

# Andrew van der Stock

7 Tierney Court, Highton  
Victoria, Australia, 3216  
[vanderaj@greebo.net](mailto:vanderaj@greebo.net)  
+61 410 685 509

## OBJECTIVES

To be a leading security innovator in the global information security community, and to build strong and secure solutions for my clients and employer.

I strongly believe in openness, learning and contributing basic research and development to application security field, with a strong focus on building secure software.

## EXPERIENCE

### Principal Consultant

February 2009 – May 2011

Pure Hacking, Geelong, Australia

Andrew was responsible for:

- Built the Web App Sec Practice from the ground up
- As Practice Lead, recruitment and growing a team of web app sec specialists
- Creating and delivering agile development security services
- Creating and delivering secure coding services, such as OWASP Application Security Verification Standard (ASVS) Level 2B and 3 Security Verifications and Security Architecture Reviews
- Creation and delivery of secure development and management training materials
- Penetration tests on web applications and infrastructure
- Research into new areas of web application security
- Speaking at conferences, breakfasts, and special interest groups

### Senior Security Engineer

November 2006 – January 2009

Aspect Security, Columbia, MD, USA

Whilst at Aspect, Andrew was responsible for:

- Delivery of acceleration services, including delivering boot camp one week induction and education
- Delivery of assurance services, code reviews, risk assessments, and penetration tests
- Research into new areas of web application security, particularly Ajax and web services and SOA security
- Creation of training materials, such as multi-day training on Ajax and Web Services / SOA and eLearning modules
- Delivery of training courses at large clients such as FedEx and Vanguard, as well as at conferences
- Speaking at conferences – multi-day training and speaking slots at Black Hat and OWASP conferences

Andrew moved to Columbia, MD (outside of Baltimore, MD) for this position.

## Skills

WebAppSec Master  
Practice Lead  
Staff Mentor  
Trainer

## Enterprise Security Architecture

Secure Architecture and Design  
Security Architecture Reviews  
Management Training  
Risk assessments  
Secure Coding Policies, Standards and Guidelines

## Web Application Security

Secure Coding Guidelines  
Secure Code Reviews  
Secure Code Advisor  
Secure Code Training  
Penetration Testing

## Languages

J2EE, .NET, PHP

## **Lead Author, SANS Top 20 (Web Application Section)**

2005 – 2008

SANS, Washington DC, USA

Andrew has led the web application security portion of the SANS Top 20 since 2005. His role includes:

- Recruiting new contributors and peer reviewers
- Writing the majority of the web application section's material, and updating it as necessary on an annual basis
- Editing contributors' material
- Managing the peer review process, and subsequent editing to reflect the comments

This is a volunteer position.

## **Project Lead / Executive Director / Global Chapters Committee**

2002 – Present

**Open Web Application Security Project (OWASP)**, an Internet project

Andrew has been a significant and long term contributor to the Open Web Application Security project. Andrew is the project lead and lead author of:

- **OWASP Guide 2.0** (2003-2005) – a 300 page book describing all facets of how to build and test secure software. Andrew re-wrote the majority of the book over a seven month period.
- **OWASP Top 10 2007** (2006-2007) – The top web application security standard, used widely by governments worldwide, the Payment Cards Industry (PCI) Data Security Standard (DSS) 1.2 – which requires all merchants worldwide to comply with the recommendations in the Top 10. Andrew performed the research, and re-wrote the Top 10 from scratch, and edited other author contributions during the peer review process.
- **OWASP Developer Guide 3.0** (2007-2009). Andrew led the OWASP Developer Guide project as of one of the three biggest projects at OWASP, updating the Developer Guide to include all the latest information that developers and architects need to create and build secure software.
- **OWASP Top 10 2010** (2008-2009). Andrew started the process of collecting the underlying statistics and research before handing over to Dave Wichers. Andrew reviewed the final output.
- **ESAPI for PHP** port (2008-). The eventual goal is to provide a feature rich, parity port of the ESAPI for J2EE implementation. This project provides common secure application controls, such as authentication, access control, logging, error handling, canonicalization for eight dialects such as HTML, JavaScript, CSS, command shells, etc, and an easy to use input validation mechanism, with automatic intrusion detection. The idea is to allow developers to concentrate on non-security related items, leaving the security elements to ESAPI, which should be secure by default.

Andrew's role on the Global Chapters Committee (2010 - ) is to provide local outreach at a global level.

As Executive Director (2005-2007), Andrew helped move OWASP to its current, more open board mechanism, and encouraged appropriate internal governance and transparency. During his tenure as Executive Director, OWASP grew immensely through his outreach efforts and conference appearances.

