OWASP
The Open Web Application Security Project

Can AppSec Training Really Make a Smart Developer?

Research From Denim Group
June 26th, 2014
AppSec EU 2014

John B. Dickson, CISSP
@johnbdickson

OWASP
The Open Web Application Security Project

- Application Security Enthusiast
- Security Professional
- ISSA Distinguished Fellow
- MBA-type and Serial Entrepreneur
- Dad

DENIM GROUP

OWASP
The Open Web Application Security Project

When I’m not thinking about appsec, I am…

Snake Hunting on Ranch in South Texas

Snake Hunting Essentials

Cool Hat

OWASP AppSec 2011 t-shirt

Cool Hat

Guy who has a machete and who actually is good at catching snakes

Snake Guards

Common Gardening Tools

Machete

Why we have Snake Hunts

"I personally believe that training users in security is generally a waste of time, and that the money can be spent better elsewhere."

Bruce Schneier

OWASP
The Open Web Application Security Project

How Developer Training is Different

- Both trying to change behaviors
  - *Target audience has more power to say "no"*
  - *Deadlines and releases drive training*
- For developers, infrequent, but more disruptive
  - *15-45 minutes vs. 2-day class*

OWASP
The Open Web Application Security Project

Yet Training is Mandated

- PCI DSS 3.0
  - ✓ *Train developers in secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory*
  - ✓ *Testing Procedures: 6.5.a: Examine software development policies and procedures to verify that secure coding technique training is required for developers, based on best practices and guidance*
  - ✓ *Testing Procedures: 6.5.b: Interview a sample of developers to verify that they are knowledgeable in secure coding techniques*
  - ✓ *Testing Procedures: 6.5.c : Examine training records to verify that software developers received training on secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory*

But Results Are Not Measured

- Harvard Business Review
  - *Large-scale organization development is rare*
  - *Measurement of results is even rarer*
- Workforce analytics rare
  - *More than 25% of survey respondents use little or no workforce analytics*
  - *The vast majority (>61%) report their use as tactical, ad hoc, and disconnected from other key systems and processes*

OWASP
The Open Web Application Security Project

Growth & Turnover Spur Sense of Urgency

- Software development field growing 30%
- Turnover
  - *Industry – 14-15%*
  - *General IT – ~20%*
  - *Software Development – ~20 – 30%*

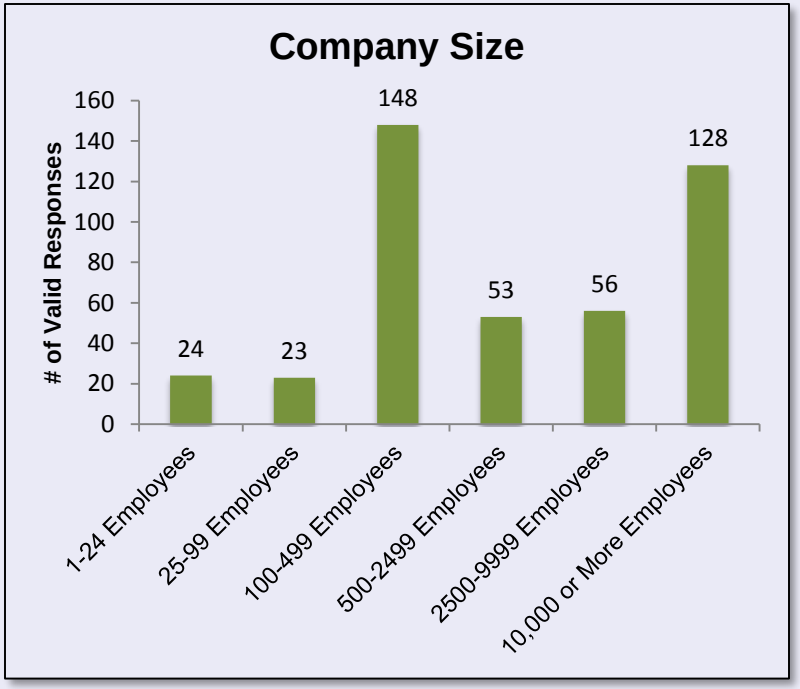
Sources: Bureau for Labor Statistics and Society of Human Resources Management

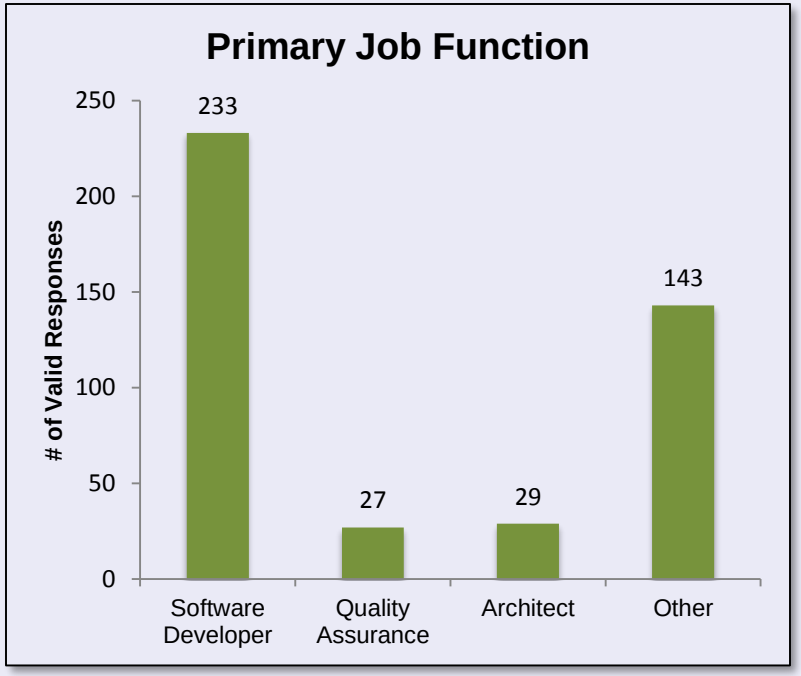
OWASP
The Open Web Application Security Project

