The Influence of Programming Language and Framework on Application Security

Matthew Finifter and David Wagner
{finifter, daw}@cs.berkeley.edu

UC Berkeley

February 14, 2011
Motivation

- Some languages and frameworks more prone to vulnerabilities?
- How can we find out empirically?
Overview

- The problem
- Experiment
- Not enough data
- How can we gather better data?
Problem

- Many language and framework choices
  - None clearly superior
- Security increasingly important
  - Languages and frameworks evolving to meet this need
- We need to measure how successful they are
Experiment

- Data gathered from a previous study (Prechelt 2007)

- 9 implementations of same web app: 3 PHP, 3 Java, 3 Perl

- Teams chose which framework(s) to use
  - Little overlap in framework choice

- Manual and black-box security analysis of each implementation
Results

Total Number of Vulnerabilities

- Java 3
- Java 4
- Java 9
- PHP 6
- PHP 7
- PHP 8
- Perl 1
- Perl 2
- Perl 5

Manual
Both
Black-box
Results (2)

M. Finifter (UCB)  Language and Framework Security  February 14, 2011
## Results (3)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Perl</td>
<td>X</td>
<td>none</td>
<td></td>
<td>opt-in</td>
<td>X</td>
<td>opt-in</td>
</tr>
<tr>
<td>2</td>
<td>Perl</td>
<td>X</td>
<td>none</td>
<td>X</td>
<td>none</td>
<td>X</td>
<td>none</td>
</tr>
<tr>
<td>5</td>
<td>Perl</td>
<td>X</td>
<td>none</td>
<td>X</td>
<td>none</td>
<td></td>
<td>opt-out</td>
</tr>
<tr>
<td>3</td>
<td>Java</td>
<td>manual</td>
<td></td>
<td></td>
<td>opt-out</td>
<td></td>
<td>none</td>
</tr>
<tr>
<td>4</td>
<td>Java</td>
<td>always on</td>
<td></td>
<td></td>
<td>opt-in</td>
<td>X</td>
<td>opt-in</td>
</tr>
<tr>
<td>9</td>
<td>Java</td>
<td>X</td>
<td>none</td>
<td></td>
<td>opt-in</td>
<td></td>
<td>none</td>
</tr>
<tr>
<td>6</td>
<td>PHP</td>
<td>X</td>
<td>none</td>
<td></td>
<td>opt-out</td>
<td>X</td>
<td>opt-in</td>
</tr>
<tr>
<td>7</td>
<td>PHP</td>
<td>X</td>
<td>none</td>
<td></td>
<td>opt-out</td>
<td>X</td>
<td>none</td>
</tr>
<tr>
<td>8</td>
<td>PHP</td>
<td>X</td>
<td>none</td>
<td></td>
<td>opt-out</td>
<td>X</td>
<td>opt-in</td>
</tr>
</tbody>
</table>
Results (4)

- A few interesting, significant results
- But not as many as we would like
Larger data set

- Programming contest
- Student programming projects
- Outsourced development
  - guru.com, rentacoder.com, etc.
Outsourced development

- We write web application in multiple languages using multiple frameworks
- Hire programmers for single security-relevant module
- Sample size vs. module size
Conclusion

- Have performed small-scale experiment
- Some evidence that language and framework choice influence security
- Need better data for study of larger scale
Thank you!

Matthew Finifter, finifter@cs.berkeley.edu
Results (5)

Number of Vulnerabilities vs. Framework Support

- XSS
- SQL Injection
- Auth. Bypass

M. Finifter (UCB)
Language and Framework Security
February 14, 2011
Results (6)

Stored XSS

Reflected XSS

SQL Injection

Authentication/Authorization Bypass