Sigurnost aplikacija: odakle početi?

IBM Security Services

Vlatko Košturjak, IBM PSS EMEA
PCI QSA, CISSP, CISA, C|EH, MBCI, LPIC-3, ...

HrOUG, Rovinj, 19.10.2011

Agenda

- Security?
- Having App Contract?
- Application Requirements
- Non-Functional app requirements
- Security requirements
- Testing security requirements
- Free tools and resources
- Q & A

30 minutes

Security

- Phewww...
- No time for that...
- No money
- Will do that on the end
- Not important (right now)...
- It's circus...

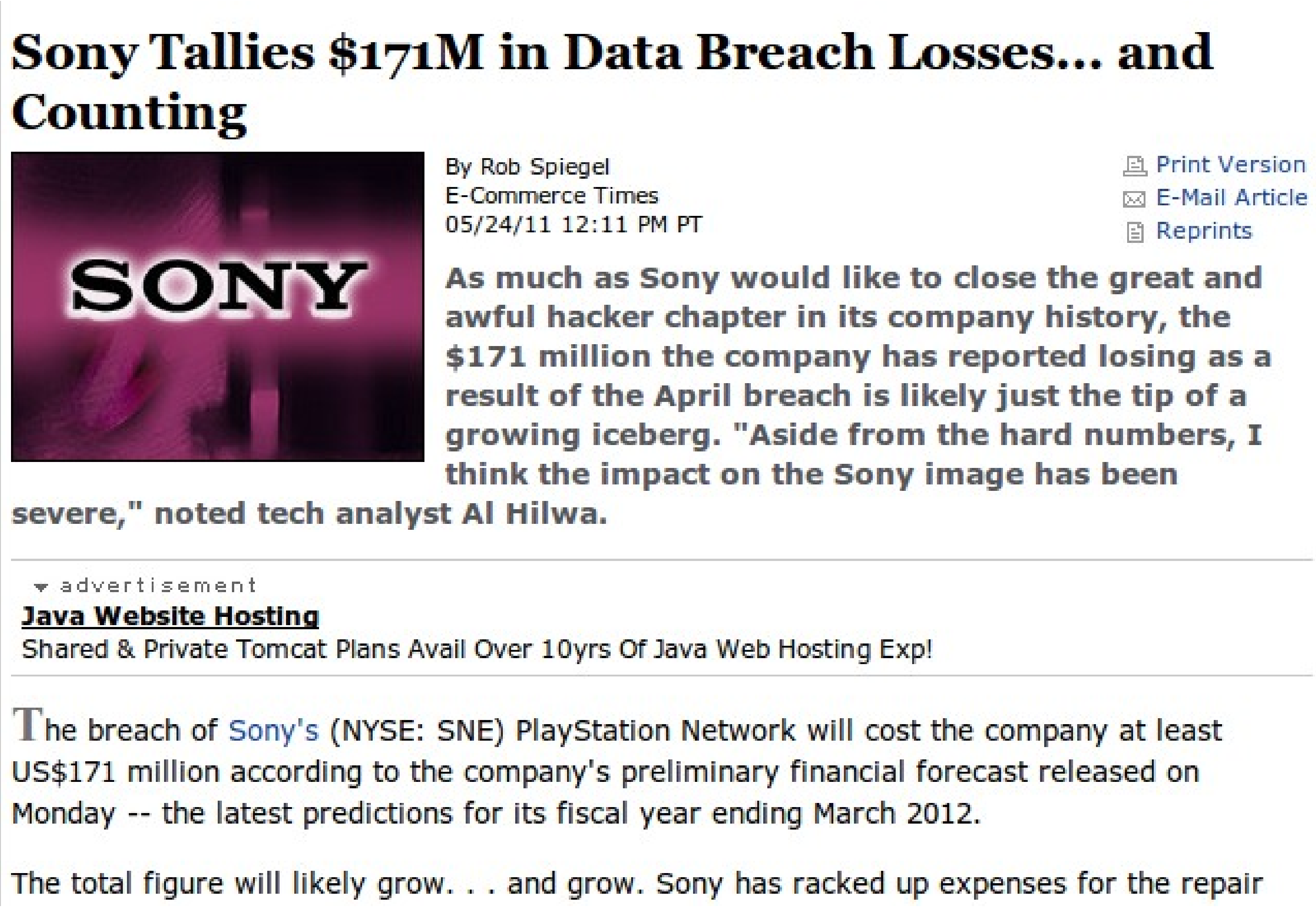
Linus Torvalds on security

..."[O]ne reason I refuse to bother with the whole security circus is that I think it glorifies - and thus encourages - the wrong behavior.
[..]
In fact, all the boring normal bugs are way more important..."

Security people are often the black-and-white kind of people that I can't stand. I think the OpenBSD crowd is a bunch of [self-stimulating] monkeys.

http://lkml.org/lkml/2008/7/15/296

...tell that to Sony!



