A Decade of Web Application Security
What have we learned?

Jason Kent, Director Web Application Security

Qualys Inc.    April 2013
Agenda

- Overview
- Review of a Decade of Top 10s
- Where are we today?
- Where are we going?
- Summary
A Decade of Web App Security

Overview

• Speaker info
  – Jason Kent, Director - Web Application Security

• Why Review History?
  – "Those who cannot remember the past are condemned to repeat it” - George Santayana

• Why a Decade?
  – Goes back a ways but vulnerabilities are still relevant
  – OWASP Top Ten documented from 2003
  – Seemed like a good, round number
A Decade of Security and...

Let's turn back the clock....

Social Networking Security Attacks: The Top Incidents of 2010

Malvertising Hits Farm Town

In April, users of the popular "Farm Town" game on Facebook were hit with a rogue antivirus scam tied to malicious advertising.
A Decade of Web App Security
OWASP Top 10 2003

2003

• A1 Unvalidated Parameters
• A2 Broken Access Control
• A3 Broken Account and Session Management
• A4 Cross Site Scripting (XSS) Flaws
• A5 Buffer Overflows
• A6 Command Injection Flaws
• A7 Error Handling Problems
• A8 Insecure Use of Cryptography
• A9 Remote Administration Flaws
• A10 Web and Application Server Misconfiguration
## A Decade of Web App Security
### OWASP Top 10 2003 - 2004

<table>
<thead>
<tr>
<th>Year</th>
<th>Flaws</th>
</tr>
</thead>
<tbody>
<tr>
<td>2003</td>
<td>• A1 Unvalidated Parameters&lt;br&gt;• A2 Broken Access Control&lt;br&gt;• A3 Broken Account and Session Management&lt;br&gt;• A4 Cross Site Scripting (XSS) Flaws&lt;br&gt;• A5 Buffer Overflows&lt;br&gt;• A6 Command Injection Flaws&lt;br&gt;• A7 Error Handling Problems&lt;br&gt;• A8 Insecure Use of Cryptography&lt;br&gt;• A9 Remote Administration Flaws&lt;br&gt;• A10 Web and Application Server Misconfiguration</td>
</tr>
<tr>
<td>2004</td>
<td>• A1 Unvalidated Input&lt;br&gt;• A2 Broken Access Control&lt;br&gt;• A3 Broken Account and Session Management&lt;br&gt;• A4 Cross Site Scripting (XSS) Flaws&lt;br&gt;• A5 Buffer Overflows&lt;br&gt;• A6 Injection Flaws&lt;br&gt;• A7 Improper Error Handling&lt;br&gt;• A8 Insecure Storage&lt;br&gt;• A9 Denial of Service&lt;br&gt;• A10 Insecure Configuration Management</td>
</tr>
</tbody>
</table>

- **Green** = New
- **Red** = Renamed/Redefined
A Decade of Web App Security

OWASP Top 10 2003 – 2004 Changes

• Replaced (1)
  – A9 Remote Administration Flaws (Dropped)
  – A9 Denial of Service (New)

• Changed Name/Scope (5)
  – A1 Unvalidated Input
  – A6 Injection Flaws
  – A7 Improper Error Handling
  – A8 Insecure Storage
  – A10 Insecure Configuration Management
A Decade of Web App Security
OWASP Top 10  2007

• Move to data driven ratings
  – Rank by frequency as identified by Mitre
  – Try to identify by vulnerability not attack
A Decade of Web App Security
OWASP Top 10 2004 - 2007

2004
• A1 Unvalidated Input
• A2 Broken Access Control
• A3 Broken Authentication and Session Management
• A4 Cross Site Scripting (XSS) Flaws
• A5 Buffer Overflows
• A6 Injection Flaws
• A7 Improper Error Handling
• A8 Insecure Storage
• A9 Denial of Service
• A10 Insecure Configuration Management

2007
• A1 - Cross Site Scripting (XSS)
• A2 - Injection Flaws
• A3 - Malicious File Execution
  A4 - Insecure Direct Object Reference
• A5 - Cross Site Request Forgery (CSRF)
• A6 - Information Leakage and Improper Error Handling
• A7 - Broken Authentication and Session Management
  A8 - Insecure Cryptographic Storage
• A9 - Insecure Communications
• A10 - Failure to Restrict URL Access

