https://www.pressetext.com/news/20180904010

Bug Bounty Programs – Vulnerabilities as a worthwhile Investment

DeepSec Conference offers trainings for security researchers

Vienna (pts010 / 04.09.2018 / 08:30) – This year, in addition to lectures about the failing of security measures, the DeepSec In-Depth Security Conference will offer a workshop for finding vulnerabilities. Unfortunately the testing of software in the context of quality assurance is no longer sufficient in the modern, networked world. The prefix "Smart" does not change anything about existing weaknesses. The training is therefore aimed at professionals, already working in development, and at security experts, to specifically strengthen the development of safer products in industry and companies.

Complex Technologies and their Susceptibility to Errors

Not only since the birth of the Internet of Things modern products can't manage without software. If you add networking and the high level of complexity of individual parts, this is a sure recipe for mistakes. Of course, there is often quality assurance and testing for the most important functions, but the consequence of serious malfunction due to the size of the lines of code is a matter of statistics. How can manufacturers and developers help themselves? If you look at the mathematical game theory, the answer is: Bounty for Bugs – Bug Bounties as a reward.

Organized Hunt for Software Errors

The Bug Bounty Programs were established as a permanent institution several years ago to, on the one hand, give security researchers the opportunity to get credit for their work of finding and locating errors. On the other hand, such a program automatically regulates the process of how critical errors are reported, documented, reproduced and corrected by the responsible developers. Unfortunately, there are still many manufacturers who do not respond to reported bugs and do not provide updates. Offering bug bounties therefore speaks for the commitment of a company and ensures the quality of its own products. On top of that, you do not learn about the failure of your own product from the press or the Internet.

The big advantage of Bug Bounty Programs is the good quality of the bug reports. Finding software bugs is the daily bread of software development, but critical vulnerabilities that pose a security issue are often not immediately recognized. Information security is an interdisciplinary field of computer science, which requires skills in software development, mathematics, reverse engineering (i.e. the reconstruction of an application or a protocol) and a lot of patience. This requires in-depth knowledge, sufficient experience and a targeted training, which not all of those, who are part of a companies development team may have acquired.

The bug bounty programs are very well received. HackerOne, a platform for the coordinated publication of vulnerabilities, keeps a record of distributions to discoverers of errors. Currently, over $20 million has been disbursed to researchers from various companies. The stated goal is to reach $100 million by 2020.

Training as a Bug Bounty Hunter

This year's DeepSec Security Conference offers a two-day Bug Hunting course. Coach Dawid Czagan, who's among the Top 10 of HackerOnes Bug Hunter List, has developed a curriculum to teach advanced users with knowledge of software development practices the approaches and thinking of security experts. Participants learn how the many parts of modern applications interact, where to enter for analyzing protocols and what to look out for. It's not just about bounty hunting: Since a lot of work now takes place via web interfaces, be it visible to the user or invisible behind the scenes, web technology will be the focus of the training.

And this workshop offers more than just dry theory. Dawid Czagan has prepared case studies from productive environments to illustrate the various classes of errors. The complete training is a mixture of short explanatory lectures followed by practical exercises to consolidate the newly acquired knowledge. The skills taught are a valuable addition to any quality assurance and a sought-after training for developers. The training is targeted at security researchers, penetration testers, consultants, software development project leaders / developers, and IT architects, who design the basic designs, applications and systems are built on.

The attackers already have these means. It's about time you catch up. Networked systems never sleep.

Program and Booking

The DeepSec conference takes place on the 29th and 30th of November.
The trainings take place on the two preceding days, the 27th and 28th of November.

Training and conference venue:
The Imperial Riding School Vienna – A Renaissance Hotel, Ungargasse 60, 1030

Vienna.

Here's the link to the current program: https://deepsec.net/schedule.html
Tickets for the conference and trainings can be ordered via https://deepsec.net/register.html

The conference blog with news and background information about the lectures and workshops can be found at the address: https://blog.deepsec.net/

Sender:	DeepSec GmbH
Contact:	René Pfeiffer
Mobile:	+43-676-5626390
E-Mail:	deepsec@deepsec.net
Website:	deepsec.net