Evan Ricafort

contact@evanricafort.com • Poblacion, Ipil, Zamboanga Sibugay • +639274917716
www.evanricafort.com

Summary

I am a Freelance Web and Mobile Application Security Researcher. I participate in Bug bounty programs in the bug bounty industry and aside from being an InfoSec guy, I am also an Electronic Dance Music (EDM) Producer.

Education

- Ateneo de Zamboanga University | La Purisima St., Zamboanga City, Philippines

2012 – Present | Associate in Computer Networking
Computer Networking and Analysis

Experience

- IWS | https://invalidwebsecurity.info

Security Researcher | October ***2013 – present***
I worked as Web and Mobile Application Security Researcher.

- Joomlart | https://joomlart.com

Security Researcher | November ***2013 – December 2013***
I worked with their development team.

- Jotform | https://jotform.com

Security Researcher | December ***2013 – January 2014***
I worked with their development team and technical support.

- Audiomack | http://audiomack.com

Security Researcher | March ***2014 – April 2014***
I worked with their development team and Administrator.

Skills

- Web Application Security
- Mobile Application Security
- Music Production
- HTML
- Web Development

Certifications

- Cyber Security and Privacy Foundation Pte Ltd - Certified White hat Hacker v1 (CWHH)
- Lavasoft Security Vulnerability Research Certification
- Apptentive Security Vulnerability Research Certification
- AVG Security Vulnerability Research Certification
- U.S Department of Homeland Security - OPSEC for Control Systems

Research Work (Vulnerabilities and Exploits)

- Cydia Logical Vulnerability – Race Condition (Write Up)

http://blog.evanricafort.com/2016/06/26/cydia-logical-vulnerability-write-up/

- Universal XSS Vulnerability in Comodo Dragon – Version 29.1.0.0 (Write Up)

http://blog.evanricafort.com/2016/04/11/universal-xss-vulnerability-in-comodo-dragon-browser-version-29-1-0-0-write-up/

- Abusing Facebook's Mailing Service – Broken Authentication or Feature? (Write Up)

http://blog.evanricafort.com/2015/12/24/abusing-facebooks-mailing-service-broken-authentication-or-feature-write-up/

Media (News and Press)

Google Nest Findings (2014)

- U.S Department of Homeland Security - Daily Reports as of Sept. 16 — http://www.dhs.gov/sites/default/files/publications/nppd/ip/daily-report/dhs-daily-report-2014-09-16.pdf (#34)
- Maryland Coordination and Analysis Center — http://www.mcac.maryland.gov/newsroom/Cyber%20News/vulnerabilities-found-in-website-of-google-owned-nest
- EMC Corporation - Community Network News Feed as of Sept. 16 — https://community.emc.com/message/838147#838147
- The Gotham Blog - Gotham Security Daily Threat Alerts — http://blog.gothamtg.com/2014/09/16/gotham-security-daily-threat-alerts-295/
- Security Week — http://www.securityweek.com/vulnerabilities-found-website-google-owned-nest

- ISVOC - Information Security Awareness Training Center — http://biweekly.isvoc.com/201409178833-vulnerabilities-found-in-website-of-googleowned-nest.html#.VBk8UFdT7f0
- ID Resolution — http://idresolution.net/vulnerabilities-found-in-website-of-google-owned-nest/
- SysInfosec - Systems and Network Information Security — http://sysinfosec.net/article.php/201409161173225794
- IT Security News — http://itsecuritynews.info/2014/09/15/vulnerabilities-found-in-website-of-google-owned-nest/
- Security National Bank — http://www.snbconnect.com/fraud-alerts.aspx (9/16/2014)
- Three Pilars Technology — http://threepillarstechnology.com/department-of-homeland-security-cyber-security-highlights/
- Hackerstorm U.K — http://hackerstorm.co.uk/denman/news/article/vulnerabilities-found-in-website-of-googleowned-nest
- Global Security Industry Alliance — http://www.gsialliance.com/industry.html (Under Security Week Category)
- Lumension Security, Inc. — http://leic.lumension.com/news/379866119ff3d9c1fd1a16daf8fb0731.html
- Silobreaker Ltd. — http://news.silobreaker.com/vulnerabilities-found-in-website-of-googleowned-nest-5_2268229839561425177
- Data Protection Center - Tech and Security — http://www.dataprotectioncenter.com/security/vulnerabilities-found-in-website-of-google-owned-nest/
- Cryto RSS — http://cryptorss.com/news/vulnerabilities-found-website-google-owned-nest
- IT Security Today E.U — http://itsecuritytoday.eu/vulnerabilities-found-in-website-of-google-owned-nest/
- Gabinete Nacional de Segurança - Portugal (Cyber Newsletter) — www.gns.gov.pt/media/5881/20140918.pdf

Featured in Pinoy Hack News

- Pinoy Hack News — http://www.pinoyhacknews.com/xss-in-natgeo-playstation-and-barack-obama

CKEditor 4.4.6 (Security Patch Released)

- CKEditor — http://ckeditor.com/blog/CKEditor-4.4.6-Released

Blesta Security Advisory – Cross-site Scripting Vulnerabilities

- Blest Security Advisory (Core-931) — http://www.blesta.com/2013/12/20/security-advisory-cross-site-scripting-vulnerabilities-2/

Acknowledgements

I was acknowledged by the following companies:

- Google
- Microsoft
- Twitter
- LinkedIn
- Apple
- Yahoo

And other hundreds of companies…