

From Vulnerability to Stability: Inside TYP03's Security Process

Elias Häußler

elias.haeussler@typo3.org

August 8, 2025



HI, I'M **ELIAS**.

❤️ **TYPO3** since 2017

💻 **Backend** Developer

🥷 **Security** Team Member



? ... **why** security matters

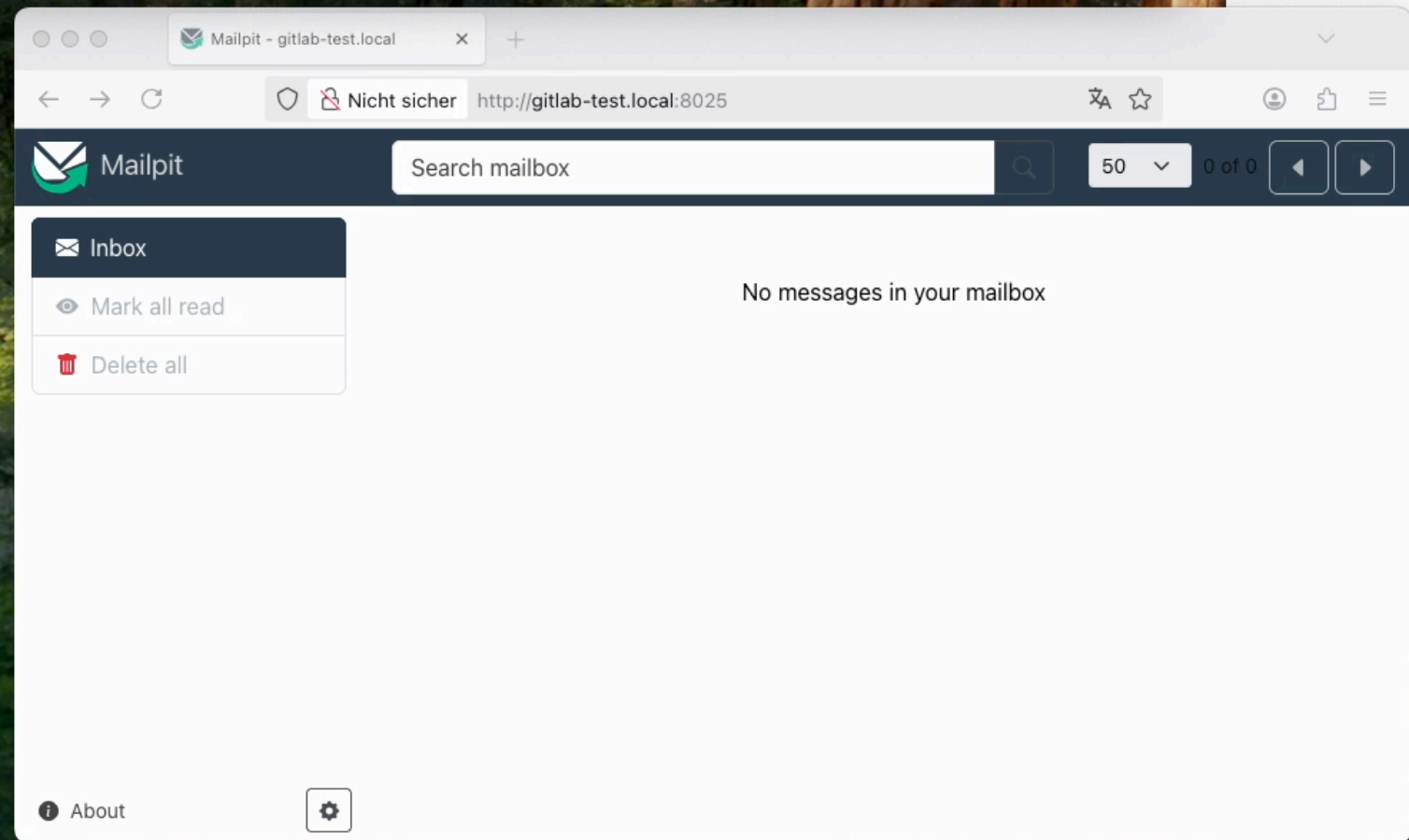
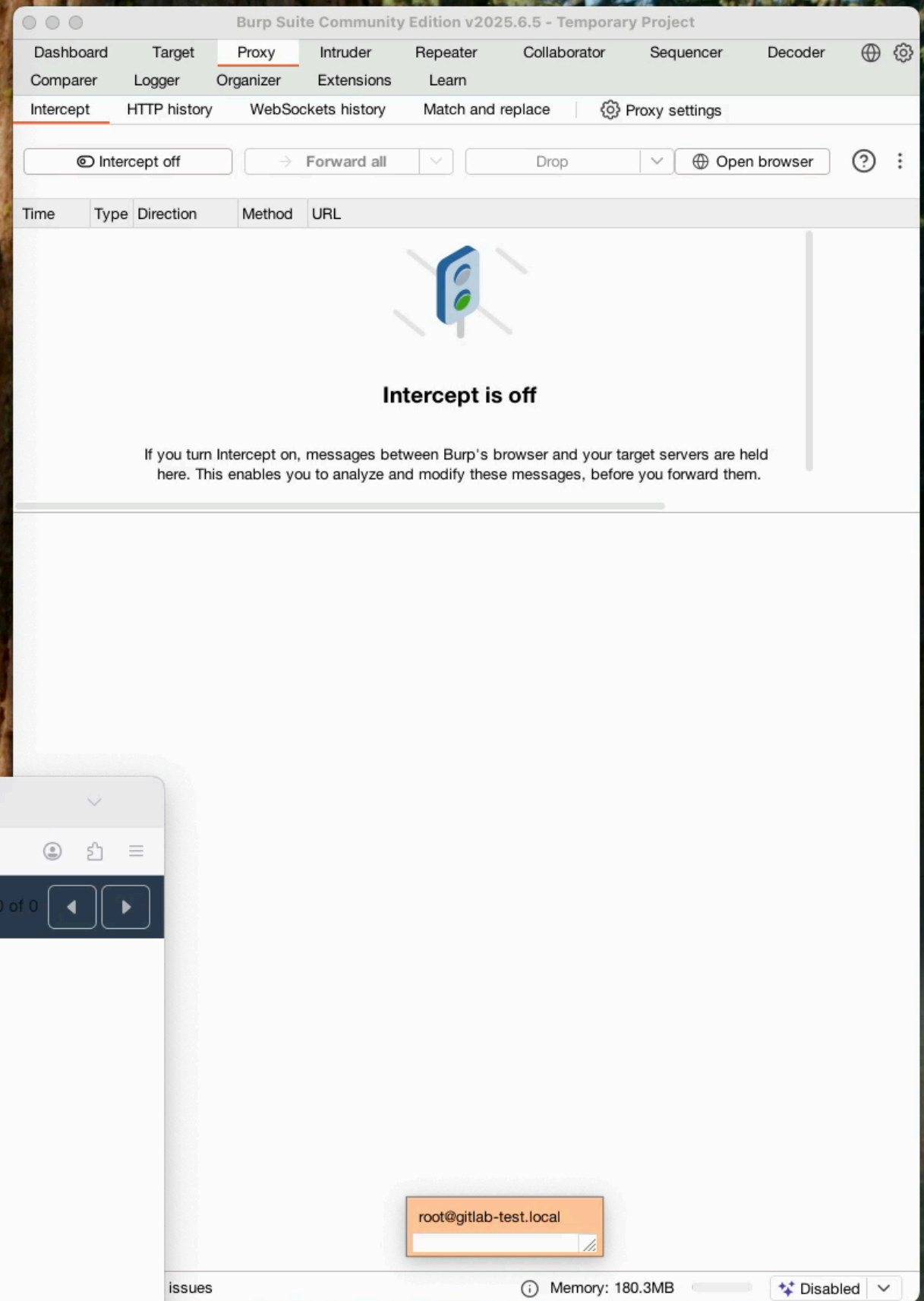
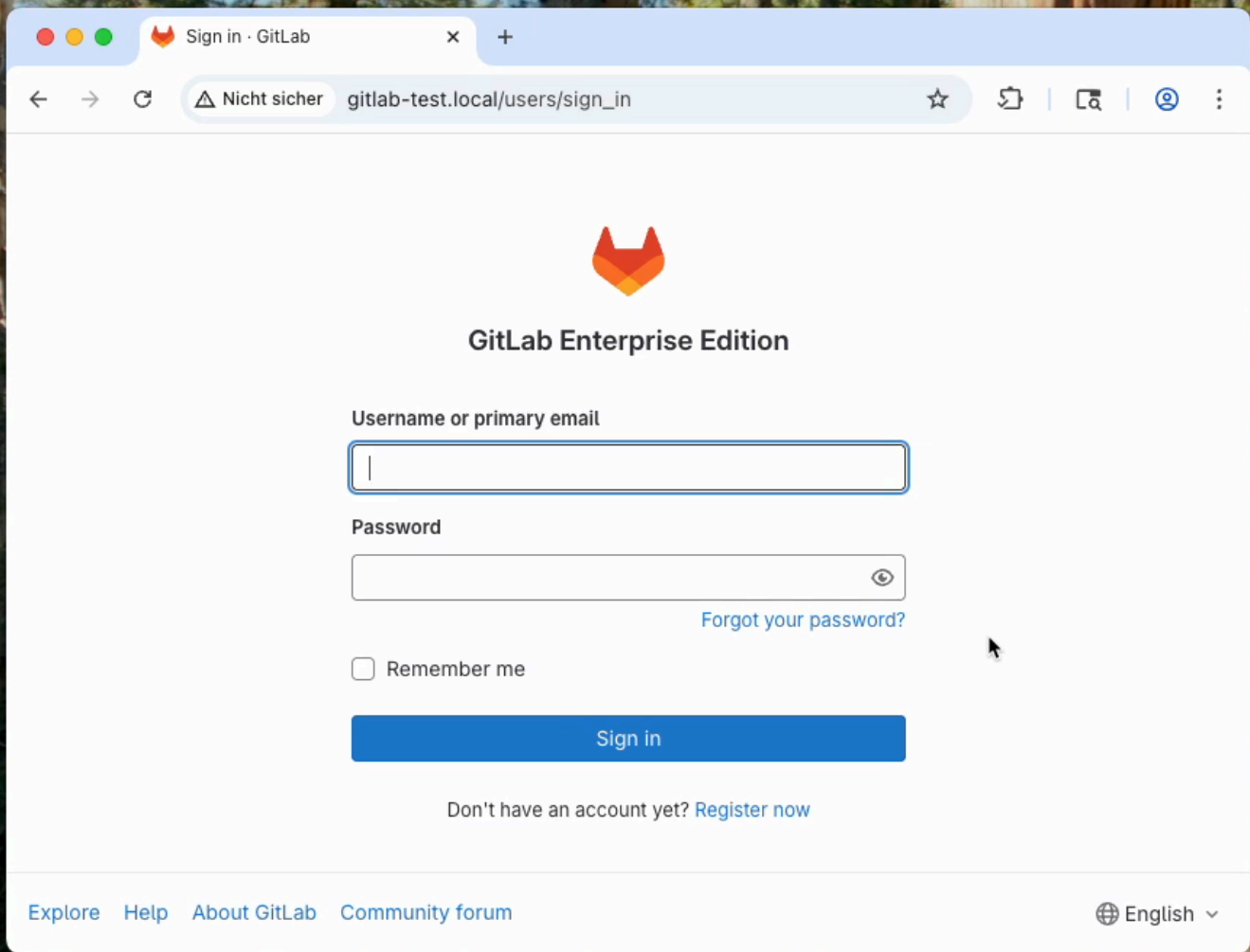
👤 ... **how** we keep TYPO3 secure

