

Taufiq Ali – Senior Security Analyst

<p>Summary</p>	<p>Taufiq Ali is a Team Lead Product Development and Senior Security Analyst at NII. His area of work includes Vulnerability Assessment, Security Audits, Penetration Test, Source Code Reviews, Computer Forensics, Ethical Hacking Trainings etc.</p> <p>He is also a Certified Ethical Hacker, and is has being a part of most of the significant InfoSec projects for some of NII’s premier customers. He has consistently impressed clients with his ability to think out of the box, and creatively attack systems, applications and problem solving and analytical skills. He is well-versed with the OWASP, OSSTMM like methodologies.</p> <p>He is active on various InfoSec communities and mailing list like Security Focus, n u, Webappsec etc.</p> <p>He currently serves as Team Lead Product Development & as a Senior Security Analyst at NII Consulting focusing on Product Design, Penetration Testing, Vulnerability Assessment, Source Code Audits, Building and Execution of various threat scenarios, test cases for projects that involve testing of the business logic, Computer Forensics like Log reviews, investigations of hacking incidents etc. He now also leads various InfoSec project at NII</p> <p>His technical abilities span a very wide range of technologies across networks, operating systems, databases, web servers, and applications; however his specialization is web applications security assessments with the execution of various threat scenarios including social engineering attacks. He possesses strong analytical skills and is a part of the research activities undertaken at NII.</p>
<p>Educational Qualification</p>	<p>Bachelor’s Degree in Computer Science University of Mumbai, India</p> <p>Master Degree in Computer Science (Advance) University of Mumbai, India</p>
<p>Certifications</p>	<p>Certified Ethical Hacker (EC-COUNCIL)</p>
<p>Detailed Experience & Expertise</p>	<p>Application Security</p> <ul style="list-style-type: none"> • Well versed with OWASP – Top Ten, WASC Threat Classifications and other Application security Forums • Expertise in Vulnerability Assessment and Penetration Testing of Web Applications including technologies like SharePoint, Silverlight, Web Application Services etc • Business-Logic based execution and testing of simple to complex threat scenarios. • Penetration testing of more complex technologies like SharePoint, Silverlight etc <p>Network Security</p> <ul style="list-style-type: none"> • Good knowledge of TCP/IP fundamentals • Well versed with various Operating Systems, databases, web servers and mail servers, content filtering technologies etc • Assessment of various network devices like routers, switches, IDS/IPS, firewalls etc • Security Configuration Review of Network Devices • Assessment of various LAN and WAN setups. <p>Computer Forensics</p> <ul style="list-style-type: none"> • Disk Imaging with Encase • Log Review • Investigation of Hacking incidents

	<ul style="list-style-type: none"> Email Address Tracking
Technical Skills	<p>Operating Systems: Windows 9x/NT/2000/XP/2003/2008/Vista, Linux</p> <p>Servers: Domain controllers (Active Directory), DNS (Microsoft DNS, BIND), DHCP, Web Servers (Microsoft IIS, Apache), FTP (Microsoft FTP, vsftp, wu-ftp)</p> <p>Databases: MS-SQL, Oracle, MySQL, IBM DB2</p> <p>Network components: Firewalls, Routers, VPN, Switches, WLAN access points</p> <p>Security tools: Well versed with most of the industry standards free and commercial tools like NMAP, Nessus, Metasploit, Burpsuite, Webscrab, Acunetix, IBM App Scan, Netsparker, Webscurfy, Metasploit Express, NeXpose, scripts on the BackTrack and other security Distro's etc.</p> <p>Languages: C, Shell Scripting, VB6, C, Core Java, Advanced Java, Lisp, SQL, HTML, DHTML, XML using CSS and XSL style sheets, ASP & JavaScript</p>
Interpersonal Skills	<p>Communication and Interpersonal</p> <p>He has good communication skill by virtue of being alumni & conducting workshops demonstrations at various seminars and interacting with professionals at various levels in public forums etc.</p> <p>Experience in product development and client interactions. Experience in leading a team & dealing with senior and middle management, system administrators, auditors, clients, customers, etc. Very strong commitment to quality of deliverables</p>
Tools Developed	<p>He is a Team Lead Product Development at NII. He leads the development of following product at NII</p> <ul style="list-style-type: none"> AuditPro Enterprise Issue Tracking System Firesec
Project Execution Domains	<p>To his credits he has completed projects successfully across below verticals</p> <ul style="list-style-type: none"> BPO's Medical Centers Online Stores Social Networking website Trading Applications Matrimonial Website Local Search Engine Health Care Companies in US, UK and India Insurance Companies. Public and Private Sector Banks from various countries and cities. Payment Gateways Aviations WAP based websites Real Estate, Telecom Providers Online Astro's Internet KIOSK Applications Online Media. ...and still counting
Hands on Experience in Infosec Domains	<ul style="list-style-type: none"> Vulnerability Assessments Web Application Security Assessments and Audits Network Security Assessments and Audits

	<ul style="list-style-type: none"> • Security Audits for Databases, Operating systems, Server Systems, etc • Source Code Reviews for technologies like PHP, ASP, ASP.NET, JSP, AJAX, CGI etc • Ethical Hacking Trainings on Operating System Security, Network Security etc • Configurations reviews for network devices, and other technologies • Computer Forensics and Investigation on Hacking Incidents, Phishing emails, research on Phishing emails etc.
Other Activities & Articles	<p>Reading on Technology, Computer Security, Science Fictions, Water Sports, Travelling etc</p> <p>Reverse Engineering & Cracking the code for newbie's (ONLY Educational)</p> <p>Hacking Microsoft Windows 2003 Server with Microsoft SQL Server 2005</p> <p>A Phishy Story (Phishing Modus Operandi)</p> <p>Concurrent RDP connections hack – XP</p>