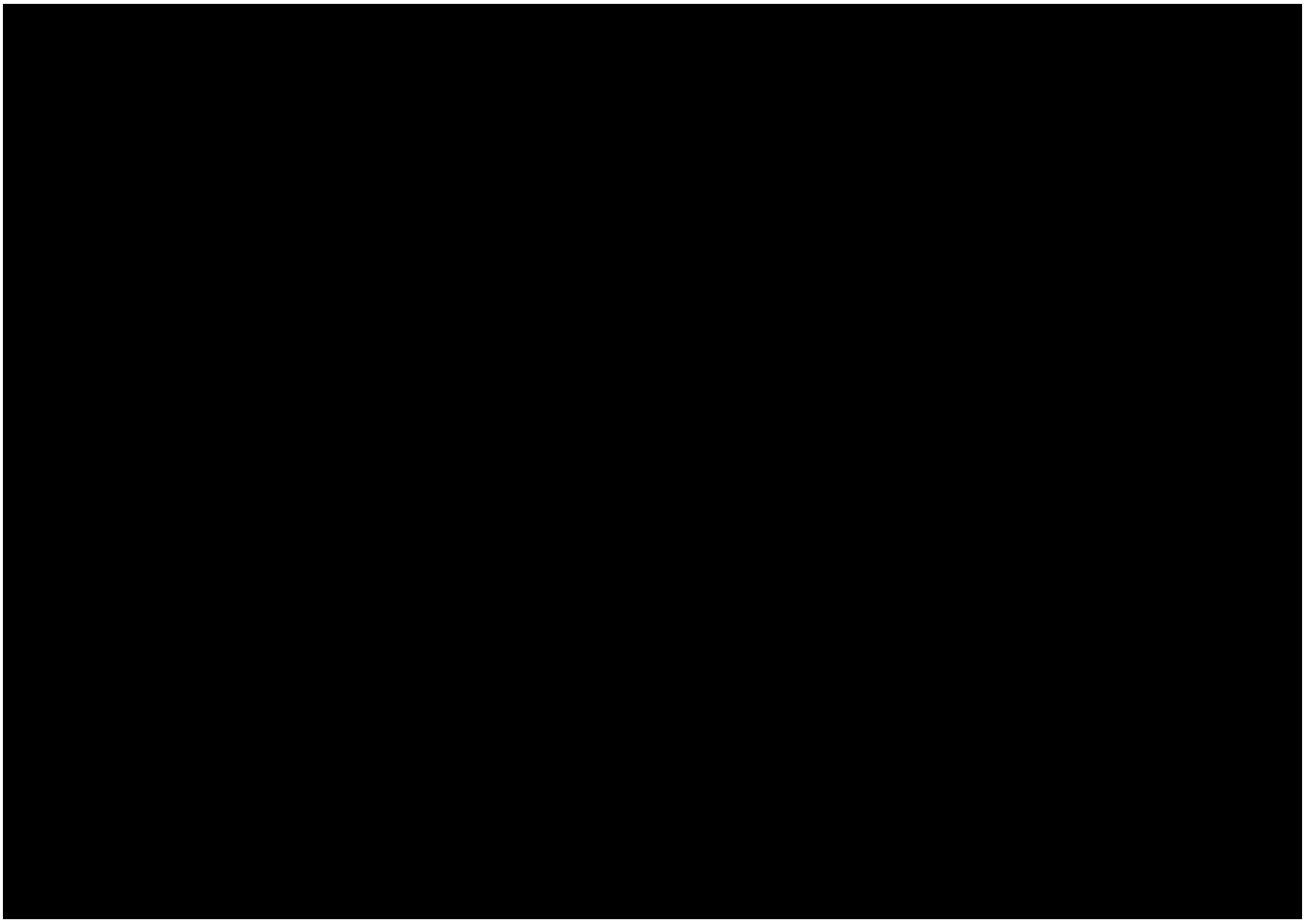
Uprising in the Valley: When Bug Bounties Went Boom, Part Two

Aug 31, 2021 **By** Dennis Fisher



Following the success of the bounty programs started by companies such as iDefense, TippingPoint's Zero Day Initiative, and Mozilla, by the late 2000s, more and more technology companies and platform providers began rolling out bounties of their own. Among the big players to enter the game were Google, Facebook, Yahoo, and eventually, Microsoft. There were plenty of growing pains in these programs and none of them debuted fully formed. Evolution and adjustment have been hallmarks of the successful programs, and from those efforts grew the idea of independent bounty platforms that could run bug bounty programs for

companies and handle the intake and triage of the vulnerabilities from hackers. Companies such HackerOne and Bugcrowd helped spur the second wave of innovation in the bug bounty community.

