Joshua Alexander Rogers

Nationality: Australian, Polish | **Phone number:** (+48) 728567782 (Mobile) | **Email address:** joshua@joshua.hu | **Website:** https://joshua.hu/ | **LinkedIn:** https://www.linkedin.com/in/joshua-alexander-rogers/ | **GitHub:** https://github.com/MegaManSec/

ABOUT ME

Nearly 15 years in security, and still having fun.

Interested in breaking things in new ways, taking advantage of things in unforeseen ways, and building things with unexpected components.

Track record of high quality results by my own accord, anywhere and anytime in the world. At first, security seemed like just a technology issue; these days, I also see it as a social issue.

I want to be part of something that I believe in, where success not only depends on me, but for which failure I am also accountable for.

WORK EXPERIENCE

01/03/2021 – 01/03/2024 Wrocław, Poland

SECURITY ENGINEER OPERA SOFTWARE

- Conducted penetration tests of Opera's desktop, mobile, and web applications.
- Conducted security assessments of IT infrastructure and network devices.
- Researched and applied new attack vectors, threats, and technologies to various internal and external Opera products.
- Independently discovered and responded to novel threats against Opera software, systems, employees, and other liabilities,
- Evaluated and compared various security tools and frameworks that helped to improve security procedures, threat intelligence and workflow automation of various departments within the company.
- Helped maintain both public and private bug bounty programs, including interacting with researchers (triaging, responses, and awarding bounties) as well as internal stakeholders (assessing triaged reports, liaising with affected teams, confirming fixes).
- Spread security knowledge internally through workshops, training sessions, and meetups, and occasionally participated in public/community security activities.
- Wrote and published various public articles about activities conducted within the security team.
- Developed internal and public security tooling for attack-surface management and automatic exploitation techniques.
- Performed various APT-style full-company compromises.
- Liaised with executive management, communicating previously unidentified risks requiring immediate attention. Also collaborated with legal, conveying policy shortcomings and tangible consequences of inaction.
- Spear-headed a total re-architecture of the central global infrastructure and network systems within the company with an emphasis on security, with immediate critical and urgent Executive Management and Board of Director backing and endorsement.
- Planned, initiated, and executed the creation of disaster recovery and incident response for all major technical teams within the company.
- Designed, developed, and deployed novel software to solve internal security problems.
- Led multiple small (3-4) teams of interns and FTEs to perform security reviews against products and services.
- Kept up with current trends and the threat landscape, identifying areas for concern internally before they became real incidents.
- Lead incident response for compromised employees and compromised systems.
- Prepared and created roadmaps for the security team.

09/2020 – 01/03/2021 Wrocław, Poland

PENETRATION TESTER OPERA SOFTWARE

- Conducted penetration tests and security assessments of Opera's muli-million DAU products, identifying security flaws in projects written in Pike, PHP, Java, Javascript, Python, C, C++, Perl, and Go. Independently fixed vulnerabilities in unmtainined projects as seen necessary.

- Performed secure design reviews of critical internal tooling.
- Performed penetration tests of opensource and enterprise software used internally.
- Evaluated Opera's systems for privacy violations (related to GDPR and NDPR) and other related consumer security value concerns.
- Produced internal reports and presentations, and showcased the results of my security assessments to multiple developmental teams within Opera.
- Maintained and ran parts of the Opera Bug Bounty, including triage, validation, communication with researchers and internal stakeholders, and payment distribution and deliberation.
- Performed penetration tests of the open source software in order to better understand the risks associated with similar, internal Opera software.
- Published security-focused software within the open-source world, and liaised with other security professionals within that community.
- Developed a framework for fuzzing internally-used open-source software, which was used to identify new vulnerabilities in open-source software used by Opera.
- Attended various security conferences and traveled to international regional offices to liaise with teams, perform trainings, and give presentations.
- Contributed to open source projects in the form of added functionality as well as security and bug fixes.

2013 – 2020 Melbourne, Australia

INDEPENDENT SECURITY RESEARCHER SELF-EMPLOYED

- Identified various vulnerabilities in forum software such as vBulletin and MyBB. See https://seclists.org/fulldisclosure/2015/Aug/58 and https://community.mybb.com/thread-136703.html.
- Provided security patches for various OSS such as bind, gnupg, and php. CVEs include: CVE-2014-9157, CVE-2014-8625, CVE-2012-5667, CVE-2015-1351, CVE-2013-6129, CVE-2014-9425, CVE-2014-9496, CVE-2015-1352, CVE-2014-9756, CVE-2014-9426, CVE-2014-8504, CVE-2012-6667, and there's definitely more.
- Identified a multitude of vulnerabilities, ranging from SQL injections, to XSS' to broken access controls, in various paid and free vBulletin 'plugins' for example in plugins such as 'vBshout', 'vBShop', and 'vBSEO'.
- Coordinated with various bug bounties and was recognized by fortune-500 companies such as PayPal, Facebook, eBay, and Google. See https://securityaffairs.com/27368/hacking/paypal-two-factor-authentication.html https://seclists.org/fulldisclosure/2014/May/124 https://seclists.org/fulldisclosure/2014/Aug/7 http://www.xsses.com/2016/02/facebook-skype-to-email-leak-worth-3000.html and a lot more online by Googling "MegaManSec", "internot.info", or my name plus "vulnerability" or "bug". Most of my findings were documented on the now-defunct OSVDB, but some more important ones have been saved https://packetstormsecurity.com/files/author/10273/
- Made national news a few times: https://www.abc.net.au/news/2014-01-08/schoolboy-exposes-security-flaw-in-public-transport-victoria27/5190536 and https://www.smh.com.au/technology/australian-teen-uncovers-security-flaw-in-paypal-20140814-1044cx.html

