Highly relevant for all organisations that purchase, outsource or develop in-house their web applications

Master Class

Advanced Application Security

Master Class Leader

Fabrice A. Marie
Senior IT Security Consultant and Director
FMA Risk Management Solutions
A Professional Hacker Entrusted to Hack Enterprise Systems to Uncover Application Vulnerabilities and Provide Solutions

3 Days, **In-Depth, Practical Hands-On** Workshop will be conducted in the Computer Lab For Experienced IT Practitioners and IT Security Executives.

Class size is limited to 15 delegates. Computers will be provided.

Training benefits:

This is an in-depth technical hands-on class that aims at imparting knowledge, techniques and processes for:

- ☐ Testing the security of existing (live or UAT stage) applications
- ☐ Developing web applications securely
- ☐ Providing a neutral and non-vendor-centric perspective to evaluate the proper web applications for purchase

Course Benefits:

- ☐ Examine threats and vulnerabilities.
- ☐ Examine trivial and advanced techniques to uncover web vulnerabilities
- ☐ Each concept has a corresponding hands-on session with the assistance of the trainer
- ☐ Detail the proper way to fix or avoid each vulnerability
- ☐ Provide general management guidelines as well as deep technical explanations

Organised by:

FMA
Risk Management Solutions

The web landscape has had an explosive growth in the recent years. Early technologies put into use are beginning to show signs of weakness. For the past 5 years, security teams and operation managers had been putting all their security focus effort onto the perimeter and network security. Eventually, today most of the organisations understand the importance of network security. But keeping in mind that security is as strong as its weakest link, one quickly realises the importance of application security. Applications are definitely at the core of the company's business processes.

A cyber attack is often like lightning bolt: it strikes where it is the easiest to go through. Since network security is widespread and relatively well implemented, a potential attacker is naturally geared towards attacking the application. **Especially since there is no real tool today to prevent an attacker from accessing the application until at least the log-in prompt.**

Web applications are also rapidly getting bigger and more complex, which makes them extremely vulnerable. This inevitably gives rise to new avenues for hackers to attack applications easily. What's worse! Most of the web applications today are either purchased from a third party that comes along with a customization contract, or outsourced to an external developer.

Unfortunately, most vendors are pressured to release their application always faster and bigger, to a point where there is a clear lack of real security controls put in place.

Senior officers and managers in charge of these applications are now challenged with some burning concerns such as:

- Is the application really meeting the industry's regulations on privacy and frauds in general?
- How can we be sure that the application is reasonably secured since we do not have the source code?
- Can the application withstand an internal attack by disgruntled employees?

In view of these and many other arising applications concerns, this in-depth technical hands-on to impart knowledge, techniques and processes involved in:

- Testing the security of existing (live or UAT stage) applications
- Developing web applications securely
- Providing a neutral and non-vendor-centric perspective to evaluate the proper web applications for purchase

Course Benefits:

- Examine threats and vulnerabilities exposed through web services
- Examine trivial and advanced techniques to uncover web application vulnerabilities
- Each concept has a corresponding hands-on session on a real-life application, with the assistance of the trainer
- Detail the proper way to fix or avoid each vulnerability
- Provide general management guidelines as well as deep technical explanations

Who Should Attend

This is a Practical, Live Demo, In-depth Hands-on workshop limited to 15 delegates only. This Master Class aims to provide Senior Project Leaders, Corporate and Public Sector Information Processing Officers, with the resourcefulness that Business and Government organisations should possess about Application Security Architecture focused on WEB Services. This course is relevant for:

CIOs, CTOs, IT Architects, Directors / Managers of IT / IS / MIS / DP, IS/IT Planners, IT Strategists, Software Project Leaders, Integration Team Leaders and Database Administrators, Business Analysts and Consultants whose responsibilities include management, high-level design or enterprise business application implementation; e-Commerce Senior Managers, Application Development (AD) Senior Managers, Systems Architects, QA Managers will find this course useful.

