Jason Magic

{"Cyber Security", "Ethical Hacker", "Bounty Hunter"};

Melbourne, Victoria

https://ret2eax.github.io jason.magic@outlook.com (+61) 0420-456-620

Jason Magic ret2eax openbugbounty h1 CTF Time Hall of Fame CVE

With a keen interest in information security from the age of 15, I have since had a devoted passion for Cyber Security. At the age of 19, my passion led to enlisting in public bug bounty programs as well as freelance work prior to commercial experience, primarily focusing on offensive application security.

SKILLS

Information Security

vulnerability assessment
security audits
threat modeling
risk analysis
isolation
risk controls

Penetration Testing

web
api
internal/external infrastructure
mobile
restricted soe's
application security
thick clients

Digital Forensics

host-based
network-based

WORK EXPERIENCE (4)

Security Consultant at HackLabs Pty Ltd

July 2018 - Current

https://www.hacklabs.com

Consultancy towards various clients pertaining to offensive security.

- Conduct pre-sale meetings to determine client expectations, requirements and focus attention to desired abuse cases derived by the client,
- Assist in project scoping and conduct client meetings before, during, and after service delivery,
- Simulate a real-world cyber attack against any developed environment (infrastructure, application, mobile, restricted SOEs, multimedia assets etc,
- Perform objective-based engagements through unconventional techniques to emulate apex threat actors,
- Conduct engagements through attack realism and stealth tradecraft to ensure client remediations and cyber defence use cases are built from relevant and realworld tactics, techniques and procedures
- Predominantly manually executed to explore attack paths tailored in context of the targeted environment,
- Focused on complete asset take over, identification and risk assessment pertaining to leverageable vulnerabilities, integrated security controls, misconfigurations and overall implementation.

Offensive Security Consultant at The Missing Link

January 2018 - July 2018

http://www.themissinglink.com.au/solutions/security

My duties as a Security Consultant at The Missing Link was to engage in offensive security projects with the primary motive of vulnerability identification, of which, is a precursor to reducing the targeted system's attack surface area.

- Conduct offensive security operations and assessments across mobile, web, network infrastructure assets, as well as, web, API and thick client applications,
- Conduct vulnerability assessments across a plethora of systems,
- Compile exploits and proof of concepts pertaining to identified security bugs,
- Compile recommendations and patches regarding identified issues,
- Liaise with the vendor and non-technical staff,
- Deliver documentation.

Cyber Attack & Response at Deloitte Australia

March 2017 - January 2018

http://cyberintelligencecentre.com.au

As part of the Cyber Attack and Response team associated with Deloitte's Cyber Intelligence Centre. It was my duty to conduct technical penetration testing strategies against client targets within a pre-determined scope either to obtain an objective or perform an assessment.

- Conduct objective-based penetration tests, vulnerability assessments, and engage in red team operations across mobile, web, computer systems, network infrastructures and applications,
- Perform security reviews of application designs, source code and deployments,
- Compile proof of concepts and exploitation scripts pertaining to identified security bugs,
- Perform incident response to breached clientele (i.e. source code audits for backdoors etc.),
- Research, document and discuss security related findings.

Bounty Hunter at HackerOne, OpenBugBounty, Freelance

August 2016 - March 2017

https://secure.sony.net/hallofthanks

As a bug bounty hunter, I identified & aided in vulnerability mitigation within a multiplex of web applications under responsible disclosure (indexed and non-indexed programs). This included applications pertaining to the following entities:

- SEA Police, US Dept. of Defence, US Army, US Navy, US Air Force, NATO, NASA, Asia-Pacific Space Cooperation Organization (APSCO), ASD Signals Intelligence Agency, Eskom (electricity public utility), Uber, Australian Securities Exchange (ASX), Cisco, Paypal, Mastercard, Sophos, HackerOne, Juniper Networks, Sony, Universal Studios, Vodacom, Vodafone, Optus, Standard Bank, Woodside Energy, Fedex, Murdoch, UWA, ASU, UCLA, Brandeis, Otago University, University of Auckland + many more.
- Liaised with the vendors' security team providing technicalities and proof-of-concepts outlining the attack vectors' exploitation and payload capabilities, all while being coordinated under responsible disclosure until it's mitigation.
- Publicly Acknowledged by Sony: https://secure.sony.net/hallofthanks