Sony Tallies $171M in Data Breach Losses... and Counting

By Rob Spiegel
E-Commerce Times
05/24/11 12:11 PM PT

Print Version
E-Mail Article
Reprints

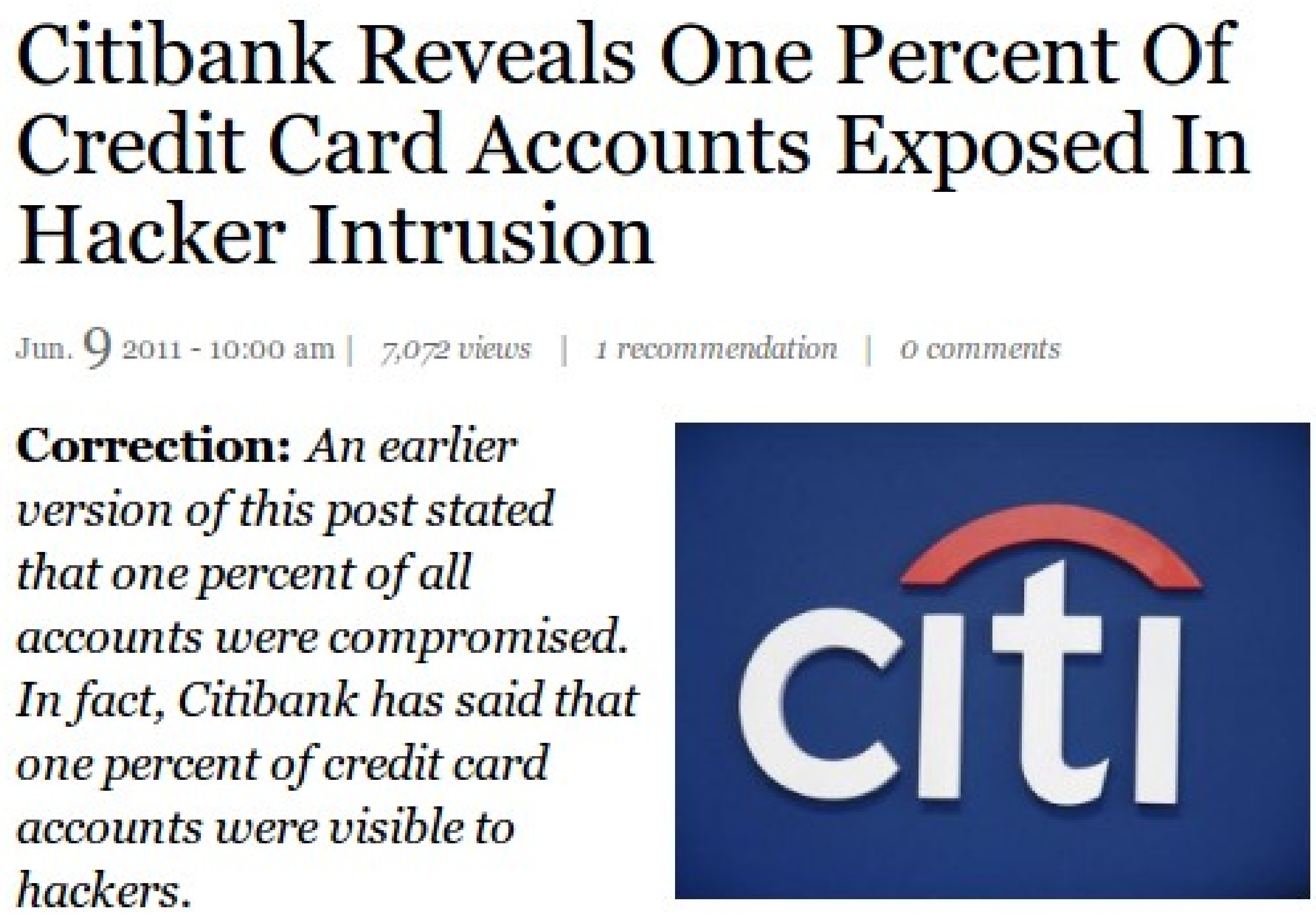
As much as Sony would like to close the great and awful hacker chapter in its company history, the $171 million the company has reported losing as a result of the April breach is likely just the tip of a growing iceberg. "Aside from the hard numbers, I think the impact on the Sony image has been severe," noted tech analyst Al Hilwa.

The breach of Sony's (NYSE: SNE) PlayStation Network will cost the company at least US$171 million according to the company's preliminary financial forecast released on Monday -- the latest predictions for its fiscal year ending March 2012.

The total figure will likely grow. . . and grow. Sony has racked up expenses for the repair

