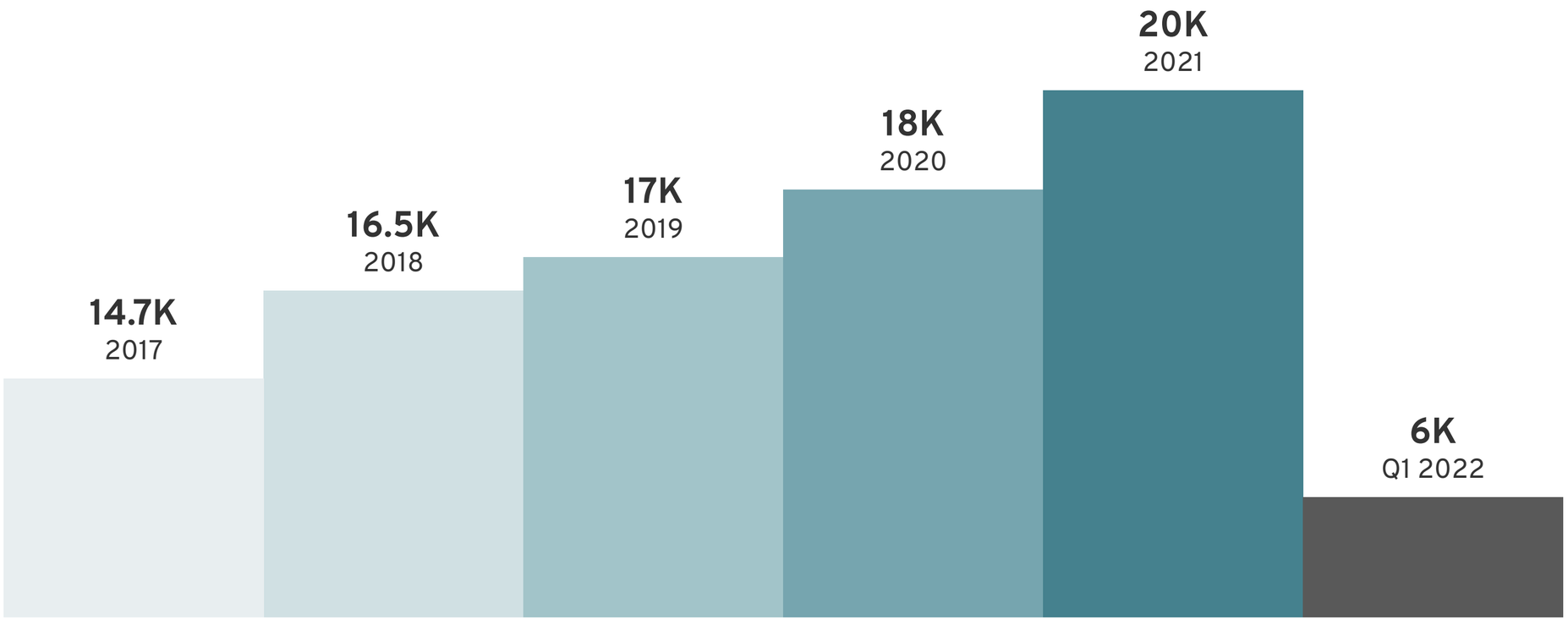
CyberSec Bug Bounty Program

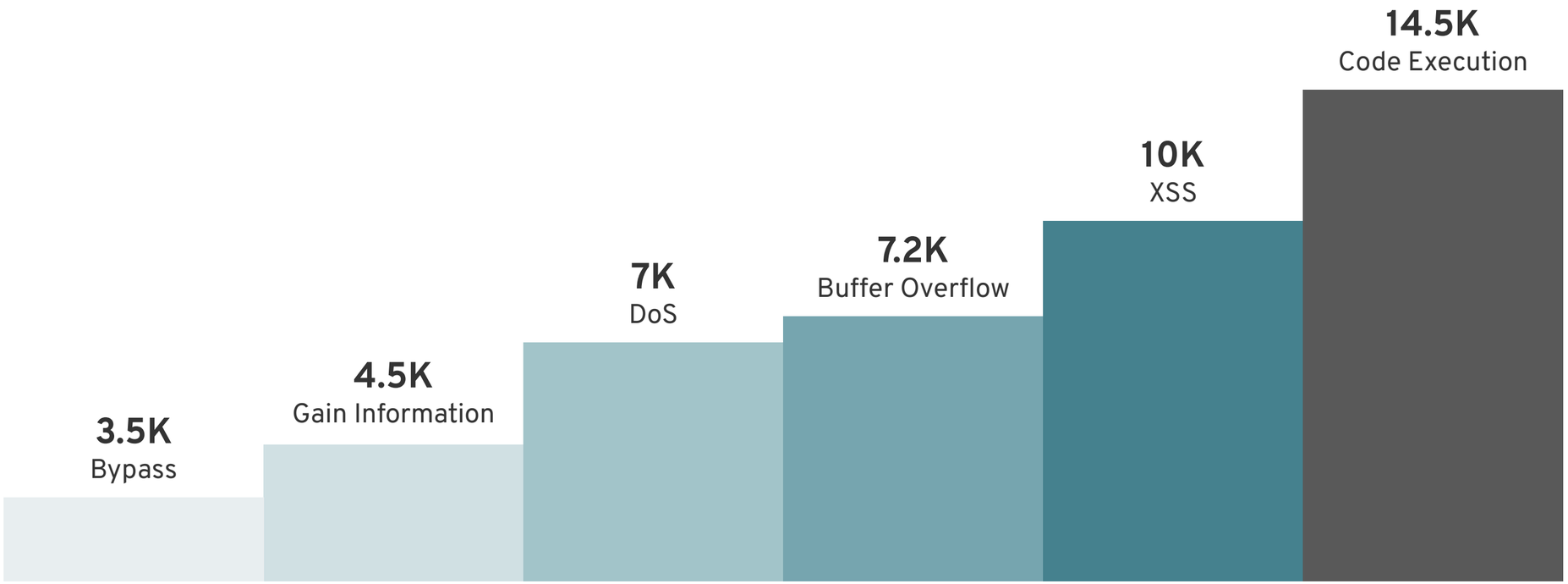
Tobias Sattler
tobiassattler.com | cybersec.help

