Secure Web Applications

The front line defense
Agenda

- Web Application Security Threat Overview
- Exploiting Web Applications – Common Attacks & Preventative techniques
- Developing Secure Web Applications – Security Considerations
- Managing Application Security
- Developing Secure Applications – Security Considerations
- Acquiring Web Applications – Security Considerations
- Auditing Web Applications
About Security-Assessment.com

• Specialise in high quality Information Security services throughout the Asia Pacific region

• Our aim is to provide the very best independent advice and a high level of technical expertise while creating long and lasting professional relationships with our clients

• We are committed to security research and development – Identifying & responsibly publishing vulnerabilities in public and private software

• We are an Endorsed Commonwealth Government of Australia supplier

• Sit on the Australian Government Attorney-General's Department Critical Infrastructure Project panel

• Certified by both Visa and MasterCard under their Payment Card Industry Data Security Standard Programs
Web Application Security Threats

Threat and Risk Overview
The Principle of Application Security Threats

Wherever a person or system interacts with, or has the opportunity to interact with an application there is a threat / risk opportunity for applications and information to be compromised.

The benefits of Web Applications including global accessibility, open source and rapid development opportunities increase these threats exponentially !!!
The Importance of Securing Applications

- Often a web application is the only thing standing in the way of an attacker and sensitive business information.

- Web application attacks account for 2/3s of all attacks.

- Firewalls only stop network service attacks.

- Depending on the application an attacker may be able to:
  - View or manipulate sensitive information.
  - Obtain unauthorised access to an application.
  - Be able to take control of the whole application.
Application Security & Cyber Crime

People are spending a lot more time online and spending a lot more money online. As the monetary value of online activity grows so does the correlation between Application Attacks and Organised and Financial Crime.

- **Industry Misconceptions**
  - One off hacks
  - Internal employees
  - Hackers out to make a name for themselves

- **The facts**
  - Organised Cells
  - Sophisticated Attacks
  - Identity Theft and theft targeting individuals.
  - Flexibility and anonymity perfect for money laundering

---

Australian High Tech Crimes Unit – Presentation on PCI Data Security Compliance
Cyber Crime - Examples

- **Feb 2006 – Sydney.** 400 customer credit card details compromised. Investigations by the HTCC identified 478 attempts over 3 days using 6 different IP’s to access administrator passwords. Intrusions originated from Germany, USA and Indonesia. HTCC Presentation on PCI Compliance.

- **Oct 2006 – Sydney.** Hackers compromised Nortel PABX to make AU$9,000 worth of calls in a week to Arab Emirates, South America and Africa. ZDNet Australia 17th October 2006

These are just a few that made the press…. Every day we see and hear so many dangers facing organisations through unsecured applications.
Hackers go after the weakest links - People and Web Applications. Advanced attacks focus on compromising applications not web servers because any information entered via the web page almost always reaches the backend database server.

Attackers only require one exploitable weakness to compromise an application.

A well planned and executed web application security review will find all potential weaknesses (at a given point of time).
Organisations may be compliant but not secure – Compliance is often little more than a false sense of security. Compliance is important – but only of value if done within the context of threat & Risk Mitigation and not just merely ticking the boxes.
Security Compliance Issues

- Standards too high level, generic and flexible to scope interpretations
  - Eg ‘Technical vulnerability management should be implemented’
    ISO 17799:2005

- Compliance Audits can give an application the tick but them be full of serious weaknesses giving a false sense of security

- IT Auditors often do not fully understand Application Security Threats and take these into consideration during an Audit. IT Auditors need better education to distinguish between compliance and security and when to bring in the experts where necessary

- Too often Application Security Audits are undertaken by organisations that are not proficiently skilled in this area
Exploiting Web Applications

Common Attacks & Preventative techniques
Web Application Exploits Overview

Application Attacks vary and evolve rapidly to exploit newly created or identified vulnerabilities as do the reasons and consequences of attacks.

