DANIELE SCANU

ISTRUZIONE

Università degli studi di Torino
2016 - 2020
Laurea magistrale in Informatica presso l'Università degli studi di Torino. Votazione 106/110.

Università degli studi di Torino
2013 - 2016
Laurea triennale in Informatica presso l'Università degli studi di Torino. Votazione 102/110.

LINGUE

Inglese B1

CERTIFICAZIONI

eMAPT
Mobile Application Penetration Tester ottenuta con il corso offerto da eLearn Security

ESPERIENZE PROFESSIONALI

Soter IT Security S.r.l. – Co-Founder & Cybersecurity Specialist
2021 - presente
Co-fondatore e co-amministratore delegato di Soter IT Security S.r.l. svolgo principalmente attività di consulenza in ambito cybersecurity. Le principali attività svolte quotidianamente sono: Penetration Test e Vulnerability Assessment in ambito infrastrutturale, web, mobile e IoT. Attività di sviluppo software per utilizzo interno e attività di ricerca con l'obiettivo di trovare vulnerabilità ancora non note (0-day).

Certimeter S.r.l. – Cybersecurity Specialist
2018 - 2021
Consulente di sicurezza informatica presso Certimeter S.r.l. Ho svolto principalmente attività di Penetration Test e Vulnerability Assessment su infrastrutture informatiche, applicativi web e applicazioni mobile sia iOS che Android. Infine ho svolto attività di ricerca e sviluppo in ambito sicurezza informatica.

Exploitnetworking – Blogger
2018 - 2019
Ho scritto amatorialmente sul blog Exploitnetworking.com parlando principalmente di sicurezza, in particolare scrivendo writeup dei vari capture the flag online.

Università degli studi di Torino – Sviluppatore
2017 - 2018
Ho collaborato al progetto di ricerca "MIMOSA (MultIModal Ontology-driven query system for the heterogeneous data of a SmArtcity)" come borsista di ricerca con borsa dal titolo: "Progettazione e sviluppo di interfaccia "naturale" per il sistema OnToMap", con il ruolo di sviluppatore software, per l'aggiornamento del sistema sia nel back-end che front-end.
I lavori principali effettuati sulla piattaforma sono stati molteplici, tra cui la ristrutturazione del front-end della piattaforma utilizzando Vuejs come libreria, l'integrazione di nuove componenti tra cui le mappe
3D utilizzando la libreria Cesium e l'integrazione dei risultati di ricerca in luoghi fuori Torino. Mi sono inoltre occupato dell'aggiornamento del back-end con l'upgrade del framework Playframework
all'ultima versione disponibile.
Durante il periodo di borsa ho avuto modo di collaborare a due articoli per la conferenza "AVI 2018 International Conference on Advanced Visual Interfaces": "Map-based visualization of 2D/3D spatial data via stylization and tuning of information emphasis" e "Transparency-based information filtering on 2D/3D geographical maps".

Tuxmaniacs – Blogger
2014 - 2017
Ho scritto amatorialmente sul blog tuxmaniacs.it che parla dell'open source, Linux, elettronica, networking e sistemi embedded.

RICERCA

Di seguito la lista dei risultati ottenuti in seguito alle ricerche effettuate in campo cybersecurity:

- CVE-2023-5593: Local Privilege Escalation via Zyxel VPN Client (Out of Bound) (Reference: Mitre, Blog post Soter IT Security, Zyxel Advisory).
- CVE-2021-41243: Arbitrary File Write via Archive Extraction (Zip Slip) (Reference: Mitre, Snyk)
- CVE-2021-23340: Local File Inclusion on Pimcore (Reference: Mitre, Snyk)
- CVE-2021-23405: SQL Injection on Pimcore (Reference: Mitre, Snyk)
- CVE-2020-7759: SQL Injection on Pimcore (Reference: Mitre, Snyk)
- CVE-2019-10763: SQL Injection on Pimcore (Reference: Mitre, Snyk)
- CVE-2019-9693: SQL Injection on module ShowTime2 of CMS Made Simple (Reference Mitre)
- CVE-2019-9692: Remote Code Execution on module ShowTime2 of CMS (Reference Mitre, Exploit-db PoC)
- CVE-2019-16317: Remote Code Execution through wrapper phar on Pimcore (Reference: Mitre, Snyk)
- CVE-2019-16318: File Extention restriction bypass on Pimcore (Reference Mitre, Snyk)
- CVE-2019-10866: SQL Injection on Wordpress plugin Form Maker (Reference Mitre, Exploit-db PoC)
- CVE-2019-10867: Deserialization on CMS Pimcore (Reference Mitre, Snyk)
- CVE-2019-9061: Deserialization on module ModuleManager of CMS Made Simple (Reference Mitre)
- CVE-2019-9060: Unauthenticated Path Traversal on module CGExtensions of CMS Made Simple (Reference Mitre)
- CVE-2019-9059: Command Injection on core of CMS Made Simple (Reference Mitre)
- CVE-2019-9058: Deserialization on core of CMS Made Simple (Reference Mitre)
- CVE-2019-9057: Deserialization on module FilePicker of CMS Made Simple (Reference Mitre)

- CVE-2019-9056: Deserialization on module FrontEndUsers of CMS Made Simple (Reference Mitre)
- CVE-2019-9055: Deserialization on module DesignManager of CMS Made Simple (Reference Mitre, Metasploit Wrap-Up, Metasploit Module PoC)
- CVE-2019-9053: SQL Injection on CMS Made Simple (Reference Mitre, Exploit-db PoC)