<table>
<thead>
<tr>
<th>Application Metadata</th>
<th>Enterprise Metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Industry vertical</td>
<td>• Flaw counts</td>
</tr>
<tr>
<td>• Application supplier (internal, third-party, etc.)</td>
<td>• Flaw percentages</td>
</tr>
<tr>
<td>• Application type</td>
<td>• Application count</td>
</tr>
<tr>
<td>• Assurance level</td>
<td>• Risk-adjusted rating</td>
</tr>
<tr>
<td>• Language</td>
<td>• First scan acceptance rate</td>
</tr>
<tr>
<td>• Platform</td>
<td>• Time between scans</td>
</tr>
<tr>
<td></td>
<td>• Days to remediation</td>
</tr>
<tr>
<td>Scan Data</td>
<td>• Scans to remediation</td>
</tr>
<tr>
<td>• Scan number</td>
<td>• PCI-DSS (pass/fail)</td>
</tr>
<tr>
<td>• Scan date</td>
<td>• CWE/SANS Top25 (pass/fail)</td>
</tr>
<tr>
<td>• Lines of code</td>
<td>• OWASP Top Ten (pass/fail)</td>
</tr>
<tr>
<td></td>
<td>• Custom policies</td>
</tr>
</tbody>
</table>
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
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%

Legend: Orange bars 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%

*Indicate categories that are in the CWE/SANS Top 25*
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

\textit{pvalue} = 0.048: Statistically, the trend is down.
DARE WE ASK, HOW IS THE GOVERNMENT SECTOR DOING?
Quarterly Trend for XSS in Government Web Applications

$pvalue = 0.215$: Statistically, the trend is flat.
Quarterly Trend for SQL Injection in Government Web Applications

\[ p\text{value} = 0.343: \text{ Statistically, the trend is flat.} \]
<table>
<thead>
<tr>
<th>Government</th>
<th>Finance</th>
<th>Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cross-site Scripting (XSS)</td>
<td>Information Leakage</td>
<td>Cryptographic Issues</td>
</tr>
<tr>
<td>75%</td>
<td>68%</td>
<td>59%</td>
</tr>
<tr>
<td>Information Leakage</td>
<td>Cross-site Scripting (XSS)</td>
<td>Information Leakage</td>
</tr>
<tr>
<td>66%</td>
<td>67%</td>
<td>59%</td>
</tr>
<tr>
<td>SQL Injection</td>
<td>Cryptographic Issues</td>
<td>Cross-site Scripting (XSS)</td>
</tr>
<tr>
<td>40%</td>
<td>53%</td>
<td>55%</td>
</tr>
<tr>
<td>Cryptographic Issues</td>
<td>CRLF Injection</td>
<td>CRLF Injection</td>
</tr>
<tr>
<td>35%</td>
<td>51%</td>
<td>54%</td>
</tr>
<tr>
<td>Directory Traversal</td>
<td>Directory Traversal</td>
<td>Directory Traversal</td>
</tr>
<tr>
<td>31%</td>
<td>47%</td>
<td>54%</td>
</tr>
<tr>
<td>Insufficient Input Validation</td>
<td>Insufficient Input Validation</td>
<td>Time and State</td>
</tr>
<tr>
<td>27%</td>
<td>30%</td>
<td>39%</td>
</tr>
<tr>
<td>CRLF Injection</td>
<td>SQL Injection</td>
<td>Credentials Mgmt</td>
</tr>
<tr>
<td>27%</td>
<td>29%</td>
<td>31%</td>
</tr>
<tr>
<td>OS Command Injection</td>
<td>Time and State</td>
<td>SQL Injection</td>
</tr>
<tr>
<td>19%</td>
<td>28%</td>
<td>30%</td>
</tr>
<tr>
<td>Time and State</td>
<td>API Abuse</td>
<td>API Abuse</td>
</tr>
<tr>
<td>18%</td>
<td>26%</td>
<td>25%</td>
</tr>
<tr>
<td>Credentials Mgmt</td>
<td>Encapsulation</td>
<td>Encapsulation</td>
</tr>
<tr>
<td>16%</td>
<td>25%</td>
<td>23%</td>
</tr>
<tr>
<td>API Abuse</td>
<td>Credentials Mgmt</td>
<td>Session Fixation</td>
</tr>
<tr>
<td>14%</td>
<td>24%</td>
<td>18%</td>
</tr>
<tr>
<td>Potential Backdoor</td>
<td>Session Fixation</td>
<td>OS Command Injection</td>
</tr>
<tr>
<td>12%</td>
<td>19%</td>
<td>14%</td>
</tr>
<tr>
<td>Session Fixation</td>
<td>Race Conditions</td>
<td>Potential Backdoor</td>
</tr>
<tr>
<td>11%</td>
<td>13%</td>
<td>14%</td>
</tr>
<tr>
<td>Encapsulation</td>
<td>Potential Backdoor</td>
<td>Race Conditions</td>
</tr>
<tr>
<td>11%</td>
<td>10%</td>
<td>13%</td>
</tr>
<tr>
<td>Untrusted Search Path</td>
<td>OS Command Injection</td>
<td>Insufficient Input Validation</td>
</tr>
<tr>
<td>3%</td>
<td>6%</td>
<td>13%</td>
</tr>
</tbody>
</table>
WHAT PERCENTAGE OF WEB APPLICATIONS FAIL THE OWASP TOP TEN?

a) 34%
b) 57%
c) 86%
d) 99%
CWE/SANS Top 25 Compliance by Supplier on First Submission
(Non-Web Applications)

- Internally Developed:
  - Acceptable: 48%
  - Not Acceptable: 52%

- Commercial:
  - Acceptable: 38%
  - Not Acceptable: 62%

- Open Source:
  - Acceptable: 26%
  - Not Acceptable: 74%

- Overall:
  - Acceptable: 42%
  - Not Acceptable: 58%
HOW LONG DOES IT TAKE APPLICATIONS TO ACHIEVE AN ACCEPTABLE RATING?
Time to Policy Achievement

- **Internally Developed**
  - 0-1 Week: 82%
  - 2-3 Weeks: 3%
  - 3-4 Weeks: 3%
  - 4+ Weeks: 12%

- **Commercial**
  - 0-1 Week: 79%
  - 2-3 Weeks: 3%
  - 3-4 Weeks: 7%
  - 4+ Weeks: 11%

- **Open Source**
  - 0-1 Week: 98%
  - 2-3 Weeks: 2%

- **Outsourced**
  - 0-1 Week: 100%

- **Overall**
  - 0-1 Week: 82%
  - 2-3 Weeks: 3%
  - 3-4 Weeks: 4%
  - 4+ Weeks: 11%
GREAT, BUT WHAT ABOUT ALL THE OTHER APPS?
Veracode Security Quality Score by Build

- Build 1
- Build 2
- Build 3
- Build 4
- Build 5
- Build 6
- Build 7
- Build 8
- Build 9

VERACODE SECURITY QUALITY SCORE

100
90
80
70
60
50
40
30
20
10
0
Veracode Security Quality Score Trend by Quarter

\[ p-value = 0.543: \text{Statistically, the trend is flat.} \]
WHO IS HOLDING THEIR SOFTWARE VENDORS ACCOUNTABLE?
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: 4%
- Healthcare: 4%
- Hospitality: 7%
<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)
Study of Software Related Cybersecurity Risks in Public Companies

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

GOLD HILL

EST. — 1859
ELEV. — 8463
POP. — 118

TOTAL — 10440

Email: ceng@veracode.com
Twitter: @chriseng