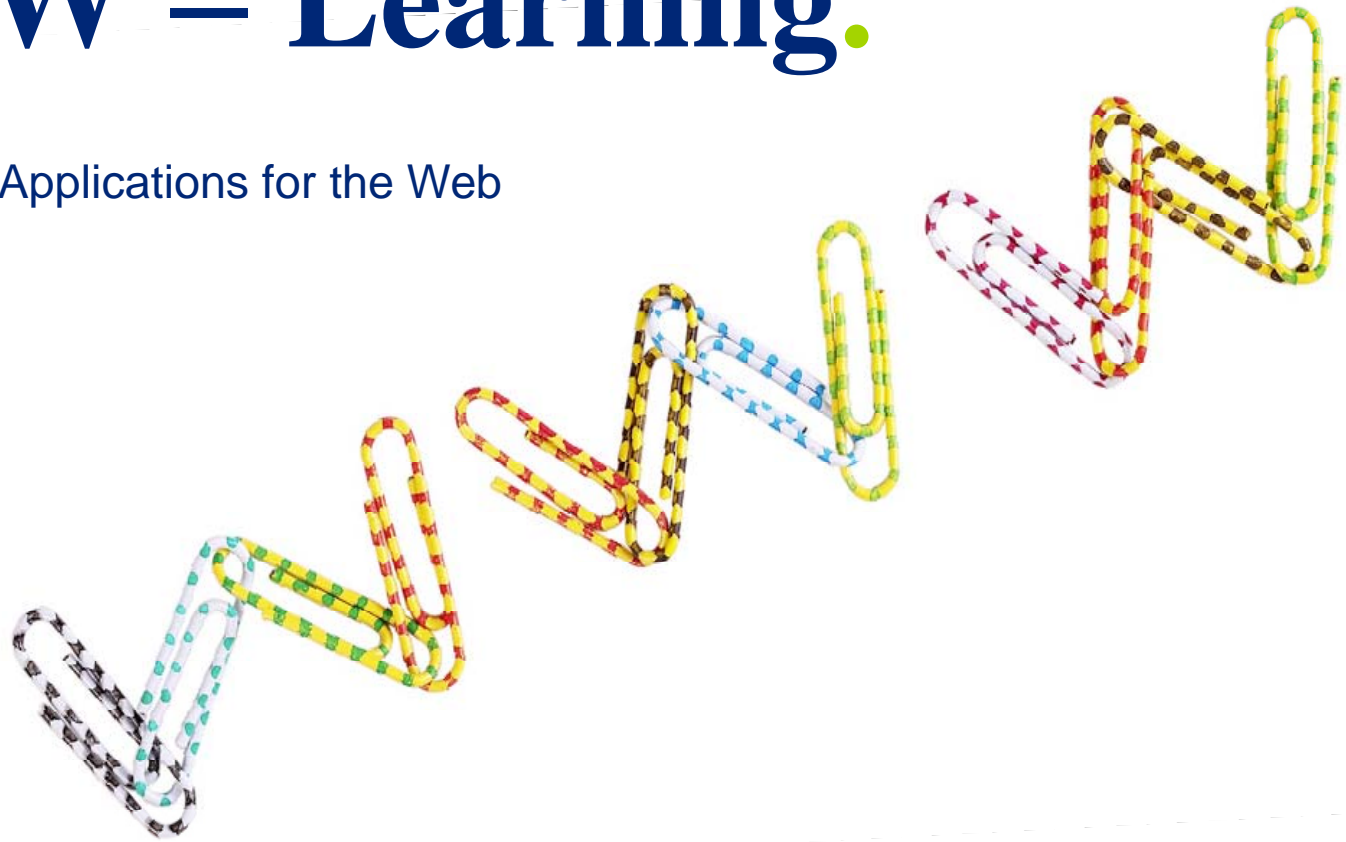


SAW – Learning.

Securing Applications for the Web



Course Introduction

Course Introduction

Welcome to the SAW (Secure Applications for the Web) classroom training.

There has been a dramatic increase in the number of web applications, due to wide reach, universal access, Web 2.0 and other factors – and a corresponding increase in attacks that target web applications. This course was developed by Deloitte Security and Privacy Services in South Africa. Its aim is to help learners gain an understanding of the web environment, common attack vectors, and how to architect, develop, and secure web applications.

