Data Mining a Mountain of Zero Day Vulnerabilities

Chris Eng
VP Research, Veracode
July 13, 2012
Central platform supports internal and third-party applications

No hardware, No software, No maintenance

APIs for SDLC integration (upload, SAML, results, Archer)

INTERIOR APPS

THIRD PARTY, OUTSOURCED, CLOUD APPS

VERACODE
Application Metadata
- Industry vertical
- Supplier (internal, third-party, open source, etc.)
- Application type
- Business criticality
- Language
- Platform

Scan Data
- Scan number
- Scan date
- Lines of code

Enterprise Metrics
- Flaw counts
- Flaw percentages
- Application count
- Risk-adjusted rating
- First scan acceptance rate
- Time between scans
- Days to remediation
- Scans to remediation
- Team comparisons
- Custom policies
- PCI-DSS†
- CWE/SANS Top25†
- OWASP Top Ten†

† Pass/Fail only
The Data Set

- Applications from over 300 commercial and US government customers
- Scanned 9,910 applications over the past 18 months
- Ranged in size from 100KB to 6GB
- Included both pre-release and production software
- Internally built, outsourced, open source, and commercial ISV code
Caveats

• Customer base is already security-conscious
• Bias toward business critical applications
• Applications are at inconsistent phases in the SDLC
• Not all flaws are necessarily easy to exploit
• Analysis technology is continuously being improved
• All security testing has False Negatives
THE LATENT VULNERABILITIES
VS.
THE ATTACKS
While other flaws such as XSS account for a higher volume of findings, SQL injection accounts for 20 percent of hacks.

*Source: WHID*
LET’S TAKE A CLOSER LOOK AT THE NUMBERS
Top Vulnerability Categories
(Percent of Applications Affected for Web Applications)

- Cross-site Scripting (XSS) 68%
- Information Leakage 66%
- CRLF Injection 54%
- Cryptographic Issues 53%
- Directory Traversal 49%
- SQL Injection 32%
- Time and State 30%
- Credentials Management 27%
- API Abuse 25%
- Encapsulation 25%
- Insufficient Input Validation 24%
- Session Fixation 21%
- Race Conditions 13%
- Potential Backdoor 9%
- OS Command Injection 9%

Indicate categories that are in the OWASP Top 10.
Top Vulnerability Categories
(Percentage of Applications Affected for Non-Web Applications)

- Cryptographic Issues: 46%
- Directory Traversal: 34%
- Error Handling: 24%
- Information Leakage: 23%
- Potential Backdoor: 23%
- Time and State: 19%
- Buffer Management Errors: 17%
- OS Command Injection: 15%
- Credentials Management: 15%
- Buffer Overflow: 14%
- CRLF Injection: 13%
- Numeric Errors: 12%
- SQL Injection: 11%
- Untrusted Search Path: 11%
- Dangerous Functions: 10%
ARE WE MAKING ANY PROGRESS AT ERADICATING CROSS-SITE SCRIPTING OR SQL INJECTION?
Quarterly Trend for XSS

$pvalue = 0.124$: Statistically, the trend is flat.
Quarterly Trend for SQL Injection

\[ pvalue = 0.048: \text{Statistically, the trend is down.} \]
WHAT PERCENTAGE OF WEB APPLICATIONS FAIL THE OWASP TOP TEN?

a) 34%
b) 57%
c) 86%
d) 99%
OWASP Top 10 Compliance by Supplier on First Submission
(Web Applications)

<table>
<thead>
<tr>
<th>Supplier Type</th>
<th>Acceptable</th>
<th>Not Acceptable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internally Developed</td>
<td>15%</td>
<td>85%</td>
</tr>
<tr>
<td>Commercial</td>
<td>14%</td>
<td>86%</td>
</tr>
<tr>
<td>Open Source</td>
<td>6%</td>
<td>94%</td>
</tr>
<tr>
<td>Overall</td>
<td>14%</td>
<td>86%</td>
</tr>
</tbody>
</table>
CWE/SANS Top 25 Compliance by Supplier on First Submission
(Non-Web Applications)

