Nishant Das Patnaik

San Jose, California, United States

nishant.dp@gmail.com

linkedin.com/in/dpnishant

Summary

Security engineering, to me, is not about making a compromise impossible. The goal is to make it difficult, expensive & noisy. I have pentested without expensive softwares, learnt technologies/protocols without formal documentation & built prototypes faster than expected. I'm happy when I can develop my own solutions, find the source of the problem or give a detailed fix or guidance to the right person. I'm happier when I can enable someone else to do the same.

[+] Public Speaking

* BlackHat Europe 2016, London
* BlackHat USA 2016, Las Vegas
* BlackHat USA 2013, Las Vegas
* NullCon Goa 2012

[+] Open Source Projects
* tweezr: www.npmjs.com/tweezr
* AppMon: dpnishant.github.io/appmon
* Raptor: dpnishant.github.io/raptor
* JSPrime: wiki.mozilla.org/Security/B2G/JavaScript_code_analysis#JSPrime
* Ra.2: github.com/dpnishant/ra2-dom-xss-scanner

[+] Text Book Publications

* Author: "Software Hacking"
* Technical Reviewer:
- iOS Penetration Testing
- Kali Linux Intrusion & Exploitation Cookbook
- Kali Linux Cookbook (2nd Edition)

[+] Security Advisories

CVE-2010-1176, CVE-2010-1177, CVE-2010-1178, CVE-2010-1179, CVE-2010-1180, CVE-2010-1181, CVE-2010-2332, EDB-ID: 13870, XFDB 65484

[+] Bug Bounty Hall of Fame Mentions

Facebook, Mozilla, eBay, Nokia, Foursquare, Pinterest, Apptentive, Atlassian, Intuit etc.

Threat Modeling, Application Penetration Testing, Privacy Advocate, Security Architecture

node.js, Python, PHP, Java, Objective-C, Android SDK, OAuth, OpenID, SAML, MySQL, MongoDB, PhantomJS, Selenium, Appium, Chrome Extensions, PCRE, Docker, AWS Lambda, Serverless

Kali Linux, Metasploit, Ollydbg, Frida, Sysinternals Suite, NeXpose, AlienVault OSSIM, Fortify, AppScan, Burp Suite

Experience

Senior Staff Security Engineer

eBay

Sep 2018 - Present (2 years 2 months +)

Some of the technically challenging problems I have designed and developed:

- Solution for fast code linting on the CI/CD pipeline for identifying security blockers for various languages including Javascript, Python, Java, Objective-C, Android, PHP, Ruby, Marko & Dust (templating engines)

- Solution for automated and deep dynamic/runtime security testing of mobile apps by interacting and navigating the app for covering user flows (for iOS and Android) in the CI/CD pipeline

- Solution to detect and mitigate automated synthetic/inorganic user registration (desktop & mobile), with negligible or no code change to existing applications.

- Solution to detect and mitigate credential stuffing attacks (automated login attempts) on eBay applications (desktop & mobile), with negligible or no code change to existing applications.

- Solution to monitor live application attacks/threats at runtime with least false positives, with negligible or no code change to existing applications.

- Solution to detect leakage of sensitive data from containerized application

Staff Security Engineer

eBay

Apr 2017 - Sep 2018 (1 year 6 months)

Some of the technically challenging problems I have architected & implemented:

- Engine to perform fast code linting on the CI/CD pipeline for identifying security blockers for various languages including Javascript, Python, Java, Objective-C, Android, PHP, Ruby, Marko & Dust (templating engines)

- Engine to perform deep, dynamic security testing and runtime security profiling of mobile apps by automatically interacting and navigating the mobile app for covering user flows (for iOS and Android) in the CI/CD pipeline

- System to detect and mitigate automated fake user registration (account creation) (desktop and mobile) and credential stuffing attacks (automated login attempts), with negligible or no code change to existing web applications.

- System to stream L7 attacks/threats signals at runtime with least false positives (contextual analysis), with negligible or no code change to existing applications, to data sciences team for early attack detection, bad actor profiling and vulnerable detection in the source-code in near-realtime.

