Securing open source software through crowdsourced security

The Background

The European Commission's Directorate General for Informatics (DG DIGIT)

The Directorate-General for Informatics (DIGIT) is the department responsible for providing digital services to support European Commission and EU institutions in their daily work.

The European Commission functions based on a set of values, some of which include diversity, openness and collaboration.

In January 2016, the European Commission launched the ISA2 Programme, which supports the development of digital solutions that enable public administrations, businesses and citizens in Europe to benefit from interoperable cross-border and cross-sector public services. The Programme supports a set of different actions to develop interoperability solutions.

One of these actions, called Sharing and Re-Use action (2016.13), was assigned to the Open Source Programme Office (OSPO). Under this action, the OSPO decided to use bug bounties as a means to secure open source software that it is widely used by public services.

DIGIT'S MISSION STATEMENT:

DIGIT'S MISSION IS TO DELIVER DIGITAL SERVICES TO ENABLE EU POLICIES AND TO SUPPORT THE COMMISSION'S INTERNAL ADMINISTRATION.

Source

The challenge

Help open source communities secure their software

The European Commission became aware of the criticality of open source software in 2014 when the Heartbleed vulnerability caused substantial losses and impact worldwide.

It was at this moment that the European Commission made a commitment to secure its open source software and help open source communities in securing their software. This effort continues in 2021 under the current action.

European Commission

CASE STUDY

Rationale using bug bounty programs with Intigriti

The European Commission considered that a bug bounty program was a good fit for their needs because of:

- **Access to talent**
  Bug bounty platforms enable businesses to approach an **already engaged community of ethical hackers around the world** who share a passion for security.

- **Cost efficiency**
  Compared to more traditional security testing channels, bug bounty programs allow organisations to **get results at a lower cost**, as they only pay for unique vulnerabilities found, rather than testing time.

- **Speed**
  The European Commission could **quickly engage** with ethical hackers around the globe through Intigriti's platform and start working on finding vulnerabilities immediately.

The solution

Secure three open source software using bug bounty services

As part of the Sharing and Re-use action (2016.31.), the Commission decided to use bug bounties, a form of crowdsourced security testing. Three bug bounty programs were launched on 11 January 2021 using the Intigriti bug bounty platform.

The selected software for the bug bounty program:

1. MOODLE
An eLearning platform widely used by public administrations and universities worldwide.

2. ZIMBRA
A popular email server solution that includes group calendars and document collaboration.

3. ELEMENT (MATRIX)
An instant messaging platform used by public services in France and Germany.

The bounties were funded by the Commission's ISA² programme but focused entirely on open-source software widely used by European Public Services.

Having a European focus, Intigriti shares the same values expressed by the European Commission.

European Commission

NUMBER EMPLOYEES
10,000+

INDUSTRY
Government administration

FOUNDED
1958

The results

Modernised security testing with immediate impact

In a matter of weeks, vulnerability reports were being submitted. In one software, three "critical" vulnerabilities were discovered. Additionally, at least one "high" vulnerability was found and disclosed for all three software projects.

Knowing these vulnerabilities meant the open source communities could quickly fix them via a patch; leading to more secure software.

When asked about their experience, Zimbra said:

- "Let's do this again! Participating in the European Commission's Bug Bounty Program was a worthy and valuable project for Zimbra. It was a great exercise for us, with mostly low to medium-security issues related to scripting and forgery that our vulnerability scanner had failed to catch, keeping us alert 24/7."

About their involvement, Moodle LMS (Learning Management System) Product Manager Sander Bangma said:

- "Security is of paramount importance to Moodle as the world's most customisable and trusted open source learning management system (LMS). Moodle's development practices include security by design and participation in the ISA bug bounty program has been a welcome addition to further enhance Moodle's security."

Regarding their experience on Intigriti's bug bounty platform, Matrix commented:

- "Intigriti provided excellent service by pre-triaging reports and ensuring that we only had to address validated submissions. Though most accepted issues were of low severity, we did receive a few higher severity reports too."

"

Bug bounty platforms align very well with open source software because what you have is a community of ethical hackers helping another community. It is collaboration at the highest level.

MIGUEL DÍEZ BLANCO
PROJECT LEAD OPEN SOURCE PROGRAMME OFFICE, AT DIGIT - EUROPEAN COMMISSION

TAKE YOUR FIRST STEPS

- Request a demo www.intigriti.com/demo
- Visit the website www.intigriti.com
- Get in touch hello@intigriti.com

- **50,000+ researchers**
- **400+ live bug bounty programs**
- **GDPR compliant**
- **Strong European presence**

INTIGRITI

Information from Q2/2022. We are constantly growing, so please contact our sales department or see our website for an accurate number.