Extensive emphasis is placed on practical learning. The course is highly participative, using a series of exercises that challenge participants to exploit, find, and fix code flaws. It also includes review sessions to reinforce the learning experience. This course will give participants the opportunity to practically apply the theoretical knowledge gained, while Deloitte's top software development specialist facilitates the learning.



Course Objectives

Course Objectives

At the end of this training, participants will be able to:

- Understand the common methods by which web applications are compromised.
- Identify code anti-patterns that could lead to a security issue.
- Correct existing flaws by writing more secure code.

Our Goals:

- Attendees should develop the ability to write better, more secure and more robust web application code
- Attendees should be able to reason more correctly about security and security countermeasures

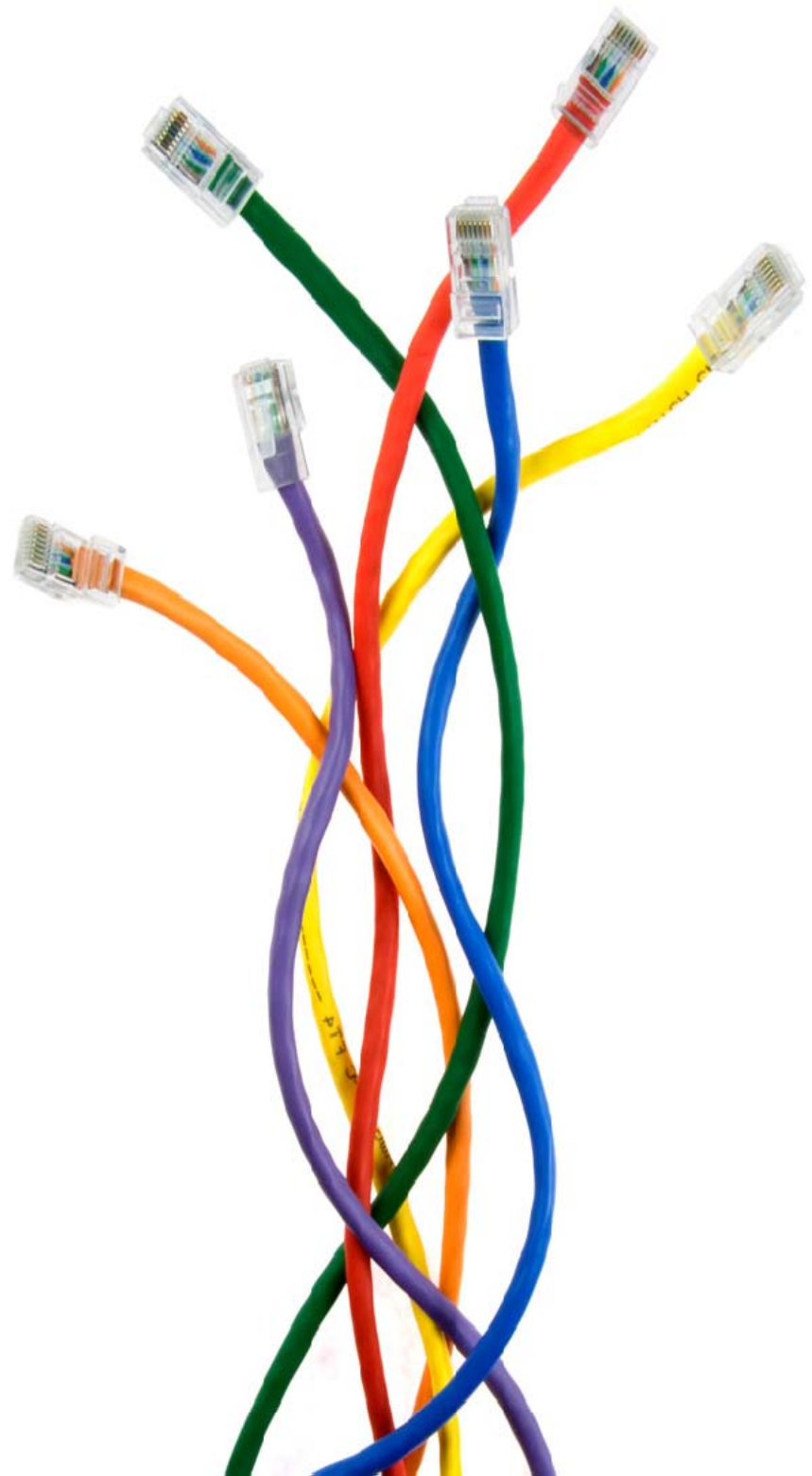
Audience?