🧚 ... **what** we do to harden the „Future TYPO3“

💰 ... **you** (wait for it!)



WHY SECURITY MATTERS



CVE-2023-7028

Critical (10.0)

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N

Attack Vector (AV)

Network (AV:N)

Attack Complexity (AC)

Low (AC:L)

Privileges Required (PR)

None (PR:N)

User Interaction (UI)

None (UI:N)

Scope (S)

Changed (S:C)

Confidentiality Impact (C)

High (C:H)

Integrity Impact (I)

High (I:H)

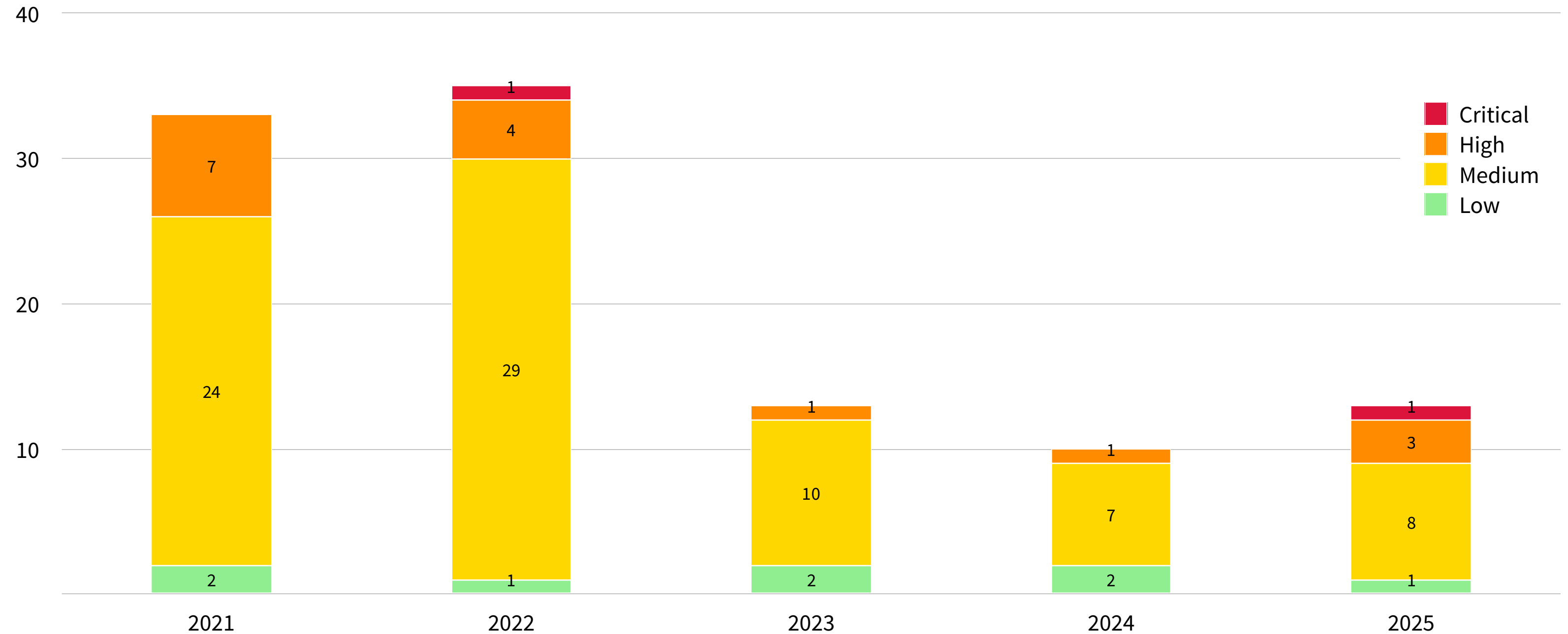
Availability Impact (A)