Lead Security Engineer

eBay
Feb 2015 - Mar 2017 (2 years 2 months)
My roles and responsibilities includes:
- Help product development teams to ensure security in engineering architecture
- Develop end-to-end automation for on-going operations within the Infosec organization
- Fast prototyping of engineering solutions for cutting edge problems
- Research & develop advanced solutions for anti-automation & anti-fraud
- Perform black-box penetration testing and code reviews of our flagship services, product offerings and partners apps.
- Guide the technology organization's security and privacy initiatives by participating in design reviews and threat modelling.
- Participate in our incident response (bug bounty/responsible disclosure) and vulnerability remediation efforts.
- Perform cutting-edge applied research on new attacks and present new findings to both internal and external audiences.
- Evaluate application security tools for internal consumption. Develop new automation and tooling to improve our detection and prevention capabilities.
- Develop secure code practices and provide hands-on training to developers and quality engineers.

Lead Security Engineer
InMobi
Jun 2014 - Jan 2015 (8 months)
* Successfully running the Information Security Program across the company,
* Ensuring adherence to Secure Development Lifecycle among various engineering functions,
* Building security standards, policies for secure coding, secure data handling, secure networking, secure crypto implementation etc.,
* Strategizing application security solutions for developers ranging from security libraries, automated source code review throughout continuous integration and deployment,
* Building & procuring continuous security scanning, monitoring & analysis of applications, networks, cloud and internal assets,
* Evangelizing security among the co-workers through casual discussions, training sessions, documentation, live demonstrations etc.

In short:

I was responsible for Information Security at InMobi - both production and corporate environments.
If our infrastructure or application was vulnerable, I tried to fix it.
If we didn't know, I tried to break it.
If it was on fire, I put it out.

Senior Paranoid
Yahoo
Aug 2011 - Jun 2014 (2 years 11 months)
Senior Product Security Engineer at the Yahoo! Paranoids organisation.

Responsible for:

* Product Security Design & Architecture Review, Threat Modelling

* Customer privacy & security advocate
* Security consulting and due-diligence for Mergers & Acquisitions
* Legal InfoSec Contract Review (New Partnerships & Alliances)
* Manual Source Code Review (Logical Flaws, RegEx Development)
* Penetration Testing & Vulnerability Assessment for Web, Desktop & Mobile Products
* Security point-of-contact for Yahoo! development teams in India
* Security Automation (Processes & Tools)
* Internal Training & Documentation

Security Analyst

eBay

Nov 2010 - Aug 2011 (10 months)

I was responsible for

* Integrating Microsoft SDL v5+ with dev teams
* Threat Modelling
- Web Applications
* Web/SOA/Mobile (Android & iOS)
- Negative/Fuzz Testing
- Penetration Testing
- Exploit Development
* Training Material Development
- Web Application
- Mobile Applications (Android/iOS)
* Evangelize Security across eBay Inc.

Education

Biju Patnaik University of Technology

Bachelor of Technology - BTech, Computer Science Engineering

2006 - 2010

Kendriya Vidyalaya

AISSCE, Maths, Physics, Chem, I.T., English

2004 - 2006

Maharishi Vidya Mandir

Matriculation, General Studies

1995 - 2004

CBSE

Skills

Security Audits • Reverse Engineering • Mobile Security • Perl • PHP • Python • MySQL • JavaScript • Penetration Testing • Application Security

Honors & Awards

Bug Bounty Hall of Fame - Intuit Inc.

May 2014
Hall of Fame: https://security.intuit.com/acknowledgements.html

Bug Bounty Hall of Fame - eBay Inc.
Feb 2014
• Hall of Fame: http://ebay.com/securitycenter/ResearchersAcknowledgement.html

Bug Bounty Hall of Fame - Facebook Inc.
Nov 2013
• Hall of Fame: https://www.facebook.com/whitehat/thanks
• Reward

Bug Bounty Hall of Fame - Apptentive Inc.
Oct 2013
• Hall of Fame
• Reward

Bug Bounty Hall of Fame - Atlassian Software Systems
Aug 2013
• Hall of Fame
• Reward