- The course is aimed at senior software developers and software developers.
- The course is recommended to web developers who are involved in the security of web applications.

Programmes that will be used

Each participant is issued with a laptop with for the duration of the course:

- WebScarab
- Visual C# 2008 Express Edition
- Visual Web Developer 2008 Express Edition
- WinZip
- MySQL
- MySQL Query Browser
- MySQL Administrator
- SQL Server 2008 Express Edition
- SQL Server Management Studio Express
- Firefox 3, with
 - Web Developer Extension
 - Firebug Extension
 - TamperData Extension
 - Add N Edit Cookies Extension



Course Facilitators

Your Facilitator for the course

Software Development Specialist



Yusuf Motara
Facilitator for this course



Yusuf graduated with a M.Sc in Computer Science from Rhodes University in 2006. Since then, he has been developing software, auditing systems, and breaking web applications. He has a good working knowledge of security threats, security models, and software development. This mix lets him go beyond identifying and exploiting flaws to providing best practise recommendations on how to fix them – and how not to make the software mistakes that lead to them in the first place.

Course Schedule

Course Schedule

Day 1

08:00 – 08:30

Participants to arrive. Tea & Coffee served

08:30 – 09:00

Course Introduction and course objectives discussion.

09:00 – 10:30

The Language of exploitation - Theory

10:30 – 10:45

Tea Break

10:45 – 12:30

Pages

- Tags and Attributes
- Encoding
- Javascript
- Embeds / Other
- CSS (less-common attack vector)

Course Schedule

Day 1 continued . . .

12:30 – 13:15

Lunch Break

13:15 – 15:00

Protocols

- HTTP
 - Post / GET syntax
- HTTPS
- Data Queries
 - SQL
 - Xpath

15:00 – 15:15

Tea Break

15:15 – 16:30

TCP

16:30 – 17:00

Recap of Day 1

Course Schedule

Day 2

08:30 – 10:00

Never Trust the Client

10:00 – 10:15

Tea Break

10:15 – 12:00

Output is Input

- Browser output is server input
- Server output is browser input
- WebApp output is WebApp input
- DB output is WebApp input
- Third-parties

12:00 – 13:00

Lunch Break

Course Schedule

Day 2 continued. . .

13:00 – 15:00

Positively Simple Security

- Must be able to reason about security
- Must be able to test security
- Must be able to diagnose security issue causes

15:00 – 15:15

Tea Break

15:15 – 16:00

Positively Simple Security continued

- Must be able to withstand mechanism exposure
- Must be able to identify “good” input

16:00 – 16:30

Recap of Day 2

Course Schedule

Day 3

08:30 – 10:00	Mind your Language <ul style="list-style-type: none">•Standardised, tested code vs. custom-developed solution
10:00 – 10:15	Tea Break
10:15 – 12:00	Defence in Depth
12:00 – 12:45	Lunch Break

Course Schedule

Day 3 continued. . .

12:45 – 14:30

Common attack vectors

1. Injection

Risk: create, modify, read, delete info in data source

Risk: foothold for further penetration

Defence: structural validation (NOT mangling!)

Defence: parameterisation

14:45 – 15:00

Tea break

15:00 – 16:30

2. XSS

- Risk: hijacked browser session, user impersonations

- Defence: output encoding

- Defence: web-application firewall

16:30 – 17:00

Recap of Day 3

Course Schedule

Day 4

08:30 – 10:00

3. CSRF

- Risk: fraudulent transactions
- Defence: per-user, per page token checks

10:00 – 10:15

Tea Break

10:15 – 12:30

Path-traversal

- Risk:read arbitrary file (passwords, usernames, source code, etc)
- Defence: Chroot() or equivalent
- Defence: least-privilege process
- Defence: resource access via indexing

12:30 – 13:15

Lunch Break

Course Schedule

Day 4 continued. . .