Green = New  Red = Renamed/Redefined
A Decade of Web App Security
OWASP Top 10 2004 – 2007 Changes

• Replaced (3)
  – A5 Buffer Overflows (Dropped)
  – A9 Denial of Service (Dropped)
  – A10 Insecure Configuration Management (Dropped)
  – A3 - Malicious File Execution (NEW)
  – A5 - Cross Site Request Forgery (CSRF) (NEW)
  – A9 - Insecure Communications (NEW)

• Changed Name/Redefined (7)
  – A1 Unvalidated Input
  – A2 Broken Access Control
  – A4 - Insecure Direct Object Reference
  – A6 - Information Leakage and Improper Error Handling
  – A7 Improper Error Handling
  – A8 - Insecure Cryptographic Storage
  – A10 - Failure to Restrict URL Access
• Move to rank by risk, not frequency
  – New risk ranking methodology
• Identify risks, not weaknesses
A Decade of Web App Security
OWASP Top 10 2007 - 2010

2007
- A1 - Cross Site Scripting (XSS)
- A2 - Injection Flaws
- A3 - Malicious File Execution
- A4 - Insecure Direct Object Reference
- A5 - Cross Site Request Forgery (CSRF)
- A6 - Information Leakage and Improper Error Handling
- A7 - Broken Authentication and Session Management
- A8 - Insecure Cryptographic Storage
- A9 - Insecure Communications
- A10 - Failure to Restrict URL Access

2010
- A1-Injection
- A2-Cross Site Scripting (XSS)
- A3-Broken Authentication and Session Management
- A4-Insecure Direct Object References
- A5-Cross Site Request Forgery (CSRF)
- A6 Security Misconfiguration
- A7-Insecure Cryptographic Storage
- A8-Failure to Restrict URL Access
- A9-Insufficient Transport Layer Protection
- A10-Unvalidated Redirects and Forwards

Green = New  Red = Renamed/Redefined
A Decade of Web App Security
OWASP Top 10  2007 – 2010 Changes

• Replaced (2)
  – A3 - Malicious File Execution (Dropped)
  – A9 - Insecure Communications (Dropped)
  – A6 Security Misconfiguration (New)
  – A10-Unvalidated Redirects and Forwards (New)

• Changed Name/Scope (2)
  – A1-Injection
  – A9-Insufficient Transport Layer Protection
## A Decade of Web App Security


### 2010
- A1 - Injection
- A2 - Cross Site Scripting (XSS)
- A3 - Broken Authentication and Session Management
- A4 - Insecure Direct Object References
- A5 - Cross Site Request Forgery (CSRF)
- A6 - Security Misconfiguration
- A7 - Insecure Cryptographic Storage
- A8 - Failure to Restrict URL Access
- A9 - Insufficient Transport Layer Protection
- A10 - Unvalidated Redirects and Forwards

### 2013
- A1 Injection
- A2 Broken Authentication and Session Management
- A3 Cross-Site Scripting (XSS)
- A4 Insecure Direct Object References
- A5 Security Misconfiguration
- A6 Sensitive Data Exposure
- A7 Missing Function Level Access Control
- A8 Cross-Site Request Forgery (CSRF)
- A9 Using Known Vulnerable Components
- A10 Unvalidated Redirects and Forwards

*Green = New    Red = Renamed/Redefined*
A Decade of Web App Security
OWASP Top 10  2010 – 2013(draft) Changes

• Replaced (3)
  – A7-Insecure Cryptographic Storage (Dropped)
  – A8-Failure to Restrict URL Access (Dropped)
  – A9-Insufficient Transport Layer Protection(Dropped)
  – A6 Sensitive Data Exposure  (New)

• Changed Name/Scope (2)
  – A9 Using Known Vulnerable Components
  – A7 Missing Function Level Access Control
# A Decade of Web App Security

