Software Security Testing

The Next Frontier

Scott Matsumoto
Principal Consultant
smatsumoto@cigital.com

cigital
Software Confidence. Achieved.

www.cigital.com
info@cigital.com
+1.703.404.9293

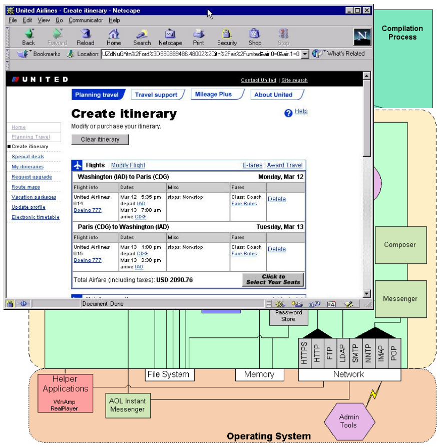
About Cigital

- A leading consulting firm specializing in helping organizations improve their software security and software quality posture
- Recognized experts in “Building Security In”
- Extensive Industry Standards, Best Practices, and Regulatory Compliance Experience

Software Security Is A Challenge

The Trinity of Trouble

- **Connectivity**
  - The Internet is everywhere and most software is on it
- **Complexity**
  - Networked, distributed, mobile code is hard
- **Extensibility**
  - Systems evolve in unexpected ways and are changed on the fly



United Airlines - Create itinerary - Netscape

UNITED

Create itinerary

Modify or purchase your itinerary.

Flights Modify Flight E-fares | Award Travel

Washington (IAD) to Paris (CDG) Monday, Mar 12

Flight info	Dates	Misc	Fares	
United Airlines 914 Boeing 777	Mar 12 5:35 pm depart IAD Mar 13 7:00 am arrive CDG	stops: Non-stop	Class: Coach Fare Rules	Delete

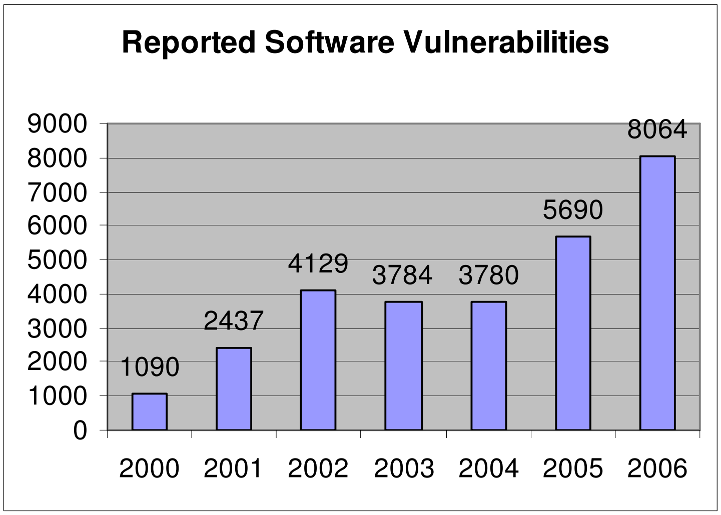
Paris (CDG) to Washington (IAD) Tuesday, Mar 13

Flight info	Dates	Misc	Fares	
United Airlines 915 Boeing 777	Mar 13 1:00 pm depart CDG Mar 13 3:30 pm arrive IAD	stops: Non-stop	Class: Coach Fare Rules	Delete

