BUCKS FOR BUGS!

Want to have your cake and eat it too? **Mayank Sharma** explores bug bounty websites and how you can fill your coffers and your karma at the same time.

Back in the American Wild West (or at least as depicted by the films) when law enforcement agencies didn't have the resources to track down outlaws, they offered cash rewards or bounties for their capture. Fast forward to the age of technology and companies are offering similar incentives with a small difference – the wanted outlaws are malicious pieces of software code and the vigilantes after them are a worldwide army of software developers.

Several tech giants including Google, Yahoo, Microsoft and Facebook offer bounties for weeding out and eliminating bugs in their software. And bug bounties aren't limited to big software companies. Open source software projects also offer bounties on bugs that plague their software. This may not make much sense at first, considering the benevolent nature of the open source software development community, whose members work on projects to satisfy their own particular itch.

"Several tech giants including Google, Yahoo and Facebook offer bounties for weeding out and eliminating bugs."

Perhaps the biggest example of this – organisations clubbing together to fund the development of a feature – has come out of the Heartbleed bug in OpenSSL. The OpenSSL project plays a crucial role in the proper and secure functioning of the internet. Yet the project was maintained by only a small group of volunteers with very little funding, and there was only one person working full-time on the project.

Experts estimate that the Heartbleed bug will cost businesses tens of million of dollars in lost productivity as they update systems with safer versions of OpenSSL. As a fallout of Heartbleed, a new group set up by the Linux Foundation has so far raised around $3m (£1.7m) with contributions from tech companies including Google, Facebook, Microsoft, Intel, IBM, Cisco and Amazon. These companies will pitch in $300,000 over the next three years. Besides maintaining OpenSSL, the fund will also be used to support development of other crucial open-source software.

Scope of bounties

But what role do bug bounties play in the larger open source development ecosystem? We asked Tony França, who runs FreedomSponsors (https://freedomsponsors.org), which is one of the most popular bug bounty websites dedicated to open source software. França explains that the effect of the bounties varies greatly from project to project.

He illustrates by comparing LibreOffice with the Jenkins project: "LibreOffice gets enough funding from companies, so the money coming from bug bounties is really a small fraction of that. Now compare that with the Jenkins project where we have helped resolve 12 of 88 issues. Jenkins officially adopted FreedomSponsors as a bug bounty platform (every issue on their JIRA has a link to be sponsored on FreedomSponsors). Because of that, they get more bounties, but those are spread among more issues, so it's still not enough to get the developers' attention to an individual issue's bounty."

But there are some exceptions to this, especially when a bug affects an important library. "There are occasions where a feature is so important that bounties start to add up organically. This is what happened with the 'OTR encryption support for Telepathy' feature. As far as I can tell, people just randomly started to offer money for that feature, until a developer named Xavier Claessens went ahead and implemented it."

"So, generally speaking, bug bounties still play a small role in the FOSS development ecosystem", he concludes. However, França believes that this is mainly because of lack of marketing of the bounties: "The users who realise that they can place bounties for solutions to problems they see every day is still a small group. But we're growing. Slowly, but surely."

Another bounty website specialising in open source software is BountySource (**www.bountysource.com**). In addition to encouraging end users and developers to support their favourite projects with their wallets or skills, the company also works with corporate donors who are interested in certain open source projects that are an integral part of their business.

The website currently hosts over 500 bounties ranging from $50 to well over $1,000. In addition to bounties, BountySource also hosts fundraisers for open source projects. Explaining its USP over traditional crowdfunding platforms like Kickstarter and

Robert Roth is a Java developer who divides his free time between playing the guitar and collecting bug bounties.

Tony França pats himself on the back every time he sees a new feature in software that was made possible because of a bounty on FreedomSponsors.

Indiegogo, which have successfully hosted many open source fundraisers, the website's CEO Warren Konkel noted in an interview with **OpenSource.com** that FOSS needs a "better funding model that's more aligned with how software is built." Both BountySource and FreedomSponsors integrate with services popular with developers, such as GitHub and Bugzilla.