None (A:N)

 \$35k

Source: <https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?name=CVE-2023-7028&vector=AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N&version=3.1&source=GitLab%20Inc.>

? WHY SECURITY MATTERS – REPORTED VULNERABILITIES IN TYPO3 (PER YEAR)





HOW WE KEEP TYPO3 SECURE

VULNERABILITY?

✅ **Qualifying vulnerabilities**

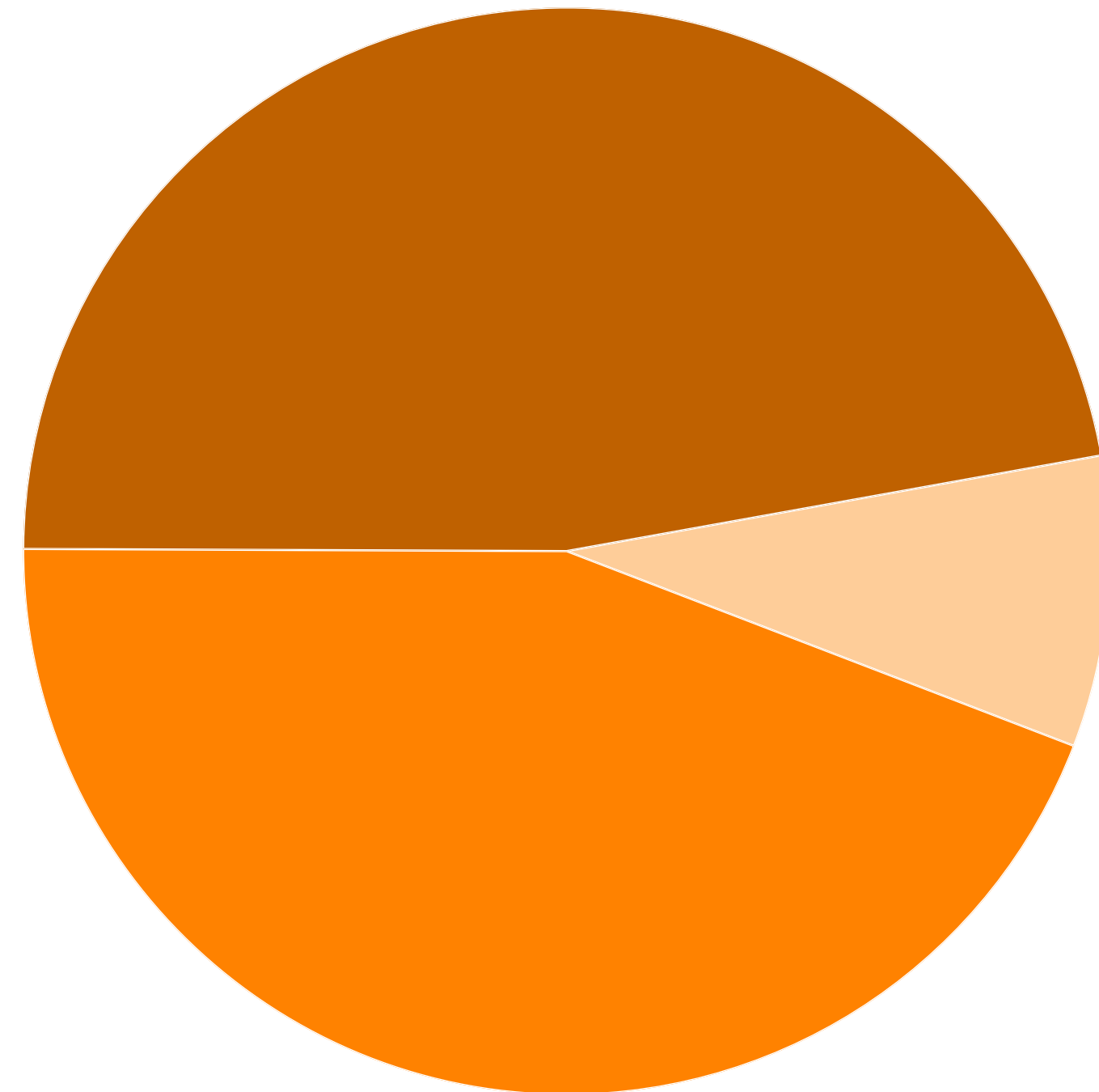
- SQL injection
- Cross-Site Scripting (XSS)
- Server-Side Request Forgery (SSRF)
- Cross-Site Request Forgery (CSRF)
- Insecure Direct Object Reference (IDOR)
- Authentication & Authorization Flaws
- (Sensitive) Information Disclosure
- *and more...*

