Web Application Security for a Smarter Planet

Danny Allan
IBM
dallan@us.ibm.com

OWASP
Sept 10, 2009

Copyright © The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document
under the terms of the OWASP License.

The OWASP Foundation
http://www.owasp.org
A Smarter Planet
The Smarter Planet

Globalization and Globally Available Resources

Billions of mobile devices accessing the Web

Access to streams of information in the Real Time

Businesses face an unparalleled rate of change

Manage business transformations
Differentiate products
React to market shifts
Delivery real customer innovation

Enable business flexibility
Exploit globalization
Manage regulatory mandates

Act quickly to seize business opportunities
Execute with reduced risk and cost
Achieve precision in desired business outcomes

The successful businesses of the future will be those that use software to a competitive advantage
Enabling business innovation and agility requires a significant investment in software

- Software is increasingly being managed as a **strategic business asset**, key enabling sustained business differentiation and flexible operations.

- Businesses everywhere are deploying increasingly **intelligent, interconnected** and **instrumented** software & products.

- Enabling innovation, lowering costs and managing change depends on **effective** and **secure software delivery**.

$600B spent annually on Software & Information Technology

---

**Innovation for a Smarter Planet**

- **INSTRUMENTED**
- **INTERCONNECTED**
- **INTELLIGENT**

---

**Computers & Electronics**
- Telecommunications
- Food Manufacturing
- Software & Information Technologies
- Chemical Manufacturing
- Hospitals
- Transportation Equipment
Increasingly interconnected software supply chain

- Acquired Software
- Manufactured Systems
- In-house Development
- Cloud / SaaS
- Outsourced projects
- End User Applications
- SOA

Composed of purchased, outsourced and in-house built software assets which are ever-evolving and increasingly interdependent
How can I improve software delivery?

“How do I further automate software delivery within my organization?”

“How can I enable collaboration throughout the software delivery process?”

“How can I unobtrusively gather measurements to ensure progress towards desired business outcomes?”

“How do I make incremental, iterative progress towards more effective software delivery?”
Software delivery is a business process that must be continuously measured and improved

CIO’s top priority on behalf of the CEO over last three years: “Improving Business Processes”

Software Security
The Security Equation Has Changed

- How businesses look at security has changed
  - Security is now business driven not technology driven
  - Security is now defined through risk management and compliance disciplines instead of threat and technology disciplines

- The threat landscape has changed
  - Traditional operating system and native client application security risks have become somewhat passé
  - Client threats are now all about the browser environment
  - Server threats are now all about web applications
The Security Landscape of Old

- Traditional Infrastructure was easier to protect . . .
  - Concrete entities that were easy to understand
  - Attack surface and vectors were very well-defined
  - Application footprint very static
  - Perimeter defense was king
Changing Security Landscape of Today

“Webification” has changed everything ...

- Infrastructure is more abstract and less defined
- Everything needs a web interface
- Agents and heavy clients are no longer acceptable
- Traditional defenses no longer apply
Growth of Web Application Vulnerabilities

- SQL injection vulnerability disclosures more than doubled in comparison to 2007
- The number of active, automated attacks on web servers was unprecedented
Attack Techniques are Plentiful and Trivial

- SQL injection and cross-site scripting are the two largest categories of Web application vulnerabilities

- Automated toolkits have allowed for mass defacements and planting of malware

Web Application Vulnerability Disclosures
2004-2009 H1

[Chart showing vulnerability trends]

Source: IBM X-Force®
Attacks & Exploitation are Rampant
Web Threats Will Become More Complex

- Web becoming main application delivery interface and ecosystem

- Popularization of new web technologies (Web 2.0) growing attack surface

- New techniques and scenarios for targeting web infrastructure
Vulnerability Probability (32,717 sites)

Source: WASC 2007 Web Application Security Statistics
Application Security Testing?