Note: All job titles and posiions reflect the person's role at the time of the events.

Read part one here.

Alex Rice (Founder and CTO of HackerOne): One of the first things that myself and Ryan McGeehan did at Facebook, was to put in our responsible disclosure policies. We were one of the first major websites to formalize a policy. Other folks had reporting channels before, but we wanted to draft it through the lens of, "It has to be safe to submit here." So we worked with Marcia Hoffman at the EFF to draft the language around that, and the responsible disclosure program rolled out. It was quite successful and reasonably high volume for a while. Then fast forward a little bit. In 2011, one of the goals that I set for the team was continuous security testing. So we had the idea that we wanted to have a different pen test firm doing a comprehensive, wide open scope pen test of Facebook every week out of the year. So we budgeted for 52 pen tests, we had three people working on the coordination of the scheduling, and we were kicking off a new pen test every week.

We were maxing out capacity, and anyone who looked competent, we'd bring them on as a pen testing pro. One of them was a small group of three Dutch guys, who had sent in a few vulnerabilities as a proof of concept. That was their lead gen for their pen testing business. So they had sent one of those in and ended up using them for a few pen tests that year. And then later on, they ended up being my co-founders for HackerOne. Because we were talking about the experience they had, their lead gen for their pen test firm was responsible disclosure. They'd made a list of 100 tech companies in Silicon Valley, found a vulnerability in every single one of them, and just tried to responsibly disclose it with very poor

success rates. But talking to them about that experience was one of the impetuses to tackling this as a more holistic problem, primarily responsible disclosure, but about bounties as well.

Sometime in 2011, Google launched their bounty program. Our continuous pen testing program had been pretty successful the year prior. It was a lot of work. We had renewed it for the next year. We had about 80 vulnerabilities come in from the 52 pen tests that we did throughout the year. And then Google did it and we were like, "Oh, yeah. This sounds like a good idea. Let's do it. We're feeling really confident right now. We're running a pen test every week, we're finding fewer and fewer vulnerabilities. We're fixing everything super fast. What could go wrong?" So I got a small discretionary budget. We decided we were going to launch it. Had one lunch with Chris (Evans), to just hear how it was going for his team. There would be no problem. We launched it on a Friday for DEF CON, and had some 300 confirmed vulnerabilities by Monday morning. So one of the more humbling, but also eye opening experiences of my career.

Chris Evans (Chrome security lead at Google): Launching the Chromium program was a fair amount of work, but most of it was trying to work out how to get a large corporation to pay individuals! There were no politics or naysayers, only support and curiosity. Corporations do get more conservative as they get larger, but this hadn't happened to Google in 2010 so the launch wasn't impeded. The overall goal of the bug bounty program was singular and simple: Make users of Chromium and Chrome safer. In order to achieve this, we needed to maximize the appeal for hackers to participate. Fortunately, Google has always been chock full of some of the best hackers in the world, so we had some instincts on how to create the modern bug bounty program to appeal to hackers. Sure, we offered reasonable reward values (for the time) and raised them regularly. But we were aware of significant non-monetary motivators for hackers and wanted to account for them.

Casey Ellis (Founder and CTO of Bugcrowd): So there was this group of tech companies that were just everywhere and that were basically having vulnerability input come to them because research is happening whether you invite it or not. And I think the consensus amongst the community at that point was that Microsoft is something that we need to do something about. We need to actually help them improve. And then with Katie and the others that were involved there at the time, Microsoft came to the table with the MSRC, and then obviously extended on that and actually launched a bug bounty program. So they're trail blazers from a corporate standpoint.