❌ **Non-qualifying vulnerabilities**

- Third-party software with known vulnerabilities
- Install Tool & Maintenance Mode Flaws
- Debug configuration
- Wrapper Extensions (e.g. phpMyAdmin)
- Public code, issues & reviews
- Presence of banner or version information
- DoS attacks
- Open ports without real security impact
- Outdated libraries without a demonstrated security impact
- *and many more...*

Source: <https://typo3.org/community/teams/security/bug-bounty-program>

- **Core** ★★ ★
- **Extensions**
- **Infrastructure**
- ⚡ **Hacking Reports**
- 💣 **Zero-Day Exploits**



*Breakdown of resolved vulnerabilities,
categorized by scope (since 2021)*

STABILITY?

Never disclose
security vulnerabilities
to **public** channels!

~~Forge~~ ~~GitHub~~ ~~Slack~~
~~Social Media~~ ~~ChatGPT~~



Write an email to
security@typo3.org
instead. Please!

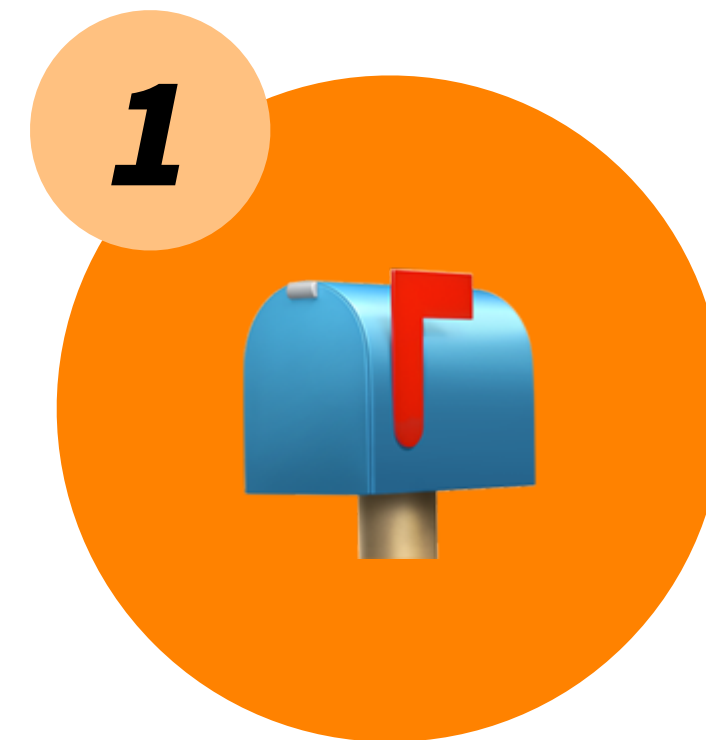
~~Forge~~ ~~GitHub~~ ~~Slack~~
~~Social Media~~ ~~ChatGPT~~



WHAT HAPPENS NEXT?

We receive your **vulnerability report.**

- TYPO3 enthusiasts
- Security researchers
- Extension maintainers
- TYPO3 Security Team members
- Public cybersecurity authorities (e.g. Swiss NCSC)



A team member performs an **initial analysis**.

- Triage
- Identify scope
- Reproduce vulnerability
- Validate qualification of report
- Consider impact of vulnerability



You'll receive an **answer** from us.

- We aim to *acknowledge* reports within 48 hours.
- We provide further responses concerning the *ongoing process* within 7 days.



CORE

EXT

INFRA

CORE

EXT

INFRA

CORE

We **discuss** the vulnerability impact.

- Create Forge ticket (internal)
- Involve selected people from the TYPO3 community („inner circle“)
- Check for related issues & vulnerabilities

4



CORE

The **Core Team** starts **developing** a security fix.

- Security Team supports
- Don't break things, ideally ⚠️
- Internal Gerrit & GitLab projects
- Established core contribution workflow applies



CORE

We check our calendars for a possible **release date**.