Research Overview

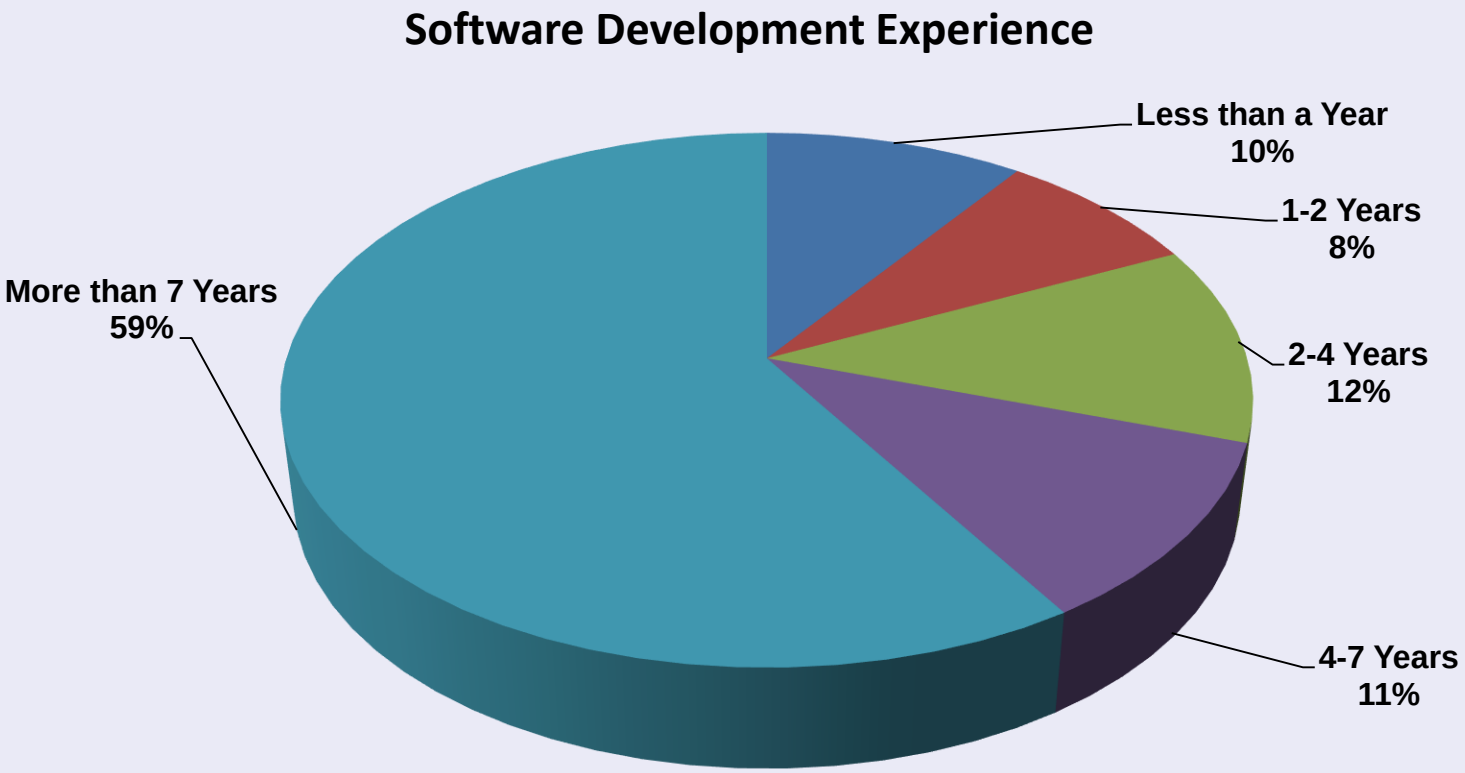
- Focus: Assess the software developers depth of software security knowledge
- Purpose: To measure the impact of software security training on that level of understanding
- Survey size: 600 software developers surveyed in North America (US and Canada)
- Vertical markets represented: financial, government, retail, educational, technology, energy and healthcare segments