Kaite Moussouris (Senior security strategist at Microsoft): Yes, we all talked, but no, none of them had my problem set and none of them could help me. What was funny was, Chris Evans thought he helped me by paying for some of Microsoft's bugs out of his own bug bounty. He started paying for Windows local privilege escalation bugs, and he shows me this right when I come back from maternity leave and I'm like, "What? What are you telling me right now? I don't understand." And he's pointing to a reward in a release note or something on Google, and it said, $5,000 for a Windows local privilege escalation bug, and he points to it on their website, and he's like, "We started paying for your bugs because they were included in an exploit chain of Chrome, and so we didn't want to leave a bug unrewarded, and so we paid for yours."

It did actually help me free up some budget later after we were already doing bug bounties to sponsor The Internet Bug Bounty. And so how I did it was using Chris Evans's example and said, "Hey folks, I know we've launched our bug bounties, and they're in very specific areas, we're not bountying Windows yet, and especially local privilege escalation bugs, which would bankrupt us, so here's what I propose, we can join this Internet Bug Bounty, I'm going to be on the advisory council, why don't we grab a couple of Windows folks, and they can advise on bounty rewards, and then Chris Evans, who's also on the council, has said that Google will

only pay for ours until somebody else does, meaning us, I guess, but maybe the IBB. So I've talked to him, he's also on the IBB council, he'll get Google to stop paying for Windows bugs if IBB pays for them, so, let me just peel off 100 grand to kickstart the IBB." And I did, I peeled off $100,000 out of my own bounty budget to kickstart The Internet Bug Bounty. And that's what started it, and that's what got Google to stop paying for Microsoft's bugs.

> ***"I cannot imagine running a world-class security program without making it attractive for every actor on the planet to participate."***

Lucas Adamski (director of security engineering, Mozilla): The other part that was interesting was then trying to evangelize this for other companies who were slowly trying to dip their toes in the water. At least people like Katie were trying to drag them almost kicking and screaming into said water, which I definitely commend her for that effort because I don't know that I could have had that much patience that she had. A lot of that was then sort of like a what-about-ism, like what about if this happens, what about if they sell it to the bad guys and the good guys? My response was like, "They can do all that anyway."

Alex Rice: I cannot imagine running a world-class security program without making it attractive for every actor on the planet to participate. Not everyone needs to do it the way that Facebook was doing it, but that was the starting point.

Casey Ellis: In 2012 or so I'd started to experiment with basically introducing gamification into testing. So I'd seen what was going on with

bug bounty hunting, I'd been a part of disclosures. I'd done all that stuff. But then in the context of the company I was doing, it's like, "Okay. Does the competitive element and does the diversity of skills applied to this problem space work better?" Because logically it's working for the bad guys. We're up against an army of adversaries. So an army of allies just seems like a logical way to balance the equation. I was already noodling on that. And basically the folklore is, and this actually happened, I took a trip down to Melbourne. I was meeting with a bunch of pen test customers. At the time Google and Facebook had just gotten a bunch of press around their VRP. I was thinking about it and everyone wanted to talk about it. And what I noticed was everyone was like, they'd reached the same conclusion. It's got some Silicon Valley issues to it and all of that, but it's actually more than that. It seems like a logical way to get access to the creativity we need to outsmart the adversary.

And it was cool because it was like, "All right. You guys understand that security is a people problem that tech speeds up. You could just stand up a page and an inbox and invite the internet to come hack you. Why aren't you doing that?" It was a loaded question. I knew there'd be strong answers to it, but that's how I teased it out. And they all said the same things. They basically said, "I don't know if I trust hackers yet. I don't know how to manage the overhead of having a conversation with the entire internet. I don't know if I could fix all of the things that got found. I don't know how to pay someone in Uzbekistan." All of that stuff. And really it was actually on the flight back from that business trip where the light bulb went off that they'd all said the same things. And I had the idea for the Bugcrowd and literally registered the domain and the Twitter handle that night. So that was the bing and it went from there.