http://www.ecommercetimes.com/rsstory/72520.html

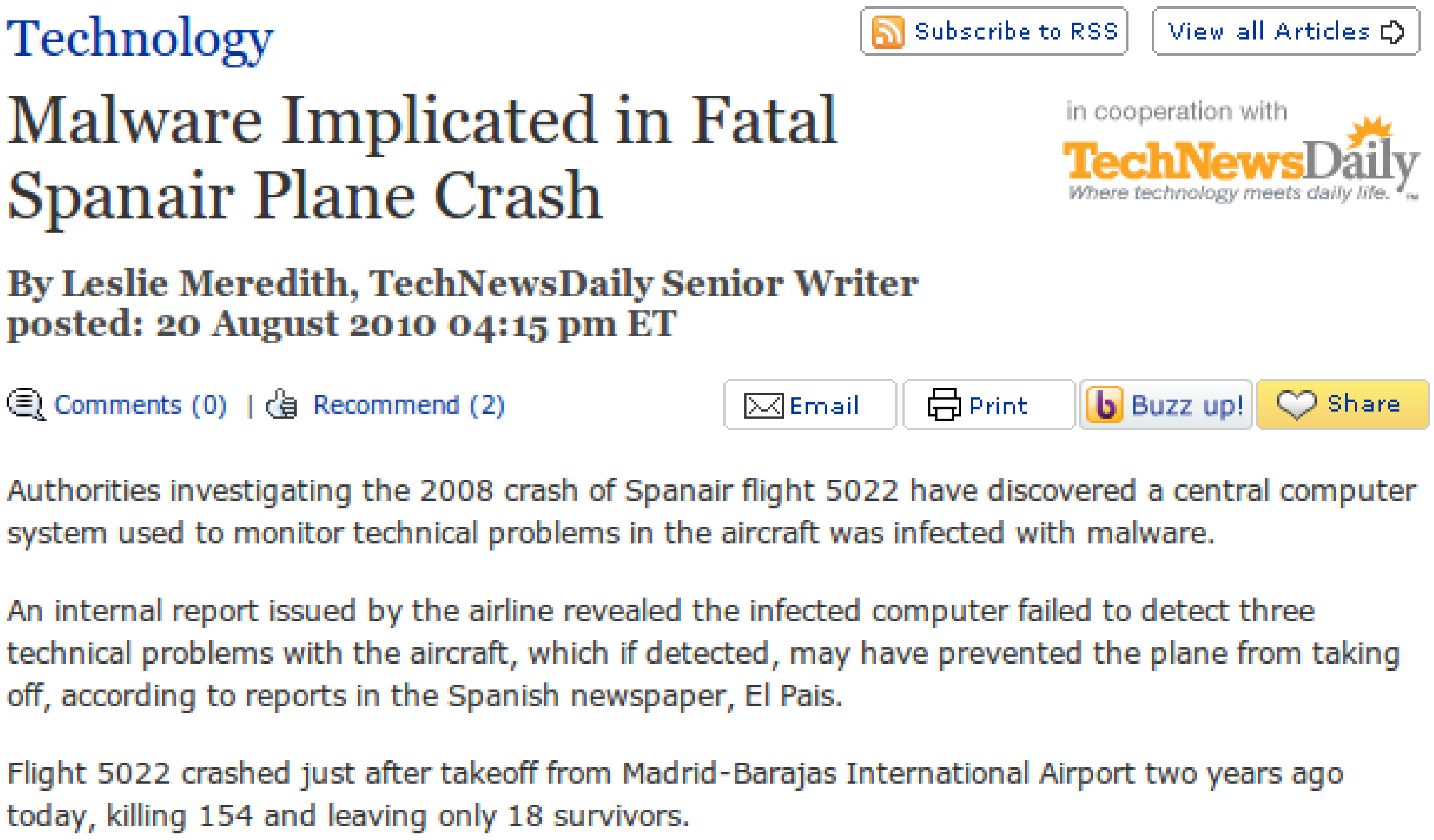
or Citibank



Citibank Reveals One Percent Of Credit Card Accounts Exposed In Hacker Intrusion

Jun. 9 2011 - 10:00 am | 7,072 views | 1 recommendation | 0 comments

Correction: *An earlier version of this post stated that one percent of all accounts were compromised. In fact, Citibank has said that one percent of credit card accounts were visible to hackers.*



Technology

Malware Implicated in Fatal Spanair Plane Crash

By Leslie Meredith, TechNewsDaily Senior Writer
posted: 20 August 2010 04:15 pm ET

Authorities investigating the 2008 crash of Spanair flight 5022 have discovered a central computer system used to monitor technical problems in the aircraft was infected with malware.

An internal report issued by the airline revealed the infected computer failed to detect three technical problems with the aircraft, which if detected, may have prevented the plane from taking off, according to reports in the Spanish newspaper, El Pais.

Flight 5022 crashed just after takeoff from Madrid-Barajas International Airport two years ago today, killing 154 and leaving only 18 survivors.

www.livescience.com/technology/malware-spanair-plane-crash-100820.html

RockYou?

December 2009

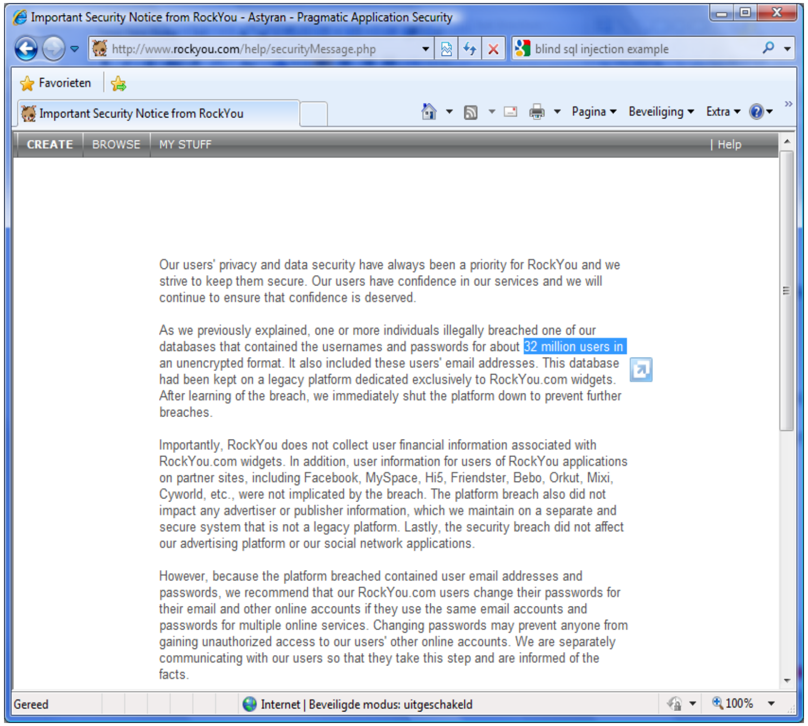
a hacker used SQL Injection techniques to hack the database of RockYou

RockYou creates applications for MySpace, Facebook, ...

Result

data of 32.603.388 users and administrative accounts was compromised (credentials + clear text passwords)

the data also contained email-addresses and passwords for 3rd party sites



Important Security Notice from RockYou - Astyran - Pragmatic Application Security
http://www.rockyou.com/help/securityMessage.php
blind sql injection example
Favorieten
Important Security Notice from RockYou
Pagina
Beveiliging
Extra
CREATE
BROWSE
MY STUFF
| Help
Gereed
Internet | Beveiligde modus: uitgeschakeld
100%

Our users' privacy and data security have always been a priority for RockYou and we strive to keep them secure. Our users have confidence in our services and we will continue to ensure that confidence is deserved.

As we previously explained, one or more individuals illegally breached one of our databases that contained the usernames and passwords for about 32 million users in an unencrypted format. It also included these users' email addresses. This database had been kept on a legacy platform dedicated exclusively to RockYou.com widgets. After learning of the breach, we immediately shut the platform down to prevent further breaches.

Importantly, RockYou does not collect user financial information associated with RockYou.com widgets. In addition, user information for users of RockYou applications on partner sites, including Facebook, MySpace, Hi5, Friendster, Bebo, Orkut, Mixi, Cyworld, etc., were not implicated by the breach. The platform breach also did not impact any advertiser or publisher information, which we maintain on a separate and secure system that is not a legacy platform. Lastly, the security breach did not affect our advertising platform or our social network applications.

However, because the platform breached contained user email addresses and passwords, we recommend that our RockYou.com users change their passwords for their email and other online accounts if they use the same email accounts and passwords for multiple online services. Changing passwords may prevent anyone from gaining unauthorized access to our users' other online accounts. We are separately communicating with our users so that they take this step and are informed of the facts.