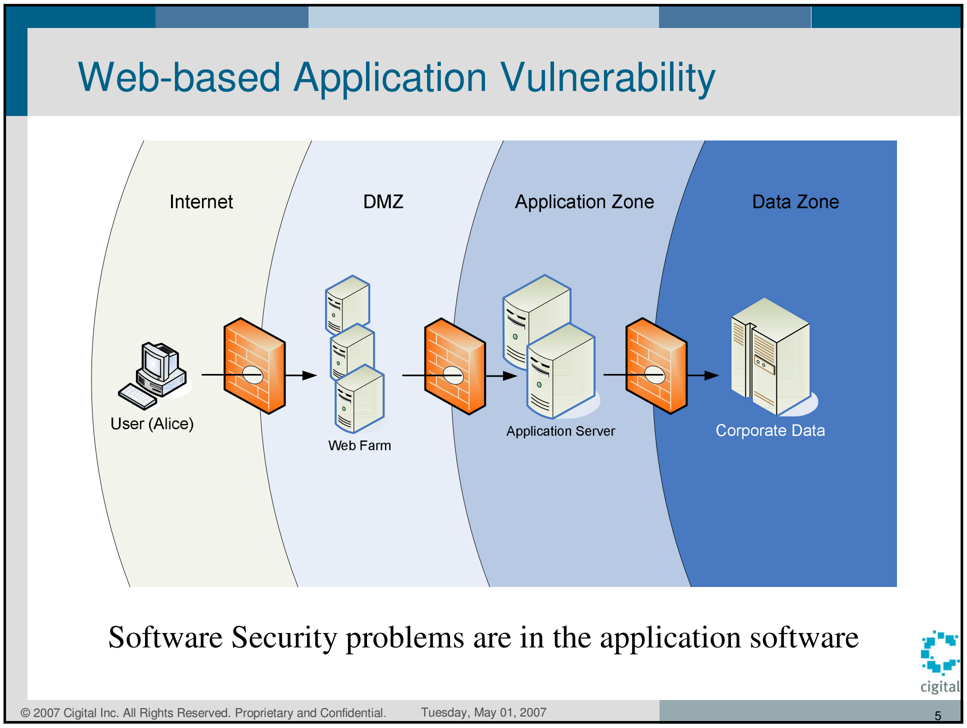
Total Airfare (including taxes): USD 2090.76

