Web Application Vulnerabilities and Countermeasures

1. Abstract of the tutorial

In the present days, web application vulnerabilities have been largely exploited by attackers for stealing confidential data and accessing corporate networks. However, it is not an easy task to build secure software, considering its complexity nowadays. Quite often a system is composed of thousands of lines of code, which invariably contain some bugs. Part of them have impact on system security and can lead, for instance, to unavailability and complete control of the machine by an attacker.

The number of vulnerabilities reported by the Common Vulnerabilities and Exposures has been increasing year after year. Buffer overflow was for a long time the most common security problem found in software, but it lost that position for vulnerabilities like cross site scripting and SQL injection. These types of weaknesses basically affect web applications and indicate:

- The popularization of that type of software, be it for electronic commerce, internet banking, or for configuring a network element, such as an access point;
- The security issues related to this domain have not been properly addressed during software development, which is aggravated by security unconscious developers and tight development schedules.

The purpose of this tutorial is to discuss the present most common web application vulnerabilities, according to OWASP, to show possible attack scenarios, how to test, and countermeasures that can be used to avoid those weaknesses.

2. Proposed duration

This tutorial is organized for a full day (6 hours).

3. Intended audience

The course targets web application developers, testers, and information security analysts who wish to work with vulnerability analysis and penetration testing.

4. Prerequisite knowledge

To improve the learning experience from the course, one expects that the attendees fulfill the following prerequisites:

- Basic knowledge of HTTP and Javascript;
- Basic knowledge of TCP/IP;
- Basic knowledge of databases;
- Basic knowledge of Cryptography.

5. Detailed outline

Each one of the vulnerabilities from OWASP Top Ten will be initially theoretically discussed, in order to make the student understand why attacks exploiting them are possible, damages that can

be caused and how to build secure systems. After that, actual attacks will be shown as well as techniques for detecting their presence on live systems. Finally, the attendees will solve some exercises to consolidate the topics learned.

The detailed course outline is presented in the table below:

Topic	Duration
Introduction and motivation about web application (in)security and the need for considering security in the whole software development lifecycle.	10 minutes
Review of fundamental concepts from cryptography (ciphers, hash functions, digital signatures, digital certificates, and SSL) and HTTP (request methods, error codes, session management, and authentication).	35 minutes
Presentation of a secure software development lifecycle.	10 minutes
Overview of OWASP and the main projects they support.	10 minutes
Break	15 minutes
Presentation of the main tools employed in web application pentesting.	45 minutes
Cross site scripting is nowadays the most common vulnerability and allows powerful attacks such as session hijacking, clipboard stealing, and network scanning.	30 minutes
Injection flaws occur when an application does not validate user input and may lead to unauthorized information access and broken authentication.	20 minutes
Lunch	
Malicious file execution may lead to complete server compromise.	20 minutes
Insecure direct object reference in URLs may be modified to allow unauthorized information access.	20 minutes
Cross site request forgery takes advantage of an authenticated session to submit valid but illegitimate requests to the application.	20 minutes
Information leakage and improper error handling may provide valuable information to a malicious user.	20 minutes
Broken authentication and session management can be the result of low-entropy session ids and inadequate protection of credentials.	20 minutes
Break	15 minutes
Insecure cryptographic storage often results from improper key management.	20 minutes
Misconfigured servers may lead to insecure communications.	20 minutes
Failure to restrict URL access can result in unauthorized information access.	20 minutes
Final remarks about web application (in)security.	10 minutes

6. Tutorial goals

The goals of this tutorial are:

- To show the main vulnerabilities found in web applications (OWASP Top Ten) and how they can be exploited by malicious users.
- To show the countermeasures that can be in place to make secure applications.
- To teach the basics of web application security testing, considering this is not performed in the same way functional tests are.
- To make people understand that security must be considered in every single phase of software development life cycle, instead of at the end of the process.

7. Presenters

7.1 Nelson Uto, M.Sc.

Affiliation: CPqD Telecom & IT Solutions.

Contact information:

Professional e-mail: uto at cpqd.com.br.
Personal e-mail: nelson_uto at yahoo.com.br.
Phone: +55 19 8181 3778.