Question: how many of those users use the same password for other sites too?

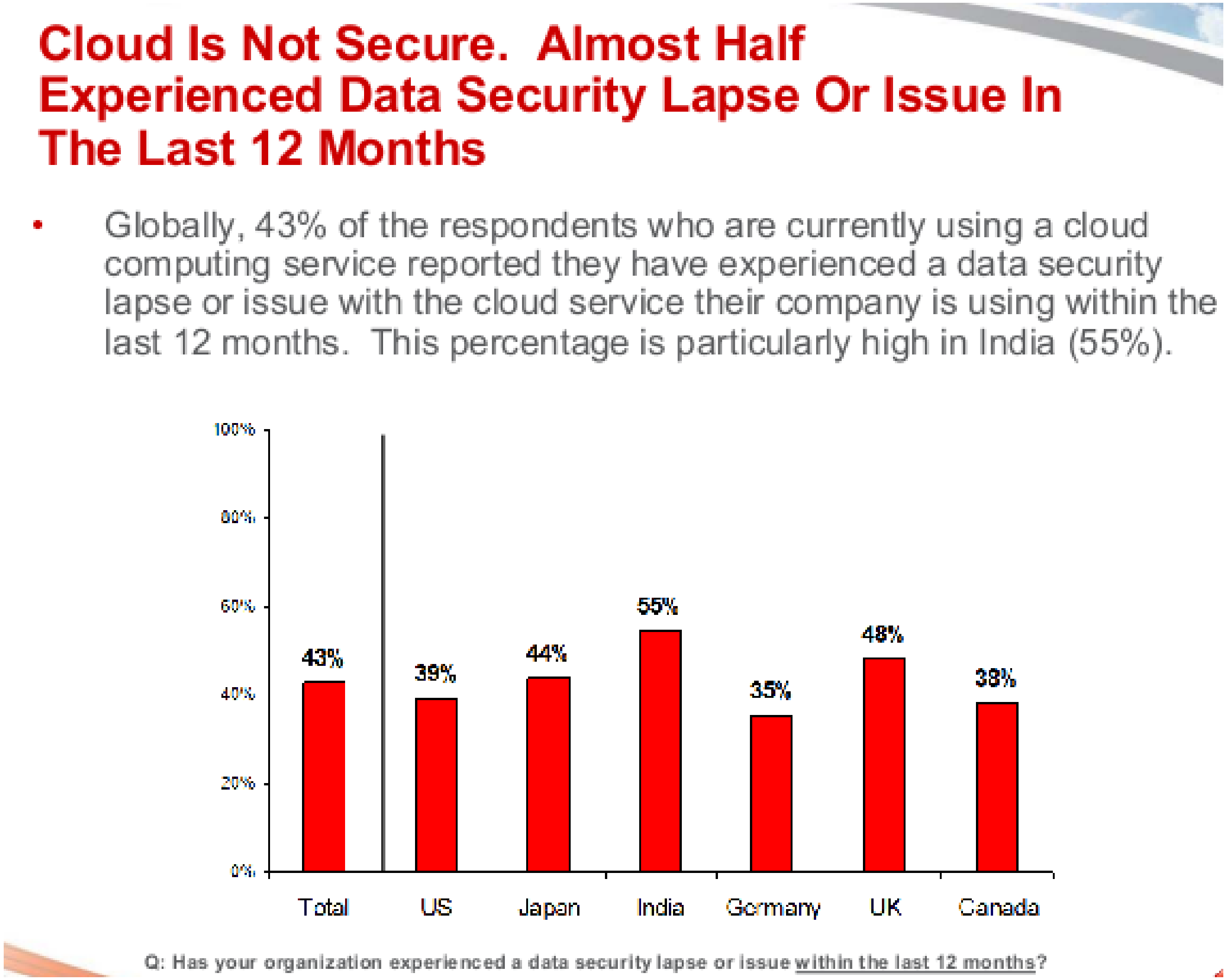
It makes you worry...

@hdmoore: There is something wrong in the world when Facebook and World of Warcraft have better security than many banks: http://bit.ly/fECg6X

Security in Cloud

We'll just move to the cloud – no worries ;)

Cloud security?