Respondent Demographics

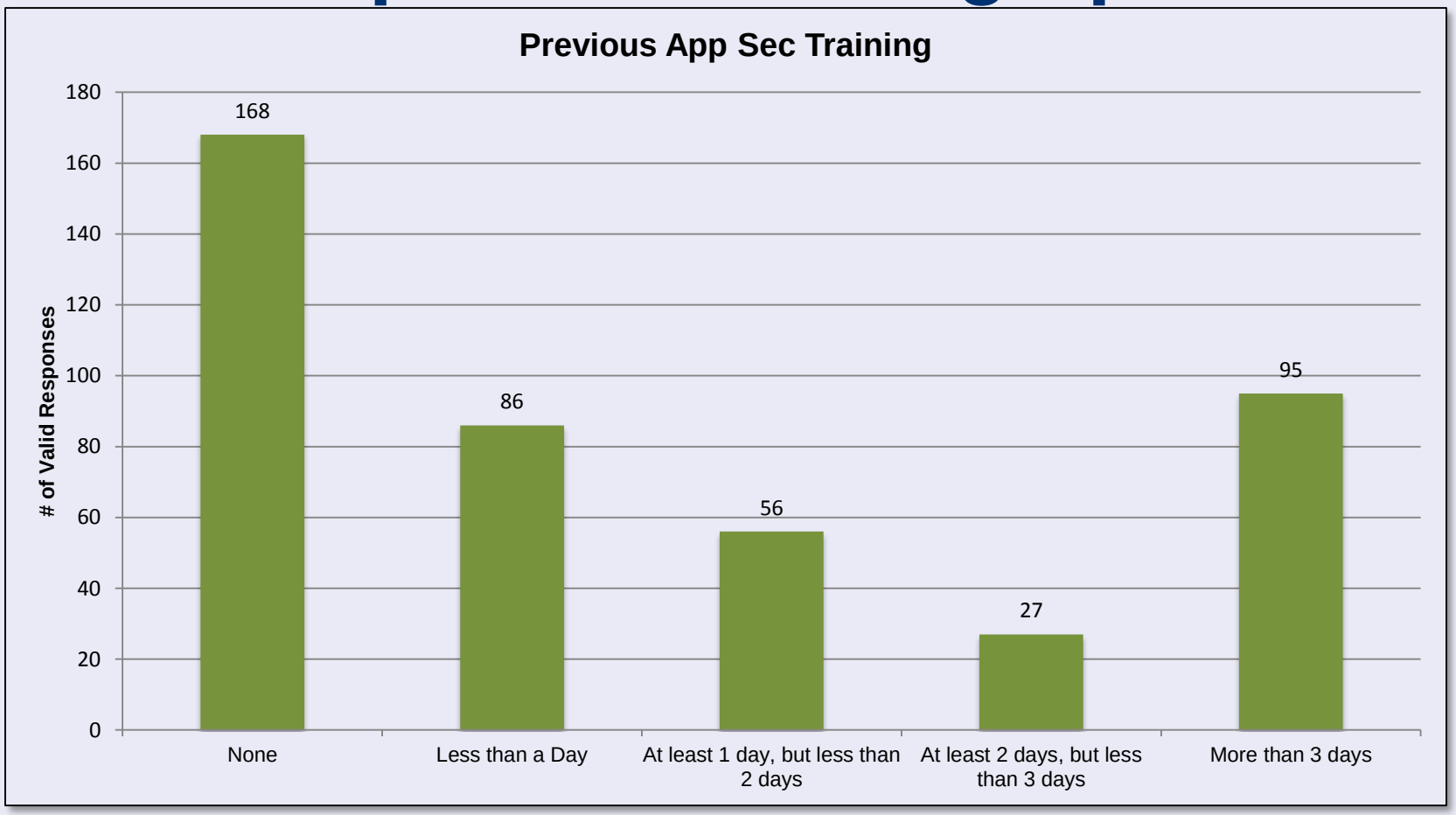




Respondent Demographics



Respondent Demographics



Methodology

- 15 Multiple Choice Quiz-Style Questions
- Targeted at Software Developers
  - Varied by years of experience, amounts of previous training, primary job function, company industry and company size
- Distribution:
  - Online (before and after)
  - Hard-copy questionnaires given to instructor-led class trainees (before and after)
  - Social media networks (sharing and some paid promotion with incentives)

OWASP
The Open Web Application Security Project

Hypotheses

1. Most software developers do not have a basic understanding of software security concepts.
2. Software security training can improve a developer's knowledge of security concepts in the short-term.
3. Certain industries, such as financial services, are more likely to have software developers that are already exposed to key software security concepts.

OWASP
The Open Web Application Security Project

Sample Questions

If an attacker were able to view sensitive customer records they should not have had access to, this would be a(n)_____breach.

___ Confidentiality
___ Integrity
___ Availability

Authentication is...

___ Proving to an application that the user is who they claim to be
___ Confirming that the user is allowed to access a certain page or function
___Verifying that the data displayed on a given page is authentic
___ Thoroughly logging all of a user's important activity

OWASP
The Open Web Application Security Project

Sample Questions

Marking a cookie as “secure” will...

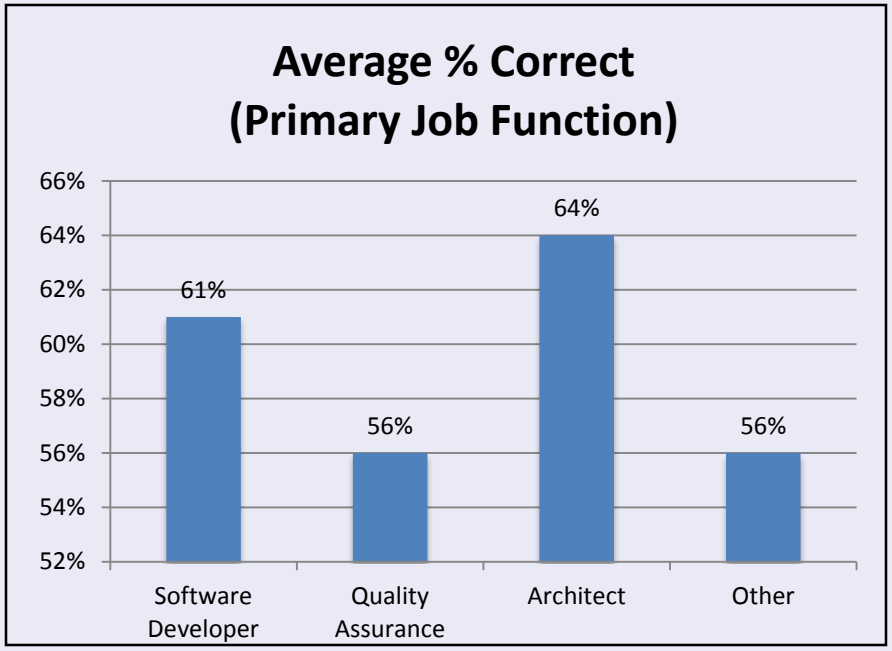
___ Force all requests that use the cookie to use SSL
___ Prevent an attacker from guessing its value
___ Encrypt it when sent over non-SSL requests
___ Tell the browser not to send it over non-SSL requests