Security vulnerabilities grew 8% annually



Reference: CVE, (2022)

Code execution is the most common issue in the last 5 years



Reference: CVE, (2022)

What is a ‘bug’?

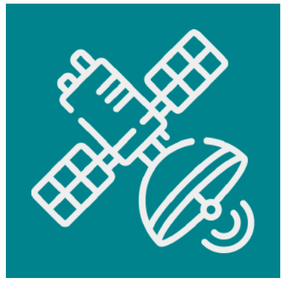
1. A bug is an error, flaw, or issue in computer software or hardware that causes it to produce an incorrect or unexpected result or behave unintendedly.

2. Most bugs arise from errors in either a program’s design or its source code or components and operating systems used by such programs.

3. A famous story is that Operators traced an error in the Mark II – a computer in 1947 – to a moth trapped in a relay, coining the term bug.

Some of the most famous bugs in software history

In 1996, the Ariane 5 rocket launched by the ESA exploded just forty seconds after its launch. The reason behind its failure was an integer overflow.



In 1999, the Mars Climate Orbiter crashed while entering the planet's orbit. The issue was that one team used the metric system in its calculations, while another group used the Imperial system.

In 2014, the music video 'Gangnam Style' broke Youtube because it hit the maximum of a 32-bit integer (aka more than 2,147,483,647 views).

How to challenge security vulnerabilities

Improve Code Quality

1. Embrace coding conventions
2. Use test-driven development
3. Use a code linter
4. Adopt continuous integration
5. Leave helpful comments
6. Facilitate interaction between developers and administrators

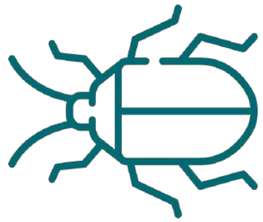
Quality Management

1. Integrate requirement engineering from the beginning
2. Test early and test often with Automation
3. Employ quality measurements

Bug Bounty Program

1. Consider a bug bounty program
2. Plan for business objectives
3. Launch, iterate, and improve your program

What is a Bug Bounty Program?



1

It is an initiative by many websites, organizations, and software developers by which individuals can receive recognition and compensation for reporting bugs.

2

Hunter & Ready, Inc set up the first program in 1983 for the Versatile Real-Time Executive (VRTX). Anyone who found and reported a bug would receive a Volkswagen Beetle.

3

Many organizations, such as Mozilla, Facebook, Yahoo, Google, Reddit, Square, and Microsoft, have implemented a bug bounty program.

How to set up a Bug Bounty Program

Plan

1. Plan for business objectives
2. Set your goals straight
3. Set your scope
4. Arrange rewards
5. Implement internal processes
6. Have a dedicated team member for this program

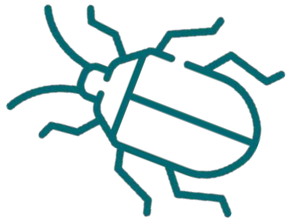
Launch & Run

1. Spread the word or sign up at a bug bounty platform
2. Monitor incoming messages
3. Be in touch with the researchers

Iterate

1. Regularly check your results with your business objectives
2. Keep an eye out for your budget
3. Check if your internal processes are working

Comparing Bug Bounty Programs (Extract)



YesWeHack	Open Bug Bounty	HackerOne	Bugcrowd
yeswehack.com	openbugbounty.org	hackerone.com	bugcrowd.com
Founded 2015	Founded 2014	Founded 2012	Founded 2011
Paris, France	–	San Francisco, U.S.	San Francisco, U.S.
+30 projects	+1,500 projects	+1,700 projects	+300 projects
Commercial	Non-profit	Commercial	Commercial

Tips to set up a Bug Bounty Program

1. Be clear on what you want to achieve.
2. Have a dedicated team member manage the program, and validate the reports. Not every report is valid.
3. Don’t be surprised if you get reports from outside the program. Word will get around.
4. Don’t be surprised if the researchers do not always follow your rules. Sometimes it’s just their job.
5. Don’t be too nit-picking and stingy. Searching and researching is a lot of effort.

Thank you!

See more on cybersec.help

References: (1) Icons made by Freepik (2) Cover made by TheDigitalArtist