Day One:

Part I – INTRODUCTION AND INJECTION ATTACKS

8.30am — Registration

9.00am — Session 1

INTRODUCTION TO APPLICATION SECURITY:

- Importance of application security
- What you will find in a typical web application
- What you need to know about vendors & outsourcing companies
- Crafting a fair contract between the licensor and the licensee.

10.20am — Morning Coffee Break

10.45am — Session 2

SUMMARY / REVISION OF HTTP "INTERESTING" FEATURES

- Introduction
- Drawbacks of HTTP and web applications
- Various encodings
- Tools used
- Information gathering in a nutshell

12.30pm — Lunch

1.45pm — Session 3

CROSS SITE SCRIPTING ATTACKS

- Definition
- Impact
- How to find cross site scripting vulnerabilities *(+ hands on)*
- How to exploit cross site scripting vulnerabilities *(+ hands on)*
- How to prevent cross site scripting vulnerabilities

3.30pm — Afternoon Tea Break

3.50pm — Session 4

SQL INJECTIONS

- Definition
- Impact
- How to find SQL injections vulnerabilities *(+ hands on)*
- How to exploit SQL injections vulnerabilities *(+ hands on)*
- How to prevent SQL injections

4.45pm — Questions and Answers

5.00pm — End of Day One

Day Two:

Part II – INJECTIONS AND FRAUDS

9.00am — Session 5

BUFFER OVERFLOWS:

- Definition
- Impact
- How to find buffer overflows vulnerabilities *(+ hands on)*
- How to exploit buffer overflows vulnerabilities *(+ hands on)*
- How to prevent buffer overflows

10.20am — Morning Coffee Break

10.45am — Session 6

XML & WEB SERVICES ATTACKS

- Definition
- Impact
- How to find Web Services vulnerabilities *(+ hands on)*
- How to exploit Web Services vulnerabilities *(+ hands on)*
- How to prevent W.S. vulnerabilities

12.30pm — Lunch

1.45pm — Session 7

LOGIC FLAW READ ATTACK

- Definition
- Impact
- How to find read logic flaw vulnerabilities *(+ hands on)*
- How to exploit read logic flaw vulnerabilities *(+ hands on)*
- How to prevent read logic flaw vulnerabilities

3.30pm — Afternoon Tea Break

3.50pm — Session 8

LOGIC FLAW WRITE ATTACK

- Definition
- Impact
- How to find write logic flaw vulnerabilities *(+ hands on)*
- How to exploit write logic flaw vulnerabilities *(+ hands on)*
- How to prevent write logic flaw vulnerabilities

4.45pm — Questions and Answers

5.00pm — End of Day Two

This course will be conducted in a Computer Lab. Every delegate will have a computer to work on during the course. As this is a practical, hands-on workshop, class size is limited to only 15 participants for maximum benefits. Hence registration is on the first-come-first-served basis. **Early confirmation is necessary to ensure vacancy.**

Day three:

Part III – MISCELLANEOUS ATTACKS AND PRACTICAL HACKING EXERCISE

9.00am — Session 9

AUTHENTICATION VULNERABILITIES

- Definition
- Impact
- How to find authentication vulnerabilities *(+ hands on)*
- How to exploit authentication vulnerabilities *(+ hands on)*
- How to prevent authentication vulnerabilities

10.20am — Morning Coffee Break

10.45am — Session 10

MISCELLANEOUS VULNERABILITIES

- Separation of duties problems
- Encryption implementation errors
- Deployment mistakes

12.30pm — Lunch

1.45pm — Session 11

SECURE DEVELOPMENT GUIDELINE

- Ultimate Input Validation
- Better Paterns
- Implementing full authentication
- Implementing full authorization
- Implementing full accountability

3.30pm — Afternoon Tea Break

3.50pm — Session 12

PRACTICAL HACKING EXERCISE

4.45pm — Questions and Answers

5.00pm — End of Course

About Your Course Leader

Fabrice A. Marie
Senior IT Security Consultant and Director
FMA Risk Management Solutions

Mr Fabrice A. Marie is the Senior IT Security Consultant and Director of FMA-RMS. He has many years of extensive and in-depth international industry experience in IT Security, spanning across the whole range of skills from security software development to security management via security testing.