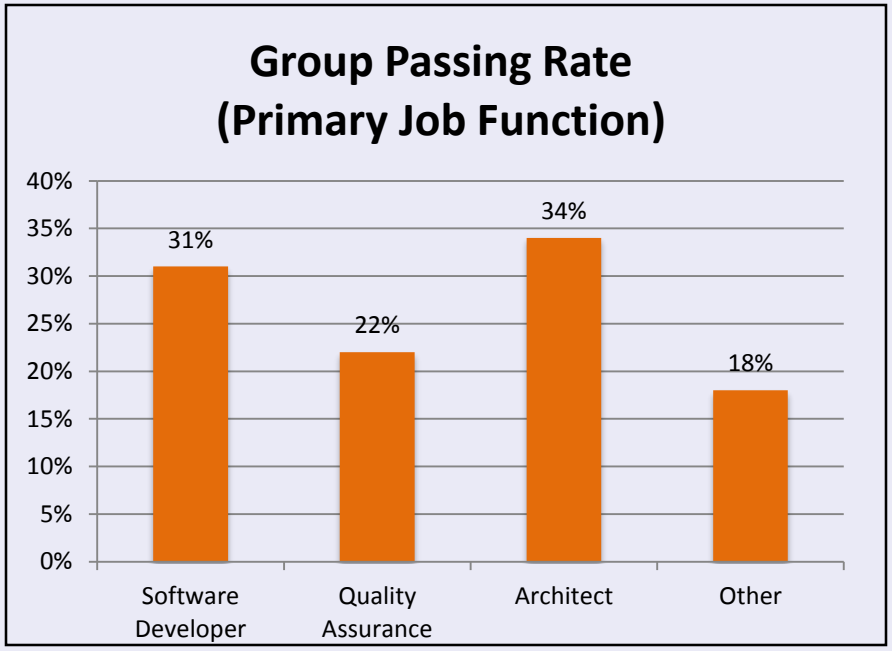
Which of the following will help protect against XSS?

___ Only accepting URL encoded GET parameters
___ Not using any JavaScript in the application
___ Only using JavaScript in .js files stored on external hosts
___ Encoding special HTML characters in data as it is rendered to the page

Key Survey Results

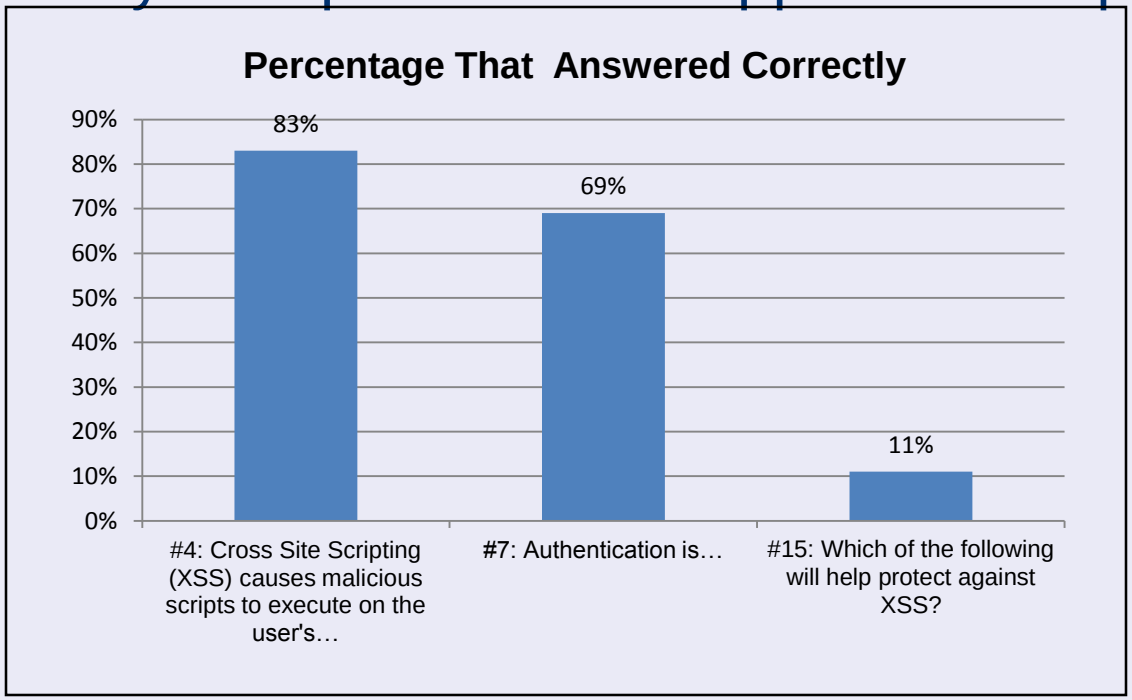
Architects and software developers had a much higher level of knowledge than QA, yet in many organizations QA has a material role in application security





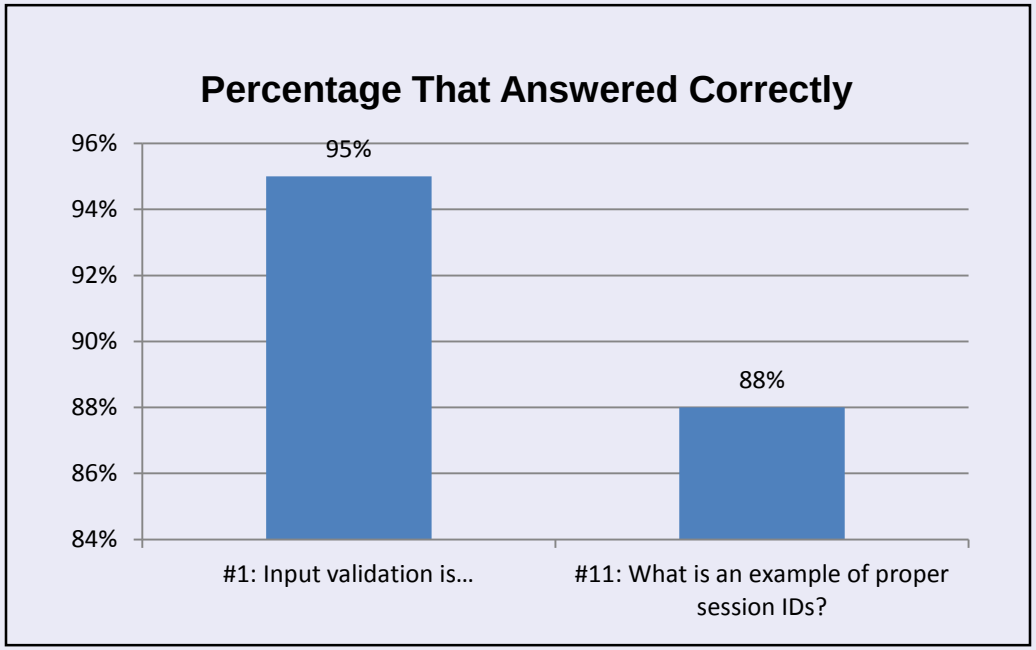
Key Survey Results

Slightly more than half of the respondents correctly answered basic awareness questions on application but struggled with ways to operationalize appsec concepts



