Intigriti – Ethical Hacking & what we have learned

Jan Holesovsky

kendy@collabora.com

Collabora Online

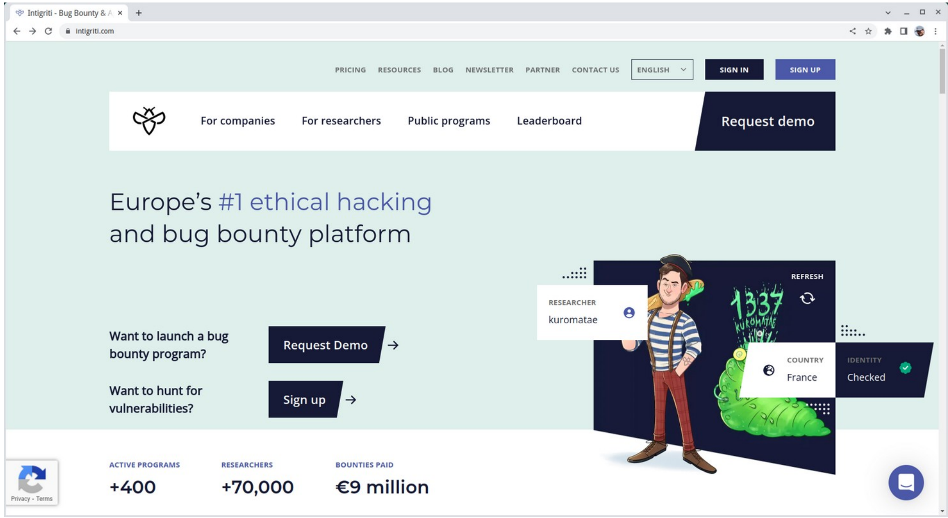
Technical Day

COOL days

LibreOffice Technology

What is Intigriti

- Ethical hacking & bug bounty platform
- We have got funding from the European Commission
  - Budget allocated for the bug bounty program
- Several calls with Intigriti
  - To set things up
  - Identify limits for various levels of bugs
  - Roll it out



Europe's #1 ethical hacking and bug bounty platform

Want to launch a bug bounty program?

Want to hunt for vulnerabilities?