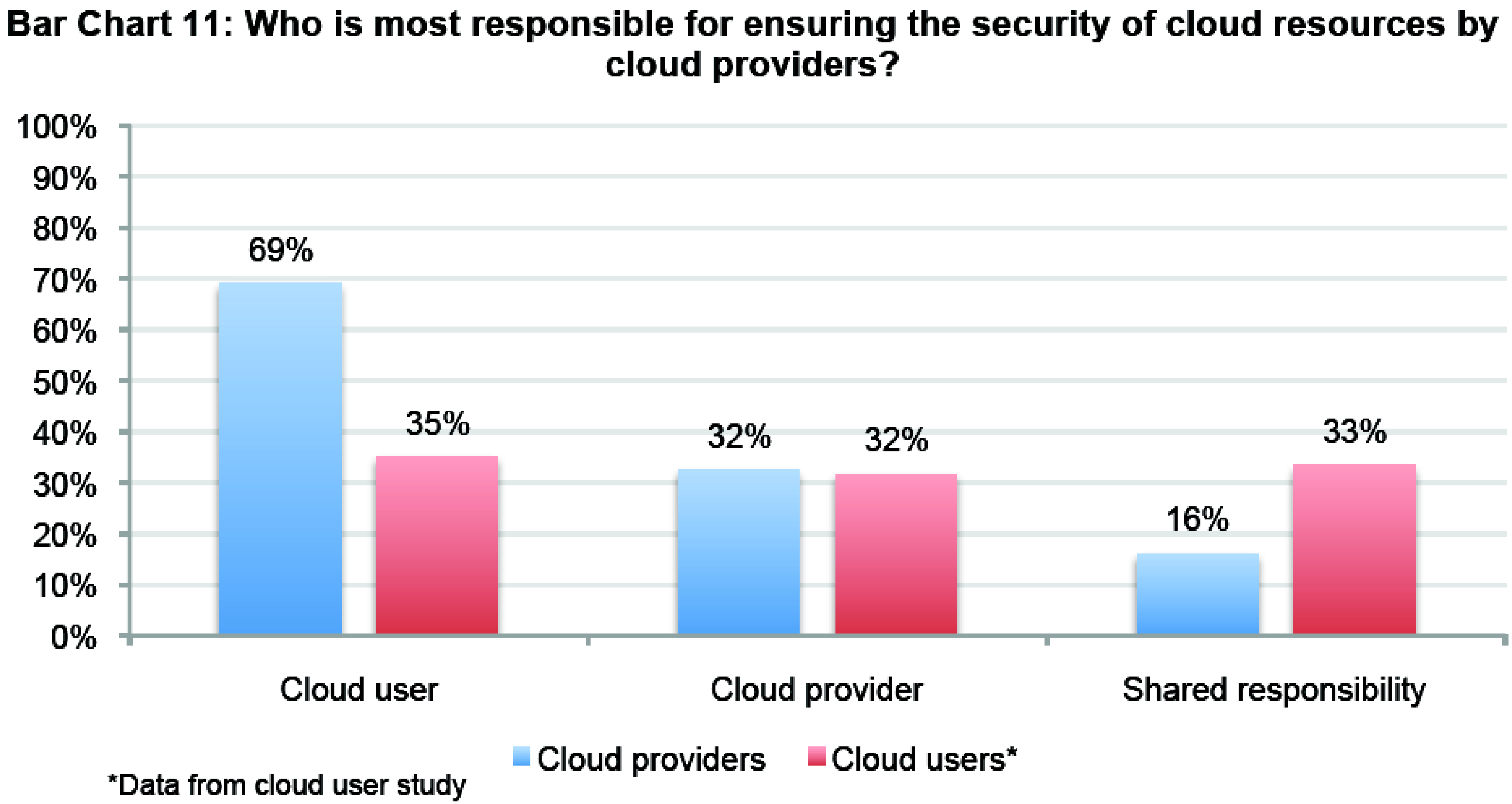


Cloud Is Not Secure. Almost Half Experienced Data Security Lapse Or Issue In The Last 12 Months

- Globally, 43% of the respondents who are currently using a cloud computing service reported they have experienced a data security lapse or issue with the cloud service their company is using within the last 12 months. This percentage is particularly high in India (55%).

Q: Has your organization experienced a data security lapse or issue within the last 12 months?

Cloud Security responsibility



Security Contract?

- Not have security responsibility in contract?
  - Requestor
    - you pay for security fixes
  - Developer
    - you don't pay for security fixes
- have security responsibility in contract?
  - Requestor
    - you don't pay for security fixes
  - Developer
    - you pay for security fixes

Let's put “security” in contract!

- That's easy!
  - We'll just add app must be secure

Mission Accomplished, Lecture over, Q&A!

Not so easy!

Is your app
"this" secure,

or "THIS"
secure?

Read ASVS.

http://www.owasp.org/
index.php/ASVS

What do I mean by secure?
is it same as you or I think?

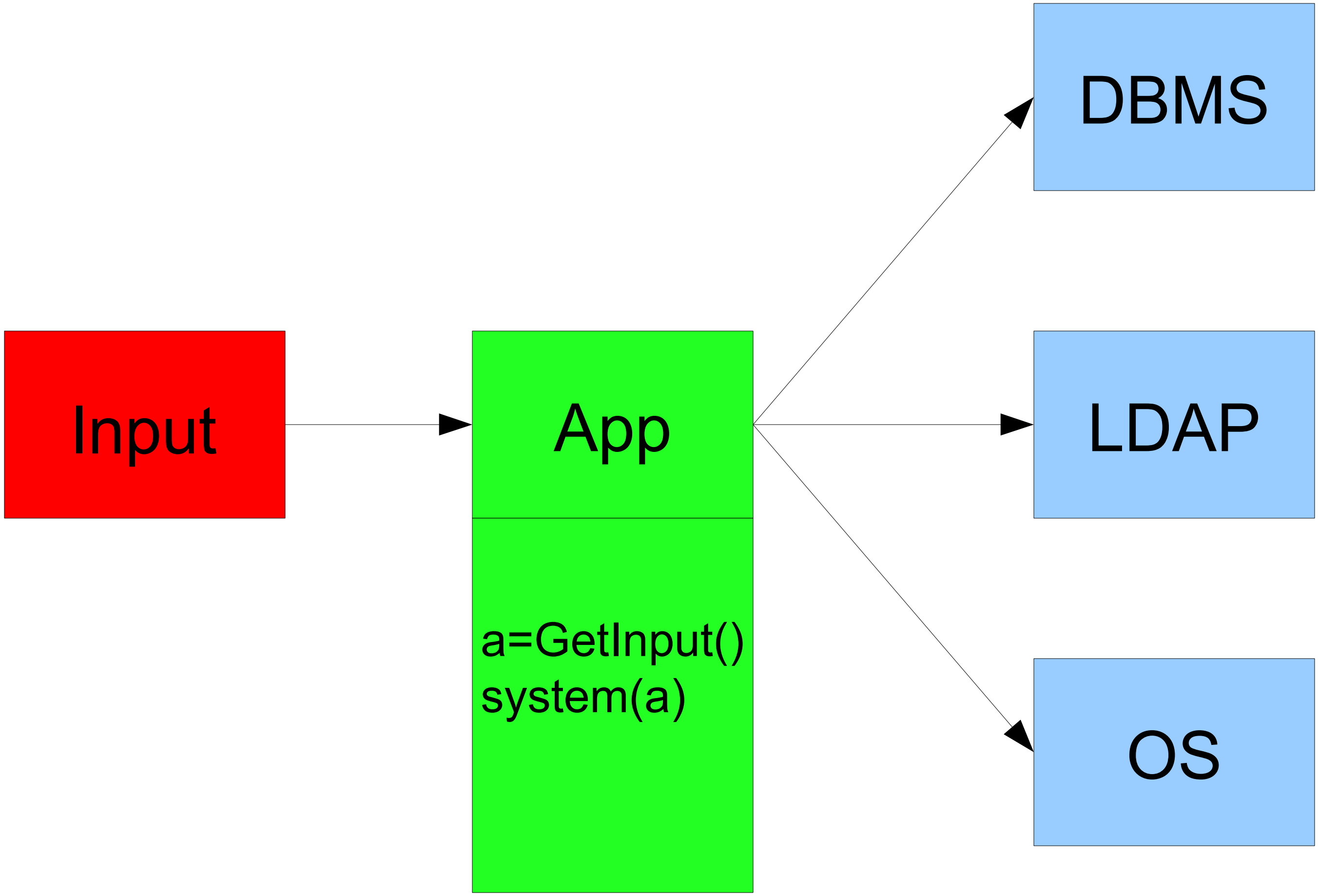
Let's do it right way!