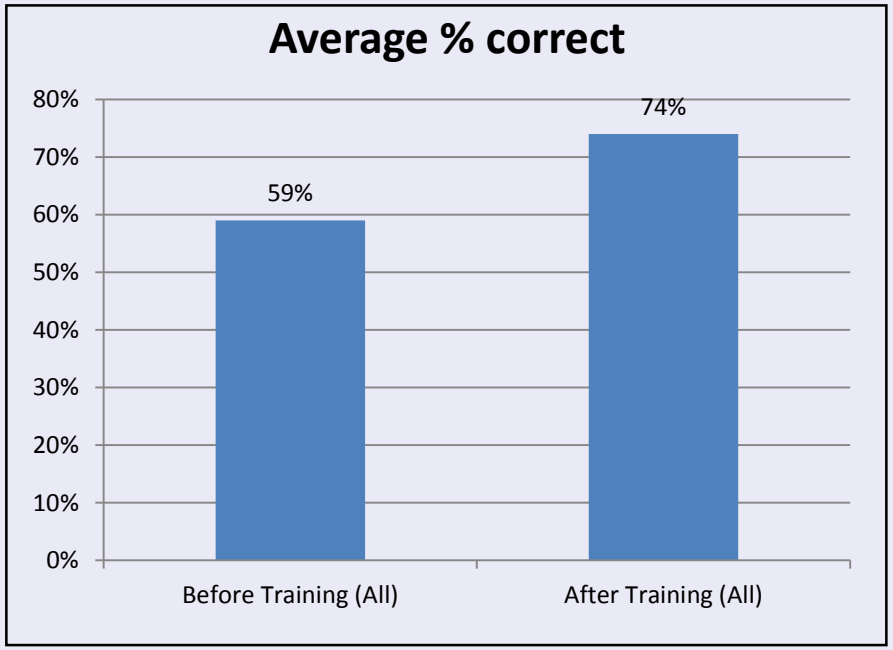
Key Survey Results

- Almost 100 percent could define input validation, demonstrating a choppy understanding of advanced secure coding knowledge
- Nearly 90 percent correctly identified proper session IDs which is reassuring



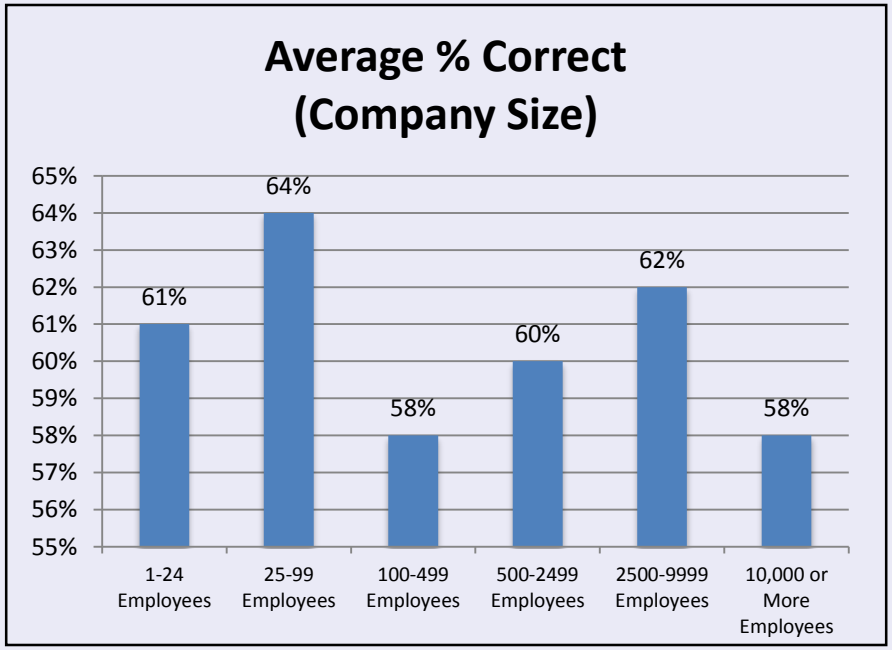
Key Survey Results

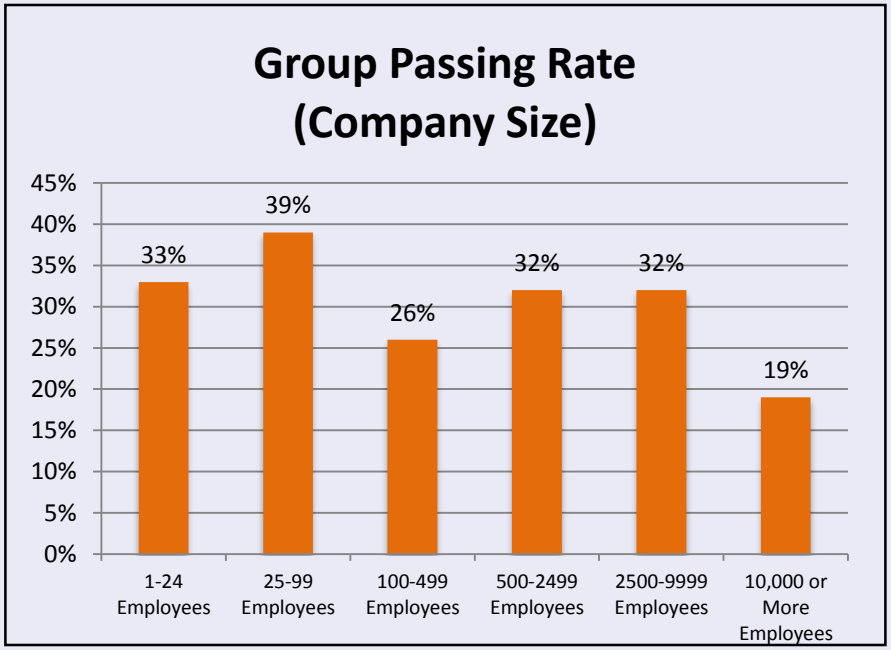
- Retention rose by more than 25 percent after completing secure coding training