Chris Evans: Vendor bug bounty programs were very uncommon in 2010, but certainly not a new idea. For example, Netscape and then Mozilla had been running a program for many years. And in public presentations on Google's various bug bounty programs, we'd always start the story in

1981 with "Knuth reward checks" -- while not necessarily security bug related, Knuth was definitely paying rewards for errors in his books. We did think the bug bounty landscape was ripe for some pioneering and innovation, though. We tried to tackle the space by bringing some fresh ideas and definitely took a "launch and rapidly iterate" mindset.

Alex Rice: The business around HackerOne started early on from those public bounty programs in tech companies. We knew it was insanely valuable for those organizations, we knew they wanted to do it. We didn't expect it was going to be as large as it was going to be. And really, the impetus for it was that most organizations struggle to run a proper bounty program at scale. If you properly incentivize several thousand hackers to go look for security vulnerabilities, most software development teams are not properly staffed to deal with that. You can pine about what that says about the state of technology as a whole, but that's just the reality that we ran into. We would launch programs with even, just security apps, that they could not handle the volume coming in. And not because they were below benchmark or they didn't care, or they were irresponsible, just security teams everywhere are at a massive disadvantage when it comes to remediation. And there's a lot of work that needs to go into them.

Dino Dai Zovi: It became like all right, now there's actual risks to doing it, and also companies started going after the researchers, lawsuits and other things. This is also risky because if you're just coming in off the street and just sending this vulnerability to this company, you are actually putting yourself at risk and you don't have any lawyers. One of the ways that I thought about it is, "Look, if there's a bug bounty, if there's money changing hands, you radically change the conversation because one, now it is not an unsolicited random thing. It is solicited, and because there's payment involved, there is some form of contractual arrangement.

And then now when there's a bounty that says, "Hey, look, here's a scope. Go to town in that scope, and basically here's the reward. So now you

know how much the reward for your time could be, you know whether you're going to spend 10 hours trying, 100 or 1,000." That just changed the conversation drastically, and that will also result in more vulnerabilities being reported. More people investing the time, you're reporting those vulnerabilities and just change the economics, change the game. And so that's sort of what I wrote up in that blog post, just to clarify for people and there was still a lot of bellyaching and those other things. Like someone at Microsoft said, "We'll pay bounties over my dead body." Last I checked, he's still alive.

Katie Moussouris: There was Microsoft, and there was me who happened to work at Microsoft, and we were not always aligned, it turns out, on what we thought the best thing to do with the hacker community was. But that's kind of why they hired me. They hired a hacker, it takes one to know one. And they had hired hackers before me, like Window Snyder. So, they weren't allergic to the opinions of hackers, but when it came to what they are going to do in terms of vulnerability reports and payment, in 2008, one of the executives had publicly said in the actual news, quoted as himself saying that as long as he worked at Microsoft, they would never pay for vulnerability information. So before Google had made its move, Microsoft had already said, no way, we're never going to pay. Microsoft controls who it allows to speak to the media pretty heavily, as most corporations do. Now, I was a trained media spokesperson and had been a spokesperson for Symantec before joining Microsoft, I was also trained as a spokesperson at Microsoft, however, even though this was my program, they decided to let an unqualified male speak about it.

So the program he was speaking on my behalf for, and on the behalf of Microsoft, was the Microsoft Vulnerability Research Program that I started in 2008. And then somebody asked the question, if Microsoft is going to start paying bug bounties and whatnot, and that's when he just volunteered this absolute that he was not given any kind of prep to answer, but he just decided since he was in charge of security response at

Microsoft, that he would be able to control that, and so he publicly said no, and it was just kind of something that came out of his mouth. So, I had this massive, not just internal inertia to deal with at Microsoft and in my own chain of command, but I also had to deal with the fact that he had made an official public statement as an officer of the company that they would never do this. So, to begin to say that there were differences in my opinion of how things should go, and Microsoft's at the time is an understatement. It was a public disagreement at that point, only I, as a subordinate, couldn't say anything. So how do you like them apples?

> ***"There was Microsoft, and there was me who happened to work at Microsoft, and we were not always aligned."***

HackerOne's live hacking event at DEF CON in 2018.

