AimValley

CVE Test Automation
Student Assignment

AimValley is a world class engineering and innovation center that designs and builds networking solutions. We are based in Hilversum, with a strong presence in the USA and India. We started in 2003 as a spin-off from Lucent Technologies (a successor from the American company AT&T), that is why we have a strong background in telecommunication solutions and have build-up vast expertise in real-time processor techniques. Most of our design & development is done in-house.

Product development entails preparation of requirement documents, specification of system architecture, electronic development (block diagrams, board design, system certification, mechanical design), FPGA/ASIC development, software development, system verification and product/factory introduction. AimValley makes use of FPGAs to process high speed transmission functions. Real-time requirements are also key in our software development.

Our business is about people and our teams are dynamic, skilled and passionate about technique. Recruiting and training the right talent is an essential part of the AimValley DNA. We have over 80 employees of which 75% works as design expert in the R&D organization. All R&D employees have a college or university level education.

Utrechtseweg 38
1213 TV Hilversum
The Netherlands

phone +31 35 689 1900
working@aimvalley.com
www.aimvalley.com

AimValley

CVE Test Automation
Student Assignment

Project Introduction - CVE Test Automation

AimValley keeps track of the vulnerabilities in the systems they develop with a tool called BlackDuck. For a more complete view of the AimValley quality system regarding FOSS have a look at the FOSS white paper. During development we apply any patches that have a score above a certain level. After a the official release of the product we track issues and when releasing a new version of the software we include the necessary patches. Reproducing issues described in a CVE is often difficult and time consuming and in addition many of our systems have been customized to meet the customer's requirements. As a result the Board Support Packages differs from the one the vulnerability has been found on.

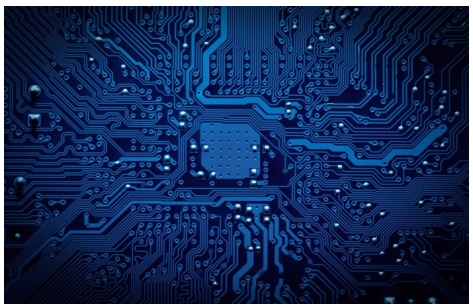
We want to investigate how to automatically reproduce a CVE on an embedded system in order to verify that a CVE is actually present in the system. Part of the investigation is to assess how many CVEs can be automatically reproduced if any at all.

Project Description

Investigate how to verify if a CVE is actually present in the described sources and then verify if the CVE is present in the custom sources. Automate the extraction of reported CVEs from BlackDuck for a project and run an automated test to verify the listed CVEs against the product.
The student needs to gather the exact requirements from the developers and devise an approach how to extract and run the automated tests and report the results. In addition a selection of a Pen test tool needs to be made.

Complexity

> Extracting the CVEs from BlackDuck
> Understanding the details of a CVE and finding proof whether a system is vulnerable or nor requires in-depth investigation and analysis of the FOSS components.
> Setup an environment to run the CVE verification tests and report if the CVE is present or fixed.



Keywords for this project	Affinity	Skills
> Python, REST API, Jenkins	> Security Testing	> Analytic Investigation
> Docker, PEN tests, Behave	> Scripting	> Independent & Communicative
> Linux, uBoot, C/C++	> Automation	> Competent in English

Are you a student with a can-do attitude and a passion for technology?
AimValley is your company!

Why not join us today: working@aimvalley.com

Utrechtseweg 38
1213 TV Hilversum
The Netherlands

phone +31 35 689 1900
working@aimvalley.com
www.aimvalley.com