Key Survey Results

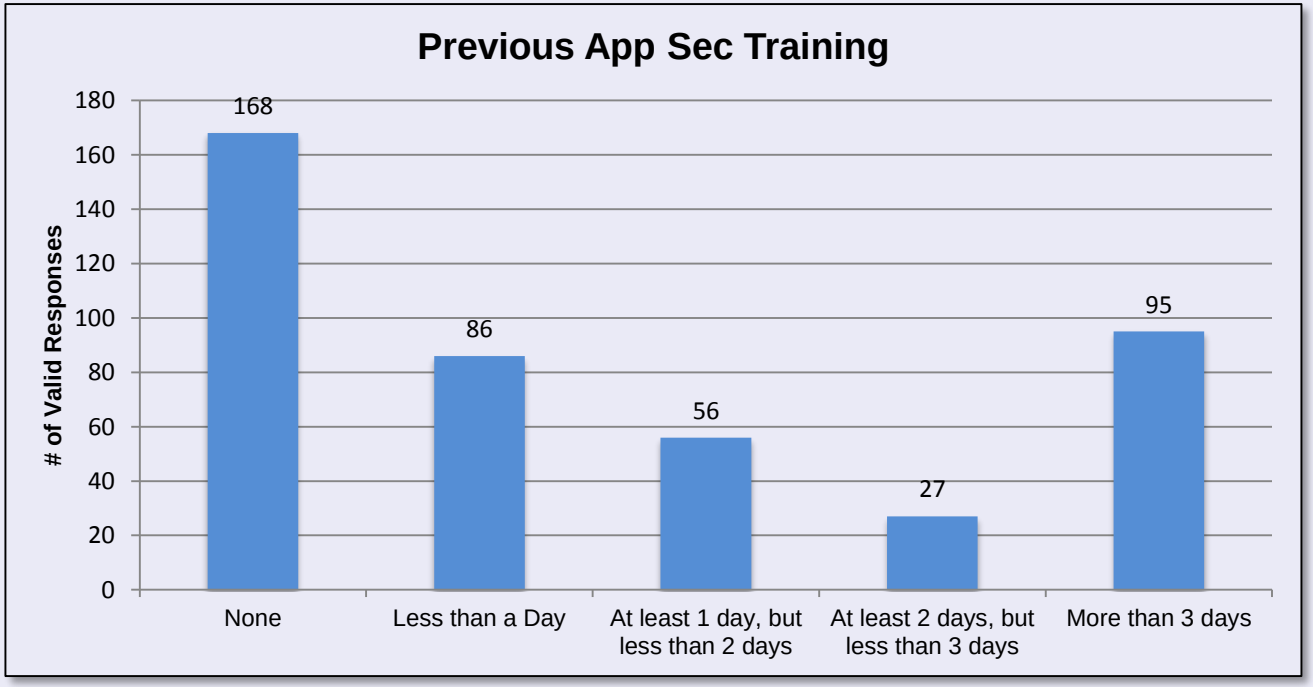
Enterprises of more than 10,000 personnel had the lowest secure coding knowledge





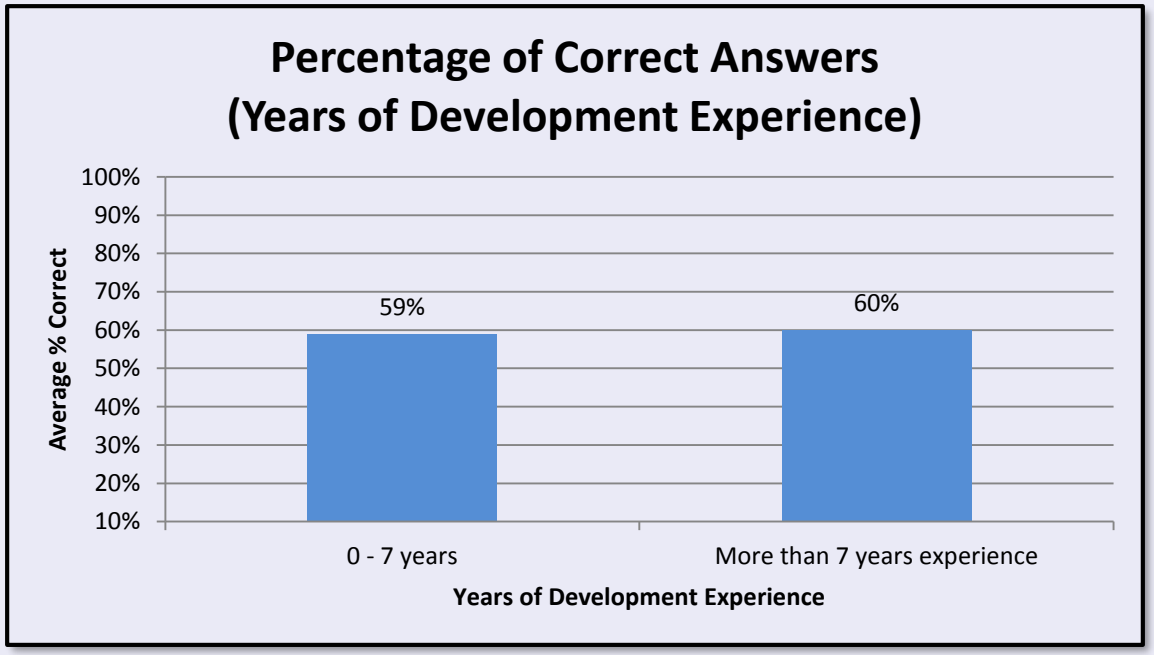
Key Survey Results

The majority of the respondents had no prior secure coding training, which might be surprising



