

Andrew van der Stock

OWASP Foundation



BLACK HAT BRIEFINGS

World Exclusive – Announcing the OWASP Guide To Securing Web Applications and Services 2.0

After three years of community development, the Open Web Application Security Project (OWASP) is proud to introduce the next generation of web application security standards at BlackHat USA 2005. The Guide to Securing Web Applications and Services 2.0 is a major new release – written from the ground up, with many new sections covering common and emerging risks, including:

- How to design more secure software
- How to conduct a security review using the Guide
- How to perform the most difficult web application processes correctly: processing credit cards, interacting with payment gateways (such as PayPal), and anti-phishing controls
- Reorganized and easily navigated chapters on web application controls including: web services, comprehensive authentication and authorization controls, session management, data validation, interpreter injection, and many new controls within existing chapters
- Secure configuration and deployment
- And software quality assurance.

The Guide has adopted and extended the popular OWASP Top 10 approach – security objectives, how to identify if you are at risk, with recommended remediations in three popular frameworks, and further reading. The Guide is platform neutral, and has examples in J2EE, ASP.NET and PHP. The Guide 2.0 is on the conference materials CD-ROM in its entirety. As it is free (as in beer as well as in freedom), you can redistribute or print it as often as you wish.

To demonstrate the incredible versatility of the Guide and its pragmatic approach, we will be conducting a live security review of software selected at random by the audience. To perform the review demonstration, we will be using just a few off-the-shelf web development tools with Firefox to demonstrate how easy it is to subvert the average application, and how simple it is to fix issues properly by using the Guide.

We expect this talk will be useful to all attendees, but those who set secure coding standards within their organization, manage risk from custom software, manage software development or are software architects or developers will benefit the most from attending this session.

Andrew van der Stock is among the many contributors to the OWASP project over the years. Andrew has presented at many conferences, including BlackHat USA, linux.conf.au, and AusCERT, and is a leading Australian web application researcher. He helps run the OWASP Melbourne chapter, started the OWASP Sydney chapter, and is ex-President of SAGE-AU, the System Administrator's Guild of Australia. You can read more about OWASP, the Open Web Application Security Project at <http://www.owasp.org/> and you can read more about Andrew at <http://www.greebo.net/>.

OWASP Guide 2.0

Andrew van der Stock, vanderaj@owasp.org

What is OWASP?

- Non-profit, volunteer driven organization
- Provide free resources to the community
- Publications, Articles, Standards
- Testing and Training Software
- Local Chapters & Mailing Lists

Projects

- Top 10
- Criteria
- Testing
- ISO 17799
- AppSec FAQ
- WebGoat
- WebScarab
- CodeSpy
- C# Spider (and other .NET projects)
- Sphinx
- Stinger J2EE Validation
- PHP validation filters

Finished!



Guide 2.0

- Three years in the making
- Major new version
- Complete from the ground re-write
- Adopts OWASP Top 10 approach
- Peer reviewed

Guide 2.0

- Now has information on web services!
- Three times the length of the old standard
- Approximately 10x controls
- Deals with nearly all web application security issues

What's New?

Lots of advice

- Advice for SOX / COBIT / ISO 17799
- Threat Risk Modelling
- Credit card and payment gateways
- Anti-phishing
- Best practices for secure development

Web Services

- Finally
- WS-Security
- SAML
- XML-DSIG
- Lots more...

Lingua Franca

- You write in .NET, PHP, J2EE, Perl, Ruby, Python
- We have examples in most languages
- PHP Security Appendix
- Web App Security is rarely about the technology in use

What's improved?

Every Chapter

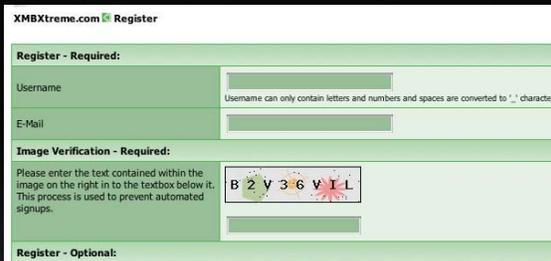
- Guide 1.0 - 92 pages, approximately 50 controls
- Guide 1.1 - 84 pages, approximately 60 controls

Guide 2.0 ~350 controls



Authentication

- Major re-write
- Best practices summarized
- Strong authentication
- ~ 30 controls
- How to test for vulnerability
- How to fix the vulnerability



XMB Xtreme.com Register

Register - Required:

Username
Username can only contain letters and numbers and spaces are converted to "." character.