Andrew has spoken at many local chapter meetings, and established two separate local chapters (Melbourne and Sydney chapters). He has appeared at Black Hat and OSCON on behalf of OWASP.

This is a volunteer position at a non-profit organization.

### **System Administrator and Owner**

2002 - Present

**Aussievedubbers**, an Internet forum

Andrew has a significant hand in the day to day running of Aussievedubbers, one of the world's largest and most active Volkswagen forums (possibly #3 after the Samba and VW Vortex).

- Created and maintain initial shared infrastructure and current virtual private server (VPS)
- Day to day system administration of the LAMP stack (Linux, Apache, MySQL and PHP)
- Manage a large number of users (11,000+)

This position is a not for profit project, assisting over 11,000 Volkswagen enthusiasts worldwide.

### **Contractor / Security Architect**

January 2005 – November 2006

**National Australia Bank**, Melbourne, Victoria, Australia

Initially employed as a contractor by the NAB's preferred contracting agency, Andrew was brought in house in August 2005 as a Security Architect. Whilst at the NAB, Andrew worked on many internal and external projects. Some of the highlights include:

- Threat risk modeling
- Creation of secure coding standards for all the NAB's global divisions
- Security architecture for CBIB / NAB Connect, the business Internet Banking project
- Code reviews of Internet Banking, Wealth Management's external application suite
- Security architecture reviews of various internal and external projects such as the new EFTPOS terminals now used widely within Australia
- Creation and delivery of three day secure application training materials to over 150 developers and architects
- Post-incident management assistance
- Visited various US suppliers to meet and discuss first hand our security concerns (Tibco in San Jose CA, an ISV in Salt Lake City UT, and an ISV in Atlanta, GA).
- Spoke at OWASP EU in Leuven Belgium, OSCON in Portland, OR on Ajax Security and visited Black Hat at Las Vegas, NV in 2006

This position required travel within Australia, Europe and the USA.

### **Author, SANS GSSP J2EE Certification**

2007

**SANS**, Miami and Chicago, USA

Andrew worked with two other SANS authors to create numerous questions for the Department of Homeland Security (DHS) funded SANS GSSP Secure Programmer (J2EE) certification.

As Andrew helped set the exam, SANS deems that Andrew has this certification.

His role included:

- Question and answer creation
- Editing and reviewing other submitted questions
- Balancing the questions through a review process

This is a volunteer position. SANS paid for airfares and accommodation.

## **Chief Technologist**

2002 – 2005

**b-sec**, Melbourne and Sydney, Australia

Whilst at b-sec, Andrew was responsible for:

- Providing the technical direction of b-sec, research and development, staff training, mentoring and partner technical briefings
- Performing secure code reviews, developer mentoring and training, web application security tests, software engineering practice reviews, and code remediation, specializing in ASP.NET, PHP, ASP, and J2EE
- Extensive Policy, Standards, and Guidelines development for large multi-nationals and Australian financial institutions
- Threat risk assessments, risk management and treatment, usually focusing on technical risks.
- Consulting with a wide variety of large corporate clients on implementation, security architecture, business continuity / DR, intrusion detection, fraud control, vulnerability assessments / penetration tests, and forensics.
- Project management
- Pre-sales
- Provide senior management briefings for completed projects
- Formulate and maintain b-sec's AS4360's compliant risk management methodology
- The technical "public face" for b-sec with press and at conferences
- Staff recruitment and hiring
- Wrote the Checkpoint and Netscreen firewall log connectors for b-sec's flagship *Incident Analyzer* product in C# and unmanaged C++

Clients included Westpac, St George Bank, Rio Tinto, Linfox, IAG (NRMA Insurance), NEMMCO, Sunwater, amongst many others.

Andrew travelled extensively for this position, spending about 50% of his time in Sydney, and the rest between Brisbane, Canberra and his home town of Melbourne.

## **Senior Consultant / Architect / Senior Architect**

1998 – 2002

**e-Secure**, Melbourne and Sydney, Australia

- Long term appointments included being the acting Information Security Manager at Optus Internet and a senior security architect at Optus, working on technical risk assessments, reviews, and mitigation for many large scale Optus projects
- Assisted Westpac and Microsoft with the Joint Development Program, for rapid deployment of Windows 2000 prior to release. Andrew worked on group policy, general security issues, secure SOE deployment, and assisting with Westpac's Active Directory architecture

- Consulting with a wide variety of large corporate clients on policy, risk management, code reviews, future strategy, intrusion detection, fraud control, vulnerability assessments, and security architecture.
- Responsible for the security architecture of a range of nationally important IT infrastructures, including the re-architecture of Optus' internal backbone (Transit project) and a new national voicemail system for Optus residential
- Conducted technical interviews for prospective staff
- Mentored junior co-workers and clients

Clients included BHP, Optus, Westpac, VEC, amongst many others.