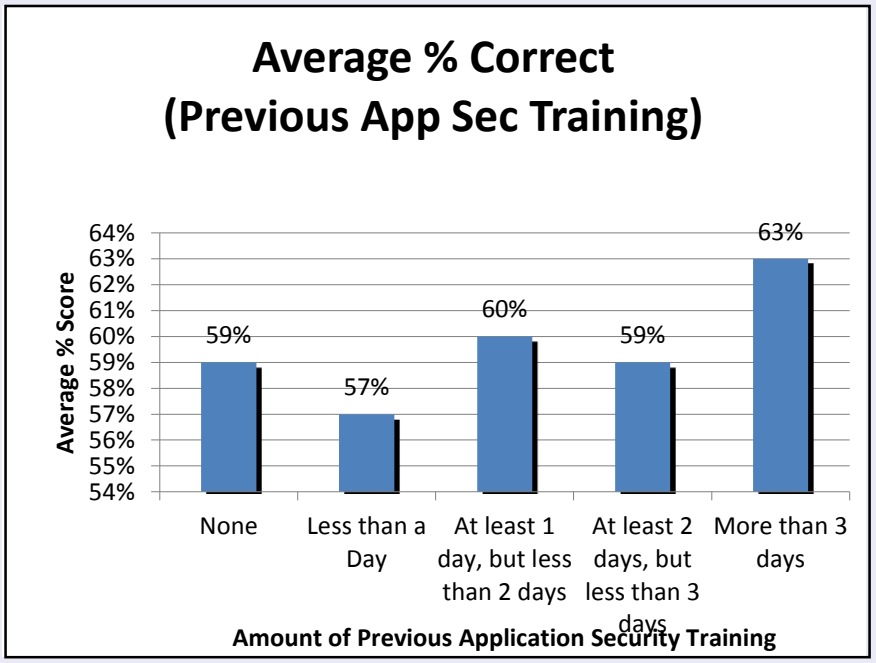
Key Survey Results

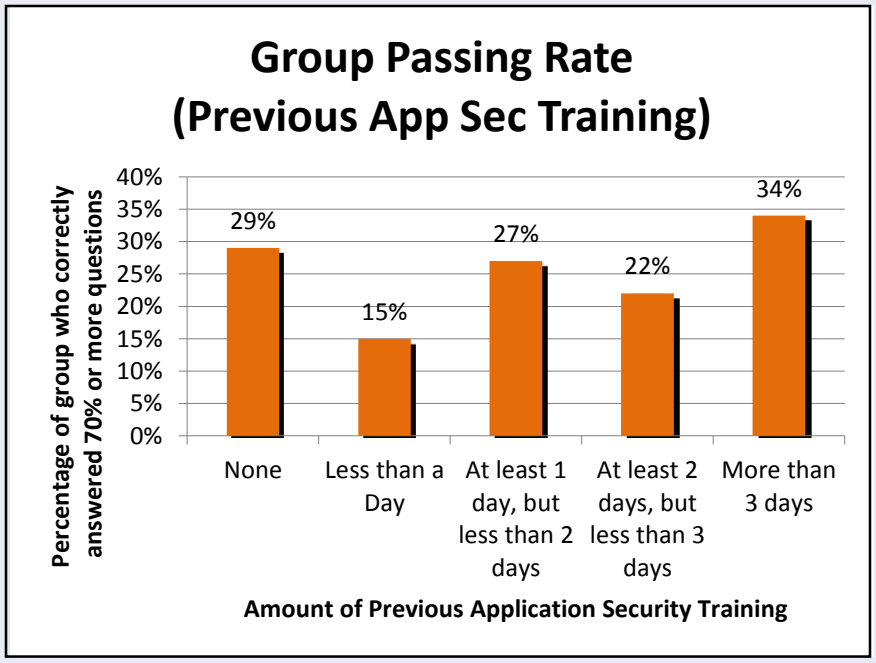
There was no correlation between years of experience and knowledge of secure coding highlighting the continued need for effective security training



Key Survey Results

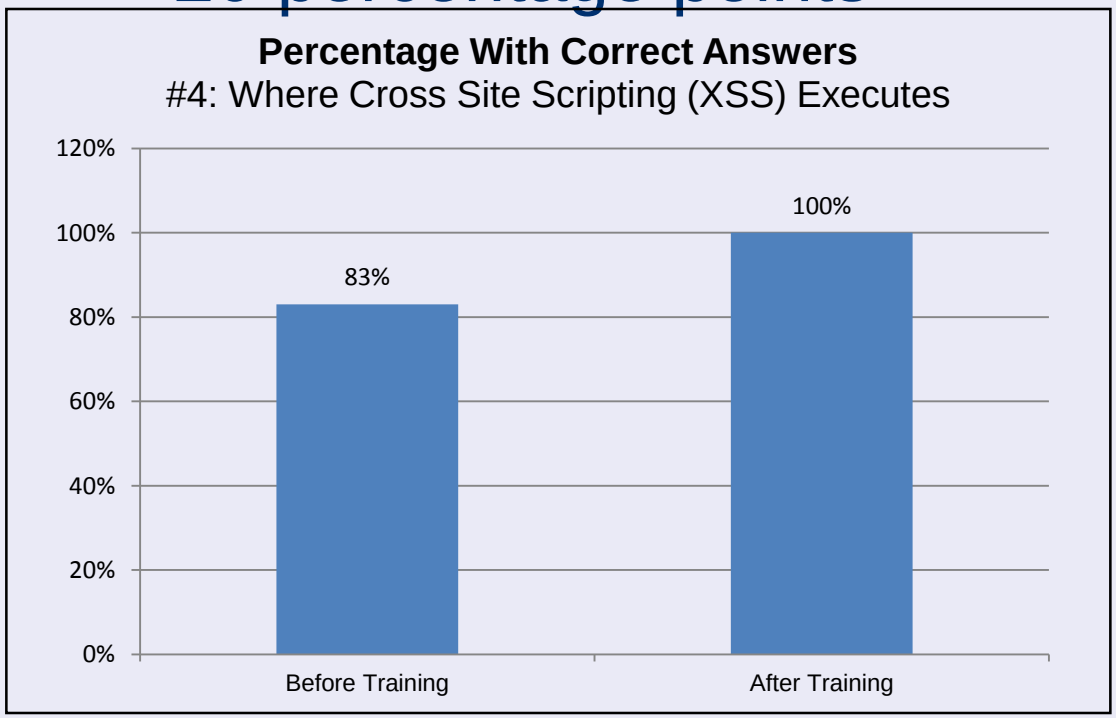
The respondents that had more than 3 days of app sec training in the past were able to answer more than half of the questions correctly