13:15 – 15:00

Resource Starvation (denial-of-service)

Risk: Strained CPU, memory, disk space, WS-handles, DB connections

Defence: backgrounded, asynchronous operations

Defence: restrict users to one expensive operation at a time

15:00 – 15:15

Tea Break

15:15 – 16:30

Indexing and Error Messages

- Risk: information disclosure
- Defence: disable indexing and error messages

16:30 – 17:00

Recap of Day 4

Course Schedule

Day 5

08:00 – 10:00

Man-In-The-Middle

- Risk: session hijacking(active)
- Risk: fraudulent transactions(active)
- Risk: information disclosure (passive)
- Risk: credential disclosure (passive)

10:00 – 10:15

Tea Break

10:15 – 11:00

Resource Prediction

- Risk: access to unauthorised information
- Defence: robust access control mechanism

11:00 – 12:00

Session prediction

Risk: user impersonation
Defence: use framework/language-provided session-handling

Course Schedule

Day 5 continued. . .

12:00 – 12:45

Lunch Break

12:45 – 13:45

Encoding Attacks (Unicode, Double-encoding)

- Risk: access to unauthorised resources, bypass of access controls
- Defence: check that returned resource is allowed AFTER acquisition and BEFORE sending

13:45 – 14:00

Tea Break

14:00 – 15:00

Client-based security mechanisms

- Risk: the mechanism can be replaced, broken, debugged, traced, sniffed etc
- Defence: don't use one

15:00 – 16:00

Recap and feedback session

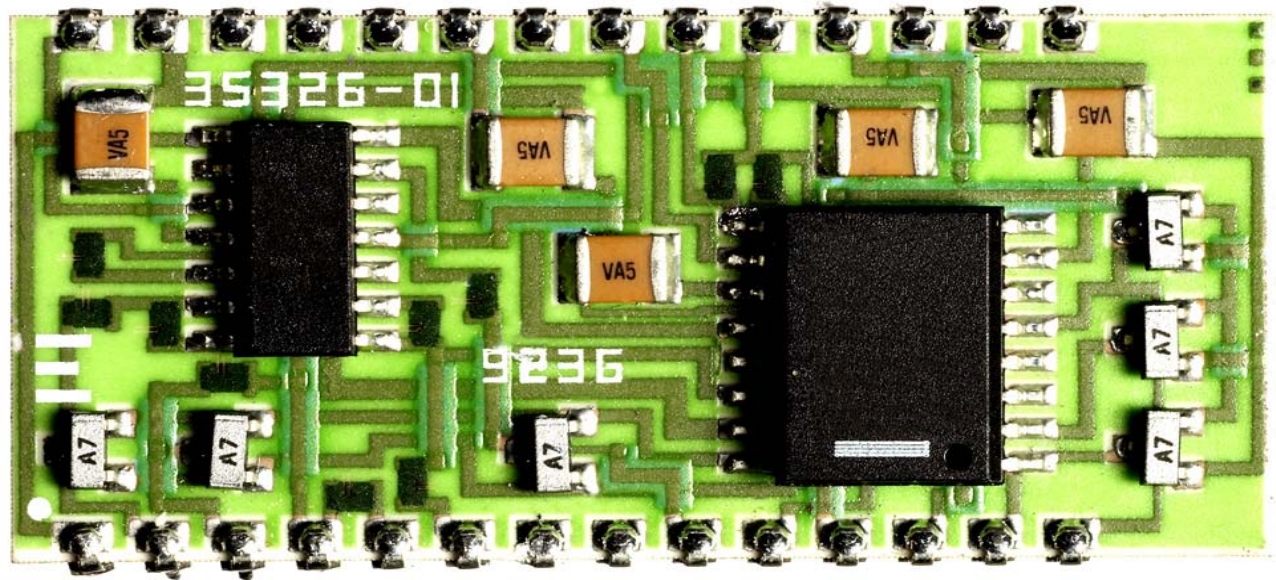
Deloitte External Learning:

Contact Carla Herbst on:

Tel: 011 806 5688

Cell: 084 443 4091

Email: cherbst@deloitte.co.za



Deloitte.