Document: Done

Software Vulnerability Growth

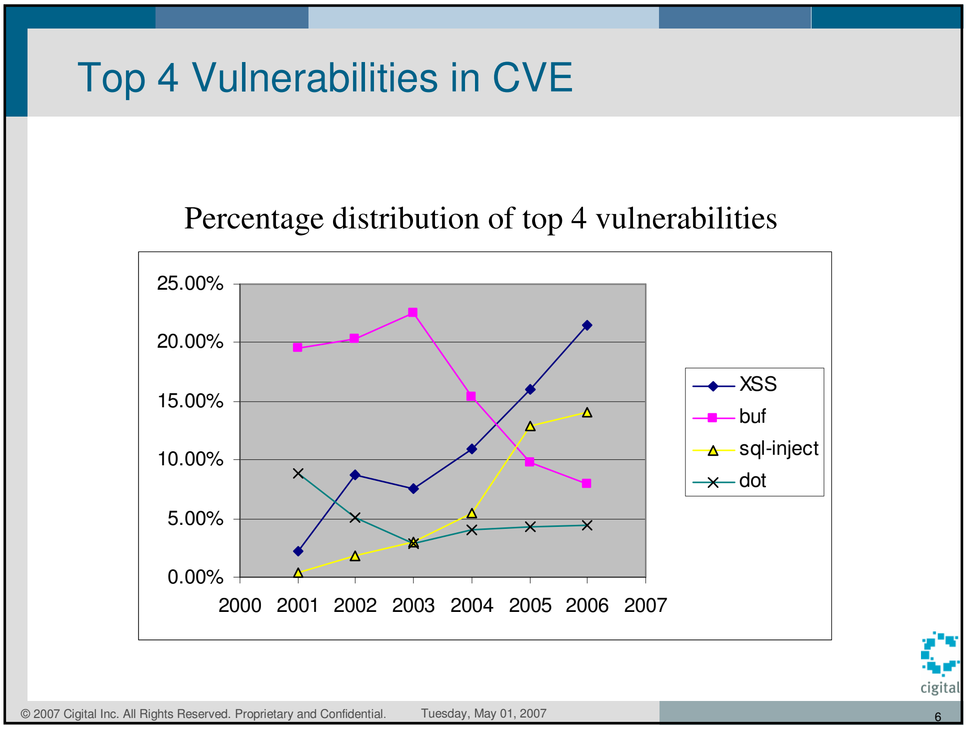


Source: CERT



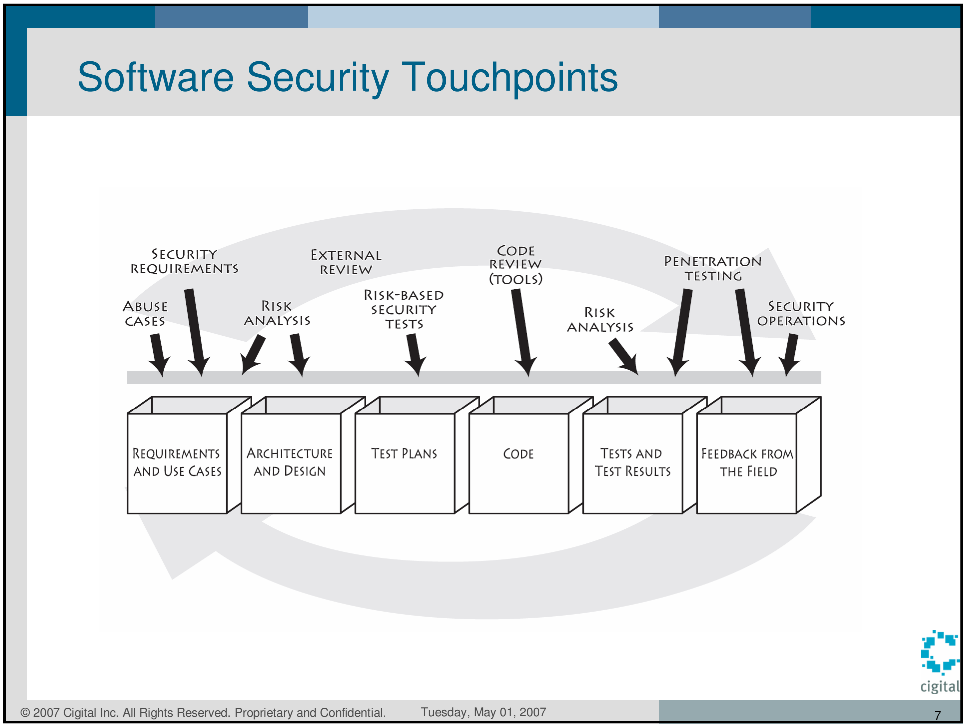
Web-based Application Vulnerability

Software Security problems are in the application software



Top 4 Vulnerabilities in CVE

Percentage distribution of top 4 vulnerabilities



Software Security Touchpoints

Security Requirements

Abuse Cases

External Review

Risk Analysis

Risk-Based Security Tests

Code Review (Tools)