Since 2002, he has been auditing major Singapore banks' Internet Banking Applications, as well as some of Singapore government's most critical applications.

He is a professional hacker, entrusted to hack and uncover the vulnerabilities of Singapore banks' internet banking before their complete online deployment, as well as for many government critical applications.

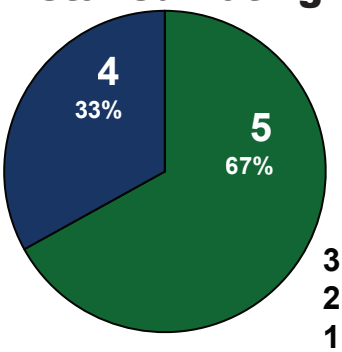
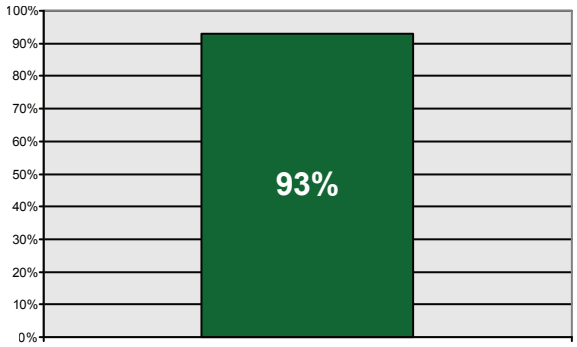
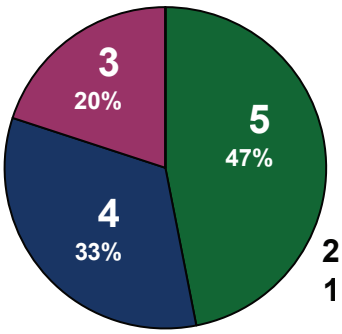
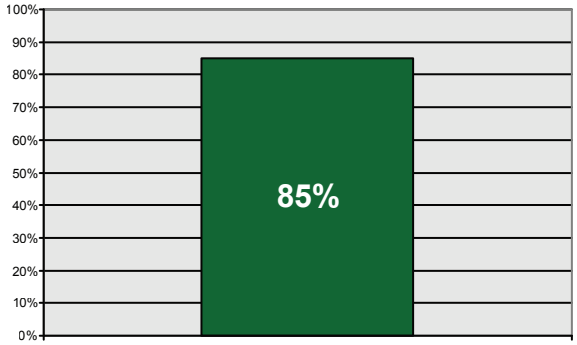
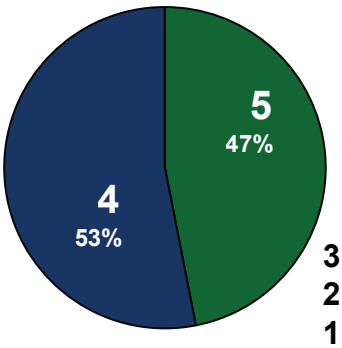
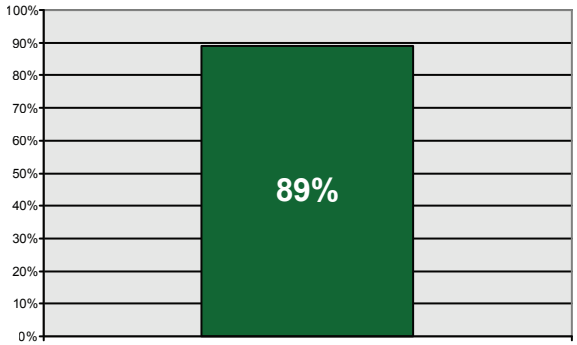
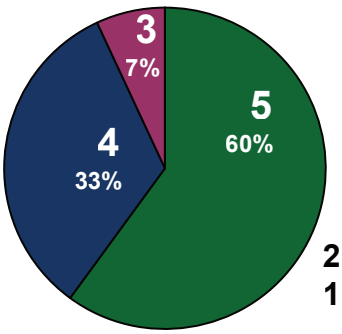
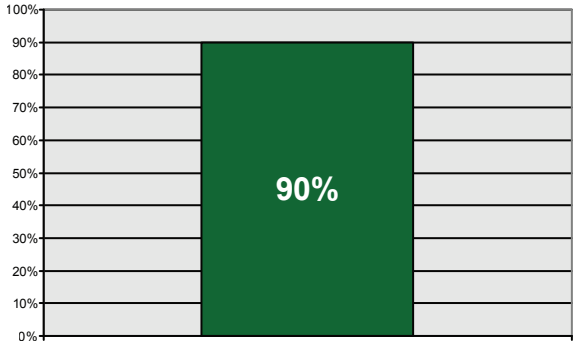
Software developer by profession, Fabrice started his career in Europe before moving to Asia. He pioneered, designed, implemented and secured Thailand's first secure payment gateway system. Since then, Fabrice has moved to Singapore. In Singapore he conducted systems and IT security courses; developed a few network security appliances; contributed to several major open source software components such as netfilter before specialising in security testing.