- LTS & ELTS backports must be finished
- Tuesday is release day in the TYPO3 world
- Avoid releases on bank holidays, if possible
- ~~Keep possible disclosure deadlines in mind~~ ⚠️



TYPO3 AS CVE NUMBERING AUTHORITY (CNA)

- 🛡️ Since 2019, TYPO3 requests and publishes a CVE for every single public vulnerability
- 🧩 ***Common Vulnerabilities and Exposures:***
Standardized way to publish vulnerabilities
- 🙅 Only authorized CNAs can publish CVEs
- 🏢 MITRE (USA) manages the CVE system

Scope

*„Vulnerabilities in TYP03 open-source products only, including **TYP03 CMS core** and **3rd party extensions** for TYP03, unless covered by the scope of another CNA.“*

Source: <https://www.cve.org/PartnerInformation/ListofPartners/partner/TYP03>

- 🕒 **Reserve** CVEs (for an upcoming disclosure)
- ✅ **Publish** CVEs (for TYPO3 core & extensions)
- ✍️ **Edit** own CVEs (after a security release)
- ⬆️ **Top-Level Root: MITRE**

CVE-2023-30451: Path Traversal Vulnerability (Authenticated)

December 25, 2023 🎄

In TYP03 11.5.24, the filelist component allows attackers (with access to the admin interface) to read arbitrary files via directory traversal via the baseuri field. This was demonstrated through:
POST /typo3/record/edit with ../../../../ and the parameter data[sys_file_storage]*[data][sDEF][\DEF][basePath][vDEF].

Uncoordinated public disclosure

Source: <https://packetstorm.news/files/id/176274>

CORE

A **security advisory** is drafted and reviewed.

- Reserve new CVE
- One CVE for each vulnerability
- Include associated CWE categories
- Team members review security advisories

7



CORE

The **core team** publishes the final **security release**.

- Upload patches to public project
- Write & publish release announcement
- Monitor public channels for possible regressions
- Security team publishes CVEs & security advisories

8



WHAT THE ... REGRESSIONS?!


YES!
REGRESSIONS CAN
NEVER BE RULED OUT.
HERE'S WHY...

TYPO3-CORE-SA-2021-013: Cross-Site Scripting via Rich-Text Content

- **Problem:** HtmlParser functionality vulnerable to XSS in RTE
- **Solution:** *typo3/html-sanitizer* package with explicitly allowed tags, attributes and values
- **Regressions:** Due to strict defaults (mostly edge cases)

TYPO3-CORE-SA-2025-014: Unrestricted File Upload in File Abstraction Layer

- **Problem:** Mismatch between file extension and MIME type
- **Solution:** MIME type consistency check and enforcement of allowed file extensions only
- **Regressions:** Due to different behaviors and missing standards


[GitLab.org](#) / [GitLab](#) / [Issues](#)

Open 24
Closed 1,538
All 1,562
New issue

🕒

Label is regression

✕

✕

🔍

Created date

⌵

📄

Commit status API returns 403 when latest pipeline for the commit is archived

Closed

👤

3

👍 1

✅ Complete

closed 4 weeks ago

#549184 · created 1 month ago by Manuel Grabowski

🔒 2

🔖 18.2

customer

devops

verify

group

ci platform

priority 2

regression

regression:17.10

section

ci

severity 2

type

bug

workflow

complete

📄

Vulnerability severity is sometimes not updated when advisories have a new severity assigned

Closed

👤

6

👍 4

🔗 1

✅ Complete

closed 1 month ago

#548960 · created 1 month ago by Brian Williams

🔖 18.2

bug

functional

customer

devops

security risk management

group

security insights

priority 2

regression

regression:17.9

section

sec

severity 3

type

bug

workflow

complete

📄

Container registry tags disappear after upgrading to 18.0.1 when using s3_v2 storage driver

Closed

👤

9

👍 4

✅ Complete

closed 1 month ago

#547084 · created 1 month ago by Adam Mulvany

🔖 18.1

Category:Container Registry

Object Storage

customer

devops

package

group

container registry

regression

regression:18.0

section

ci

severity 3

type

bug

workflow

complete

📄

When creating a new issue, can't paste an image into the Description in rich text editing mode

Closed

👤

2

✅ Complete

closed 1 month ago

#545934 · created 2 months ago by Richard Lloyd

🔖 18.1

Category:Text Editors

UX

automation:ml

bug

functional

customer

devops

plan

frontend

group

knowledge

priority 2

regression

regression:17.11

section

dev

severity 2

type

bug

workflow

complete

📄

/due quick action isn't working on work item creation

Closed

👤

5

✅ Complete

closed 2 months ago

#542291 · created 2 months ago by Amanda Rueda

🔒 2

🔖 18.1

On track

Product Planning

P1

backend

devops

plan

group

product planning

priority 2

regression

regression:18.0

section

dev

severity 2

suppress-contributor-links

type

bug

workflow

complete

CORE

You'll finally get paid –
here's your **bug bounty**.

- Critical: Up to 600 €
- High: Up to 300 €
- Medium: Up to 150 €
- Low: Up to 50 €

9



***Note:** We may grant higher or lower bug bounties,
based on the actual impact on the TYPO3 community.*

HOW DO YOU MEASURE THE SEVERITY OF A VULNERABILITY?

