THE DZONE GUIDE TO APPLICATION SECURITY

2015 EDITION

BROUGHT TO YOU IN PARTNERSHIP WITH

BLACKDUCK

YOTTAA

Executive Insights on Application Security

BY TOM SMITH

QUICK VIEW

01 There were four major themes that emerged when discussing Application Security: 1) awareness, training and education; 2) two-factor authentication; 3) making testing integral to the development process; and, 4) developer behavior with regards to security.

02 The skills that make a developer good at developing secure applications are curiosity and critical thinking.

03 The most frequently mentioned things that developers need to keep in mind when working on application security was to develop a security mindset.

To more thoroughly understand the state of application security, and where it's going, we interviewed 19 executives with diverse backgrounds and experience in application security. Specifically, we spoke to:

Craig Lurey, CTO and Co-Founder, Keeper Security • **Max Aulakh,** CEO, MAFAZO • **Chris Acton,** Vice President of Operations, RiskSense Inc. • **Alexander Polyakov,** CTO, ERPScan • **Julien Bellanger,** CEO and Co-Founder, Prevoty • **Kevin Sapp,** VP of Strategy, Pulse Secure • **Francis Turner,** VP Research and Security, ThreatSTOP • **Jessica Rusin,** Senior Director of Development, MobileDay • **Ari Weil,** Vice President of Marketing, Yottaa • **John Pavone,** CEO, Aspect Security • **Rami Essaid,** CEO, Distil Networks • **Kevin Swartz,** Marketing Manager, NowSecure • **Jon Gelsey,** CEO, Auth0 • **Amit Bareket,** CEO, SaferVPN • **Mark O'Neill,** Vice President Innovation, Axway • **Deena Coffman,** CEO, IDT911 Consulting • **Walter O'Brien,** Founder and CEO, Scorpion Computer Services • **Walter Kuketz,** CTO, Collaborative Consulting • **Sam Rehman,** CTO, Arxan Technologies

It seems that application security is still a low priority with most enterprises with tens of thousands of applications on the web that have never been tested. Older enterprises seem to be less aware of, or willing to admit, this is a problem. Perhaps this "head in the sand" attitude is why only 52% of the Fortune 500 in 2000 are still in the Fortune 500 today? Will we see the same thing from companies that fail to secure their applications? Here's what we learned.

01

- While there was no definite agreement to the most important elements of application security across those we interviewed, there were four themes: **1) awareness, training and education; 2) two-factor authentication; 3) making testing integral to the development process; and, 4) developer behavior with regards to security.**
- Companies are beginning to realize the importance of security and that application security is not the same as web security. There needs to be more awareness, training and education in terms of protecting applications, potential vulnerabilities, and how to integrate security into the application development lifecycle so it's considered from the beginning rather than as an afterthought.
- Two-factor authentication, knowing who your user is, and who your user isn't, is important to application development and having a security mindset during the development process.
- Static and dynamic platform testing needs to be integral to the application development process so holes and bugs can be identified as the application is being built rather than after the app has been built and companies are anxious to go to market. This puts pressure on the developer not to make the fixes that were identified during testing.
- Developers need to understand the importance of a secure app and how to securely write code for apps. There are a

number of off-the-shelf plug-ins that will encrypt data and provide other security features so the developer does not need to create these from scratch.

02

When we asked respondents "who are the most important players in application security?," the most frequent response was "developers." **Developers are the most important players in application security, not a vendor or a solution provider.** Developers represent the domain knowledge of development and the implementation decisions that affect security is in their hands. Whether they find the vulnerabilities or not, developers are the people that will fix them—or not.

There were several mentions of infrastructure providers, like AWS and Cisco, building platforms with inherent security features like multi-factor authentication. AWS is ahead of the curve. They use APIs and low level products, host their applications on their services, configure network level security firewalls, enable you to create databases and secure storage of encrypted data, and manage access to the system. This is a far superior solution than buying a server from a random hosting provider and then using products that provide a low level of authentication.

03

"Peace of mind" is the greatest value being provided by application security. Not that there is not a long way to go. Every day another company is hacked and has to tell their customers about a security breach. This news is helping c-level executives understanding the importance of protecting their brand and protecting their personal customers' information. Awareness and education about the need to prevent malicious hacks, to prevent knowledge loss and mitigate risk is growing. On person responded to our question with a question, "How do you calculate the value of not being attacked?"

04

The skills that make a developer good at developing secure applications are **curiosity, critical thinking,** the ability to write good code, attention to detail and a passion for security. Some people mentioned thinking like a hacker and understanding testing tools. However, other mentioned that developers are builders and hackers are breakers, as such, it is very challenging for a developer to "think like a hacker."

05

The biggest obstacles to the success of application security initiatives is at the business level—**failure to have a security mindset**—security is an afterthought or not a significant priority. Procurement is the enemy of security because it takes three or four years to buy technology and install it - by then it's out of date. Even after all of the news, the majority of older enterprises have their head in the sand and refuse to admit they've been hacked.

A number of large corporations are paying $10,000 for a security certificate in which nothing was found versus those willing to pay for a legitimate security audit that uncovers hundreds or thousands of vulnerabilities. This is because the time and cost of fixing the vulnerabilities are greater than the cost of the insurance premium that cover any losses due to the vulnerabilities.

In time, insurance companies will raise premiums so high, or refuse to pay for a $50 million loss. When this occurs, every viable company will realize the necessity of developing a security mindset and making application security part of the application development process.

06

The future of Application Security is in the cloud. As already mentioned, AWS is doing a great job of providing secure applications and requiring their users to have API keys for more secure APIs. As a function of requiring customers to comply with their security standards, AWS is building awareness of the importance of application security and educating customer how to improve their application security processes.

Companies need to get out of the business of running their own data centers and move to secure clouds. If one cloud company is holding the data centers of 100 Fortune 1000 companies, they can afford to invest in the high level of security we're talking about. Right now we're putting $1 trillion under the mattress every year and it's getting stolen.

Put customers and security first - ahead of the shareholders. If a bank ever differentiates themselves as being the most secure bank, they will earn a lot of business. There are opportunities for brands to adopt a more secure solution and make that part of their marketing. There's an opportunity for more cloud migration.

07

The most frequently mentioned things that developers need to keep in mind when working on application security was to **develop a security mindset**. Learn the fundamentals of security. Join the Open Web Application Security Project (OWASP). Wholly embrace security as part of your responsibility - while it may not be right now, you will become more valuable if you make it so as it will become your responsibility in the future.

Additional suggestions included: 1) Test everything statically and dynamically while embracing security testing as part of your application design implementation process from beginning to end. 2) Study best practices and don't try to build from scratch. Build on top of proven secure applications while keeping abreast of updates to ensure you are using the latest version of that app with the most recent security updates.

The executives we spoke with are working on their own products or serving clients. We're interested in hearing from developers, and other IT professionals, to see if these insights offer real value. Is it helpful to see what other companies are working on from a senior industry-level perspective? Do their insights resonate with what you're experiencing at your firm?

We welcome your feedback at research@dzone.com.

TOM SMITH is a Research Analyst at DZone who excels at gathering insights from analytics—both quantitative and qualitative—to drive business results. His passion is sharing information of value to help people succeed. In his spare time, you can find him either eating at Chipotle or working out at the gym.