RESEARCHER kuromatae

COUNTRY France

IDENTITY Checked

ACTIVE PROGRAMS +400

RESEARCHERS +70,000

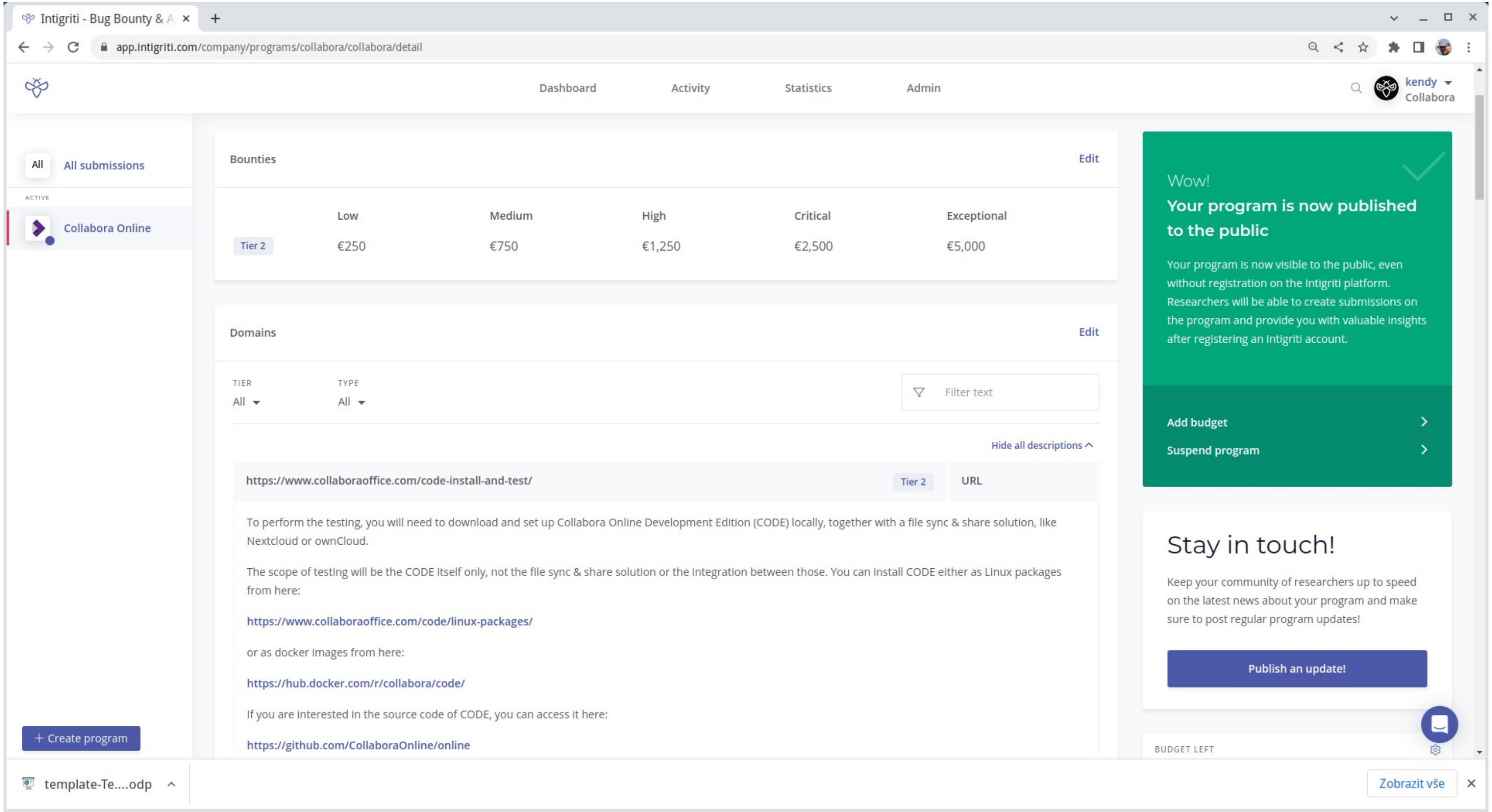
BOUNTIES PAID €9 million

Technical Day

COOL days

LibreOffice Technology

The Collabora Online setup



Intigriti - Bug Bounty & A

app.intigriti.com/company/programs/collabora/collabora/detail

Dashboard Activity Statistics Admin

kendy
Collabora

All All submissions

ACTIVE

Collabora Online

+ Create program

Bounties Edit

	Low	Medium	High	Critical	Exceptional
Tier 2	€250	€750	€1,250	€2,500	€5,000

Domains Edit

TIER All
TYPE All

Filter text

Hide all descriptions

https://www.collaboraoffice.com/code-install-and-test/ Tier 2 URL

To perform the testing, you will need to download and set up Collabora Online Development Edition (CODE) locally, together with a file sync & share solution, like Nextcloud or ownCloud.

The scope of testing will be the CODE itself only, not the file sync & share solution or the integration between those. You can install CODE either as Linux packages from here:

https://www.collaboraoffice.com/code/linux-packages/

or as docker images from here:

https://hub.docker.com/r/collabora/code/

If you are interested in the source code of CODE, you can access it here:

https://github.com/CollaboraOnline/online

Wow!

Your program is now published to the public

Your program is now visible to the public, even without registration on the Intigriti platform. Researchers will be able to create submissions on the program and provide you with valuable insights after registering an Intigriti account.

Add budget

Suspend program

Stay in touch!

Keep your community of researchers up to speed on the latest news about your program and make sure to post regular program updates!

Publish an update!

BUDGET LEFT

template-Te....odp

Zobrazit vše

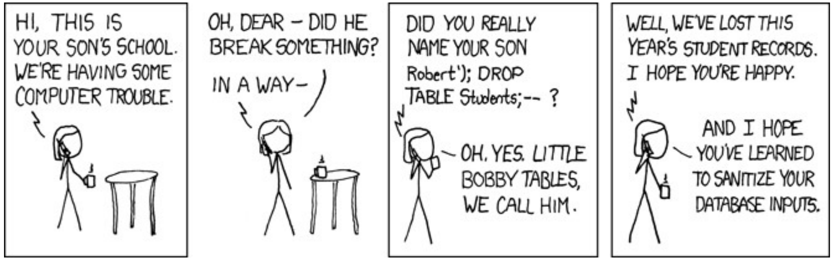
Collabora Online

And we started receiving reports...

- Good news: not a disaster in general!
    - No exceptional bug, only 2 critical ones
    - A bit of budget still left – no more finds
- But got a lot of good reports from the researchers
    - Most of them cross-site-scripting (XSS)
        - Allows the attacker to run their JS code
    - But other ones allowed including a file from the jail to the document
        - Luckily nothing really interesting in the jail though

Main lesson learned

- Always sanitize!
  - Sadly cannot go into details in the presentation – we don’t have CVE’s for all the bugs yet
  - But in most cases, the bugs included a series of events of the type “name the document this special way, and then when the admin visits page X, it can lead to XSS”; or “when a user inserts a specially crafted comment, and the other user does action Y, it can lead to XSS”
- Root of all evil: ‘innerHtml’
  - Try to avoid it
  - Or if you need that, sanitize carefully


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

Overall a very good experience

- Intigriti is great as a platform
- The researchers are very professional, describe the bugs carefully
    - Make them easy to reproduce
    - Communicate well and to the point when clarification is needed
- Intigriti does a lot of pre-screening
    - Checking the scope etc.
- Big thanks to European Commission for the funding!

Collabora Online

Technical Day

COOL days

LibreOffice Technology

Thank you!

By Jan Holesovsky

@CollaboraOffice
hello@collaboraoffice.com
www.collaboraoffice.com

T S P D