



THINK LIKE A HACKER

Training In Real World Systems Security

Web Application Insecurities and Solutions Course

Online Course delivered from Sydney Australia

Register at <http://www.purehacking.com/training/>



PureHacking
Protecting Business Intelligence

Learn How To Think Like A Hacker

Are you a web application developer who needs to know how to code securely? How about a security professional who wants to learn more about attacks that can be performed against your web applications?

Pure Hacking is the only dedicated, vendor neutral Penetration Testing company in Australia providing training in up to date ethical hacking techniques.

Web Application Insecurities and Solutions Course

Learn the latest attack techniques commonly used to breach and exploit web applications today, and arm yourself with the ability to implement secure code and system configurations in order to actively protect against these attacks. This course bridges the vast security knowledge gap by:

- Educating students on the wide range of web application hacking concepts,
- Providing hands-on practical labs on exploiting these vulnerabilities to enforce the students understanding, and
- Arming each student with the ability to understand and implement the required countermeasures to ensure that your web applications, systems and data remain safe.



About Pure Hacking

Pure Hacking specialises in conducting independent security penetration testing and we are an impartial authority in the security field. Operating in 14 countries, Pure Hacking conducts internal and external penetration testing and application audits, providing ongoing security management and performing our penetration testing services globally.

Pure Hacking is engaged to assess the security of IT infrastructure and web applications that are at risk from internal and external threats which threaten business continuity.

Working with companies both large and small, predominantly in data intensive industries including government, finance, business services, communications, education and health, we have built a reputation for quality and excellence and our skills transfer is second to none.

"The team at Pure Hacking distinguish themselves by successfully communicating difficult concepts to all levels. They also followed through with their promise to continue support in explaining these concepts long after our contract finished."

IT Manager – Production Systems, International Business Services Corporation

Course Facilitator:

Ty Miller (OPSA and OPST, Certified OSSTMM Trainer)

Ty Miller is the Chief Technical Officer and Penetration Tester at Pure Hacking in Sydney, Australia. Ty has performed penetration tests against countless systems for large Banking, Government, Telecommunications, and Insurance organizations worldwide, and has designed and managed large security architectures for a number of large Australian organizations within the Education and Airline industries.

Ty presented at Blackhat USA 2008 in Las Vegas on his development of Reverse DNS Tunneling Staged-Loading Shellcode. He was also involved in the development of the CHAOS Linux distribution, which aimed to be the most compact, secure OpenMosix cluster platform available.

Ty is also one of the authors of the latest Hacking Exposed Linux book (3rd Edition) with his focus being on Web Application hacking.

He is a certified ISECOM OPST and OPSA Instructor, and contributes to the Open Source Security Testing Methodology Manual.

Ty holds a Bachelor of Technology in Information and Communications Systems from Macquarie University, Australia. His interests include web application penetration testing and shellcode development.

Web Application Insecurities and Solutions Course

Hacking web applications is now the primary attack vector to compromise an organizations systems and data. This is due to the lack of security awareness of web application developers and administrators. This results in vulnerable code being developed and insecure system configurations being deployed.

This course is a critical, eye-opening class for web application developers, web application system administrators, security professionals, and network architects.

The course teaches web application hacking concepts, with practical hands-on exploitation exercises to support concept understanding, as well as teaching students how to implement countermeasures for each attack technique in order to ensure that each student leaves the course armed with the ability to implement secure code and hardened web application system configurations.

Web Application Insecurities and Solutions Course is delivered online via the WebEx Training Center, enabling students to gain access cutting edge security professionals from their own workplace. Students perform lab exercises on virtual lab machines that are remotely controlled via a WebEx Hands-On Lab environment, providing each student with access to purpose built vulnerable web applications designed to teach students web application security concepts.

Prerequisites

Pure Hacking recommends students have some knowledge of web application concepts, such as coding and design. However, all required concepts will be covered throughout the course.

Since this course is delivered online, students are required to have a headset so that they can hear the audio of the course instructor and a microphone if they wish to participate or ask questions verbally. A text-based chat option is also available if a microphone is unavailable or not working correctly.

All students should have a fast Internet connection to ensure that a clear audio and video stream is to a high quality. Students will remote control virtual lab machines during each interactive activity.

Course Outline

Evolution of Hacking

A brief history of hacking, and how it has evolved into the advanced web application hacking techniques that we see exploiting organizations today.

OWASP Top 10 Overview

An overview of the top ten most common web application vulnerabilities being exploited in the wild.

Google Hacking

Students learn Google Hacking techniques to realise how easy it is to break into vulnerable web applications, and therefore the importance of web security.

HTTP Basics

Learning exactly how HTTP works brings varying skill levels of students up to scratch, and allows developers to fill the gaps in basic knowledge.

Web Application Profiling

Introduction into using penetration testing tools to quickly assess basic security of a web application.

Cross Site Scripting

XSS concepts, exploitation techniques, practical exercises, and countermeasures.

Sqli

Sql Injection concepts, exploitation techniques, practical exercises, and countermeasures.

Malicious File Execution

Learn how web applications can be manipulated into downloading malicious files to compromise web servers.

Insufficient Access Controls

Discuss common techniques that can be used to compromise the confidentiality and integrity of data.

Cross Site Request Forgery

Determine how it is possible to manipulate authenticated users web browsers in order to compromise their account.

Information Leakage and Error Handling

Learning how information leaked through HTTP headers and default errors can be used against an application.

Broken Authentication and Session Mgmt

Thorough analysis of how to bypass authentication controls and manipulate sessions to gain unauthorized access.

Insecure Cryptographic Storage

Discuss the techniques that should be used to protect the data stored within web application databases.

Insecure Communications

Using man-in-the-middle attacks to capture sensitive data including session tokens and authentication credentials.

Failure To Restrict URL Access

Exploiting a lack of access controls around restricted URLs to gain unauthorised access to application functionality.

Additional Course Information:

Duration	1 day (9am to 5:30pm)
Dates	Please check the Pure Hacking website for dates: http://www.purehacking.com/training/
Facilitator	Ty Miller, Chief Technical Officer
Cost	\$AUD1500 (x GST) – GST free for non Australian businesses
Location	Online via WebEx delivered from Sydney, Australia

To Register Visit Pure Hacking at <http://www.purehacking.com/training/>
Contact Robert McAdam on **1300 884 218** or training@purehacking.com
Book early to avoid disappointment

PROTECTING BUSINESS INTELLIGENCE

www.purehacking.com

Head Office

SYDNEY
Unit 13, Level 3,
84 Pitt St
Sydney, NSW 2000
Australia

MELBOURNE
Level 50,
101 Collins St
Melbourne, VIC 3000
Australia

POSTAL ADDRESS
GPO Box 3368
Sydney, Australia 2001

Tel: +61 2 9231 1134
Fax: +61 2 9231 1117
Free Call 1300 884 218
info@purehacking.com

Internet

B2B

Applications

VoIP

Wireless

Infrastructure

