

Alvise Rabitti

curriculum vitae

Informazioni personali

Nome Alvise Rabitti

Esperienza lavorativa

Periodo

2021-oggi

Responsabile per la sicurezza informatica di Ateneo

Datore di lavoro

Università Ca'Foscari - Venezia

Settore

Educazione / ricerca

Tipo di impiego

Lavoro dipendente

Principali mansioni e responsabilità

Supporto al CIO e al DPO, definizione e verifica dell'implementazione di policy di sicurezza e protezione dei dati, redazione di DPIA, pianificazione di attività di formazione, monitoraggio SIEM, gestione degli incidenti informatici, audit di sicurezza interni e su fornitori, penetration test, threat analysis e risk assessment.

Periodo

2018-2021

Specialista di sicurezza informatica, supporto alla ricerca

Datore di lavoro

Università Ca'Foscari - Venezia

Settore

Educazione / ricerca

Tipo di impiego

Lavoro dipendente

Principali mansioni e responsabilità

Audit di sicurezza interni, supporto a CIO e personale IT nelle decisioni legate alla sicurezza informatica, nella definizione di policy di accesso e nell'analisi di log, attività di vulnerability assessment, penetration test, threat analysis e risk assessment.

Gestione delle risorse IT che l'università mette a disposizione per i progetti di ricerca: individuazione di soluzioni tecniche e coordinamento dell'implementazione di tali soluzioni.

Periodo

2013-2018

Ricercatore in sicurezza informatica

Datore di lavoro

Università Ca'Foscari - Venezia

Settore

Educazione / ricerca

Tipo di impiego

Lavoro dipendente

Principali mansioni e responsabilità

Sviluppo di tool per collezionare e analizzare grandi moli di dati, prototipi per la ricerca automatizzata e semi-automatizzata di vulnerabilità, estensioni di browser e server per rinforzare la sicurezza di siti e sessioni.

Ricerca di vulnerabilità in siti e applicazioni e conseguente responsible disclosure (tra cui CVE-2017-11863 per responsible disclosure di vulnerabilità in Microsoft Edge).

Partecipazione e pubblicazione di lavori in alcune tra le più prestigiose conferenze mondiali di sicurezza informatica (USENIX, Computer and Communications Security, Security & Privacy) e in molte altre venue e riviste, tra cui Wired italiano e USA.

Periodo

2020

Datore di lavoro

Docente per il corso di Computer Science, SIE Foundation Year

Settore

Università Ca'Foscari - Venezia

Tipo di impiego

Educazione / ricerca

Contratto di insegnamento

Periodo

2002-2018

Tipo di impiego

Consulente IT

Principali mansioni e responsabilità

Libera professione

Progettazione, implementazione e gestione di infrastrutture di rete, server e web application per piccole e medie imprese.

Implementazione di reti private e pubbliche con vari livelli di accesso. Configurazione di firewall, VPN, sistemi di rilevamento delle intrusioni e policy dedicate.

Istruzione e formazione

Qualifica conseguita

2013

Nome e tipo di istituto di istruzione o formazione

Laurea in Informatica

Università Ca'Foscari - Venezia

Titolo della tesi

Towards formal verification of Liferay Role Based Access Control

Relatore

prof. Michele Bugliesi

Qualifica conseguita

1998

Nome e tipo di istituto di istruzione o formazione

Diploma di Maturità scientifica (Piano Nazionale Informatico), con voto 54/60

Liceo Scientifico G. B. Benedetti, Venezia

Capacità e competenze personali

Madrelingua

Altre lingue

inglese

francese

Capacità e competenze relazionali

Capacità e competenze organizzative

Capacità e competenze tecniche

italiano

Comprensione		Parlato		Scritto
Ascolto	Lettura	Interazione	Produzione orale	
C1	C1	C1	C1	C1
B1	B1	B1	B1	A2

Attitudine al lavoro in gruppo sviluppata attraverso l'attività di ricerca accademica e molti anni di scoutismo, nel ruolo prima di educatore di ragazzi tra i 16 ed i 21 anni e poi di coordinatore di adulti educatori.

Capacità di comunicare le problematiche relative alla sicurezza informatica sviluppata durante l'attività di consulenza.

