State of Software Security 2023

At A Glance

In the State of Software Security 2023, we used hard data to establish what factors go into flaw introduction, faster remediation, and lower security debt.
Flaw Prevalence

Over 74% of applications have at least one security flaw found in the last scan over the last 12 months. These include over 69% have at least one OWASP Top 10 flaw, and over 56% have at least one CWE Top 25 flaw.

Flaw Prevalence by Language

JavaScript generally has fewer flaws with just over half of applications with any flaws reported, while about four out of five Java and .NET applications have any flaws.
Flaw Introduction by Age of Applications

While over 30% of applications show flaws at the first scan, this number drops to approximately 22% shortly after before rising to 30% again at four years.

The number of applications with new flaws then increases further to approximately 35% of applications over four and a half years old.

Scan Frequency

- **Scans Last Month**: 0.4%
  - Reduction in the probability that new flaws will be introduced into applications *

- **Every Month Since Last Scan**: 1.3%
  - Increase in the probability that new flaws will be introduced into applications *

- **1.6%**
  - Reduction in the number of flaws introduced when flaws are introduced into the application

- **5.1%**
  - Increase in the number of flaws introduced when flaws are introduced into the application

*From a base of 27% in any given month.*
Application Size by Age of Applications

Applications grow in size by about 40% year on year irrespective of their original size.

Developer Education

Completion of 10 Security Labs Trainings

1.8%

Reduction in the probability that new flaws will be introduced into applications *

12.1%

Reduction in the number of flaws introduced when flaws are introduced into the application

*From a base of 27% in any given month.
### Top Flaws by Scan Type

The top flaws vary markedly by scan type. While this is not news, it does highlight the importance of using a variety of scan types to ensure finding hard-to-identify flaws that may only be detectable by one type of scan.

<table>
<thead>
<tr>
<th>Scan Type</th>
<th>Percent of Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>API Abuse</strong></td>
<td>10.0%</td>
</tr>
<tr>
<td><strong>Command or Argument Injection</strong></td>
<td>11.1%</td>
</tr>
<tr>
<td><strong>Server Configuration</strong></td>
<td>11.3%</td>
</tr>
<tr>
<td><strong>Time and State</strong></td>
<td>14.0%</td>
</tr>
<tr>
<td><strong>Encapsulation</strong></td>
<td>19.9%</td>
</tr>
<tr>
<td><strong>Authentication Issues</strong></td>
<td>19.2%</td>
</tr>
<tr>
<td><strong>SQL Injection</strong></td>
<td>22.5%</td>
</tr>
<tr>
<td><strong>Cross-Site Scripting (XSS)</strong></td>
<td>38.5%</td>
</tr>
<tr>
<td><strong>Insufficient Input Validation</strong></td>
<td>41.6%</td>
</tr>
<tr>
<td><strong>Deployment Configuration</strong></td>
<td>41.7%</td>
</tr>
<tr>
<td><strong>Directory Traversal</strong></td>
<td>46.7%</td>
</tr>
<tr>
<td><strong>Credentials Management</strong></td>
<td>55.6%</td>
</tr>
<tr>
<td><strong>Information Leakage</strong></td>
<td>59.3%</td>
</tr>
<tr>
<td><strong>Cryptographic Issues</strong></td>
<td>59.8%</td>
</tr>
<tr>
<td><strong>Code Quality</strong></td>
<td>64.8%</td>
</tr>
</tbody>
</table>

### Reductions

- **2.0%** Reduction in the probability that new flaws will be introduced into applications.*

- **17.9%** Reduction in the number of flaws introduced when flaws are introduced into the application.

*From a base of 27% in any given month.
Next Steps

Continue your journey to improving your application security program for 2023 and beyond. Reach out to our team or schedule a demo with one of our experts.

Contact Our Team  Schedule a Demo
Veracode is a leading AppSec partner for creating secure software, reducing the risk of security breach, and increasing security and development teams’ productivity. As a result, companies using Veracode can move their business, and the world, forward. With its combination of process automation, integrations, speed, and responsiveness, Veracode helps companies get accurate and reliable results to focus their efforts on fixing, not just finding, potential vulnerabilities.

Learn more at [www.veracode.com](http://www.veracode.com), on the Veracode blog and on Twitter.