<table>
<thead>
<tr>
<th>Supplier Type</th>
<th>Acceptable</th>
<th>Not Acceptable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internally Developed</td>
<td>48%</td>
<td>52%</td>
</tr>
<tr>
<td>Commercial</td>
<td>38%</td>
<td>62%</td>
</tr>
<tr>
<td>Open Source</td>
<td>26%</td>
<td>74%</td>
</tr>
<tr>
<td>Overall</td>
<td>42%</td>
<td>58%</td>
</tr>
</tbody>
</table>
HOW LONG DOES IT TAKE APPLICATIONS TO ACHIEVE AN ACCEPTABLE RATING?
Development agility and application security are not mutually exclusive!
GREAT, BUT WHAT ABOUT ALL THE OTHER APPS?
Only about half of companies resubmit more than 90% of their *most critical* applications!
Refresher: Whisker Plots

- Maximum
- Upper Quartile
- Median
- Lower Quartile
- Population Size
- Minimum
Veracode Security Quality Score Trend by Quarter

\textit{pvalue} = 0.543: Statistically, the trend is flat.
WHO IS HOLDING THEIR SOFTWARE VENDORS ACCOUNTABLE?
Requestor Type by Industry

- 54% - Software/IT Services
- 39% - Financial
- 3% - Aerospace and Defense
- 2% - Oil and Gas
- <1% - Telecommunications
- <1% - Entertainment
- <1% - Government
- <1% - Other

Third-party Assessments by Application Purpose

- 54% - Operations
- 22% - Financial
- 12% - Security Product
- 4% - Learning and Growth
- 4% - Customer Support
- 3% - Healthcare
- 1% - Other
- <1% - Other
Performance Against Enterprise Policy by Application Purpose

- **Security Product**
  - Fail: 74%
  - Pass: 26%
  - Pass Conditionally: 2%

- **Operations**
  - Fail: 71%
  - Pass: 28%
  - Pass Conditionally: 2%

- **Learning and Growth**
  - Fail: 37%
  - Pass: 63%
  - Pass Conditionally: 2%

- **Healthcare**
  - Fail: 67%
  - Pass: 33%
  - Pass Conditionally: 5%

- **Financial**
  - Fail: 37%
  - Pass: 58%
  - Pass Conditionally: 5%

- **Customer Support**
  - Fail: 46%
  - Pass: 45%
  - Pass Conditionally: 9%

- **Overall**
  - Fail: 60%
  - Pass: 38%
  - Pass Conditionally: 2%

- **Other**
  - Fail: 54%
  - Pass: 46%
SO I HEAR YOU CAN RUN APPLICATIONS ON SMART PHONES?
Android Applications by Industry Vertical

- Retail: 33%
- Technology: 26%
- Finance and Services: 19%
- Bank: 7%
- Media: 7%
- Healthcare: 4%
- Hospitality: 4%
<table>
<thead>
<tr>
<th>CWE Category</th>
<th>CWE</th>
<th>Percent Applications Affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insufficient Entropy</td>
<td>331</td>
<td>61%</td>
</tr>
<tr>
<td>Use of Hard-coded Cryptographic Key</td>
<td>321</td>
<td>42%</td>
</tr>
<tr>
<td>Information Exposure Through Sent Data</td>
<td>201</td>
<td>39%</td>
</tr>
<tr>
<td>Information Exposure Through Error Message</td>
<td>209</td>
<td>6%</td>
</tr>
</tbody>
</table>
WHEN GIVEN AN EXAM ON APPLICATION SECURITY FUNDAMENTALS, OVER HALF OF DEVELOPERS...

a) Receive an A
b) Receive a B or worse
c) Receive a C or worse
d) Fail (receive a D or F)
Account Average SQS vs Average Quiz Grade
State of Software Security Report

The Intractable Problem of Insecure Software

December 7, 2011

http://www.veracode.com/reports
Study of Software Related Cybersecurity Risks in Public Companies

http://www.veracode.com/reports
QUESTIONS?

ceng@veracode.com
@chriseng