Andrew relocated to Sydney for three years, and travelled extensively along the east coast of Australia.

**Developer / Security Manager / Lead Developer** 2004 – (On Hold)  
**UltimaBB**, an Internet forum open source project

UltimaBB is a descendant of XMB. It is what XMB 2.0 would have been, if it were to be released.

Andrew worked on:

- Integrating and creating many new features destined for XMB 2.0
- Significant security review and remediation of the code base
- Porting the code to PHP 5
- Porting the SQL layer to prepared statements, making this the only PHP based forum that is invulnerable to SQL injection
- Refactoring the code to be modular and object oriented

Although UltimaBB runs a very large production forum (Aussievedubbers), development is on hold so that Andrew can concentrate on OWASP projects. There are no active developers, and the team has dissipated. It is envisaged only minor security fixes will be made on this project going forward.

This position was a volunteer open source project.

**Developer / Security Manager / Lead Developer** 2002 – 2004, 2008  
**XMB**, an Internet forum open source project

When Aussievedubbers was established, XMB was selected as the forum software. Unfortunately, it was found to be somewhat insecure, and so Andrew contributed initially a lot of security fixes, but eventually took over the reigns of the project.

Andrew worked on:

- Significant security review and remediation of the code base
- Writing significant portions of the current code base
- Released the long delayed XMB 1.9.x branch, which is still current today
- Acting as security manager, and encouraging XMB to close all known security holes (which resulted in XMB 1.9.10 and soon XMB 1.9.11)
- Refactoring the PHP scripts to be modular and object oriented

This position was a volunteer open source project.

## **Developer**

1999 - 2001

**pnm2ppa**, a low level print driver open source project

Andrew was a developer on the pnm2ppa project, which is included in most Linux distributions. The driver is written in C and X86 assembly.

- Incorporated changes to allow the HP 720c to print
- Sped up the implementation and reduced memory usage

This project is an open source volunteer project.

## **Senior System Administrator**

1997 – 1998

**North Western Health Care Network (NWCHN)**, Melbourne, Australia

- Responsible for the day to day management of one third of Victoria's health care system's IT infrastructure
- Primary e-mail administrator of 4500 users using Microsoft Exchange
- Primary DBA of production health system running Sybase under Unix
- Designed, architected, and secured network, Windows NT and Unix solutions to replace aging technology, including Year 2000 remediation
- Managed all DMZ infrastructure including proxy and firewalls
- Project management for a wide range of small to mid-range projects.

## **System Administrator / Senior System Administrator**

1996 - 1997

**St Vincent's Hospital**, Melbourne, Australia

- Responsible for the day to day management of St Vincent's 40+ servers and 1000 users.
- Primary NT, SMS, SCO Unix, e-mail administrator
- Designed, architected, and secured network, Windows NT and Unix solutions with particular reference to patient privacy issues
- Connected St Vincent's to the Internet
- Firewall, web and proxy manager
- Project management for a wide range of small to mid-range projects.

## **Developer**

1996 - 1998

**XFree86.org**, a low level graphic driver open source project

Andrew was a developer on the XFree86 project, primarily working on the Matrox Millennium graphic drivers in low level C, assembly and opcodes used by the GPU.

- Helped bootstrap the initial Matrox driver with others
- Sped up the driver to be one of the fastest and most stable 2D drivers in XFree86
- Worked on the Millennium II 8MB and Mystique (low cost) driver changes

This project was an open source volunteer project.

## **System Administrator / Tutor**

1995 - 1996

**RMIT University Business Faculty**, Melbourne, Australia

- Responsible for system administration of RMIT Business Faculty's servers and 700+ users.
- Responsible for e-mail, Novell, and Macintosh systems
- Developed and delivered a 13 week tutorial course on Internet technologies for Business faculty post grad students
- Tutored CS 101 for undergraduates

## **Web Master / Project Worker**, Sociology Department

1994 - 1995

**University of Melbourne**, Melbourne, Australia

- Established and managed one of the first web sites at University of Melbourne
- Performed project work for the YARN project, part of the Department of Sociology