- Some of the common attack methods / strategies.
  - Cross Site Scripting
  - Cookie Attacks
  - HTML Page Inclusion
  - Site Redirection
  - Page Order skipping
  - Command Execution through scripts
  - Filename attacks
  - Database Interaction
  - SQL injection
  - SMTP Command injection
  - File upload system attacks
  - HTTP Headers
  - Hidden Fields
  - Page Naming
  - HTML Comments
  - Extreme Conditions / DOS
  - Error Messages
  - Help Files
OWASP Overview

- De-facto industry standard for web application security
- Open source initiative maintained & developed by information security professionals world wide.
- Promotes security research around new web based vulnerabilities and provides tools and methodologies for conducting web application security assessments.
- Publishes the OWASP Guide for building secure web applications.
- Sets the minimum security baseline for a web application
- List of weaknesses that are actively sought out and exploited by attackers within web applications
OWASP Top 10 Security Threats

- **No validation of user input.**
  - Most commonly found vulnerability. User input is entered via the browser is automatically trusted by the server to be correct & logical
  - Little to no validation performed by server code to determine whether or not the input supplied was valid
  - Ensure that the application accepts known, good input & verifies the supplied input at every instance it is received

- **Improper access control**
  - improper enforcement of restrictions on actions that an authenticated user is able perform
  - Difficult to implement robust access control and authorisation
  - Examples – Accessing another user's data, Access to sensitive files, Administrative functions
  - Document a Security Policy & Access Control Matrix defining access control rules. Do not allow admin login over the internet, TEST, TEST, TEST
OWASP Top 10 Security Threats

- **Improper Authentication & Session Management.**
  - Common problem with web applications. Even when authentication is carried out properly, the authentication credentials are not adequately protected
  - Insecurities in credential management – e.g. password reset, change, remember etc
  - Examples
    - A google search for “inurl: phpsessionid” returns many examples of poor session management
    - Credentials passed within unencrypted transport for sites conducting financial transactions
    - Sequential session tokens e.g. 1000, 10001, 1002
  - Protection – Plain old password policies, protections for Session ID’s, Avoid implicit trust relationships
OWASP Top 10 Security Threats

• **Cross Site Scripting**
  – Attack directed against the users of a website by exploiting flaws within web pages. Malicious code sent to users web browser
  – Goal is usually to steal login credentials, conduct phishing attacks & gain access to user machines
  – Protection – Ensure application performs rigid validation of all input

• **Buffer Overflow Attacks**
  – Server components can contain routines that do not properly validate user input causing the process to either crash or be remotely controlled by the attacker
  – Usually results in either a Denial of Service or server compromise allowing an attacker to gain complete control of the system
  – Buffer overflows found in widely used server products are likely to become widely known and can pose significant risk to users of these programs
  – Protection – Develop an ongoing Vulnerability Management Program
OWASP Top 10 Security Threats

• **Code Injection**
  – Malicious Code is relayed via the web application to another system. E.G. calls to the underlying operating system or backend databases
  – Example SQL Injection
  – Protection – Validate all data provided to ensure that it does not contain malicious content. Use Stored procedures where possible, check all application return codes and error codes to determine if an error or incident has occurred. Undertake source code review

• **Improper Error Handling**
  – Error conditions that occur during normal operation may not be handled properly
  – If an attacker can cause errors to occur that the web application does not handle, they can gain detailed system information, deny service, cause security mechanisms to fail or servers to crash
  – Fail Open Errors
OWASP Top 10 Security Threats

• Insecure Storage
  - Most web applications need to secure information in transit and / or storage
  - Weak mechanisms (poor development standards)
  - Credentials stored insecurely on the server
  - Protection – Instead of storing and encrypting credentials, require them to be provided whenever required and use well known and publicly validated encryption algorithms instead of proprietary techniques, Secure storage of tokens away from public access

• Denial of Service
  - Attempt to consume web application resources to the point where regular uses can no longer use the application
  - Locking out user accounts en-masse
  - A web application cannot tell the difference between a normal request and a DoS attack
  - Protection – Limit the allocation of resources to user sessions. Avoid granting unnecessary access to resources for unauthenticated users
OWASP Top 10 Security Threats

- **Insecure Configuration Management**
  - Vendors server products are usually not shipped secure out-of-the-box. They come with a large number of configuration options most of which may be turned on by default.
  - These configuration settings may introduce weaknesses that can be exploited.
  - Examples – Directory traversal, unpatched software, sample files and admin scripts, improper file permissions, default user accounts, detailed error messages.
  - Protection – create a hardening guide for servers, configure all security mechanisms (or at least evaluate and document their use, create a set of operational procedures, logging, monitoring and reporting.)
Demo

Hackme
A Practical Demonstration on how Attackers exploit web applications

AND HOW WE FIND YOUR VULNERABILITIES BEFORE THEY DO.
Managing Application Security

A Strategic Security Management Framework
Don’t use 17799:2005, PCI DSS or any other standard as a fits all checklist. Control definition needs to be integrated with the risk management process.
Strategic Security Management Principles