2010 – 2016 Melbourne, Australia

SYSTEMS ADMINISTRATOR / FORUM ADMINISTRATOR SELF-EMPLOYED

- Linux Sysadmin working with on Ubuntu and Debian servers.
- Head Administrator of a 25,000-user forum dedicated to hacking, glitching/bug-abusing, and gaming.
- Developed custom addons for the vBulletin forum software.
- Created custom defenses against external attackers and internal threats.
- Working with KVM, LAMP, sql (postgres and mysql) mailing servers, networking, monitoring, and security defences.
- Innovative backup and firewalling techniques, multi-server systems, and so on.

01/03/2018 – CURRENT Krakow, Poland

RECEPTIONIST & BARTENDER & EVENTS COORDINATOR THE LITTLE HAVANA PARTY HOSTEL

- Welcoming guests into the property, responding to emails, socializing with guests, and providing up-to-date tourism information to ensure the best possible experience.
- Data-entry and identifying any quality assurance issues with respect to reservation information and payments.
- Marketing, sales, and planning, of tours supplied by partner tourism organizations.
- Liaison and regular communication with third-party providers to ensure consistent information for customers.
- Leading large groups of people (100+) as an events leaders and resolving situations appropriately as they arose.
- Bartending, including pouring drinks, handling cash and card payments, stock-take, cleaning, and general upkeep.
- Training new staff members and introducing junior staff members to various systems.

2013 – 2018 Melbourne, Australia

SALES AND REPAIR SELF-EMPLOYED

- Attaining $2.5K per month in sales of retro video games.
- Buying and selling second-hand retro video games from a range of suppliers.
- Servicing, repairing, and refurbishing of consoles, games, and peripherals.

- Shipping products both domestically and internationally in a secure manner to avoid physical damage via transport.
- Keeping up-to-date with current trends and prices of popular retro gaming systems to forecast profitable acquisitions.
- Constantly communicating with suppliers and clients.
- Introduced automation to achieve higher profits than other stores.

EDUCATION AND TRAINING

Melbourne, Australia
BACHELOR OF SCIENCE Swinburne University of Technology

Field of study Applied Mathematics | **Final grade** 3.31

Melbourne, Australia
BACHELOR OF ARTS Swinburne University of Technology

Field of study Cinema Studies | **Final grade** 3.31

2024
CERTIFIED INFORMATION SECURITY MANAGER (CISM) ISACA

2024
CERTIFIED INFORMATION SYSTEMS AUDITOR (CISA) ISACA

LANGUAGE SKILLS

Mother tongue(s): **ENGLISH**

Other language(s):

	UNDERSTANDING		SPEAKING		WRITING
	Listening	Reading	Spoken production	Spoken interaction	
POLISH	B1	B1	B1	B1	B1
RUSSIAN	A1	A2	A1	A1	A1

Levels: A1 and A2: Basic user; B1 and B2: Independent user; C1 and C2: Proficient user

PROJECTS

SSH-Snake

A self-propagating, self-replicating, file-less script that automates the post-exploitation task of SSH private key and host discovery.

Link https://github.com/MegaManSec/SSH-Snake

PikeProof

A Wycheproof implementation in the Pike scripting language.

Link https://github.com/operasoftware/nettle-wycheproof-testsuite

Squid Caching Proxy Security Audit

55 vulnerabilities and 35 0days when published.

Link https://megamansec.github.io/Squid-Security-Audit/

GTFOArgs

A curated list of programs and their associated arguments that can be exploited to gain privileged access or execute arbitrary commands, using argument injection.

Link https://gtfoargs.github.io/

Privoxy Security Audit

An audit of the Privoxy HTTP caching proxy.

https://blogs.opera.com/security/2021/05/fuzzing-http-proxies-privoxy-part-1/
https://blogs.opera.com/security/2021/10/fuzzing-http-proxies-squid-part-2/
https://blogs.opera.com/security/2022/01/fuzzing-http-proxies-privoxy-part-3/

Game Lost

An Analysis of Video Game Preservation in the Digital Age.

Link https://joshua.hu/files/GameLost.pdf

Digital Heritage Research

I have worked with various projects preserving the digital heritage of video games and looking at their histories from regions such as Australia, Africa, and Eastern Europe.
My work has been picked up by larger publications a few times, and I have presented my research on various platforms, including at the PAX Australia 2016 convention, and PAX Online 2020.

Link https://www.youtube.com/watch?v=kh1drqSLzPM

11/2020 – 02/2021

Simplified Functional Forms of Greenhouse Gases and CO2 Equivalence

I took part in a supervised 6-week mathematics research scholarship, investigating how different mathematical functional forms can be used to approximate Carbon Dioxide emissions when compared to Methane.

During this time, I:
- Independently researched and studied current literature on emission equivalences of different greenhouse gases.
- Employed mathematical analysis to improve the understanding of greenhouse gas equivalences.
- Modelled simplified functional forms to allow for approximation of equivalences between different greenhouse gases such as carbon dioxide, methane, and nitrous oxide.
- Wrote a 15-page research paper to be published by the Australian Mathematical Sciences Institute.
- Represented Swinburne University during a 20-minute presentation over a 3-day conference, showcasing my research.

Link https://joshua.hu/files/VRS_Mathematics_Report.pdf