NETSQUARE
secure • innovate • automate

CASE STUDY

VAPT Annual Engagement Model– Procurement Solutins Company In India

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.
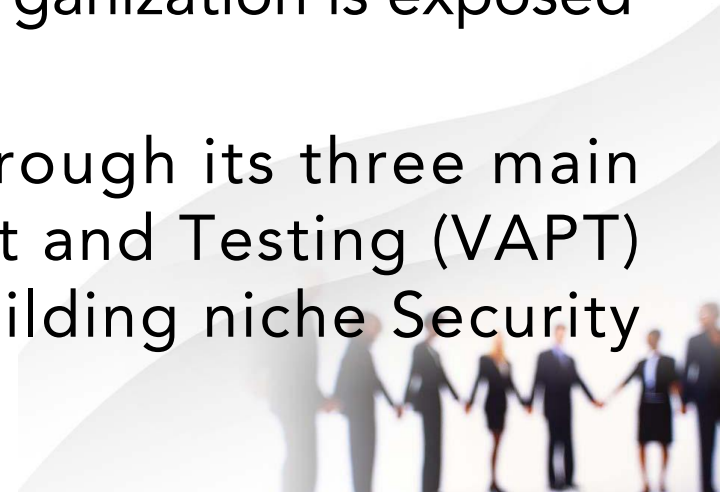
About Our Client

- The client is one of the leading product solutions company, which caters its client with enterprise procurement solutions. These solutions can be accessed by their clients on a SaaS model and are exposed on the internet.

- The challenge faced by the client was in securing the solutions from possible external threats, which could compromise the security of the solutions. With a large number of application portfolio, their expectation was to achieve high efficiency without compromising the quality of assessment.

- Client wanted to conduct a penetration testing exercise from a professional service provider to take measures in securing it's wide range of procurement solutions and provide detailed penetration testing reports.

The Mandate

- Our client has provided it's entire solution suite consisting of 12 different solutions to Net Square for penetration testing exercise. Along with application security, Net Square also conducted VAPT on entire solution hosting environment.

- Net Square deployed two security analysts at client location for 2 months to conduct penetration testing and co-ordinate with client's internal team to ensure the engagement was completed in the allotted time frame. With Net Square's no stones left unturned approach, critical vulnerabilities were discovered by Net Square analysts which were not discovered in the earlier assessments.

- An in-depth view of security was presented to client's team in detailed reports. Apart from reporting all the vulnerabilities, Net Square analysts also spent additional effort and time helping client's team to understand the issues and how they should be fixed.

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 attacker can gain unauthorized access to critical data saved on the data server

- How phishing attacks could have been launched to redirect victim users to a malicious website

- How attackers can exploit reflected XSS vulnerability, which could leak confidential information

- How a malicious user can gain SSO session cookie to gain unauthorized access to the users account and can perform unauthorized actions
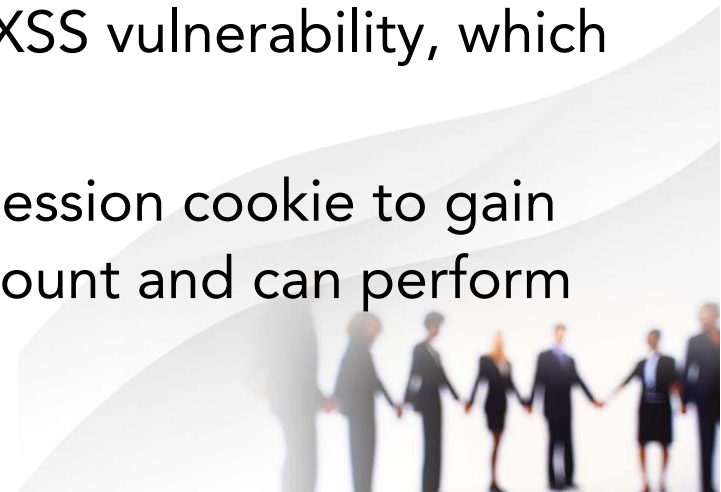
Annual Security Engagement

Net Square carried out the annual engagement as per the scope

mentioned below and deployed one dedicated security analyst at client

location to conduct

    1) Application security testing

    2) Incremental code review exercise on the periodic enhancements of solutions

    3) Network VAPT

    4) Architecture review

Roles and Responsibility

- Assessment of complete procurement solution was performed using Net Square's testing methodology.

- Security code review of the incremental changes made to the products as a part of SDLC. The work prioritization was assigned by the project co-ordinator from client and host based assessment of the application environment for the solution performed.

- Net Square Analysts had performed revalidation of the findings identified by Net Square Analyst during testing exercise

- Net Square had provided an assessment report for all the activities in a format which is acceptable to both parties.

- Report readout session was conduced and Net Square Analsysts had co-ordinated with the developers and QA team to provide the appropriate fixes for all the security bugs.

The Trust

Net Square evokes trust from the experienced and senior ITprofessionals 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.