Dino Dai Zovi: I don't have a good number, but (the research community) was small enough that everyone kind of knew who could land exploits and who couldn't. I remember when I first started working at @stake, I showed up and then I could land real exploits. And everyone was just like, "Who the fuck is this guy? Where the fuck did he come from?" Because it was just a small community, and everyone's just like, "We know everyone and he can land real shit. That's..." This is how one of my friends mentioned it to me, because I was like, "Why does everyone not like me in the office? Why is everyone being weird to me?" And he's like, "Yeah, we kind of could just do whatever we wanted, and then you showed up out of nowhere with actual skills and you wore button-up shirts and slacks and you stayed late. And we were used to just doing whatever we wanted," and that was kind of a buzzkill.

Casey Ellis: So I think vulnerability disclosure, as it exists today, wasn't

anywhere near as noisy or topical. There was a subset of security that cared about it, the rest of security that was aware of it, and then no one else really knew what was going on. So the whole idea of no free bugs and all that kind of thing... people that did vulnerability research and people that worked in this space directly were onboard with that and had their opinion on it and whatever else. I think, for the better part, most of the rest of the internet didn't actually know it was even necessarily happening at that point. And that's not a dis on those guys. It's more just that's where we're up to at that point. So I think it was this confluence of different things that came together because there was that original OG disclosure posse, like the Dinos and the Charlies and those guys. And then there was this new wave of folk that were coming in from pen testing or some variation of that that were looking at it and thinking, "I could hack on some cool stuff that I don't get to hack on in my day job." Or, "I can use this as a way to actually transition into security, all sorts of other things." They didn't really have that. They didn't bring that history in with them.

Ramses Martinez (director, Yahoo Paranoids): When I first took over the team that works with the security community on issues and vulnerabilities, we didn’t have a formal process to recognize and reward people who sent issues to us. We were very fast to remedy issues but didn’t have anything formal for thanking people that sent them in. I started sending a t-shirt as a personal “thanks.” It wasn’t a policy, I just thought it would be nice to do something beyond an email. I even bought the shirts with my own money. It wasn’t about the money, just a personal gesture on my behalf. At some point, a few people mentioned they already had a t-shirt from me, so I started buying a gift certificate so they could get another gift of their choice. The other thing people wanted was a letter they could show their boss or client. I write these letters myself.

Katie Moussouris: Here was the thing, Microsoft was open to this kind of romantic idea of flipping offensive researchers to looking at defense. And I kind of let them have that funny idea in their heads that that was a real

thing that could happen. I mean, it's not exactly what could happen. More likely is that offense-minded researchers are looking at defeating your existing mitigations, and the next time they see new mitigations, they'll look at defeating those to. They're not necessarily thinking, what would defeat me in my attempt, what would have stopped me? So, you can get them to think about that a little bit more, turns out, if you dangle a quarter million dollars in front of their faces, which is what the BlueHat prize was.

And it was also very deliberately looking for talent. So, we weren't saying we're going to completely outsource this forever, and we're always going to look for our next platform level mitigations from the crowd, we're not going to crowdsource our defenses, but this is a hard place to hire for, and we want to find people who are offensive-minded who can turn that into practical defense. And so it had all of these goals. So originally, I set the top prize for $200,000, which it was, and the Microsoft folks were like, "Why does it have to be $200,000? Why can't it be $100,000?" And I looked across the table and I said, "You know as well as I do that marketing spends more on that Black Hat-DEF CON party than $100,000." At least at the time, this was a decade ago, "But they don't spend $200,000. So if you're telling me that a night of drinking fun is worth more to you, Microsoft, than an entire platform level architectural mitigation, then we just definitely have to understand your priorities more." And they just kind of said, "Okay, 200k it is." I'm like, "That's what I thought."

Chris Evans: We were aware of significant non-monetary motivators for hackers and wanted to account for them. First, hackers are highly motivated by conversation and collaboration. So we didn't place any restrictions on publication. Money wasn't used to buy silence -- quite the contrary, we encouraged quality write-ups and publications for interesting issues. And critically, we made sure we set the reporting channels up so that we had "hackers talking to hackers and engineers". A bug report wasn't just a report, it was a two-way conversation and discussion of possibilities and ideas. One failure mode you unfortunately still see is

when hackers talk exclusively to a triage/response organization, cutting off discussion from security experts and/or owners of the code in question.