**OWASP Top 10 2003 – 2013 (rc)**

<table>
<thead>
<tr>
<th>Year</th>
<th>Flaw</th>
</tr>
</thead>
<tbody>
<tr>
<td>2003</td>
<td>A1 Unvalidated Parameters</td>
</tr>
<tr>
<td></td>
<td>A2 Broken Access Control</td>
</tr>
<tr>
<td></td>
<td>A3 Broken Account and Session Management</td>
</tr>
<tr>
<td></td>
<td>A4 Cross Site Scripting (XSS) Flaws</td>
</tr>
<tr>
<td></td>
<td>A5 Buffer Overflows</td>
</tr>
<tr>
<td></td>
<td>A6 Command Injection Flaws</td>
</tr>
<tr>
<td></td>
<td>A7 Error Handling Problems</td>
</tr>
<tr>
<td></td>
<td>A8 Insecure Use of Cryptography</td>
</tr>
<tr>
<td></td>
<td>A9 Remote Administration Flaws</td>
</tr>
<tr>
<td></td>
<td>A10 Web and Application Server Misconfiguration</td>
</tr>
<tr>
<td>2013</td>
<td>A1 Injection</td>
</tr>
<tr>
<td></td>
<td>A2 Broken Authentication and Session Management</td>
</tr>
<tr>
<td></td>
<td>A3 Cross-Site Scripting (XSS)</td>
</tr>
<tr>
<td></td>
<td>A4 Insecure Direct Object References</td>
</tr>
<tr>
<td></td>
<td>A5 Security Misconfiguration</td>
</tr>
<tr>
<td></td>
<td>A6 Sensitive Data Exposure</td>
</tr>
<tr>
<td></td>
<td>A7 Missing Function Level Access Control</td>
</tr>
<tr>
<td></td>
<td>A8 Cross-Site Request Forgery (CSRF)</td>
</tr>
<tr>
<td></td>
<td>A9 Using Known Vulnerable Components</td>
</tr>
<tr>
<td></td>
<td>A10 Unvalidated Redirects and Forwards</td>
</tr>
</tbody>
</table>

**Notes:**
- Green = New
- Red = Renamed/Redefined
- Partial Red = Partially Renamed/Redefined
A Decade of Web App Security
OWASP Top 10 2003 – 2013(draft) Changes

• Only really one new vulnerability type in 10 years
  – Cross Site Request Forgery (CSRF)

• Little bit of history repeating
  – These are really just changing how we name them or classify the issues associated.
  – The risks all existed in 2003 and arguably 2013s list could have been valid in 2003
A Decade of Web App Security
What about now... where are we?

IBM X-Force 2012 Mid Year Trend and Risk Report
### Table 15. Threat actions used in single-action breaches

<table>
<thead>
<tr>
<th>Rank</th>
<th>Threat action</th>
<th>Category</th>
<th>All Orgs</th>
<th>Larger Orgs</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Exploitation of default or guessable credentials</td>
<td>Hacking</td>
<td>104</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>Tampering</td>
<td>Physical</td>
<td>52</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>Pretexting (classic Social Engineering)</td>
<td>Social</td>
<td>24</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>Brute force and dictionary attacks</td>
<td>Hacking</td>
<td>21</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>SQL Injection</td>
<td>Hacking</td>
<td>12</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>Abuse of system access/privileges</td>
<td>Hacking</td>
<td>12</td>
<td>3</td>
</tr>
</tbody>
</table>
A Decade of Web App Security
But Why?

• **Study**

  Vulnerability Factors in New Web Applications: Audit Tools, Developer Selection & Languages

• **Interesting Reading:**
  
  – Startup/Freelance developers create more than 4 XSS/SQLi vulnerabilities per 1000 LOC
  
  – “loose correlation between vulnerability rate and <security>quiz score implies some disconnect between security knowledge and its implementation”
  
  – “they may not understand the potential vulnerabilities but still avoid them due to framework features”
A Decade of Web App Security
Where to go from here?

• **Continue to Educate**
  – Need to start earlier – push security into college/university courses so developers arrive trained.
  – Ensure security training includes practical delivery of knowledge

• **Enhance Frameworks/IDEs**
  – Ensure strong centralized validation features and default output encoding (moving in this direction already)
  – Warn by default when risky methods are used (do we really need SCA for this?)

• **Measure/Compensate**
  – Create incentives for developers to learn and use secure design/coding