

To know more about our services, email us to info@net-square.com

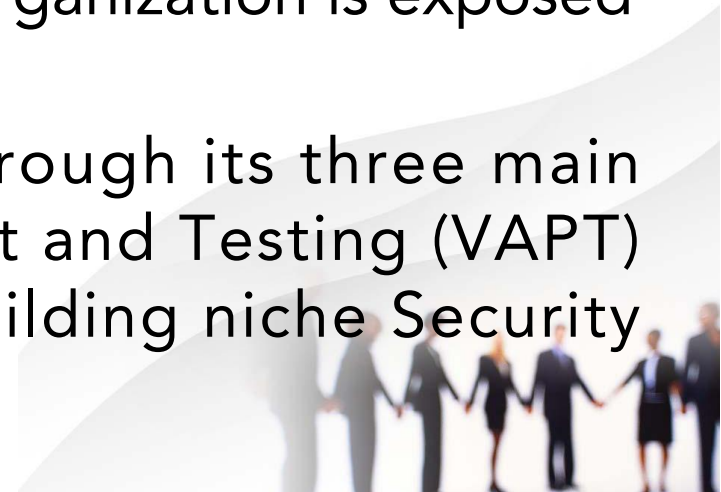


Case Study on Pentesting Complete Portfolio of Applications for a leading Cellular Company in India

Engagement for Web / Mobile Applications Pentesting

Net Square at a Glance

- Net Square has set itself the mission to be the partner of choice for Organizations that seek deep insights into the Network and Application Security. To address this challenge, Net Square has built great depth in both these key areas of Information Security.
- Our thoroughly researched methodologies and our knowledge of the latest attack vectors help us in providing our clients insights into the gaps in the security posture and the possible business risks the organization is exposed to.
- Net Square delivers this value through its three main activities Vulnerability Assessment and Testing (VAPT) services, Security Training and building niche Security Products.



About Our Client



- The client is one of the leading mobile network operator in India and with its current growth strategy the company will soon gain the position to be the largest telecom company in India by subscribers and by revenue.
- Over the years, the company has built various applications / offerings in the mobile service provider space to surpass the competition and cater the needs of their users. With a large number of application portfolio, their expectation was to achieve high efficiency without compromising the quality of assessment.
- They wanted to engage with Information Security service provider who should be willing to go the extra mile to uncover all possible hidden flaws within the applications.
- They were clear about not hiring agencies who only used automated testing tools or who only paid lip service to undertaking manual testing. Therefore Net Square team and our AppSec testing methodology was a right fit as per their requirement.

The Mandate

- The Company had identified 30 mobile applications and 50 web application in the first phase of VAPT exercise to be covered over a span of one year.
- Net Square assigned a team of security analysts and coordinated with internal infosec teams to ensure the engagement was completed in the allotted time frame with high quality delivery.
- Through the testing conducted by Net Square, critical vulnerabilities were discovered by the Net Square analysts which were not discovered in the earlier assessments.
- Net Square not only provided the report of vulnerabilities identified in each application, but also spent time helping the IT team and vendors of the company understand what the issues were and how they should fix the issues.



The Results

The result was a set of findings which provided insights into:

- ✓ How attackers could access system files.
- ✓ How users could escalate privilege and commit frauds.
- ✓ How leakage of personally identifiable information (PII) could expose the Company
- ✓ How phishing attacks could have been launched to steal user credentials.
- ✓ How account details could be changed in a/cs without proper authorization.
- ✓ How weak passwords could be decrypted and accounts can be taken over.
- ✓ How SQL injection could result in data to be stolen.



The Engagemen

- Due to the insights provided by Net Square to the Company, there were many important strategic initiatives taken by the Company to strengthen the application security
- The Company embarked on Phase II of the Application Security Testing initiative and again engaged Net Square's services for the same
- Though some of the applications being tested were less critical, Net Square could show how vulnerabilities in non-critical systems could be used to pivot to attack critical systems
- Net Square has also proposed for a secure coding training to the Company's development team and also suggested the Company for an architecture security review to be conducted by Net Square senior Consultants during next phase of AppSec testing, to eliminate business logic issues



The Trust



Net Square evokes trust from the experienced and senior IT professionals who manage and lead the team.



Hiren Shah-President
hiren@net-square.com

Hiren is President at Net Square and leads Client-Relationships, Business Development and also acts as a Mentor to the team. Hiren is a business cum technology leader with more than 20 years of experience in IT Governance, Management of IT Infrastructure, IT Risk and Information Security, Enterprise Architecture and Global Resource Management.

He is also a functional expert in financial services industry, specially capital markets and risk management. He has presented many papers at seminars on various aspects of Infosec.

Previously Hiren completed 8 years at the helm of CRISIL Ltd. a subsidiary of S&P as a CIO. Earlier he held various IT and Business Management positions at CRISIL. Hiren graduated as a Physics and Electronic major from Mumbai University and then qualified as a Chartered Accountant (Equivalent to CPA in US). He is also a CISA and a CGEIT.



Saumil Shah-CEO

saumil@net-square.com

Saumil is the Founder and CEO of Net Square and leads the Delivery and R&D effort at the company. Saumil has more than ten years of experience in performing various ethical hacking exercises for many well known companies. Saumil has been a regular speaker and trainer at conferences such as Black Hat, RSA, Hack-in-the-Box, IT underground, CanSecWest, EuSecWest, Hack.Lu, etc.

Previously Saumil held the position of Director of Indian operations at FoundStone Inc. and a Senior Consultant with Ernst & Young. Saumil graduated from Purdue University with a Master's Degree in Computer Science and a strong Research background in Operating Systems, Networking, Information Security and Cryptography. He got his undergraduate degree in Computer Engineering from Gujarat University, India. Saumil is also a CISSP.