His career includes a broad span of projects on which he focuses on Information Security design, implementation and testing. Fabrice is a regular speaker and workshop leader at regional and international conferences on the subject of in-depth application security and in particular on the subject of Hacking Internet Banking Applications.

Fabrice's expertise and interests lie in secure programming, trusted operating systems, network protocols, advanced debugging techniques, cryptography as well as firewalling techniques.

Feedback Statistics

We are constantly seeking ways to improve the quality and relevance of our courses. Hence after each course, we invite our students to kindly give us feedback on how to better fulfill their needs. While this definitely helps us to increase the quality of our courses, it also provides a realistic and updated raw benchmark by which future attendees can judge the course.

	Detailed Rating	Average Satisfaction
Speaker's Knowledge	 3: 0% 2: 0% 1: 0%	
Speaker's Content	 2: 0% 1: 0%	
Speaker's Style	 3: 0% 2: 0% 1: 0%	
Speaker's Communication Skils	 2: 0% 1: 0%	

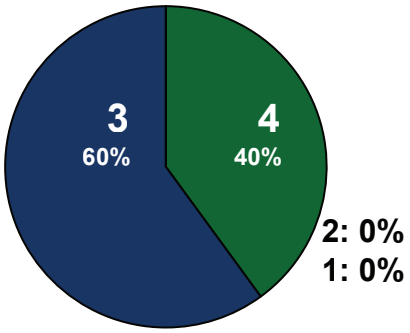
Ratings range between 5 (excellent) and 1 (weak).

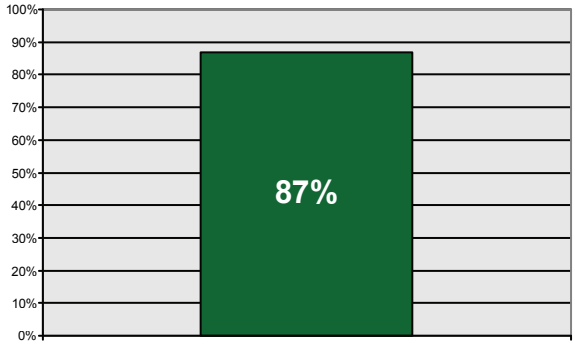
Feedback Statistics

Detailed Rating

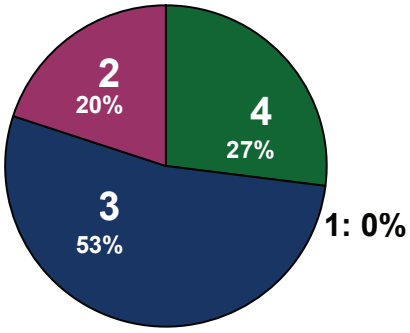
Average Satisfaction

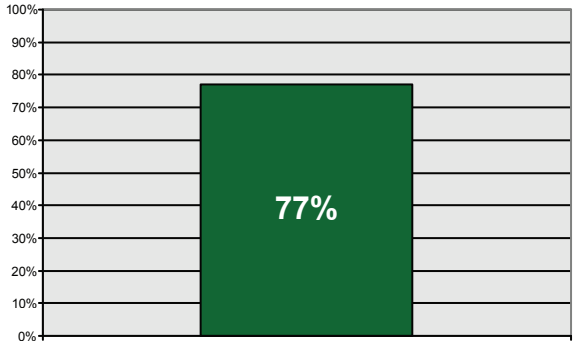
The program as achieved all if its objectives



