Jay Patel

Penetration Tester | Test Engineer

📞 +61 449 043 794

✉ Jaypatel5809@gmail.com

in www.linkedin.com/in/jaypatelk

🐦 twitter.com/jpjaypatel34

I have five years of experience in Penetration Testing, working with multinational clients across countries in the public and private sectors. Mainly expertise in web application penetration testing, mobile penetration testing, Network(host) penetration testing, software testing, load testing and security static code review. Also, I spend my free time improving my penetration testing skills and participating in private bug bounty programs on the Synack platform and Cobalt labs.

💼 Work History

2022-09 - Current

Analyst Offensive Security (Penetration Tester)

National Australia Bank

- Work with project stakeholders to identify assets and define test scopes - evaluating the breadth and depth on which testing should take place based on varying factors.
- Execute penetration tests, either in a team or individually, to identify vulnerabilities and weaknesses that could impact bank systems;
- Including testing of web applications, mobile applications, web APIs, Infrastructure, Cloud technologies, and hardware.
- Triage vulnerabilities and justify the risk in alignment with common vulnerability scoring systems, considering the environment and context.
- Triage incoming bug bounty vulnerability findings.
- Report testing results to key project stakeholders in varying formats (i.e. traditional reports, bug tickets), including verbal communication.
- Be involved with internal projects and initiatives to uplift team capabilities.
- Provide QA reviews for testing scopes and reports from your peers to ensure high quality and accuracy of testing.
- Assist with other offensive security activities within the team (e.g. red team activity).
- Self-manage penetration testing projects from end to end; Perform other 'run the business' activities as assigned by the team manager, such as maintenance and uplift of the penetration testing environment.

2021-12 - 2022-09

Technical Consultant (Pentester & Test Engineer)

DXC Technology

- Perform penetration testing for numerous Australian blue-chip companies

and Australian Federal and local state government agencies.
- Perform functional testing for the developed project.
- Maintain/develop security and functional test plans for various software changes, including web services and user interfaces.
- Consult with application developers to demonstrate security testing results, explain the result's threat, and consult on remediation.
- Test software products based on the test plan, personal judgment and follow standard procedures to ensure the product's quality is tested.
- Provide feedback to the reporting manager about QA and security testing.

2019-04 - 2021-12

Associate Consultant Technical

DXC Technology
- Created accurate and successful test scripts to perform testing of certain products and features.
- Determined server operating limits by conducting weekly load tests.
- Wrote and optimized test cases to maximize the success of manual software testing with consistent, thorough approaches.
- Collaborated with developers and product owners to stay current on product features and intended functionality.
- Fixed identified issues to increase productivity and boost workflows.
- Conducted regression testing, analyzed results and submitted observations to the development team.
- Reviewed requirements, specifications and technical design documents to provide timely and meaningful feedback.
- Perform penetration testing for numerous Australian blue-chip companies and Australian Federal and local state government agencies.

2018-03 - 2019-04

Penetration Tester

Global Garner Sales Services
- Perform threat, vulnerability and risk assessment on the product.
- Monitor system performance.
- Vulnerability scanner.
- Security event logging and analysis.
- Intrusion detections and firewall logs.
- Maintain WAF(Cloudflare).
- Followed AGILE methodologies for development and QA cycles.
- Manage bug bounty program.
- Validating incoming security vulnerability threats.

Freelancer Bug Bounty Experience

2021-12 - Current

Cobalt Core Pentester Tester - Part Time

Cobalt
The Cobalt labs is a community of highly skilled pen-testers who are passionate about what they do and who are always striving to be at the top

of their game. This curated community is made up of security professionals with many years of experience as well as talented pen-testers who are eager to learn the trade and show their skills. They all have a strong drive to keep to up to date on the latest vulnerabilities and exploits, and the tools and methodologies to find them.

2021-02 - Current

Synack Red Team Member

Synack

Synack Red Team provides security work for security researchers around the world. The majority is bug bounty-style hunting, where researchers compete on the skill, speed and report quality to get their work accepted and ultimately paid. As a private network of highly curated and vetted security researchers, the SRT is challenged every day to deliver exploitation intelligence for some of the biggest brands in the world.

2016-01 - Current

Security Researcher

HackerOne

HackerOne is a platform where I spend my free time improving my penetration testing skills, participating in a private bug bounty program, and helping the reputed organisation secure their platforms. Also, participating in HackerOne CTF.

Skills

- Web application penetration testing
- Manual OWASP top 10 testing
- IOS Mobile application penetration testing
- Andriod Mobile application penetration testing
- Network Penetration testing
- Vulnerability assessment with Automated tools
- Cloud Penetration Testing
- Gray-box testing
- Black-box testing
- White-box testing
- Load testing

Technology Snapshots

- Web application vulnerability scanning tools: Acunetix, BurpSuite scanner,SQLmap,Hydra,Nikto and open source vulnerability scanning tools.
- Operating System: OS-X, Ubuntu, Kali-Linux and Windows.
- CDN (ContentDelivery Network): Cloudflare.

- Cloud Services: Amazon and Azure.
- Programming Language : Basic Python scripting, Bash scripting and JavaScript.

Certification

- OSCP - Currently pursuing
- EWPTXv2 - eLearnSecurity Web Application Penetration Testing EXtreme
- Microsoft Azure Security Engineer Associate (AZ-500)
- ISTQB® Certified Tester Foundation Level
- Microsoft Virtual Academy Certification
- Certified Professional Ethical Hacker (CPEH)
- Microsoft Virtual Academy Certification
- Oracle Database 10g: Introduction to SQL
- Oracle Database 10g: Administration Workshop I Release 2

Education

2018-01 - 2018-09

ACS Professional Year • Hobart • Tasmania
A Professional Year Program is a structured professional development program combining formal learning and workplace experience for international students who have graduated from a university in Australia.

2016-01 - 2017-01

Master of applied information technology • Victoria University • Sydney.
Advanced training in Information Technology focusing knowledge and skills to real-world problems and scenarios guaranteeing preparation for a career in:
- Advanced Object Oriented Programming
- Advanced Project.
- Database Analysis and Design
- Information security.
- Networking.
- ICT training.
- Two major thesis.
- Data warehousing.
- IT consultancy.

2012-01 - 2015-01

Bachelor of Science in information technology • Ganpat University • India.
Basic fundamental of computer Science in information technology and guaranteeing preparation for a career in:
- Information security.
- Networking.
- Fundamental of Algorithms.
- Introduction to programming - I / II.

- Database management system.

Publications

- **"Prevention of Cross-Site Scripting Attacks in Web Applications,"** at **IEEE-EECCMC** Conference.

References

- References will be provided upon request.