- Add security responsibilites
- Define requirements as part of contract, appendix or part of general requirements
  - functional
  - non-functional
    - performance
    - security

What do we mean by security or secure?

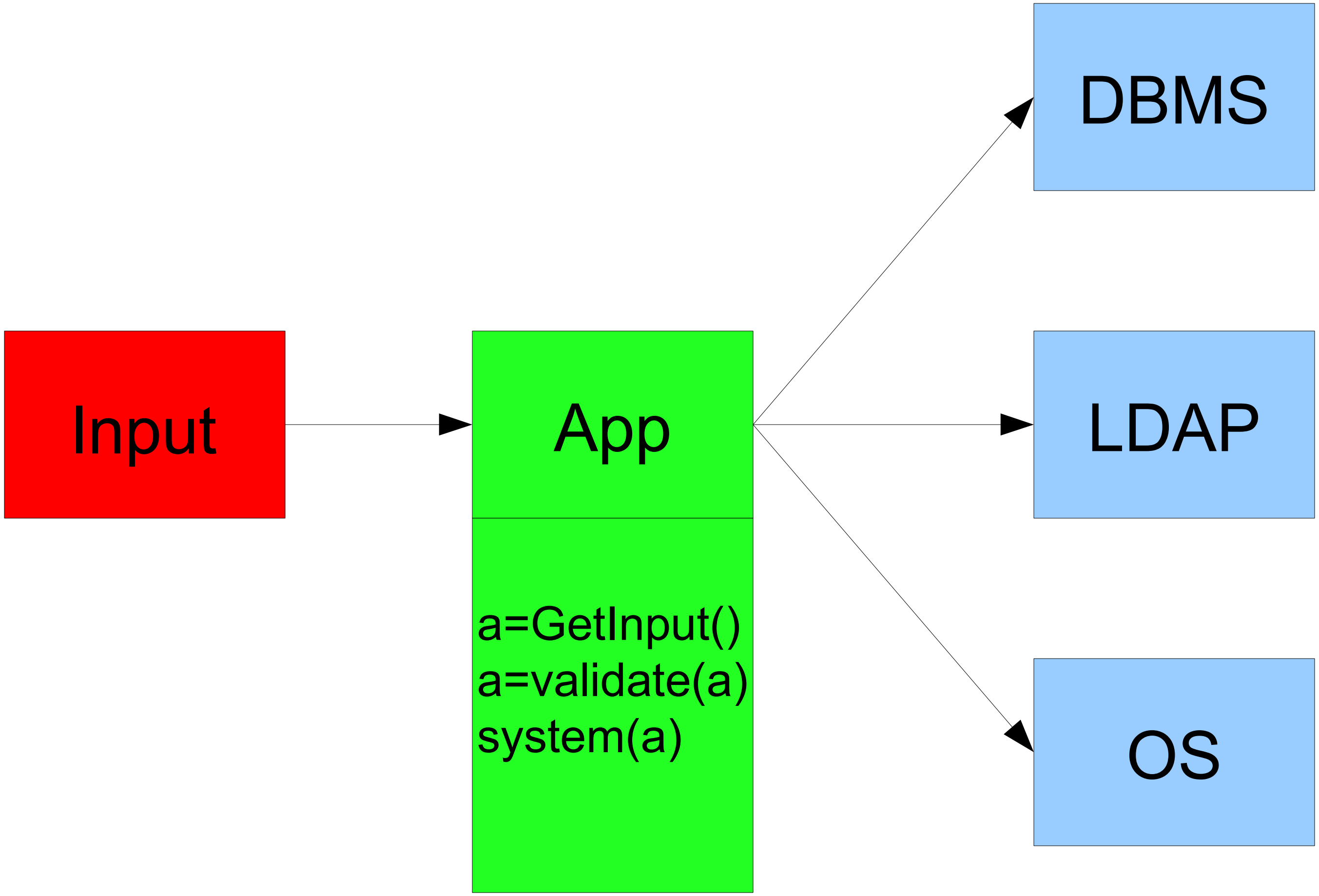
- From whom/what we're defending?
- Programmers/Developers don't expect
  - Buffer overflow
  - Injections
    - SQL
    - LDAP
  - Cross Site Scripting (XSS)
  - ...

Taint?