## **Programmer / Software Quality Assurance**

1993 - 1995

**Nemostar**, Melbourne, Australia

- |      |   |
|------|---|
| 1993 | Ported a Windows 16 bit marketing database product to Macintosh (C++, using classic 32 bit MacOS API) |
| 1995 | Assisted with the development of the Macintosh version of Flexifax (C++)                              |
| 1995 | Software Quality Assurance for Flexifax   |

## **EDUCATION**

---

### **Industry training and certifications**

- |      |   |
|------|---|
| 2007 | Set the SANS GSSP Secure Coding Professional Certification (Java), and as such, Andrew is deemed to hold this certification |
| 2000 | Microsoft Certified Systems Engineer (Windows 2000 MCSE)  |
| 1998 | Microsoft Certified Systems Engineer (NT 4.0 MCSE)  |
| 1997 | Networking Essentials (Self Paced, CBT)   |
| 1997 | Supporting Systems Management Server 1.2 (Aspect ATEC)  |
| 1997 | Exchange 5.0 Core Technologies (Aspect ATEC)  |
| 1997 | Microsoft SQL 6.5 Administration (Aspect ATEC)  |
| 1996 | Supporting Windows NT Workstation 3.51 (Educom ATEC)  |
| 1995 | Supporting Windows NT Server 3.5 (Aspect ATEC)  |

## **Computer Science / Software Engineering, Bachelor of Applied Science** 1990 – 1994

**RMIT University**, Melbourne, Australia

Studies included CS first and second year subjects, and second year software engineering subjects and team projects. Elective studies included Beginner Japanese and Mandarin Chinese context curriculum classes.

This degree is incomplete, with approximately 50% of the classes successfully undertaken. A full transcript of results can be supplied if required.

## **Electronic Engineering, Bachelor of Engineering**

1989

**Monash University**, Clayton, Victoria, Australia

Andrew enrolled in this course, and quickly realized that he was better suited to Computer Science as he achieved a high distinction in that subject.

This degree is incomplete.

## **Higher School Certificate, "A" (Science) Stream**

1984 – 1988

**Melbourne High School**, South Yarra, Victoria, Australia

Andrew attended one of Australia's premier elective entry schools. Melbourne High School regularly tops the academic ladder in Victoria. Melbourne High School alumni have the largest number of entries in the Australian Who's Who compared to any other Australian school, with many prime ministers, politicians, doctors, researchers and other notables. A full transcript of results is available if required.

## **CONFERENCES, PAPERS AND SYMPOSIUMS**

---

Andrew is an accomplished public speaker, and relishes any opportunity to present, entertain or educate – preferably all three! The following list does not include OWASP local chapter or other user group appearances, such as PHP meet ups or similar.

2011	itSMF, Perth, Australia, Speaker
2011	AusCERT 2011, Gold Coast, Australia, Trainer
2009	OWASP AU, Gold Coast, Australia, Speaker
2008	BlackHat, Las Vegas NV, Trainer
2007	SANS Top 20, 2007, Lead Author of Web Application Section
2007	OWASP Top 10 2007, Project Lead / Lead Author
2006	SANS Top 20, 2006, Lead Author of Web Application Section
2006	OSCON, Portland OR, Speaker
2006	OWASP EU, Leuven, Belgium
2005	SANS Top 20, 2005, Lead Author of Web Application Section
2005	OWASP Guide 2.0 For Building Secure Software, Project Lead and Lead Author
2005	Ruxcon, Sydney, Invited speaker
2005	Blackhat, Las Vegas, Invited speaker
2003	SAGE-AU, Tasmania, Invited speaker
2003	AusCERT, Gold Coast, Tutorial Presenter
2002	SAGE-AU, Melbourne, Tutorial Co-author
2002	AusCERT, Brisbane Tutorial Presenter
2002	linux.conf.au, Brisbane, Speaker
2001	Blackhat, Las Vegas, International Speaker
2001	linux.conf.au, Sydney, Speaker
2000	AOSS2, Adelaide, Speaker
2000	SAGE-AU, Gold Coast Australia, Speaker

1999 SAGE-AU, Sydney, Tutor & Speaker  
1997 SAGE-AU, Melbourne, Speaker

## **ELECTED POSITIONS**

---

2010 – Global Chapters Committee, OWASP  
2005 – 2007 Executive Director, OWASP  
2000 – 2001 SAGE-AU President  
1999 – 2000 SAGE-AU Executive Committee Member  
1998 – 1999 Vice President, SAGE-Au Victorian Regional Group  
1997 – 1998 National Returning Officer for SAGE-Au  
1995 – 1996 Publicity Officer for SAGE-Au

## **AWARDS**

---

2007 Aspect Security Rock Star Award  
2002 SAGE AU Award for Outstanding Contribution