Alessio Santoru

Curriculum Vitae

+39 3774399335
alessiosantoru@gmail.com
https://github.com/santoru
01-01-1994

Work Experience

November, 2019 – Present — **Product Security Engineer**, N26.

- Work closely to the software engineers to develop Secure by Design features, to Threat Model each of them and to perform security tests, uncovering and fixing application vulnerabilities, as well as logical vulnerabilities, before they hit production.
- Lead the periodical review of the mobile release from a Product Security standpoint, in order to deliver in time a secure mobile application on both Android and iOS platform.
- Implement and enroll a Security Champions training for company's engineers to cover different aspects: the security process that each release/deploy should follow, a focus on the Threat Model review process and the OWASP Top 10 standard, with two practical session for the Threat Model and Security Test of OWASP Top 10.
- Develop a micro-service with intended vulnerabilities that cover the OWASP Top 10 list to teach and train security champions on common risks and threats. The same service has been used as a challenge to assess candidates and their knowledge of computer security.

April, 2017 – October, 2019 — **Security Consultant**, Horizon Security.

- Analysis and assessment of multiple devices and appliances intended for business audience and enterprise environment like router, IoT devices, multifunction printers, laptops.
- Penetration test of Mobile Application for large projects and written with different technologies, like native mobile applications (Objective C/Swift and Java) or modern cross-platform technologies. The penetration tests involved also reverse engineering to access and control the internal of the application.
- Web application penetration test / vulnerability assessment for enterprise solutions and known frameworks as well as custom web application. The security tests involved different back-end languages like PHP, ASP, C#, Java and Python.
- Multiple experiences that involved working directly with enterprises and startup clients, in order to organize and plan a security assessment.
- Multiple experiences that involved working directly with vendors in order to resolve and disclose unknown vulnerabilities identified during the assessments.

October, 2016 – December, 2016 — **Internship**, CIPS Informatica.

- Server virtualization and fail-over clustering with high availability.
- Analysis of network and security appliances.

Education

2013–2016 — **Bachelor of Computer Science**, *Università degli Studi di Perugia*, Italy, Bitcoin address retrieval from the web.
Final mark: 110/110

2015–2016 — **Erasmus+ Student (Computer Science)**, *Politechnika Krakowska im. Tadeusza Kościuszki*, Poland.

2008–2013 **High School of Science and Technology**, *Liceo Scientifico Tecnologico*.

Achievements

CVE-2018-20122 **Remote code execution in Fastweb FASTgate router** The cgi binary exposed through the web interface fails to sanitize the user input leading to remote code execution.

CVE-2018-17172 **Command injection in Xerox Altalink's web application** The web application on Xerox AltaLink allows unauthenticated command injection that lead to remote code execution.

CVE-2018-7064 **Cross-site scripting (XSS) Reflected in Aruba Instant web interface**

CVE-2017-17663 **Buffer overflow in mini_httpd/thttpd** The htpasswd implementation of mini_httpd before v1.28 and of thttpd before v2.28 is affected by a buffer overflow that can be exploited remotely to perform code execution.

Certifications

2018 Offensive Security Certified Professional - OSCP

Languages

Italian **First language**

English **Intermediate - B2** *Professional working proficiency*

Public speaking

2017 **Real-time Auditing on macOS with OpenBSM** *University of Utah, MacAdmins Meeting*

Technical skills

OS Linux, macOS, Windows

Mobile Security iOS/Android Application security

Languages Python, Java, PHP, C, Go, Shell scripting

Technologies Docker, AWS

Relevant software BurpSuite, Nessus, sqlmap, nmap, netcat, Hopper disassembler, git

Other skills

Excellent knowledge of networking and security appliances

Excellent knowledge of vulnerabilities and most common threats, especially for web and mobile applications