1. Explore source code and/or web site to detect structure

2. Identify Vulnerabilities ranked after severity and show how it was identified

3. Advanced remediation, fix recommendations and security enablement
Web Application Security for a Smarter Planet
Secure Web Applications: Who is responsible?

**Organization**

- **Application Development**
  - Requirements
  - Secure Design
  - Dynamic Analysis
  - Static Analysis

- **Secure Hosting Environment**
  - Backend Server
  - Database
  - Application Server
  - Web Server
  - Vulnerability management
    - Network
    - Host
    - Application
  - Incident & event management
  - Identity & access management
  - Malware detection

- **Defend Network**
  - Firewall
  - IDS / IPS
  - Web App Firewall
  - Anti-virus

- **Protect Data across Internet**
  - SSL Encryption

**Client**

- **Desktop**
  - Anti-virus
  - Anti-malware
  - Personal firewall

---

OWASP
Secure Application Development

**Challenge**
- Ensure the creation of high quality, secure and compliant software
- Ensure effective management of secure requirements, design and testing
- Lifecycle management of vulnerabilities
- Application Lifecycle Management (ALM)

**Industry Technologies**
- Dynamic Analysis
- Static Analysis
- Runtime Analysis
Essential Technologies for Secure Software

1. Source Control & Change Request Management
2. Requirements & Test Management
3. Education Services
4. Development Automation
5. Artifact Management
WHAT IF ...

We introduced ESAPI into the major frameworks
Secure Hosting Environment

■ Challenges
  ‣ Maintain a secure environment
  ‣ Ensure security policies are implemented and enforced
  ‣ Lifecycle management of vulnerabilities and incidents
  ‣ Assess production systems for malware

■ Industry Solutions
  ‣ Automated Scanners
  ‣ Manual Analysis
  ‣ Operational Management
Essential Technologies for Secure Operations

■ Protect
  ▸ Web Application Firewalls

■ Assess
  ▸ Host Configuration
  ▸ Network
  ▸ Application

■ Management
  ▸ Vulnerabilities
  ▸ Incidents
WHAT IF ...

There was correlation between the engines
Defending the Network

■ Challenge
  ▸ Protect your business from Internet threats without jeopardizing bandwidth or availability
  ▸ Protect your end users from spam and other productivity drainers
  ▸ Conserve resources by eliminating the need for specialized security expertise

■ Industry Solutions
  ▸ Firewalls
  ▸ Intrusion Detections Systems
  ▸ Intrusion Prevention Systems
WHAT IF ... 
We could turn on the IPS
Encrypting transmission across the Internet

**Challenge**

- Ensuring data and intellectual property is not stolen while crossing the Internet
- Ensuring that data is not tampered with or altered between the server and client
- Ensure that a malicious site does not impersonate the legitimate server and establish communication with the client

**Industry Solutions**

- SSL Encryption
WHAT IF ...

We dropped MD5 hashes and used SSL properly
Client-side Security

- *Organization can not control their external clients*

- Internal client challenges
  - Mitigating risks posed by zero-day, targeted attacks
  - Protecting critical data and intellectual property
  - Minimizing costs and lost productivity associated with remediating infected endpoints
  - Reducing help desk calls

- Industry Solutions
  - Anti-virus
  - Anti-malware
  - Personal firewall
WHAT IF ...

We could deliver a level of control to the server
Web Applications: A Smarter Approach

Organization

Application Development
- Requirements
- Secure Design
- Dynamic Analysis
- Static Analysis

Secure Hosting Environment
- Backend Server
- Application Server
- Database
- Web Server
- Vulnerability management
  - Network
  - Host
  - Application
- Incident & event management
- Identity & access management
- Malware detection

Defend Network
- Firewall
- IDS / IPS
- Web App Firewall
- Anti-virus

Protect Data across Internet
- SSL Encryption

Desktop
- Anti-virus
- Anti-malware
- Personal firewall

OWASP
Thank You