Buona capacità di relazione con il pubblico.

Capacità organizzative, di coordinamento e gestione anche amministrativa di gruppi di persone.

Attitudine ad assumere responsabilità, a prendere decisioni e a risolvere conflitti interpersonali.

Buona esperienza nel gestire flussi di lavoro articolati all'interno di organizzazioni complesse.

Conoscenza approfondita della piattaforma web e delle sue problematiche di sicurezza.

Esperienza nella ricerca di vulnerabilità e nella *responsible disclosure* delle stesse.

Esperienza certificata in *penetration testing* con e senza l'utilizzo di framework (metasploit, ZAP, Burp).

Esperienza nella pianificazione e implementazione di configurazioni di sicurezza in firewall, Intrusion Prevention Systems, Intrusion Detection Systems.

Esperienza nella definizione di politiche di logging.

Esperienza certificata con *Security Event Management Systems* (SIEM), in particolare nella definizione di alert, dashboard e politiche di monitoraggio degli eventi.

Esperienza in interventi di *incident response*.

Esperienza nella gestione e prioritizzazione delle vulnerabilità informatiche.

Conoscenza approfondita dei protocolli di rete e dei relativi strumenti di analisi.

Conoscenze di crittografia applicata e dei principali protocolli crittografici.

Esperienza nel raccogliere ed analizzare grandi insiemi di dati.

Esperienza nella gestione di dati in ottemperanza al GDPR e con attenzione alle problematiche legate alla privacy.

Interventi a conferenze

Esperienza nella scrittura e nell'analisi di procedure legate alla sicurezza informatica.

Conoscenza approfondita dei sistemi Unix, GNU/Linux e Microsoft Windows.

Conoscenza dei seguenti linguaggi di programmazione: Python, Javascript, PHP, C.

Speaker a *ItaliaSec*, 2021 con l'intervento **Come Migliorare la Sicurezza Informatica della Supply Chain - La Nostra Esperienza**

Speaker a *Italian Conference on Cybersecurity (ITASEC)*, 2020 per il paper **A hard lesson: Assessing the HTTPS deployment of Italian university websites**

Presentatore a *Cyber Security Awards Europe (CSAW Europe)*, 2019 del paper **Postcards from the post-HTTP world: Amplification of HTTPS vulnerabilities in the web ecosystem**, vincendo il 3° premio nella categoria Applied Research

Speaker a *Formal Techniques for Distributed Systems (FORTE)*, 2019 per il paper **Semantically sound analysis of content security policies**

Speaker a *Italian Conference on Cybersecurity (ITASEC)*, 2018 per il paper **Dr Cookie and Mr Token – Web session implementations and how to live with them**

Atti di conferenze internazionali con revisione

The security lottery: measuring client-side web security inconsistencies con Stefano Calzavara, Sebastian Roth, Moritz Wilhelm e Ben Stock, in *USENIX Security Symposium*, 2022

A tale of two headers: A formal analysis of inconsistent click-jacking protection on the Web con Stefano Calzavara, Sebastian Roth, Michael Backs and Ben Stock, in *USENIX Security Symposium*, 2020.

A hard lesson: Assessing the HTTPS deployment of Italian university websites con Stefano Calzavara, Riccardo Focardi, e Lorenzo Soligo, in *Italian Conference on Cybersecurity (ITASEC)*, 2020

Testing for integrity flaws in web sessions, con Stefano Calzavara, Alessio Ragazzo e Michele Bugliesi, in *European Symposium On Research in Computer Security (ESORICS)*, 2019

Semantically sound analysis of content security policies, short paper con Stefano Calzavara e Michele Bugliesi, in *IFIP Joint International Conference on Formal Techniques for Distributed Systems (FORTE)*, 2019

Mitch: A machine learning approach to the black-box detection of CSRF vulnerabilities, con Stefano Calzavara, Mauro Conti, Riccardo Focardi, e Gabriele Tolomei, in *IEEE European Symposium on Security and Privacy (EuroS&P)*, 2019

Postcards from the post-HTTP world: Amplification of HTTPS vulnerabilities in the web ecosystem, con Stefano Calzavara, Riccardo Focardi, Matus Nemec and Marco Squarcina, in *IEEE Symposium on Security and Privacy (S&P)*, 2019. (ripreso anche da Wired ITA e USA)