Short biography:

Nelson Uto holds a bachelor's and a master's degrees in Computer Science from State University of Campinas – Unicamp. During his M.Sc., worked, under the supervision of Dr. Ricardo Dahab, on a mobile agent systems security project, specially developing new security mechanisms for the Aglets system. Also reviewed scientific papers for conferences (SSI 2001, WSeg 2003, and CTIC 2003) and for the Journal of Universal Computer Science and published himself several academic papers in national and international security conferences.

Nelson has been an Information Technology professional for 13 years and an Information Security specialist for the last 7 years. He currently works at CPqD Telecom & IT Solutions as a Security Consultant and Researcher, in the areas of Cryptography and Application Security, and also as a PCI QSA and a PCI PA-QSA: he worked on cryptographic key management, evaluated free libraries supporting elliptic curve cryptography for the XScale and x86 platforms, performed pentests on several web applications as part of a risk analysis project, prepared hardening guidelines for Oracle and Unix systems, researched the application of K-Means clustering algorithm for semi-automatic generation of security event correlation rules, specified a security event management system, and elaborated security policies.

He also worked as a C/C++/Assembly x86/Java programmer and as an Oracle DBA. The most interesting projects he got involved include an ODBC-JDBC driver and a 4GL to Java translator, which automatically generated semantically-equivalent Java code from 4GL programs.

Finally, he coordinates a graduate program on information security and is a professor at graduate and undergraduate levels. He taught the following courses so far: "Information Security", "Introduction to Cryptography", "Operating Systems", "Data structures", "Object-oriented programming", "Introduction to Information Technology", and "Programming techniques".

Previous tutorials and talks:

- Software (In)security, in Portuguese, Puccamp, Sep/2008, 80 attendees.
- Introduction to Quantum and Elliptic Curve Cryptography – Part II, in Portuguese, Advanced Topics in Information Security, Stefanini-ITA, Feb/2008, 20 attendees.
- Software (In)security, in Portuguese, CPqD, Feb/2008, 90 attendees.
- Introduction to Quantum and Elliptic Curve Cryptography – Part I, in Portuguese, Advanced Topics in Information Security, Stefanini-ITA, Feb/2008, 20 attendees.
- Software Security, in Portuguese, Executive IT Meeting, Oct/2007, 25 attendees.

7.2 Sandro Pereira de Melo, M.Sc.

Affiliation: Locaweb.

Contact information:

Professional e-mail: sandro at 4nix.com.br.
Personal e-mail: sandro at ginux.ufla.br.
Phone: +55 11 9420 2941.

Short biography:

Sandro Melo has been working with Information Technology for 16 years, specially, as a network and security analyst. He worked for large companies such as EDS and currently he is employed by Locaweb, the largest hosting company in Latin America, where he is responsible for security incident response, computer forensics, and Linux administration and deployment.

He holds a bachelor's degree in Data Processing from Mackenzie University and a master's degree in Network Engineering from IPT/USP. He also attended graduate programs in System Analysis and Computer Networks from Mackenzie University and UFLA, respectively. During his M.Sc., worked under supervision of Dr. Antonio Rigo, wrote several technical reports and reviewed scientific papers for conferences. Sandro holds the following professional certifications: SCSA, Novell CLE, Novell CLP, Novell CLA, RHCT, LPIC 3, LPIC 2, and LPIC 1.

Besides articles in newspapers and specialized magazines, Sandro has published the following books by Alta Books:

- Security with Free Software, ISBN: 8576080265;
- BS7799 – From Tactics to Practice in Linux Servers, ISBN: 8576081261;
- Exploiting Vulnerabilities in TCP/IP Networks, ISBN: 8576081342;
- Computer Forensics with Free Software, ISBN: 9788576082880.

The most important professional achievements worth mentioning are:

- Invitation from Brazilian Presidential Committee on Information Security to give a Linux security course to high ranking army officers;
- Invitation from LPI Canada to prepare questions for the certification exam;
- Invitation from Italian consulate to work for the Kantea Project.

Previous tutorials and talks:

- Exploiting vulnerabilities and computer security, in Portuguese, Police Electronic Crimes Investigation Units of São Paulo, Rio de Janeiro, Pará, and Mato Grosso states, 12 attendees on average.
- Server-side Pentest, in Portuguese, Brazilian Presidential Committee on Information Security, 25 attendees.
- Server-side Pentest, in Portuguese, Ulbra University, 70 attendees.
- Computer Forensics, in Portuguese, Federal University of Ceará, 30 attendees.
- Network Forensics, in Portuguese, Federal University of Ceará, 30 attendees.