- Security Controls must be wrapped within a Strategic Security Management Framework that includes:
  - Management & Governance
  - A Definition of accountabilities, roles & responsibilities
  - A strong Risk Assessment framework
  - A process to define, consolidate and rationalise the organisations regulatory, compliance & contractual security requirements
  - Policies & Standards aligned to business processes, communicated and understood across the organisation and endorsed by business leaders
  - A training & awareness program
  - A continuous Security compliance & assurance program to ensure policies are being implemented as expected, and to identify information security gaps and emerging threats
  - A process for planning for and managing security incidents
Strategic Security Management Framework

- A management methodology for managing information security
- Aligns to all industry standards such as ISO 27001, ISO 17799, PCI DSS, AS 8015 etc
- Puts structure, accountability & performance tracking around the implementation & management of security controls & risk mitigation strategies.

Security-Assessment.com’s strategic security management framework
Developing Web Applications

Security Considerations
The most common SDLC Security Issues

• Poor security & compliance requirements definition

• Inadequate IT Security and IT involvement during definition, design testing & review

• Inadequate development team knowledge - application security threats & secure application development principles

• Inadequate security controls throughout the SLDC (e.g. Security Considerations during Business Impact and Threat Assessments, Problem and Change Management, Testing)

• Inadequate security testing

• Bespoke and rapid development of web applications

• Inadequate independent and qualified security assessments

• Unqualified assessors undertaking security reviews
Risk Strategies – in house developed Applications

- Develop security controls throughout the SLDC.

- Provide adequate security training to those designing and developing applications (Stakeholders, Project Managers, BA’s, Architects, Coders and testers.)

- Undertake application security review such as design reviews, code reviews & Penetration Testing at various intervals during the SLDC – not two days before go live.


- Develop reusable SECURE code blocks.
Acquiring Web Applications

Security Considerations
Issues with 3rd Party developed Web Applications

• All the issues described in the proceeding section of course relate to 3rd Party developed Web Applications – However with one exceptionally big risk – Knowledge & control of:
  – the development environment & how the application is developed
  – Development team skill & security knowledge
  – Access Control over information and application source.
  – The level of security controls applied in the source
  – The security of the environment and platform (particularly in hosted environments)
  – The security of the outsourcing organisation as a whole & their level of commitment to security in general and how weaknesses here may impact the quality & security of deliverables they provide.
Risk Strategies - 3rd Party developed Applications

- Ensure 3rd Party Contracts explicitly define at least (but not limited to):
  - Security Measures to be met & Security Certifications required.
  - Allocation of Intellectual Property & Confidentiality requirements.
  - Security requirements for personnel & contractors
  - Information disclosure restrictions
  - Conditions for independent security assessments & assurance as conditions for final acceptance and as ongoing assurance.
  - Isolation from other information systems (hosted systems & in development)
  - Access Control Requirements
  - Conditions and sanctions for non compliance.

Requirements must be clear, comprehensive and unambiguous. ‘The Application must be secure’ is NOT a requirement.
Risk Strategies - 3rd Party developed Applications

- Ensure all parties writing security requirements and detailed requirements documents are competent and that input from security specialists is obtained.

Application development & maintenance can be outsourced but accountability cannot.
Auditing Web Applications
Overview and Objectives
Web Application Audit Fundamentals

- Web Application Audits are a point in time exercise - They need to be regular and part of an ongoing assurance program and complement other activities such as Vulnerability and Patch Management to keep pace with new and evolving vulnerabilities and threats.

- Web Application Security Reviews need to be put in the context of business value and risk. A 60 page report highlighting vulnerabilities does not put it in sufficient context for executive and non technical management to accurately assess their business context.

- Web Application audits should be addressed in the context of other compliance audits.
Web Application Audit Fundamentals

- Web Application Reviews must be undertaken by specialised web application testers as technology and attack methods evolve rapidly.

Organisations that do bring in specialist security assessors can let all their good intentions fail by choosing the wrong security assessor and not understanding the scope of testing they propose.

Anyone can run freely available “hacking” and “security” tools or work from an audit checklist and achieve a level of results. Some organisations profess to providing penetration testing services but in reality only provide high level branded Vulnerability Assessments using freely available tools such as Nessus. But, are those results a true reflection of the risks in the environment and have all the major risks been identified?

A Vulnerability Assessment is NOT a web application security review
Security-Assessment.com

Helping organisations to:

- Understand their state of security
- Understand their security regulatory and compliance obligations
- Align security to the business
- Identify system and process weaknesses
- Develop robust, business appropriate security plans and policies
- Improve the quality of processes, applications and system builds.
- Plan for and respond to incidents