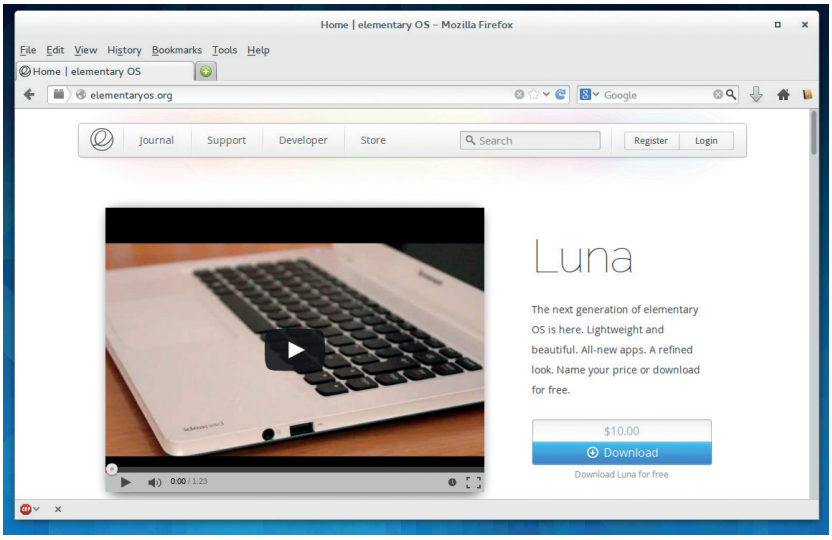
Fundraisers on BountySource are time-limited campaigns that aim to raise money for a specific goal, such as the next major release of an open source application. Unlike other platforms, BountySource also handles the pledge rewards for the project; so if a project is offering T-shirts to contributors, the website will take care of the printing and shipping.

However, when LV spoke to him, Konkel said that he believes the future of crowdfunding in open source is a bounty-based model: "Issue trackers can quickly become overwhelming and bounties allow backers to focus development efforts on the issues that matter to them." In the **OpenSource.com** interview Konkel notes that, generally speaking, there are more bounties on bugs than on feature requests: "This seems to be normal behaviour, as developers will often encounter a bug and want an immediate resolution."

Fostering interactions

Konkel adds that bounties often lead to a flurry of comments that end up fleshing out the details behind a feature request: "With bounties, developers can quickly understand what a community is most interested in seeing improved."

Philip Horger, one of the leading contributors at FreedomSponsors, illustrates the importance of communication in creating effective bounties. When he put up a bounty to improve the LibreOffice user interface, a member of the actual LO team showed up and advised everybody that sponsoring such a wide-scope issue was, while an encouraging sign for the developers, not a realistically useful way of making user interface improvements happen. He advised that Horger should in fact sponsor more specific improvements. "So I broke up my offer among more



The Elementary OS project uses the donations it receives to put up bounties.

specific sponsorships and revoked the old one. The total sponsorship was the same in the end, but more usefully distributed."

Robert Roth, a software developer from Romania, has worked on and collected several bounties on BountySource. While working on the bounties of the Elementary OS project, Roth says the developers and designers from the project provided useful feedback, usually in a matter of hours, and suggestions in case the fixes were not perfect. That's mostly because the bounties were put up by the developers of the Elementary OS itself. "So the requests are valid requests. You won't have to convince the maintainers that a feature will be used, and they will most likely be accepted, after the fix is validated by a developer."

This is in stark contrast to the bounties he has worked on for larger projects such as Gnome. "In these cases usually the person putting up the bounty validated the fix or requested various improvements quickly, but with the maintainers being fairly busy, getting a proper review and getting the patch to be accepted and committed takes longer (days, or even weeks, and even up to 1–2 months)."

Roth concludes by saying that all the bounties he's worked on have received attention from both the person putting the bounty and the maintainers of the project: "If you are willing to communicate and iterate your patches, the contributions are always welcome."