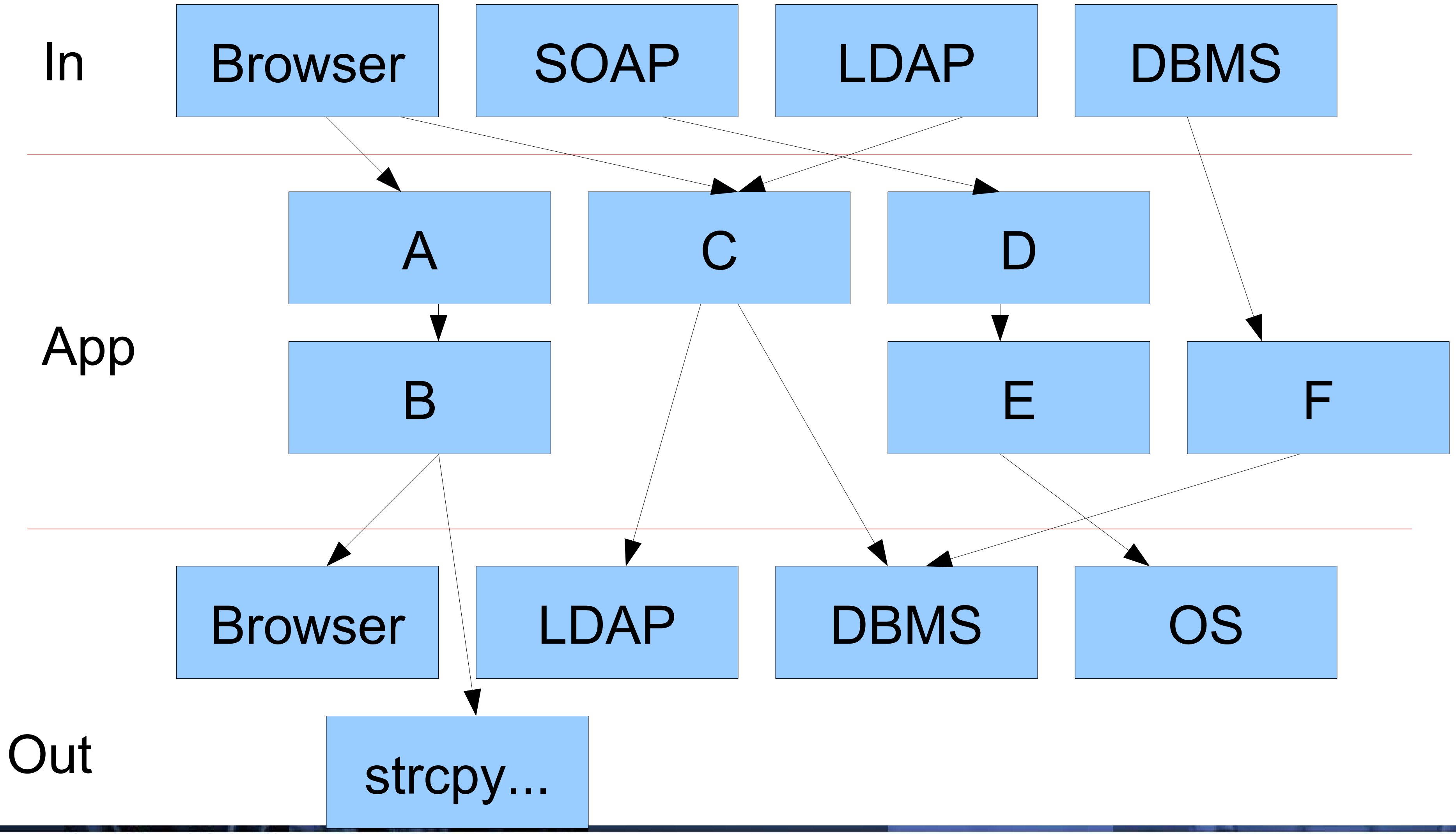
```
a=GetInput()
system(a)
```

Taint?



```
a=GetInput()
a=validate(a)
system(a)
```

Data flow



In

Browser

SOAP

LDAP

DBMS

App

A

C

D

B

E

F

Out

Browser

LDAP

DBMS

OS

strcpy...

OWASP Top 10 - 2010

- Injection
- Cross Site Scripting (XSS)
- Broken Authentication and Session Management
- Insecure Direct Object References
- Cross Site Request Forgery (CSRF)
- Security misconfigurationh
- Failure to Restrict URL Access
- Unvalidated Redirects and Forwards
- Insecure Cryptographic Storage
- Insufficient Transport Layer Protection

http://www.owasp.org

Huh!

Too much stuff to put...

OWASP (again) comes to rescue...

OWASP contracting project

https://www.owasp.org/index.php/Category:OWASP_Legal_Project

Development starts

It's going really great....

really!

...but Web developer have questions about “that security part”....

OWASP (again) comes to rescue

OWASP Development Guide

https://www.owasp.org/index.php/Category:OWASP_Guide_Project

Wooho! It's over!

- Development is finished
- Contract fullfiled
- Everything is secure by contract!

Talk is finished. Q&A

Well, not really....

How we will check that contract requirements are met?

:)

By testing, of course!!

Application security test

- Review/check of application
  - Goal: find vulnerabilities and identify risks
- Various types of testing
  - White-Box
  - BlackBox
- Code review
  - Static analysis
    - Code is not executed
  - Dinamic analysis
    - Code is executed

Will conduct Vulnerability assessment and Penetration test

- We'll do it ourselves
  - OWASP comes to rescue
    - OWASP testing project
  - https://www.owasp.org/index.php/Category:OWASP_Testing_Project

- We'll hire someone

WastedStrand on Penetration testing "It is like being on a date and finding out how far he or she is willing to go"

Sony

@wikidsystems: Sony: "Why pay for pentesting when we can get it free!" - Same test quality, but open source reporting ;)

Free tools

- w3af
- skipfish
- wapiti
- OWASP webscarab
- Paros / ZAP / Andiparos
- ...
- Browser addons
  - XSSme
  - SQL injectme
  - ...

Thoughts

- Application has passed penetration test
  - With automatic tool?
  - What privileges were used?
  - With all dana?
- Application was audited
  - ...audit report says OK
- We have application level firewall
  - Correctly implemented? Configured?
  - Only protection layer
- We reviewed source code of the application
  - With automatic tool?
  - Manually? How skilled?

Example of penetration testing fail

```
# pseudo code example

if (action==doreport) {
        If (userlevel==bla) {
                If (usergroup==trans) {
                        If (timeofweek=='wednesday') {
                                system(userinput)
                        }
                }
        }
}
```

Tests?

CANONICAL
VIDI
DORS / CLUC
Dani otvorenih računalnih sustava
Croatian Linux Users' Convention
www.dorscluc.org
18. - 19. svibnja 2011.

Mark Shuttleworth at #dorscluc: "*...it's harder to produce good tests than the code itself...*"

Code review

- requirement
  - Source code available
- Different ways
  - grep dangerous f()
  - control flow
  - data flow
  - ...

OWASP comes to rescue!

OWASP Code Review Project

https://www.owasp.org/index.php/Category:OWASP_Code_Review_Project

Taint checks?

