A Two-day Workshop
on
Android app pen testing and web app security

Conducted by

Teknotrends Software Pvt Ltd

Dr Samir Kelekar
Dinesh Bareja.

Introduction:

India now is almost the startup capital of the world with startups in ecommerce especially and in the Android app area ruling the roost. These startups mostly depend on websites (http/s) traffic for their application. When we looked at a few of the popular apps, we found security holes in them. This 2 day hands on workshop conducted by Dr. Samir Kelekar and Dinesh Bareja will train you in how to find security holes in your app/website and give guidance on how to fix them.

The Workshop:

The two-day workshop covers the following aspects:

Two sessions in the morning of 2 hours each every day understanding various possible vulnerabilities. These sessions cover types of security holes such as infrastructure vulnerabilities, web app vulnerabilities such as sql injection or XSS. What these holes/Vulnerabilities are and how they occur will be discussed.. Then, some simple examples will be shown, along with techniques on how to detect the security holes/Vulnerabilities including penetration testing. Use of various tools to detect will be introduced in these sessions. Finally, guidelines will be given on how to fix the security holes. Focus will also be given on live interactions between the participants and the presenter.

We will demonstrate some of the hacks in the workshop. We will demonstrate some critical vulnerabilities in India's ecommerce infrastructure and payment gateways.

As far as Android apps are concerned, we will get into apk files, and some amount of reverse engineering of the apps. Also, most android apps connect to http servers and so they are subject to similar vulnerabilities as a regular website is.

2) Hands-on laboratories will be conducted in the afternoon sessions every day. Participants will get hands on practical experience on the discussed topics. The laboratory will be of at least 2 hours every day. The participants will do practical exercises on how to perform testing to find the security holes/Vulnerabilites using the tools and topics understood in the morning sessions.

Pre-requisites for this workshop:

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

The detailed program follows.

Day	Topic		Morning Lecture	Afternoon Hands-on Lab
Day 1 Friday June 10 2016	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, . A tutorial on http; use of androidstudio, emulator to security test android apps.	Use of Nmap, Use of Nessus, Use of Wireshark. Running VA scans and understanding reports. Understanding http protocol.
Day 2 Saturday June 11 2016	Android app / Web App Security		XSS, CSRF, parameter validation, Authorization checks, A tutorial on html, sql. Basics needed to understand web application security. Use of webscarab proxy. Session Hijacking, sql injection. Also, reverse engineering android apps.	Finding XSS, CSRF, parameter validation, authorization holes, Use of webscarab. Doing session hijacking via webscarab. Doing sql injection via webscarab.
Closing session on both days	Business needs to enable and empower security		A look at business practices, challenges and solutions that form part of the security consciousness and are favoured by CxOs – the mistakes and the lackof foresight (or risk management practices) that may lead to incidents. Essential hygiene issues that must be addressed by organizations. The importance of logs, logging mechanisms and a look at the convergence of technology logs / data with business and environmental information.	

Other points:

Customers to whom a large part of the training is given include Canara Bank, Tecnotree, Redbus, GE Health, Pandesa, Narus, TCS, Versa Networks. Academic institutes include SIT, Kristu Jayanti College.

Profile of Dr. Samir Kelekar:

Samir has a Btech from IIT Bombay, and Phd from Columbia University with a total of 30 years of experience. He has worked at IBM Research, Motorola, Alcatel and a number of startups. He

has consulted for a number of top companies and found security holes in a number of websites and softwares. He owns two US patents in the area of security. Samir is also a prolific communicator, a writer, a blogger and a columnist. Links to some of the articles are given below.

http://www.thehindubusinessline.com/todays-paper/tp-eworld/falling-short-on-security/article1084119.ece
Falling short on security, Hindu Business Line interview.

https://www.indusface.com/blog/?p=368
Has dDOS become the hacker's number 1 choice of attack?

http://www.deccanherald.com/content/175732/hackers-may-catch-indian-banks.html
Hackers may catch Indian banks napping.

http://www.dnaindia.com/bangalore/report-it-firms-lack-cyber-security-experts-1214342
IT firms lack cyber security: experts

Alloted Patents:

http://www.google.com/patents/US8789193

http://www.google.co.in/patents/US8127359?trk=prof-patent-title-link

Profile of Dinesh Bareja:

Dinesh Bareja is a senior consultant who is a Microsoft MVP, a CISA, and a CISM. He is trained in ITIL, ISO27001 and is a certificate holder in IPR and ERM. He is a principal consultant at Pyramid Cyber Security & Forensic FZE, Dubai & India and founder of Open Security Alliance; Indian Honeynet Project, IndiaWatch. He is member (IGRC) Bombay Stock Exchange, former Cyber Surveillance Advisor: CDRC - Jharkhand Police).

Dinesh is an Information Security, Management and Audit professional practising in the domain for over a decade. He is a specialist in cybersecurity, infrastructure, policy and strategy and has worked with Governments and Enterprises for Security Audits, Architecture, Strategy, Policy Definition, Planning, and re-Engineering.

He is recognized authority in the cybersecurity domain and for national and enterprise strategy and operations. In staying current with technology his present interests are in Cloud Computing, IoT, Data Classification, Threat Intelligence, Managed Security, Cyber Insurance and more.

He enthusiastically supports security awareness and career mentoring activities and firmly believes that the use of commonsense may be the silver bullet for information security woes.

He is a regular writer, blogger and a hobbyist photographer.