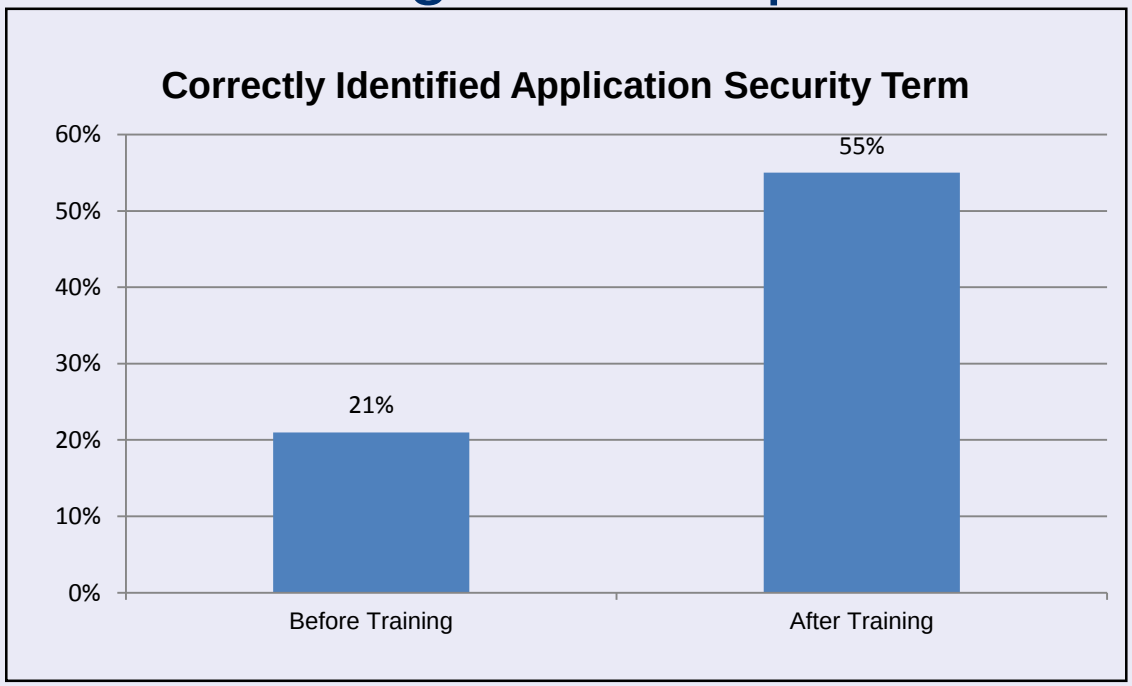
Key Survey Results

100% correctly identified where cross site scripting executes after completing training, an increase of almost 20 percentage points



Key Survey Results

The number of respondents able to correctly identify what is application security more than doubled after training was complete



Other Observations

- Software Developers Learn Differently than Companies Teach
  - *Companies teach via structured e-Learning and classroom training*
    - *Formalized, structured, and repeatable*
    - *Auditable*
  - *Developers Learn in much more unstructured and less formal ways*
    - *RSS feeds, Twitter*

- Incentives Matter
  - *Sobering "before" and after observations on survey completions*
  - *Observations relevant to corporate application security managers rolling out training*

So How Do Developers Learn?

- *Informally and in an unstructured way via:*
  - *Blogs & RSS feeds*
  - *Social media with emphasis*
  - *Developer websites*
  - *Influential e-mail lists*
  - *Safarionline*
- *The Rise of Social Learning Systems*
  - *Informal, collaborative learning activities of individuals, teams and communities of learners.*
  - *Focus is on connections, content, conversations, collaboration and influence to drive relevant, contextual learning and knowledge sharing across the enterprise.*

- Source: “IT Market Clock for Human Capital Management Software, 2013,” Gartner, Aug 2013

OWASP
The Open Web Application Security Project

Don’t Ignore Basics of Training

- Refresher training is still needed
- Training must be included in performance plans
- Managers increasingly want an ROI

Incentives Matter!

CONCLUSION

- Software developers still largely do not understand key software security concepts
  - *73% of respondents "failed" the initial survey*
  - *Average score of 59% before training*
- However, software developers' understanding of key software security concepts did increase after training
- QA staff struggled to understand software security concept vs. architects and software developers

Where do we Go from Here?

OWASP
The Open Web Application Security Project

Potential Follow ups

- Determine how this applies to you
- Ask for my deck!
- Consider reviewing white paper draft
- Participate in Survey 2.0 – starts July 2014
  - *How does your organization stack up against others?*

OWASP
The Open Web Application Security Project

Questions and Answers?

John B. Dickson
@johnbdickson
john@denimgroup.com