- Ruby
  - -T level
- Perl
  - -t (warnings)
  - -T (blocks)
- Python?
  - Of course, not ;)
  - -t

Tools

- Simple - Unix/Linux/Windows(Cygwin)
  - cat
  - less
  - more
  - grep
  - awk
  - sed
  - vi(m)
  - ...

Tools: open source

- Flawfinder / Rats
- CLANG
- C code analysis (CCA)
- Graudit (grep)
- SWAAT (OWASP)
- Yasca
- FindBugs
- pylint
- ...

O2 Platform
http://o2platform.com

.NET
!Mono

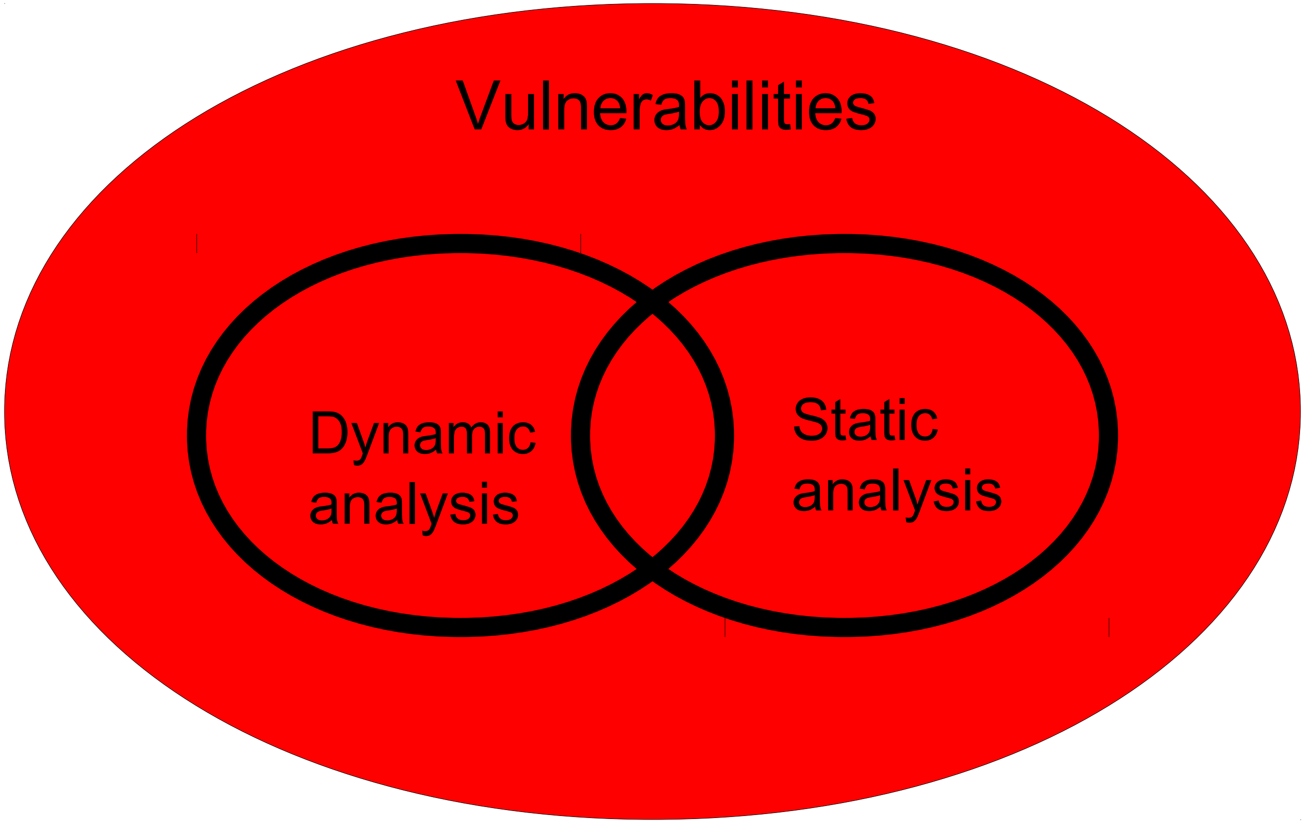
Tools: commercial

http://en.wikipedia.org/wiki/List_of_tools_for_static_code_analysis

- **Rational Appscan**
  - Web based apps
  - JavaScript Static Analyzer (JSA) - 8.0
  - DOM based XSS
- **Rational AppScan Source**
  - ex. Ounce Labs
  - Web and GUI
  - Halfautomatic tool
  - Java, C/C++, PHP, ...

- Burp
- Fortify (HP)
- Veracode
- Justcode
- Coverity
- Parasoft
- ...

Coverage



All in scope? Physical, infrastructure, ...

Nekoliko preporuka

- Ako vodite programere
  - Uključiti sigurnost u kompletan proces razvoja
    - Dizajn!
  - Uključite testiranje u kompletan proces razvoja
- Ako ste programer
  - Filtriraj
    - Svaki izlaz iz aplikacije
  - Ne vjeruj korisničkom unosu i radi provjeru
    - Svakog ulaznog podatka u aplikaciju
  - Razmišljaj kao napadač
- Ako ste naručitelj posla
  - Uključite odgovornost za sigurnost u ugovor
    - Odgovornost je naručitelja ili izvođača?
  - Pitajte za implementirane sigurnosne zaštite
    - I Tražite ih!
    - Prihvatljiva zaštita
  - Razvijte nefunkcionalne zahtjeve za aplikaciju
    - Naravno, prvo funkcionalne ;)
- Testirajte aplikaciju
  - Različiti oblici testiranja
    - Penetracijski testovi, Pregled izvornog koda, ...
    - ...

OWASP Croatia

- OWASP
  - http://www.owasp.org
- OWASP Croatia
  - https://www.owasp.org/index.php/Croatia
  - Translated Contracting part on Croatian

JOIN US! :)

Lecture number: 309

Q(&)A

@s_bergmann:
Take me down to the paradise city where the code is clean and the tests are pretty.

vlatko.kosturjak@hr.ibm.com
http://twitter.com/k0st