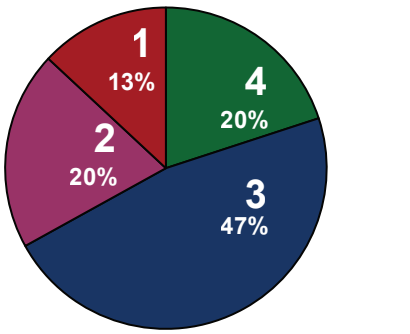


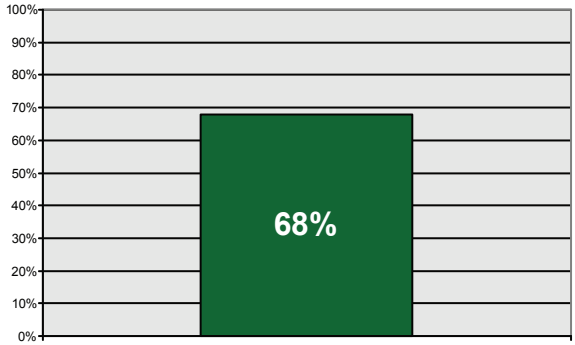
My personal expectations of the program have been met



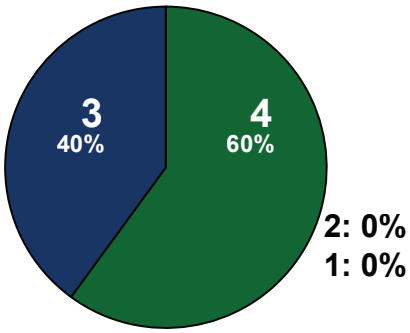


The topic is relevant to my current job scope and it provides me with a valuable knowledge and tools that is easily applicable to my current job scope

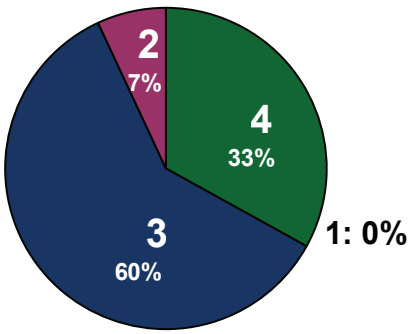


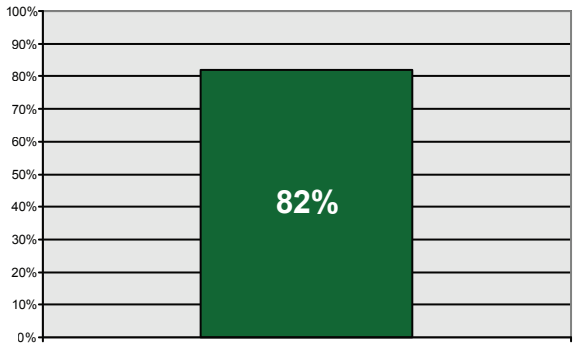


How do you rate our staff service and assistance?



