What You Can Learn From Small Companies About AppSec

SANS AppSec Las Vegas 2012

Nick Galbreath @ngalbreath nickg@etsy.com

Who is Etsy? nickg?

- Etsy is the “marketplace for small creative businesses”
- Alexa rank of #51 in USA
- > $500MM/year in transaction volume
- Nick Galbreath is a Director of Engineering focusing on Security, Fraud, Internal Analytics, Internal Tools

FACT

Being at patch level for your OS and applications eliminates the *vast majority* of desktop attacks

The Exploit Intelligence Project, Dan Guido 7/25/2011 http://bit.ly/KiWhmw

FACT

You have security problems on your website *right now*

(although perhaps not currently not exploited)

Your development environment *is* different than production

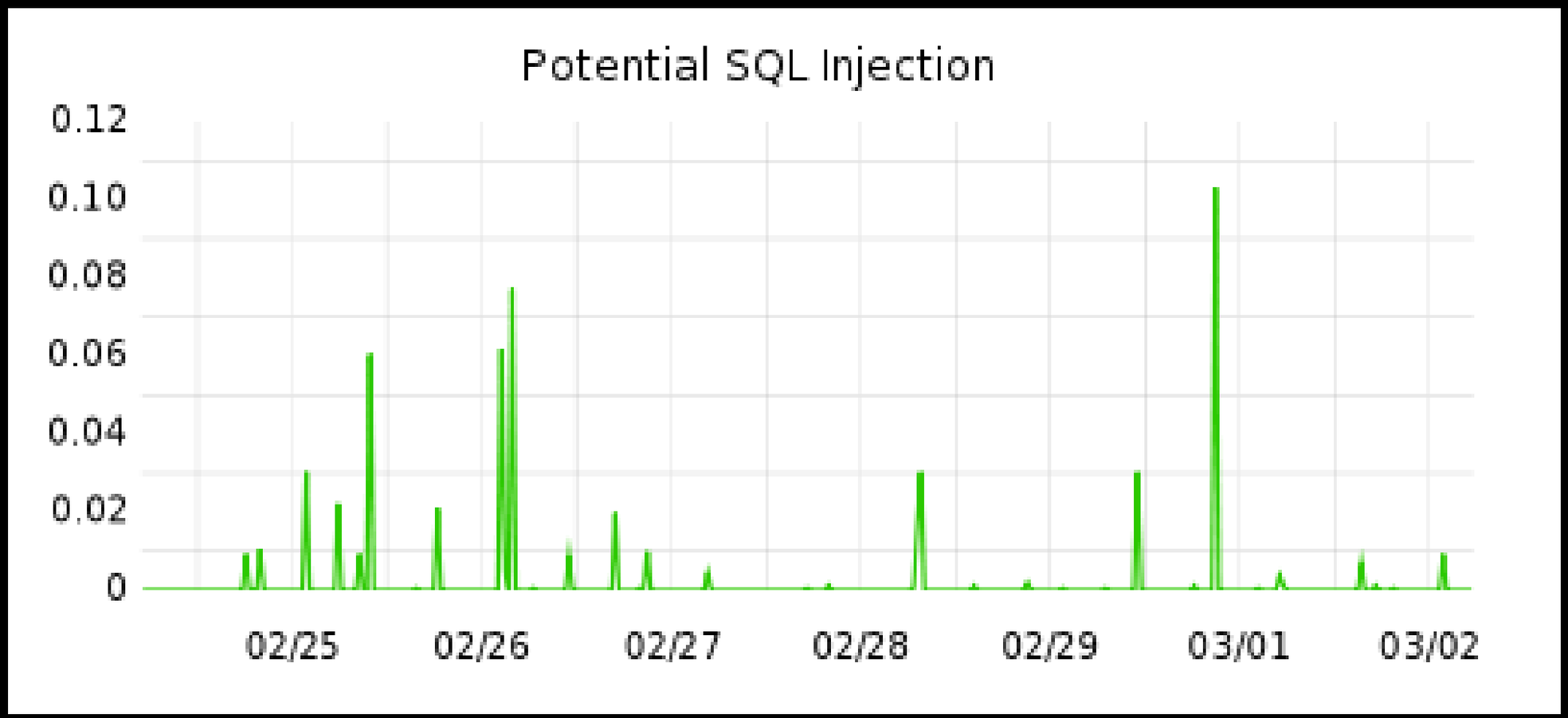
No amount of QA can guarantee “security”

Being able to deploy quickly is my #1 security feature

- This implies a standardized, automated system and configuration management.

Your Server, OS, Desktop, Applications, Routers, etc

Security Feature #2: Being able to graph/log everything



Use attacker-driven security testing

But doesn't rapid change (lean, devops, agile) make things less secure?

Well compared to....

We'll rush that security fix. It will go out in next release in about 6 weeks.

former vendor at Etsy

Etsy

Nick Galbreath nickg@etsy.com
@ngalbreath
SANS AppSec Las Vegas 2012