Bug Bounty Hall of Fame - Mozilla Corporation
Jul 2013
• Hall of Fame: http://www.mozilla.org/security/announce/
• Reward

Bug Bounty Hall of Fame - Facebook Inc.
Jun 2013
• Hall of Fame: https://www.facebook.com/whitehat/thanks
• Reward

Bug Bounty Hall of Fame - Foursquare Inc.
Jun 2013
• Hall of Fame: https://foursquare.com/about/security
• Reward

Bug Bounty Hall of Fame - Pinterest Inc.
Jun 2013
Hall of Fame: http://about.pinterest.com/terms/responsible-disclosure/

Bug Bounty Hall of Fame - Nokia Corporation
May 2013

• Hall of Fame: http://www.nokia.com/global/security/acknowledgements/

Innovation Spot Award 2016 - Director, Global Information Security
Dec 2016
This spot-award was granted to conceptualize, design and implement a novel solution to detect non-human traffic (automated bots) for abuse prevention.

InMobi HackWeek 2015 (1st Runner-up) - CEO, InMobi
Nov 2014
I was the 1st Runner-up (2nd prize) of the winners of the HackWeek conducted internally by the InMobi Tech team.

Yahoo! SecurityWeek CrackDay Winner 2013 - David Filo (Co-Founder), Peter Ellehauge (Director, Threat Response), Christopher Harrel (Director, Product Security)
Sep 2013
Yahoo! SecurityWeek is a annual event and CrackDay is a day dedicated to find exploitable security flaws in any of the Yahoo! products, on the spot. All the submissions are evaluated on the following criteria to decide the winner:
1. Complexity of the attack
2. Innovation in the attack methodology (aka "coolness" factor)
3. Impact/Risk to the users/employees
4. Explanation/Documentation/Demo of the attack

Hackovation Winner - Yahoo!
May 2013
Built a JavaScript static security analyzer for developers to test JavaScript based applications vulnerable to known security risks. It features:

- Code Execution Order aware
- Scope Aware
- Data-flow aware
- OOP Compliant
- Filter-function aware
- based on Esprima parser
- server application written on Node.JS

3rd Position in eBug - 2010 - General Manager, eBay India Product Center
Dec 2010
Won 3rd Prize in “eBUG” contest, an annual contest by eBay India Product Center to find security bugs across all of eBay's of applications within a period of 45 days open to all eBay employees

Best Product Watcher - 2010 - General Manager, eBay India Product Center
Dec 2010

Won “Best Product Watcher 2010” award, in the 1st month of joining, for indentifying the highest number security vulnerabilities in the maximum possible products of eBay Inc.

Excellency in Evangelism - General Manager, eBay India Product Center
Mar 2011
Won “Excellency in Evangelism”, in March 2011, for outstanding contribution towards evangelizing application security among Dev. & QE organizations across eBay Inc.

Out of the Universe - Senior Director (QA), eBay Inc.
Mar 2011
Won “Out of the Universe”, in March 2011, Spot Cash Award as a work appreciation.

Security Champion - CISO & VP (Information Security), eBay Inc.
Jul 2011
Awarded the title of “Security Champion”, in July 2011, at eBay India by the Global Fraud Risk & Security organization of eBay Inc.

Microsoft Student Partner 2008-2010 - Director, Microsoft ACAD Team
Oct 2008

State Youth Icon - Centre Head, 93.5 RedFM
Jun 2009

Champion 33rd CBSE National Science Exhibition - Kendriya Vidyalaya Sangathan & CBSE
Dec 2005

Top Performer, 5th National Cyber Olympiad - National Cyber Olympiad Association
Sep 2005

Science Quiz Topper - District Level, Interschool Science Quiz Competition
2003

Innovation Spot Award 2017 - Director, Global Information Security Team
Dec 2017
Built the core static source code scanning engine. That is integrated in the CI/CD pipeline of code release process fornentire eBay. Due to scale of the releases happening at eBay, performance of scanners was a huge concern with commercial scanner, which was solved by the in-house scanner built by me. It covers Java & Node.js at the moment.