

Do you know that on most LANs, wired or wireless, your neighbor can watch all your data, and vice versa?

Do you know that at least one of India's popular \*payment gateways can be compromised --- that is you can fool it into approving a purchase of an item at any price that you want?

Learn the technics of hacking into and securing web applications.

## *"Here is the opportunity"*

Teknotrends Software Pvt Ltd, Bangalore is conducting a Two day hands-on workshop on Saturday 4<sup>th</sup> and Sunday 5<sup>th</sup> of February 2012 at Almaz Software Center, Koramangala.

### Details:

With a major part of internet access now consisting of website access, security holes appearing in web applications have gained much importance. Hackers too have concentrated their efforts on hacking into web applications such as banking applications where many users perform financial transactions online. This Two day hands-on Workshop attempts to cover major aspects of infrastructure and Web application security by shedding light on security holes related to Networks and web applications where users need to share their personal and financial data over the internet.

### Workshop Schedule:

- 1) Two sessions in the morning of 2 hours each day understanding various possible vulnerabilities. These sessions cover types of security holes such as sql injection, XSS, parameter validation, session hijacking and others. What these holes/vulnerabilities are and how they occur will be discussed with examples, and techniques to detect the security holes/vulnerabilities will be taught.
- 2) Use of Various tools to detect the holes in the web applications
- 3) Hands-on laboratories will be conducted in the afternoon sessions every day.

**Works shop Schedule details:**

Day	Topic	Morning Lecture	Afternoon Hands-on Lab
Day 1	Infrastructure Security	Networking Concepts, TCP/UDP protocols, IP, ARP, DNS protocols. Other concepts in networking. Security Issues in infrastructure components such as operating systems, web servers etc. Use of Wireshark, Port scanner - nmap. VA tool - Nessus, Use of SSLStrip	Use of Nmap, Use of Nessus, Use of Wireshark. Running VA scans and understanding reports. Use of SSLStrip. Use of ARP Spoofing.
Day 2	Web App Security	XSS, CSRF, parameter validation, fuzzing, Authorization checks, A tutorial on http, html, sql. Basics needed to understand web application security. Use of webscarab proxy. Session Hijacking, sql injection, CRLF injection, XPATH injection.	Finding XSS, CSRF, parameter validation, authorization holes, CRLF injection, XPATH injection. Use of webscarab. Doing session hijacking via webscarab. Doing sql injection via webscarab.

**Pre-requisites for this Workshop:**

- Basic knowledge of Windows operating systems.
- Basic knowledge of networking technologies.
- Basic exposure to information security will help.
- Knowledge of using / developing web applications, and an exposure to html and http is desirable.

**Registration and Contact Details:**

Those interested in participating in this workshop should send their nominations to "info@teknotrends.com"

Contact Number for any queries: 98450 44403

**Address for communication:**

Teknotrends Software Pvt Ltd  
A-5, Kudremukh Colony,  
Off Sarjapur road,  
Koramangala 2 Stage  
Bangalore 560034

**Other issues:**

Each participant will be provided a soft copy of the course material on a CD. A participation certification will be given at the end of the course.

**Fee & Payments:**

INR 12000/- inclusive taxes for individuals.  
INR 15000/- inclusive taxes for corporates.

Bulk discounts are available.

This fee includes: Technical sessions, Lab, Material (CD), Lunch, Tea and snacks for 2 days.

Cheques/drafts should be drawn in favor of "Teknotrends Software Pvt. Ltd"

### Profile of Dr. Samir Kelekar

Dr. Samir Kelekar has around 28 years of experience in industry and academics combined. He has a BTech from Indian Institute of Technology, Bombay, an MS in Computer Engineering from Clemson University, Clemson and a PhD in Electrical Engineering from Columbia University New York. He has lead teams and worked in both managerial and technical capacity for some of the world's leading companies such as IBM (T J Watson Research Center), Motorola, Alcatel. For Narus, a Silicon Valley startup in the area of IP traffic monitoring, he developed the world's first skype detection system which gave Narus worldwide publicity. He has also developed a product on real-time vulnerability assessment. He has published in top journals and is owner of a U.S. patent (accepted for allotment) in the area of real-time Vulnerability assessment. He was also on the Board of Infotech Corporation of Goa, a state-govt. owned firm to promote IT in Goa.

He is the founder-director of Teknotrends Software Pvt Ltd (<http://www.teknotrends.com>) which does consultancy in security, among other things. Teknotrends has discovered security holes in softwares of major companies in India. Teknotrends also sells a skype / website unblocker product called Black Byte Networks ( <http://www.blackbytenetworks.com> ) that has thousands of users, and hundreds of paying customers. It has also pioneered iOpenvpn, world's first port of openvpn VPN for iphone.

This is available at <http://www.iopenvpn.com>

Samir has conducted trainings in network / web applications security for Narus, a silicon valley company, TCS, Tecnotree Convergence Ltd and several other institutions including academic institutes and industry. He was invited by Huawei Technologies to give a specialized talk on ISP security. He has given a number of technical talk on security including one at ICICI Bank fraud detection division, Mumbai. He has consulted in the domain of security testing for financial companies based in the US and other international telecom providers.

Samir widely writes on technology and is a columnist for Moneylife magazine ( <http://www.moneylife.in> ).