Common Vulnerability Scoring System

- We use the CVSS to calculate the severity of a known vulnerability.
- The severity level is a good first indicator for the possible security impact.
- Calculation is based on various metrics, targeting confidentiality, integrity & availability.

Severity levels

- 🐛 None (0.0)
- 👁️ Low ($\geq 0.1 < 4.0$)
- ⚡ Medium ($\geq 4.0 < 7.0$)
- 💣 High ($\geq 7.0 < 9.0$)
- 💥 Critical (≥ 9.0)

*We use version 4.0 of the CVSS
(version 3.1 until 06/2025).*

Metrics

- Attack Vector (AV)
- Attack Complexity (AC)
- Privileges Required (PR)
- User Interaction (UI)
- Scope (S)
- Confidentiality Impact (C)
- Integrity Impact (I)
- Availability Impact (A)

CORE

EXT

INFRA

EXTENSIONS

We contact the **extension author.**

- Issue details
- Reproduction steps
- Suggestions for possible fixes
- Reference to our security policy



EXTENSIONS

The extension author
pushes **security fixes**.

- Internal GitHub repository
- Two Security Team members review and test the provided fixes
- Reviews are based on the latest version



EXTENSIONS

We check our calendars for a possible **release date**.

- Tuesday is *the* day
- Try to combine multiple extension releases into one day
- Keep in close contact with extension author



EXTENSIONS

A **security advisory** is drafted and reviewed.

- Reserve new CVE
- One CVE for each vulnerability
- Include associated CWE categories
- Team members review security advisories

7



EXTENSIONS

Final security releases
and advisories are published.

- Extension author publishes releases
- We publish CVEs & security advisories
- Mark affected releases as insecure in TER
- Send announce mail & publish on social media

8



EXTENSIONS

You'll finally get paid –
here's your **bug bounty**.

- Critical: Up to 300 €
- High: Up to 150 €
- Medium: Up to 100 €
- Low: Ø



***Note:** We may grant higher or lower bug bounties,
based on the actual impact on the TYPO3 community.*

CORE

EXT

INFRA

INFERA

We **discuss** the vulnerability impact.

- Create Forge ticket (internal)
- Involve related teams, if necessary (e.g. Server Team or TYPO3 GmbH)
- Check for related issues & vulnerabilities

4



INFERA

The **responsible team(s)** start **fixing** the vulnerability.

- Security Team supports
- Depends on the affected service(s)
- Issues may have to be fixed upstream (e.g. when third-party software is used)

5



INFERA

Fixes are **deployed** to production, once finalized.

- Again: Depends on the service(s)
- Monitored services: *typo3.org*, *TER*, *Docs*, *My TYPO3*, *Gerrit*, *GitLab*, *SSO*, *Localization server*, *GitHub organizations*, ...

6



INFRA

In some cases,
we **publish a PSA.**

- **P**ublic **S**ervice **A**nnouncement
- Only for critical vulnerabilities and in some other cases (e.g. data breaches)
- In most cases, you won't notice that something happened

7



INFERA

You'll finally get paid –
here's your **bug bounty**.

- Critical: Up to 300 €
- High: Up to 150 €
- Medium: Up to 100 €
- Low: Ø

8



Note: We may grant higher or lower bug bounties,
based on the actual impact on the TYPO3 community.

Thank you
for keeping
TYP03 secure!





WHAT WE DO TO HARDEN THE „FUTURE TYPO3“

We're **planning** to integrate a **SAST** job in the TYPO3 workflow.



- **Static Application Security Testing**
- Code is analyzed for **insecure patterns** & known **vulnerabilities** (White-Box-Testing)
- Part of pre-merge CI pipeline (every patch) to establish a **Continuous Security** workflow

We're currently **trying out** various software **candidates**.

- Semgrep
- Opengrep
- Bearer






Scan details

Hide details

Download results ▾

All tools 

Status	Severity ↓	Description	Identifier	Report type	Activity
Needs Triage	High	Semgrep - javascript.lang.security.detect-insecure-websocket.detect-insecure-websocket in UriTest.php typo3/sysex/core/Tests/Unit/Http/UriTest.php:46	Semgrep - javascript.lang.security.detect-insecure-websocket.detect-insecure-websocket	SAST	
Needs Triage	High	Semgrep - php.lang.security.eval-use.eval-use in EmConfUtilityTest.php typo3/sysex/extensionmanager/Tests/Unit/Utility/EmConfUtilityTest.php:81	Semgrep - php.lang.security.eval-use.eval-use	SAST	
Needs Triage	High	Semgrep - php.lang.security.eval-use.eval-use in PersistenceManagerTest.php typo3/sysex/extbase/Tests/Unit/Persistence/Generic/PersistenceManagerTest.php:361	Semgrep - php.lang.security.eval-use.eval-use	SAST	

 Extended **code search** for extensions published in TER

 **AI-assisted analysis** for incoming vulnerability reports

 We're **experimenting** with
Software Bill of Materials (**SBOM**)

 We're planning to build
an integrated **security center**
for the TYPO3 backend (stay tuned!)

