Nishant Das Patnaik

Senior Staff Security Engineer at eBay

PROFESSIONAL PROFILE

Summary

"**Security engineering, to me, is not about making a compromise impossible. The goal is to make it difficult, expensive & noisy**". I have conducted penetration tests without expensive softwares, learnt technologies/protocols without formal documentation & built MVPs for real-world application security problems. 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

- Speaker at Black Hat Europe Arsenal 2016, London
- Speaker at Black Hat USA Arsenal 2016, Las Vegas
- Speaker at Black Hat USA Briefings 2013, Las Vegas
- Speaker at NullCon 2012, Goa

Open-Source Projects

- AppMon: Runtime security testing & profiling framework for native apps
- tweezr: a NPM module to reverse search values within a JS object & generate *eval*-able dot-notation query selectors
- Raptor: Continuous Source Code Vulnerability Scanning Framework
- JSPrime: JavaScript Static Security Analysis Tool
- Ra.2: Blackbox DOM-based XSS Scanner

Book Publications

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

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

CONTACT

Phone: **+1 (650) 283-3279**
Address: **San Jose, CA**
Website: **nishant.daspatnaik.com**
Email: **nishant.dp@gmail.com**

Facebook, Mozilla, eBay, Nokia, Foursquare, Pinterest, Exotel, Apptentive, Atlassian, Intuit

Generic Technology Experience

nodejs, Python, PHP, Java, Objective-C, Android SDK, Puppeteer, Web-Driver, Appium, Esprima, Escodegen, MySQL, MongoDB, Chrome Extensions, PCRE, Docker, AWS Lambda, Serverless, Chrome Debugger Protocol

Security Experience

Process: DevSecOps, Automation & Anti-Automation, Penetration Testing, Secure design & architecture, Data Privacy, Threat Modeling, Risk Assessment, Applied Cryptography

Protocols: HTTP/2, OAuth, OpenID, SAML

Tools: Frida Framework, Ollydbg, .NET Reflector, SysInternals Suite, JAD, JSScrambler, Burp Suite, ModSecurity, AlienVault OSSIM, Nessus, Metasploit, aircrack-ng suite, nmap, HP Fortify 360/SSC, Checkmarx, IBM AppScan, NeXpose, Radware Defense Pro, Distil Bot Prevention

OPEN SOURCE

tweezr

April 2017

https://www.npmjs.com/package/tweezr

A NPM module to reverse search values within a JS object & generate dot-notation query selectors, in context of the specified object. You may also use it to "walk" through the structure one step at a time to read/write values. Think of it as an equivalent of the XPath generator for a matched keyword, in a JS object (or a deserialized JSON).

It is useful for analyzing JSON structures with variable schema.

AppMon: Runtime security profiling framework for native apps

April 2016

http://dpnishant.github.io/appmon

AppMon is a runtime security testing & profiling framework for native apps on macOS, iOS and Android.

It is useful for mobile penetration testers to find security issues as well as validate them with the ones reported by a source code scanner. It works by instrumenting system API calls at runtime. It is also useful for monitoring the app's overall activity and focus on things that seem suspicious e.g. data leaks, credentials, tokens etc. You may either use pre-defined scripts or write your own to modify the app's functionality/logic in the runtime e.g. spoofing the Device ID, spoofing the GPS co-ordinates, bypassing fingerprint authentication e.g. TouchID, bypassing root/jailbreak detection etc.

Raptor: Continuous Source Code Vulnerability Scanning Framework

January 2015

http://dpnishant.github.io/raptor/

Raptor is a github centric source-code vulnerability scanner available in web-based as well as cmdline interfaces. It can, on-demand, scan a github repository with just the URL or execute automated scans on every commit or merge via webhooks. The results are available as JSON or via the web dashboard. More details on the project's homepage: http://dpnishant.github.io/raptor/

JSPrime: Javascript Static Security Analyzer

March 2013 to Present

https://www.github.com/dpnishant/jsprime

[+] Citations

* http://blog.veracode.com/2013/07/veracode-picks-for-blackhat-2013/
* https://wiki.mozilla.org/Security/B2G/JavaScript_code_analysis
* http://blog.nvisium.com/2014/06/javascript-security-tools.html

[+] Presentations
* BlackHat USA Briefings, Las Vegas, 2013
* Slide deck: http://www.slideshare.net/nishantdp/jsprime-bhusa13new

Ra.2: Blackbox DOM XSS Scanner

November 2011 to February 2012

http://code.google.com/p/ra2-dom-xss-scanner

Ra.2 - Blackbox DOM-based XSS Scanner is our approach towards finding a solution to the problem of detecting DOM-based Cross-Site Scripting vulnerabilities in Web-Application automatically, effectively and fast.

Ra.2 is basically a lighweight Mozilla Firefox Add-on that uses a very simple yet effective and unique approach to detect most DOM-based XSS vulnerabilities, if not all.

Being a browser-add on its a session-aware tool which can scan a web-application that requires authentication, although the user needs to manually needs to authenticate into the application, prior to scanning. Ra.2 uses custom collected list of XSS vectors which has been heavily modified to be compatible with its scanning technology. The add-on also implements basic browser intrumentation to simulate a human interaction to trigger some hard to detect DOM-based XSS conditions.

Available on Google Code: https://github.com/dpnishant/ra2-dom-xss-scanner

EXPERIENCE

ebay Inc.

Sept 2018 - Present

Member of Technical Staff 2

Some of the technically challenging projects I have contributed 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)

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

- Detect and mitigate automated fake user registration (account creation) (desktop and mobile), with negligible or no code change to existing applications.

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

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

- Detect leakage of sensitive data from containerized application

ebay Inc.

Mar 2017 to Sept 2018

Member of Technical Staff 1

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.

ebay Inc.

Feb 2015 – Mar 2017

Security Engineer 3

My roles and responsibilities included:
- 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 modeling.
- 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.

InMobi Pte. Ltd.

June 2014 to Jan 2015

Lead Security Engineer

- 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 all things Information Security at InMobi - both production and corporate environments.

Yahoo Inc.

August 2011 to June 2014

Senior Paranoid

Senior Product Security Engineer at the Yahoo! Paranoids organisation.

Responsible for:

- Product Security Design & Architecture Review, Threat Modelling
- Customer Privacy and 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)
- Training & Documentation

PayPal India Pvt Ltd.

November 2010 to August 2011

Security Analyst

Responsible for

- Integrating Microsoft SDL v5+ with dev teams
- Threat Modeling: 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 PayPal & eBay Inc.

EDUCATION

Biju Patnaik University of Technology

2006 TO 2010

Bachelor of Technology (B.Tech)

Major - Computer Science & Engineering

College: NMIET, Odisha

Score: 7.0 (CGPA)

Kendriya Vidyalaya

2004 TO 2006

Intermediate of Science (ISc.)

Physics, Chemistry, Mathematics, Information Technology

Board: CBSE

Score: 70%