eShard

Vulnerability research using the REVEN fuzzing platform

Internship

The eShard's REVEN reverse-engineering platform can integrate with a fuzzer such as AFL so as to triage and automatically analyze the fuzzer's output.

With this internship, your goal will be to implement one or several vulnerability search campaigns using REVEN's fuzzing platform.

This will include identifying and characterizing a target, implementing fuzzing, processing the fuzzer output and REVEN's outputs to triage crashes and establish root causes.

In the process, you will perform manual analysis when needed or develop new algorithms to analyze a trace automatically using the REVEN Python API. This work will also result in additional notebooks to disseminate new examples and capabilities to our users.

COMPANY

eShard is a technology company specializing in security testing: electronic chips, mobile applications, communicating objects, servers and desktops, for which there is both storage of personal data and exchange of information.

Our role is to provide our customers, designers or users of connected objects and systems with the means to control cyber risk and to ensure that they integrate the right level of protection: understand the threat, carry out automatic checks, obtain the knowledge of attacks.

To do this, we have assembled a team of specialists, researchers who are experts in cryptography, IC security and security of mobile applications, servers and desktops. We offer our customers a range of tools and services: SaaS platform, software, technical training and security testing service.

As part of the development of our activity, we are recruiting an intern in our System Security R&D team to work on this topic during a 5-month paid internship.

🗓️ **Desired start date:** February 2023.

📍 The position is based in **Pessac (33)**, next to Bordeaux.

Your day-to-day would be:

Directly attached to a member of the REVEN R&D team, you will be in charge of the following missions:

- Identify some targets and select which one will be studied first.
- Perform reverse engineering discovery work on the target to characterize the attack surface.
- Setup, configure and maintain the REVEN fuzzing platform with regard to the target under study.
- Analyze the results provided by the REVEN fuzzing platform and further:
    - Document the results (with a write-up for example).
    - Complete the results, using the Axion GUI or the REVEN Python API and third-party tools.
    - Propose UX and technical enhancements.
    - Enrich the automated analysis capabilities of the REVEN fuzzing platform.
- Collect information about state-of-the-art fuzzing and analysis techniques.

You're perfect for us, if...

- You are already proficient in reverse engineering, which is a passion of yours.
- You participated in CTFs or other contests and got significant results.
- Not mandatory but potentially aligned with the internship duration, you are preparing a master degree and are in your last year of study.
- You have developed a particular interest in:
    - Fuzzing
    - Reverse Engineering in the Windows environment
    - Root cause analysis
    - Development with Python
- You have some good knowledge of x86/x64 architectures, Assembly, C programming, IDA or Ghidra, WinDbg, and other tools.
- You are hacker minded, responsive and have the spirit of initiative.
- You demonstrate autonomy in your assignments.
- You demonstrate good interpersonal skills that will allow you to work as a team effectively.
- You have a good writing level in English.

Benefits

- ➔ Support from professionals in a cutting-edge and booming business sector.
- ➔ Dynamic work environment within a young and friendly team.
- ➔ High performance work equipment.
- ➔ Flexible working hours.
- ➔ Space dedicated to talent development.
- ➔ “Tickets restaurant” covered up to 50%
- ➔ Annual events, snacks and drinks

Interested?

Contact us by sending your resume to

intern@eshard.com