(No sneak preview, yet. Sorry! 😬)

 Increase **awareness** of TYPO3
in the security sector

 Organize **campaigns** like
Double Bug Bounties (2024)




LET'S TALK ABOUT YOU!

 TYPO3 is **evolving** more and more

 Every **contribution** is welcome

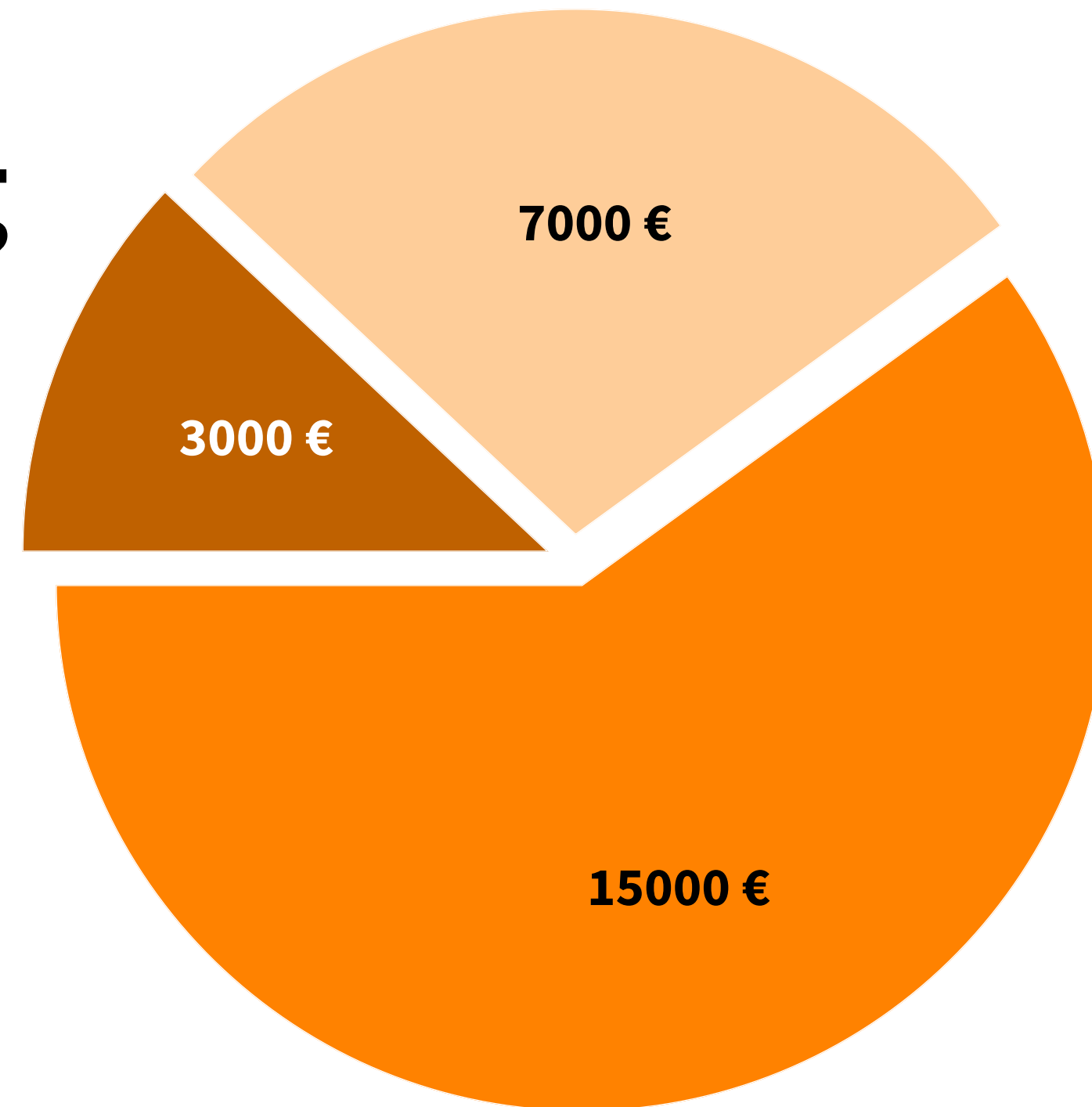
 We need more **community power**

 You're a true **superhero!**

 It's **worth** the effort (if you know, you know)

-  **Security Handling**
-  **Travel costs**
-  **Bug Bounty**

BOUNTY



WRITE TO
SECURITY@TYPO3.ORG
OR TALK TO US HERE AT
#T3DD25

Thank you!



@elias



@eliashaeussler



elias.haeussler@typo3.org