EDUCATION (2)

Offensive Security Certified Professional at Offensive Security

2019 - Current

in progress

Bachelor of Science, Cyber Security at Edith Cowan University

2014 - 2020

ethical hacking & defense | information security | cryptography | computer security | wireless security | network security | digital forensics | information warfare | unix & c | reverse engineering | it security management | programming secure software systems | programming

AWARDS

CVE Block at CVE Mitre

2018

Pending verification for the following CVEs: CVE-2018-16995, CVE-2018-16995, CVE-2018-16997, CVE-2018-16998 pertaining to application security.

CVE-2017-12439 at CVE Mitre

2017

Awarded a CVE reference as a result of identifying a vulnerability pertinent to Flash Slideshow Maker Professional v5.20 and below. Details here: https://www.cvedetails.com/cve/CVE-2017-12439

Security Researcher Hall of Fame at Sony

2016

Awarded with public acknowledgement via Sony's Hall of Fame in response to responsibly disclosing a security vulnerability effecting the confidentiality and integrity of Sony's products, services and customers.

PUBLICATIONS

Owning Organisations through Exchange in Australian Information Security Association

In Progress

Hunting Bugs via Shockwave Flash Analysis in Australian Information Security Association

4 April 2018

An introductory article explaining the attack vectors pertaining to shockwave.

Socusoft Buffer Overflow Local Exploit in Exploit Database

1 December 2017

Local Buffer Overflow Exploit Proof of Concept (ExploitDB).

Socusoft Buffer Overflow Local Exploit Advisory in Packetstorm Security

1 December 2017

Socusoft's Photo 2 Video Converter v8.0.0 (Free and Professional variants) contains a local buffer overflow condition within the 'pdmlog' DLL library. Exploitation can result in register rewrites to control program execution flow, therefore, resulting in the ability to execute arbitrary shellcode leading to complete system compromise.

Flash Slideshow Maker Professional Exploitation Advisory in Packetstorm Security

1 August 2017

A security advisory outlining a web-app exploit pertinent to a 0day vulnerability identified within the exported contents associated with an advanced slideshow theme generated from software known as; Flash Slideshow Maker Professional. It appears as though that this vulnerability applies to all current versions (v5.20 and below).

An Introduction to Bug Bounty Programs in Australian Information Security Association

15 July 2017

As a contributor to the Australian Cyber Security Magazine, I published a feature article outlining an introduction to bug bounty programs, and the successes of being a bug bounty hunter.

From Student to Professional in Australian Information Security Association

21 May 2017

As a contributor to the Australian Cyber Security Magazine, I shared my story of how I became a Cyber Security professional within the offensive industry.

LANGUAGES

English

Native speaker

INTERESTS

Cyber Security

exploit dev | 0day hunting | crypto | scada | incident response | malware analysis | reversing | hardware hacking

Hobbies

music | skate | film | travel | kite-surf | surf | learning

REFERENCES

> " I'd like to personally thank Jason for identifying and responsibly disclosing a security vulnerability associated with the Australian Securities Exchange Internet perimeter. Your feedback was valuable for us and was acted on promptly. "
>
> **Cyber Security Manager, Australian Securities Exchange (ASX)**
>
> " I wish to Thank Jason for his detailed report on the issue. We have now updated our service to remove the potential for any abuse of this vulnerability. "
>
> **Australian Signals Directorate - Reveal their secrets, protect our own. (via CERT & Defense Web Services)**
>
> " Jason was incredibly timely, helpful and friendly in identifying the vulnerability and verifying that we had patched it. Thanks again! "
>
> **IT Security, Brandeis University**