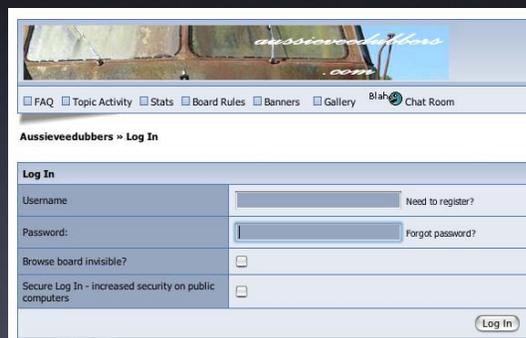
E-Mail

Image Verification - Required:

Please enter the text contained within the image on the right in to the textbox below it. This process is used to prevent automated signups.



Register - Optional:



Aussievedubbers » Log In

Log In

Username Need to register?

Password: Forgot password?

Browse board invisible?

Secure Log In - increased security on public computers

Authorization

- Access controls
- Coverage
- Client side SSO tokens
- Administrative interfaces

Session Management

- Complete re-write
- What does your app really need?
- Session Fixation
- HTTP Split Session Attacks
- HTTP Request Smuggling

Error / Log / Auditing

- Complete re-write
- Traceability - aims for SOX compliance
- Minimal information gathering surface area
- Don't log noise

The MOST important
control is ...

Data Validation

- Complete re-write
- Shorter!
- State of the art validation strategies
- “Sanitize” is no longer an acceptable first choice
- Offers practical advice in several languages

Interpreter Injection

- SQL Injection

Interpreter Injection

- SQL Injection
- User agent injection
- Code Injection
- LDAP Injection
- ORM Injection
- OS Injection
- XML Injection (XPath / XSLT)

Canoncalization

- One of the last bastions of unexplored vulnerability
- Very hard to protect against
- Unicode
- Locale
- Canonicalization

File System

- Minimize dangers from file based operations
- Unreferenced files
- Permissions
- Unmapped extensions
- Temporary files

Buffer overflows

- New(ish) section for one of the oldest security problems
- Heap, Stack, Buffer overflows
- Integer and array overflows
- Unicode overflows
- String format overflows

Administrative Interfaces

- There aren't many things required by law
- This one is.

Administrative Interfaces

- Must have segregation of duties
- Security through obscurity is no longer good enough
- Strong authentication

Cryptography

- Revamped section
- Future proofing (SHA1 / MD5)
- How to select algorithms
- Poor secret storage
- Which SSL algorithms you need to disable

Privacy

- Completely revamped
- Various EU, AU, and US laws compared
- Information disclosure
- “Front page of the paper” test

Secure Deployment

- New section
- Secure out of the box
- Automated installs
- Minimal attack surface area by default

Configuration

- New Section
- Code Access Security Policies
- Default passwords (NO!)
- Clear text passwords in config files
- Connecting to RDBMs and middleware
- When is encrypted data necessary

Software Quality Assurance

- New Section
- How to improve your SQA to cover web application security
- Coverage
- Types of testing (unit, injection, code reviews, pen tests)

PHP

- Chapter dedicated to PHP
- Lots of cool information on writing secure PHP scripts
- Will be joined by ASP.NET and J2EE in 2.1

XSS Cheat Sheet

- Robert Hansen (RSnake)'s Cheat Sheet
- 95 different ways to inject code
- Essential to test your apps with this list

Does it actually work?

XMB

- Yes
- Only one patch since May 2004
- Previous releases used to require quarterly updates (roughly the same as phpBB today)

What's next?

Guide 2.1

- Due November 2005
- Fixes, reviews, and new content
- Available in Word, PDF... and *book* form
- **No Starch Press** will be publishing the Guide 2.1 around November 2005

What's in the pipeline?

Testing Project

- Guide is good for developers
- The Testing Project: How to perform
 - Threat Modeling
 - Code Reviews
 - Penetration Testing

Call to action!

BLACK HAT BRIEFINGS

- Firewalls don't help any more
- Review the Guide
- Make it your standard
- Threat Model
- Review your code and fix the problems



www.owasp.org