França, on the other hand, doesn't see too many discussions. "One would think that there would be a lot of interaction between sponsors and developers on bug bounties, but what happens is quite the opposite. Most of the conversations we see on paid bounties are just quick progress reports and people thanking each other – there's not much talk about how the problem will be fixed."

He pins this on two factors. For starters "when a task comes to the point of being sponsored, it's already very well defined so there's really no need to discuss it further." Secondly, he believes that a bug bounty platform is not the right place to discuss solutions: "You should use the project's issue tracker for that. It would be bad for project management if the requirements for an issue were documented on FreedomSponsors instead of the project's own issue tracker! I guess people just understand that and use the right place for the right conversation."

Encouraging developers

Besides helping open source projects improve the quality of their software, bug bounties also offer an opportunity to young and talented developers to showcase their skills and make some cash.

Roth, a full-time Java developer with a young family, became a bounty hunter when he was on the lookout for some extra cash. "I was investigating how one could get paid for working on open source software, and found that there are various possibilities. Reading about all of them, I found that the option provided by BountySource was the best fit for me – getting paid for occasional bugfixes, whenever I have time, while improving free software by adding features and fixing bugs that are important for other users."

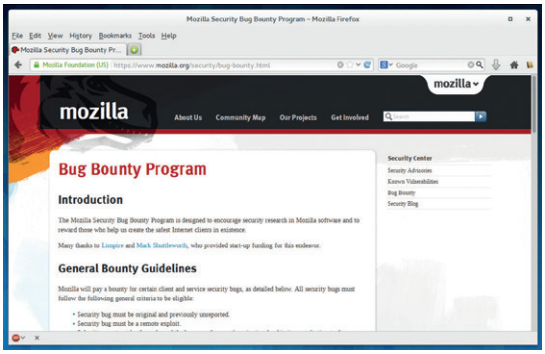
Recalling his motivations behind starting FreedomSponsors, França says that one day while playing with an issue with Jenkins' OpenID plugin, he ran into a documented bug. "Maybe I could try to debug it, but boy that would take a long time, I mean I

Bug bounties on the tech high street

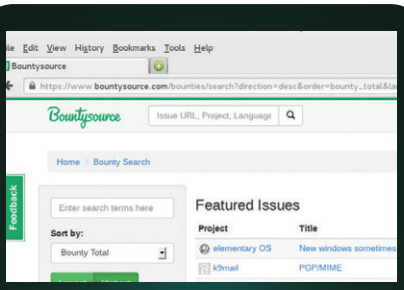
A security hole in a big product such as Facebook could have far-reaching consequences if the information made its way to the cyberspace black market. Which is why a lot of tech companies announce bug bounty programs to encourage white hat security researchers and developers to share the information in exchange for money and fame.

These public programs increase the chances of discovering exploits and vulnerabilities. Companies including Facebook, Google and Yahoo offer thousands of pounds in rewards for finding software vulnerabilities, based on how damaging the discovered vulnerabilities are. Facebook recently awarded a bounty of $33,500 to an engineer in Brazil for unearthing an error that could have allowed access to almost any file on Facebook's servers. Yahoo too wised up after a firm discovered four critical vulnerabilities in their offerings, and instead of T-shirts now pays bounties of up to $15,000.

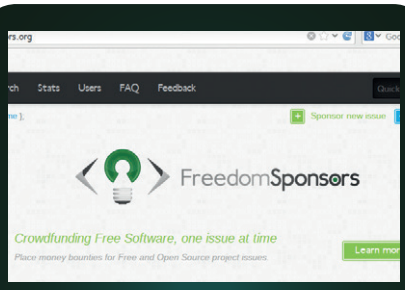
Google has broadened its bug bounty program to cover all Chrome apps and extensions made by company. It has also upped payments for its Patch Rewards Program, which focuses on improving security for select open source projects. The company will now offer $5,000 for moderately complex patches, and $10,000 for complicated improvements that prevent major vulnerabilities in the code.