Overall assessment of the course





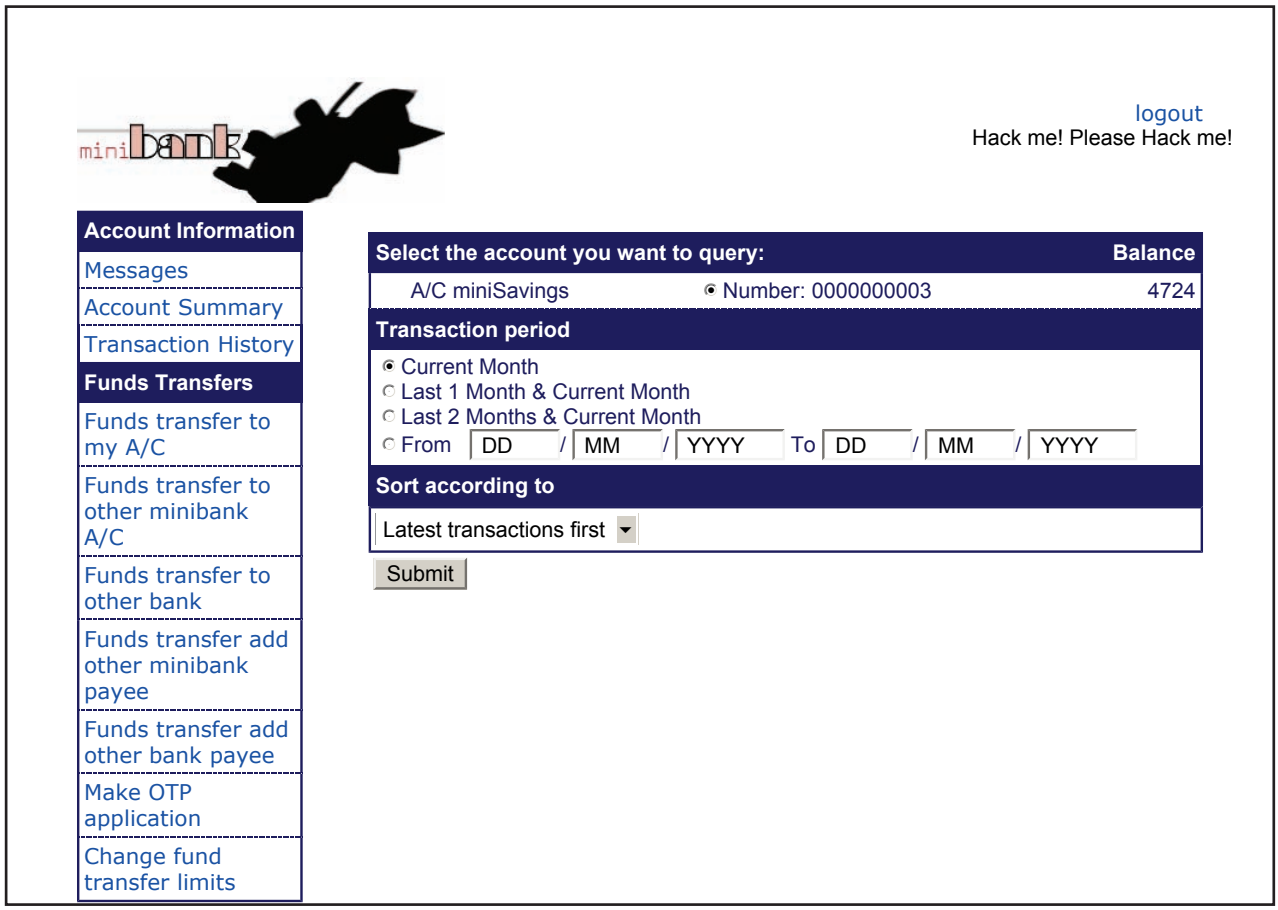
4: Excellent 3: Good 2:Satisfactory 1: Poor.

What You Get

Course attendees will get in a large binder:

- Hard-copy of all the slides
- Hard-copy of the hands-on assignments and solutions
- CDROM containing all the tools used during the course, and additional tools
- Free email questions to the trainer after the course
- An attendance certificate

We developed a mini internet banking application that mimics as close as possible real features as well as real security vulnerabilities. Attendees will apply their newly acquired knowledge by attempting to exploit the various security vulnerabilities we planted in the application, at the end of each session, with the assistance of the trainer.



More Feedback

"The course was held during an important phase of an ongoing project which is highly relevant"
– System Analyst in a Ministry

"Very much helps me designing proper security components"
– IT Department Head in a large Insurance Company

"Excellent!"
– IT Security Executive in a Ministry

"Refreshing and Enriching"
– Web Security Consultant working for our competitor!