Second, hackers are motivated if you take their work seriously. One way you can express this is to fix reported vulnerabilities quickly. It's easy to underestimate the power of this, but not only does it motivate hackers to work with you again, it obviously makes your users safer so it's a win-win. Another way to take someone's work seriously is to celebrate it. So we made sure to credit rewards in the main Chrome release notes, as well as referencing great findings and researchers in official blog posts. Third, hackers love to challenge themselves. We used a little bit of signposting in our rewards structure and it really worked. Aside from the obvious idea of paying more for more serious vulnerabilities, we also had bonuses for particularly interesting or creative research; for high quality write-ups; for good analysis of exploitability; and for providing a patch to fix the issue. We were serious about these bonuses and we used them generously.

Alex Rice: From the very beginning, we tried to design this from the researcher's experience in mind. It's always been a continuous process of learning for us, where it's like, someone will take issue with this term and we'll adjust them. I think we pretty quickly got to a state where the vast majority of researchers are comfortable doing this. The only scenarios we arrive at today are people that want to be completely anonymous, which we just can't facilitate. We can keep them anonymous from the customer, but not from law enforcement, and not from ourselves. That's the only thing we hear today around, resistance of not wanting to use this process. It makes sense. Security researchers have inherently been distrustful. There are scenarios where people will uncover vulnerabilities where, the circumstances through which they discovered that vulnerability, is not something they want to disclose. But they're still trying to do it through the disclosure. So we'll handle those out of hand as we need to, but today that's the blocker that we have on it.

> ***"Hackers are highly motivated by conversation and collaboration. So we didn't place any restrictions on publication. Money wasn't used to buy silence."***

Bugcrowd's Grace Hopper tribute shirt.

Katie Moussouris: So, is it money? Is that it, we just need to pour more money into it? The answer's no. When we modeled the system, we basically were like, "Look, people come in, they aren't born with this skillset, they have to grow it somehow, and both the offense side of the market, and the defense side of the market need to grow people with these skill sets." So let's take a look at the populations and see what we can tell about these populations and how long are they able to find vulnerabilities at the top of their skill set level, the real zero-days, the zero-click vulnerabilities, jailbreaking an iPhone, that level of skill, right?

And there's maybe a few thousand people worldwide at any given time. Why? Because new people are scaling up, while the people who have been there for a while are deciding to do something else with their lives, or simply being outpaced by the technology. People who could write exploits for Office 2010 might not be able to write an exploit for modern Office with its current mitigations, that may have outpaced their skill level. So essentially we looked at that, and then we said, "Well, we're throwing more money at it, tip the advantage to defenders." And the answer is, not really, because it doesn't actually speed them up in knowing what they need to know and learning what they need to learn. What we found was that investing in tools to determine whether or not a particular bug is exploitable, that was the key place. That if we could invest in more tools that would determine exploitability.

Chris Evans: The success of the Chromium program was clear quite quickly. The obvious next step was to launch a broader program for Google: the Google Web program. The Google Web program was in many ways more novel than the Chromium program. I believe it was the first major program to target live web apps backed by live services. Launching was one of those situations where it would have been easy to "what if" the whole thing and panic ourselves into not launching -- perhaps on some legal, safety or PR concern. Fortunately, no one was pessimistic or overly conservative, so I drove forward with the launch. I was still in the Chrome org at the time so while I decided we should do this, many others stepped up to do the actual preparation and hard work. I think we all owe them a debt, because a bug bounty program for web properties and services is now a firm industry best practice with hackers, corporations and ultimately end users benefiting.

Pedram Amini: Look at what it takes to pop Chrome. It's not from my time where it's a single bug that you can exploit with relative ease. You're talking about chaining a dozen things together. It's black magic basically to get exploitations to work in something like Chrome.

Tomorrow: Part three.

All material from author interviews, except Ramses Martinez quote, which is from a Yahoo blog post.

First image courtesy of Katie Moussouris; second image courtesy of HackerOne; third image CC By 2.0 image from Flickr.

Bug Bounty

Vasilis Pappas accepting the $200,000 reward for winning the first Microsoft Blue Hat Prize in 2012.