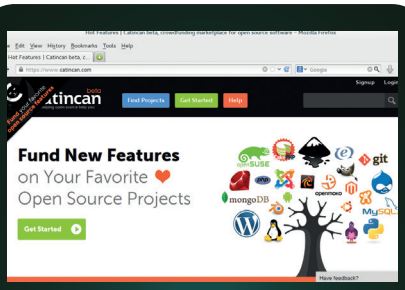
From a security standpoint, public bug bounty programs lead to broader coverage of scrutiny on the app.



Web www.bountysource.com
Funding model Bounty/All or Nothing
Fees 10% non-refundable fee for placing bounties
Payments Bitcoin, PayPal, cheque, Google Wallet, wire transfer
About Designed for crowdfunding bugs and features in open source software, and is used to fund for new projects.



Web http://freedomsponsors.org
Funding model Bounty
Fees 3% + payment processing fees
Payments Bitcoin and PayPal
About Enables several users to chip in to a bounty. Bounties are paid only after the sponsors have verified the work. Uses PayPal's parallel payment type to split bounties between developers.



Web www.catincan.com
Funding model All or Nothing
Fees 10% after funding amount has been reached.
Payments Bitcoin, PayPal, wire transfer
About Only allows developers of existing projects to create campaigns. Features are screened and developers have 60 days to reach the funding goal.

had never even looked at Jenkins code before. Then I thought there could be some people out there that would be willing to even pay a few bucks to whoever fixed it. The moment I thought that, a storm of ideas came rushing into my head. Someone should build a website for that. So I did."

Horger, who also donates directly to various projects, shares another interesting perspective comparing bounties with traditional donation. "Sponsoring on FreedomSponsors is inherently more fine-grained and personal than donating. Your offer is tied to a specific and achievable outcome, which means you feel stake and responsibility in that sponsorship's success. It is more gratifying and tangible to be able to point to some distinct feature of some popular program, and say to the person next to you, "I helped make that happen."

Horger also has an interesting use for the bounties. He puts up bounties for his own projects! It might sound odd for a developer to pay others to do things he could more easily do himself. But Horger says rewarding external development allows him to foster a community around his projects. This "not only will take programming and maintenance load off of me in the long run, but also means that my projects can easily live on if I get hit by a bus!"

Putting up a bounty

All bug bounty websites function in a similar way. A bounty is created either to fix a bug in software or add a feature to a project. Once the bounty is created, users can contribute towards that bounty. That's when a developer comes along and fixes that bug or adds that feature and checks the changes to the website revision control system. Once the changes have been merged into the project, the developer gets paid.

Catincan (**www.catincan.com**) is another bug bounty website that looks after open source projects. However, unlike the other two bug bounty websites, only active developers on existing open source projects can put up a bounty. While users not associated with the project can make suggestions, a proposed feature cannot be shifted into funding mode until one of the project developers is ready to take on responsibility for completing it. This makes the platform ideal for managing feature requests and creating funding opportunities for open source projects. Also, the website doesn't charge developers any fees for putting up a bounty.

In contrast, both BountySource and FreedomSponsors are open to users and projects. Anyone can put up bounties, contribute to an existing bounty and collect the bounty after successfully squashing the bug.

In a reassuring sign that the system works, both BountySource and FreedomSponsors use their respective platforms to improve themselves by putting up bounties on components that power them. The logo of FreedomSponsors, and its Bugzilla plugin, are two examples of improvements that came about this way. BountySource too uses software that it has helped fund, such as the JSHint syntax checker, and also puts up bounties on software it uses including Textmate and AngularJS.

"A bounty is created either to fix a bug in software or add a feature to a project."

At first glance, writing code for money seems to be against the ethos of free and open source software. But if you look at it, money has been a part of open source for quite some time. Many open source developers are paid by their employers to work on open source software. Others have consulting businesses around their projects. As long as good quality code makes its way into a project and improves it, the motivations behind the code shouldn't matter. Bug bounties provide the ideal avenue for users to make identifiable contributions to their favourite projects. LV