Dr Cookie and Mr Token – Web session implementations and how to live with them, con S. Calzavara e M. Bugliesi. In *Italian Conference on Cybersecurity (ITASEC)*, 2018

CCSP: Controlled relaxation of content security policies by runtime policy composition, con S. Calzavara e M. Bugliesi. In *USENIX Security Symposium*, 2017

Content Security Policy: A Broken Promise?, con S. Calzavara e M. Bugliesi. Short paper per *Italian Conference on Cybersecurity (ITASEC)*, 2017

Content Security Problems? Evaluating the effectiveness of Content Security Policy in the wild, con S. Calzavara e M. Bugliesi. In *ACM Conference on Computer and Communication Security (CCS)*, 2016.

Static detection of collusion attacks in ARBAC-based workflow systems, con S. Calzavara, E. Steffinlongo e M. Bugliesi. In *IEEE Computer Security Foundations Symposium: 29th Symposium (CSF 2016)*. IEEE, 2016.

Compositional Typed Analysis of ARBAC Policies, con S. Calzavara e M. Bugliesi. In *IEEE Computer Security Foundations Symposium: 28th Symposium (CSF 2015)*, pagine 33-45. IEEE, 2015.

Formal verification of Liferay RBAC, con S. Calzavara e M. Bugliesi. In *Engineering Secure Software and Systems: 7th International Symposium (ESSoS 2015)*, volume 8978 of *Lecture Notes in Computer Science*, pagine 1-16. Springer, 2015.

Pubblicazioni su rivista

Measuring web session security at scale con Stefano Calzavara, Hugo Jonker, Benjamin Krumnow, in *Computers & Security (CoSe)*, 2021

Machine learning for web vulnerability detection: the case of cross-site request forgery con Stefano Calzavara, Mauro Conti, Riccardo Focardi e Gabriele Tolomei, in *IEEE Security & Privacy Magazine*, 2020

Sub-session hijacking on the Web: root causes and prevention, con S. Calzavara e M. Bugliesi, in *Journal of Computer Security (JCS)*, 2018

Semantics-based analysis of Content Security Policy deployment, con S. Calzavara e M. Bugliesi, in *ACM Transactions on the Web (TWEB)*, 2018

Capitoli di libri

Cryptographic Web Applications: from Security Engineering to Formal Analysis con Michele Bugliesi e Stefano Calzavara, in *Handbook of Formal Analysis and Verification in Cryptography*, Taylor & Francis / CRC Press, 2023

Certificazioni

Offensive Security Defense Analyst (OSDA) conseguita il 21 ottobre 2023 (id: OSDA-8887)

Offensive Security Certified Professional (OSCP) conseguita il 4 ottobre 2021 (id: OS-101-55005)

Ulteriori informazioni

Docente per Cyberchallenge (sede di Venezia), la principale iniziativa italiana di formazione per la sicurezza informatica, <https://cyberchallenge.it>

Co-relatore delle tesi di laurea triennale: "Mitch+: un web crawler per la rivelazione di vulnerabilità CSRF", "Analisi e diffusione di vulnerabilità crittografiche nel Web", "Outlier Analysis for Intrusion Detection Systems".

Co-assegnatario di CVE-2017-11863 per vulnerabilità in Microsoft Edge

3° classificato al Cyber Security Award Europe 2019, categoria Applied Research, con il paper "Postcards from the post-HTTP world: Amplification of HTTPS vulnerabilities in the web ecosystem"

Membro del comitato di programma per la conferenza di sicurezza informatica SECURWARE dal 2020

Revisore di articoli accademici sulla sicurezza informatica per le riviste peer-reviewed Symmetry (MDPI), Information (MDPI), Applied Sciences (MDPI), Electronics (MDPI), Future Internet (MDPI) e Computer Modeling in Engineering & Sciences (TSP)

Il sottoscritto Alvisè Rabitti, ai sensi del DLgs. 196/03 e dell'art.13 del GDPR (Regolamento UE 2016/679), esprime il consenso al trattamento dei dati presenti nel proprio Curriculum Vitae per fini di selezione del personale.

Alvisè Rabitti