Risk Analysis

Penetration Testing

Security Operations

Requirements and Use Cases

Architecture and Design

Test Plans

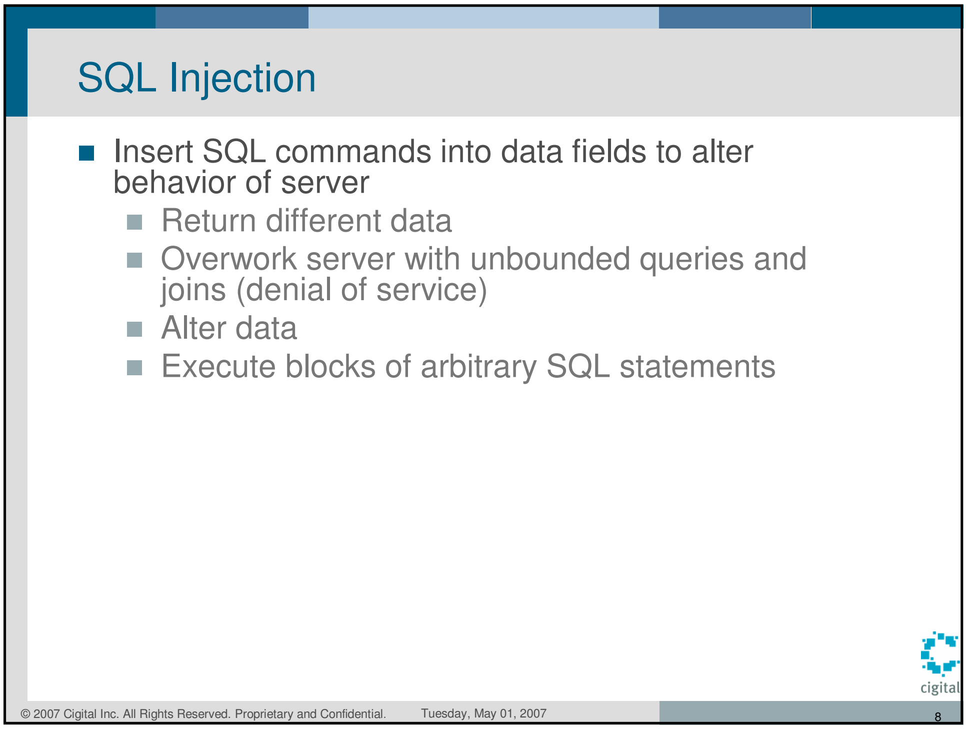
Code

Tests and Test Results

Feedback from the Field

cigital

Tuesday, May 01, 2007



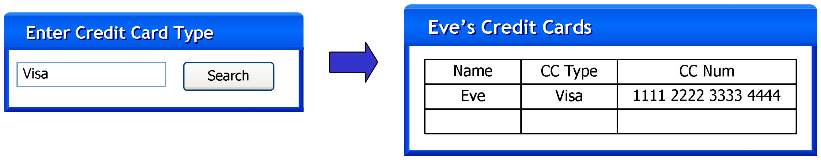
SQL Injection

- Insert SQL commands into data fields to alter behavior of server
  - Return different data
  - Overwork server with unbounded queries and joins (denial of service)
  - Alter data
  - Execute blocks of arbitrary SQL statements

cigital

Tuesday, May 01, 2007

Example SQL Injection Vulnerability



Enter Credit Card Type

Visa

Eve’s Credit Cards

Name	CC Type	CC Num
Eve	Visa	1111 2222 3333 4444

- Compose a dynamic query based on user input:

```
SELECT cc_type, cc_num FROM cc_data
  WHERE id=‘%s’ AND cc_type=‘%s’
```

- Normal **cc_type** = ‘Visa’:

```
SELECT cc_type, cc_num FROM cc_data
  WHERE id=‘123456789’
  AND cc_type=‘Visa’
```

cigital

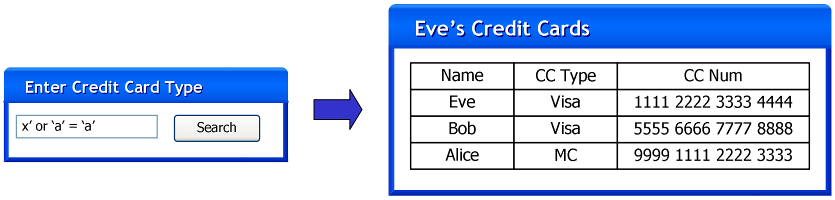
JRM2

SQL Injection

- Insert SQL commands into data fields to alter behavior of application
- Example: Enter x’ OR ‘a’=‘a instead of “Visa” to produce

```
SELECT cc_type, cc_num FROM cc_data
  WHERE id=‘123456789’ AND
  cc_type =‘x’ OR ‘a’ = ‘a’
```

- Results in all credit card data being returned



Enter Credit Card Type

x’ or ‘a’ = ‘a’

