The PHP Stack's Supply Chain

Sebastian Bergmann
- **Sebastian** since 1978
- **Computers** since 1990
- **PHP** since 1998
- **Open Source** since 1998
- **PHPUnit** since 2000
- **thePHP.cc** since 2009
"The Settlers" (1993)

- 1 developer (Volker Wertich)
- ~70 KLOC (M68K Assembly)
- 0 external dependencies (educated guess)
Web Application (2023)

- Full Stack!
- But what is the full stack?
„I have ranted about the absurdity of the term "full stack engineer" (I mean, show me the web dev who also writes their own device drivers 😞) but I'd like to recant.

Annoying it may be, but it's the term we've got to describe the most significant shift in eng roles since devops.”

https://nitter.net/mipsytipsy/status/1659607267598307328
„What I want to see from people: Sure, I mainly do PHP, but if the house is on fire, I'll go fix it.

It doesn't matter if it's a kernel setting, an error in JavaScript, or if I have to call a service provider because their server is down.

I run off and learn what I need to solve the problem (or find help) along the way.”

Volker Dusch
Sorry for getting sidetracked ...
What could possibly go wrong?

- Hardware Bug with Security Implications
- Software Bug with Security Implications
- Software Feature with Security Implications
- Supply Chain Attack
April 2014
Heartbleed
https://heartbleed.com

March 2016
NPM package left-pad depublished
https://nitter.net/seldo/status/712414400808755200

October 2018
Malware in Python package colo(u)rama
https://bertusk.medium.com/b66b8a534a8

January 2018
Meltdown and Spectre
https://meltdownattack.com

January 2019
Remote Code Execution in apt
https://justi.cz/security/2019/01/22/apt-rce.html

January 2019
pear.php.net compromised
https://thephp.cc/articles/blast-from-the-past

June 2020
Signature Verification Bypass in fwupd
https://access.redhat.com/security/cve/cve-2020-10759

August 2020
Commits from umn.edu in Linux kernel repository
https://www.youtube.com/watch?v=wBjbfQjSZXw

March 2021
Malicious commits in PHP Git repository
https://news-web.php.net/php.internals/113838

April 2021
Supply Chain Attack on Composer
https://blog.sonarsource.com/php-supply-chain-attack-on-composer

December 2021
log4shell
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228

December 2021
"American Megatrans" sticker
https://www.servethehome.com/dude-dell-hpe-ami-american-megatrans
February 2022

Attack on KA-SAT modems

March 2022

Embedded Malicious Code in node-ipc
https://github.com/advisories/GHSA-97m3-w2cp-4xx6

March 2022

Supply Chain Attack on PEAR
https://blog.sonarsource.com/php-supply-chain-attack-on-pear

April 2022

Composer Command Injection Vulnerability

April 2022

Attack(s) using stolen GitHub OAuth tokens

May 2022

DDoS Attack on phar.phpunit.de
https://thephp.cc/presentations/ddos-attacks-on-open-source-infrastructure

May 2022

Fork of hautelook/phpass compromised

June 2022

Hertzbleed
https://www.hertzbleed.com

June 2022

Public Travis CI Logs (Still) Expose Users to Cyber Attacks
https://blog.aquasec.com/travis-ci-security

June 2022

OpenSSL Remote Memory Corruption
https://guidovranken.com/2022/06/27/notes-on-openssl-remote-memory-corruption/

July 2022

CuteBoi
https://cuteboi.info

July 2022

python-atomicwrites deleted and recreated
https://nitter.net/balloob/status/1545509863651811333
Developers submit unauthorized changes (A), compromise the source repository (B), or submit modified source code (C) to introduce vulnerabilities. The build process is compromised (D) or the resulting packages are compromised (G). If a developer uploads a modified package (F) or uses a compromised dependency (E), it can also lead to integrity issues. Finally, if an attacker compromises the package repository (H), vulnerabilities are introduced.

For more information, visit: https://slsa.dev/spec/v0.1/#supply-chain-threats
“TL;DR: Combining pull_request_target workflow trigger with an explicit checkout of an untrusted PR is a dangerous practice that may lead to repository compromise.”

https://securitylab.github.com/research/github-actions-preventing-pwn-requests
„I really need to pin github action versions.
A base dependency upgrade (ubuntu 20.04 security issue fix) caused a mess all across my CI supply chain today -.−”

https://nitter.net/Ocramius/status/1536625991098978304
Dear Provider,

We are reaching out to you as a provider of the Slic3r software utilized by us for running its business.

We are reaching out to you in response to the zero day log4j vulnerability the details are published by Apache: https://logging.apache.org/log4j/2.x/security.html

Please confirm whether the system provided by you to us is susceptible to the log4j vulnerability.

Please confirm which steps we are to take in order to protect its assets from possible attacks related to the software vulnerability.