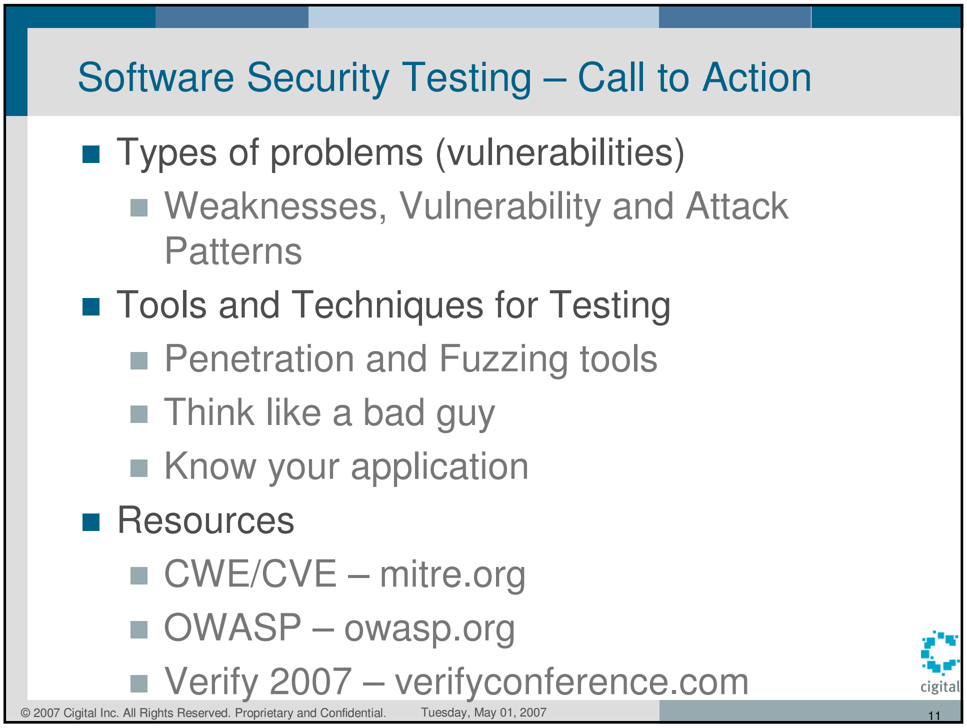
Eve’s Credit Cards

Name	CC Type	CC Num
Eve	Visa	1111 2222 3333 4444
Bob	Visa	5555 6666 7777 8888
Alice	MC	9999 1111 2222 3333

cigital

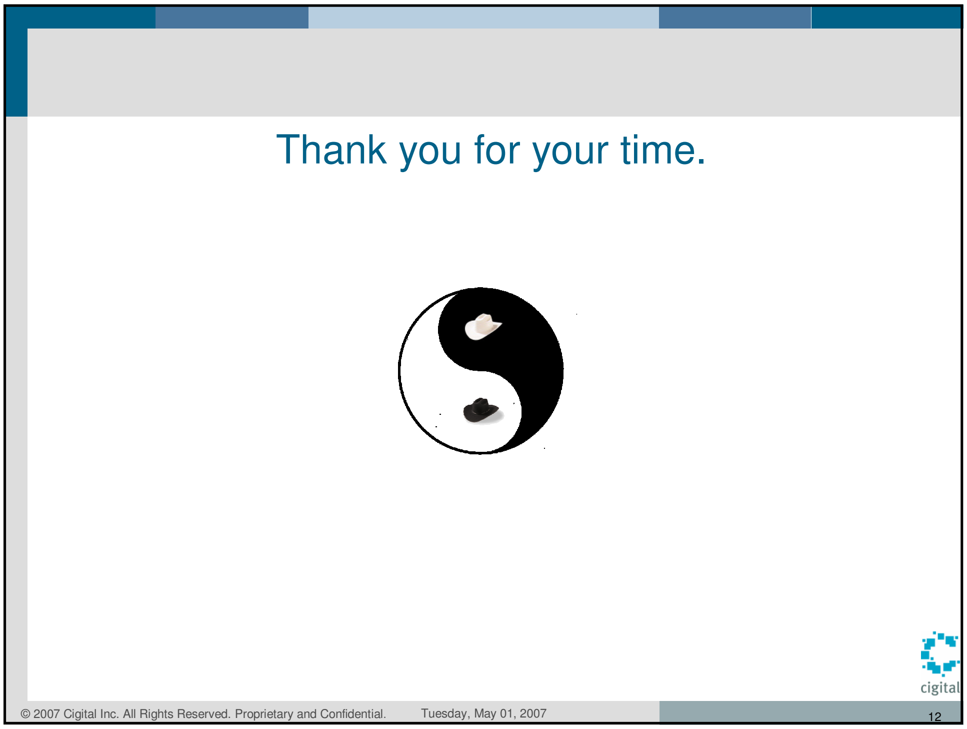
Slide 10

JRM2 Brook: Explain why this is important to morgan.
rmills, 11/6/2006



Software Security Testing – Call to Action

- Types of problems (vulnerabilities)
  - Weaknesses, Vulnerability and Attack Patterns
- Tools and Techniques for Testing
  - Penetration and Fuzzing tools
  - Think like a bad guy
  - Know your application
- Resources
  - CWE/CVE – mitre.org
  - OWASP – owasp.org
  - Verify 2007 – verifyconference.com



Thank you for your time.