Best regards / Cordialement.

https://nitter.net/alranel/status/1478383193787187201
„I have to tip my hat to $bigcorp whose software supply chain inventory is comprehensive enough to contact individual open source maintainers.”

https://nitter.net/dnlongen/status/1478737214179844100
supply chain inventory

software

https://nitter.net/dnlongen/status/1478737214179844100
U.S. Executive Order 14028

https://www.federalregister.gov/executive-order/14028
$ wget https://phar.phpunit.de/phpunit-10.3.0.phar

$ php phpunit-10.3.0.phar --sbom

<?xml version="1.0"?>
<bom xmlns="https://cyclonedx.org/schema/bom/1.4">
  <components>
    <component type="library">
      <group>phpunit</group>
      <name>phpunit</name>
      <version>10.3.0</version>
      <purl>pkg:composer/phpunit/phpunit@10.3.0</purl>
      <description>The PHP Unit Testing framework.</description>
      <licenses>
        <license>
          <id>BSD-3-Clause</id>
        </license>
      </licenses>
    </component>
    <component type="library">
      <group>myclabs</group>
      <name>deep-copy</name>
      <version>1.11.1</version>
      <purl>pkg:composer/myclabs/deep-copy@1.11.1</purl>
    </component>
  </components>
</bom>
<p>pkg:composer/phpunit/phpunit@10.3.0</p>

<p>pkg:composer/myclabs/deep-copy@1.11.1</p>
All modern digital infrastructure

A project some random person in Nebraska has been thanklessly maintaining since 2003

https://xkcd.com/2347
„Giving a GitHub project «stars» as a thank you is the «thoughts and prayers» of Open Source. If you really want to support an Open Source developer then give them money [...]. Stars don't put food on the table.”

https://nitter.net/crell/status/964524639857926145
„Sebastian, why do you contribute to Open Source?”
I get that question a lot.
I work on Open Source for over two decades now.
I should have stopped to do so long ago.
Because of parasitic corporations that exploit Open Source without giving back.
„Open Source» was the attempt to turn the free software movement into unpaid labor for capital.”

https://nitter.net/tante/status/1581903206069587968
„[B]eneficiary of open-source is incredibly keen on open-source continuing to provide them with huge benefits. And will pay for marketing for that, but not so much actually sponsoring developers.”

https://nitter.net/MrDanack/status/1547233934127366144
„Fortune 500 companies would very much like there to be an expectation that open source projects must do extra work of managing a community, so that there are backup maintainers waiting to take over.”

https://nitter.net/MrDanack/status/1547272884246257666
„Being a company and installing dependencies from public, free package indexes is like going to the library every day and checking out 50 books that are necessary to run your business. Getting mad when the library gives you the wrong book is a dick move.”

https://nitter.net/theavalkyrie/status/1567660615103123456
To establish the duties of the Director of the Cybersecurity and Infrastructure Security Agency regarding open source software security, and for other purposes.

IN THE SENATE OF THE UNITED STATES

SEPTEMBER 21, 2022

Mr. Peters (for himself and Mr. Portman) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

A BILL

To establish the duties of the Director of the Cybersecurity and Infrastructure Security Agency regarding open source software security, and for other purposes.
„This is likely going to create a real demand on OSS maintainers to step it up with regards to security. But it doesn't explain how it's going to help with that burden, if at all.”

https://nitter.net/di_codes/status/1574447938054410246
„The nine most terrifying words in the English language are: I'm from the Government, and I'm here to help.”

Ronald Reagan
EU Cyber Resilience Act

„If the [Cyber Resilience Act] is, in fact, implemented as written, it will have a chilling effect on open source software development as a global endeavour, with the net effect of undermining the EU’s own expressed goals for innovation, digital sovereignty, and future prosperity.”

Because of toxic users that threaten with violence when their change request is not implemented.
“(What feels like) a lifetime of maintaining open source projects has left me with some things to say about the haters. I'm not sure why. Trying to do a light take of it instead of getting mad, here is a post categorizing them.”

https://seld.be/notes/a-nomenclature-of-hate
Because of Distributed Denial of Service attacks on my project's infrastructure.
DDoS Attacks on Open Source Infrastructure
Sebastian Bergmann and Arne Blankerts

https://thephp.cc/presentations/ddos-attacks-on-open-source-infrastructure
But I fundamentally believe that infrastructure such as operating systems, programming languages, and development tools must be Open Source.
This is why I continue to work on Open Source.
https://thephp.cc
sebastian@thephp.cc
@sebastian@thephpcc.social
@sebastian@phpc.social
Image Credits

- https://www.amigapcb.org/
- https://slsa.dev/images/supply-chain-threats.svg
- https://commons.wikimedia.org/wiki/File:Seal_of_the_President_of_the_United_States.svg
- https://commons.wikimedia.org/wiki/File:European_Commission.svg