BlueHat v8

Real World Code Review

SDL Sessions, Day 2
October 17, 2008

Hello!

Vinnie

- Sleeps during the day.
- Comes out at night to **review code**.

Perspective

- Big companies in the **Fortune 200**.
- From code review **experience.**

Our Topic Today

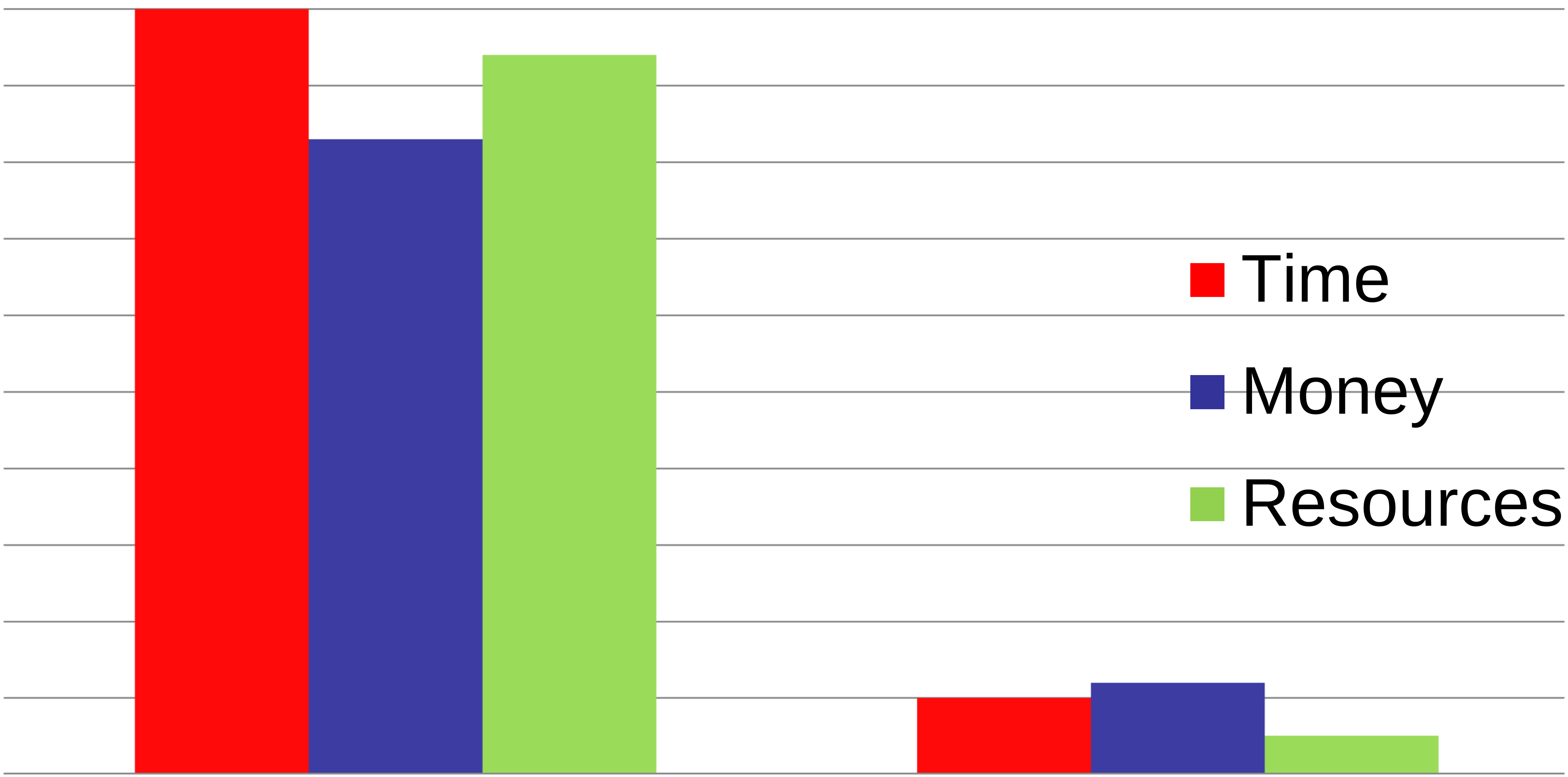
We will see…

- How to use tools **effectively** and **practically**.
- Why examining code can **fry your brain**.
- Retiring of **common misconceptions**.

We will not…

- Make up big numbers to scare you. Sell you a tool. Tell you how to live your life.

Microsoft's Fairytale…



Real World…

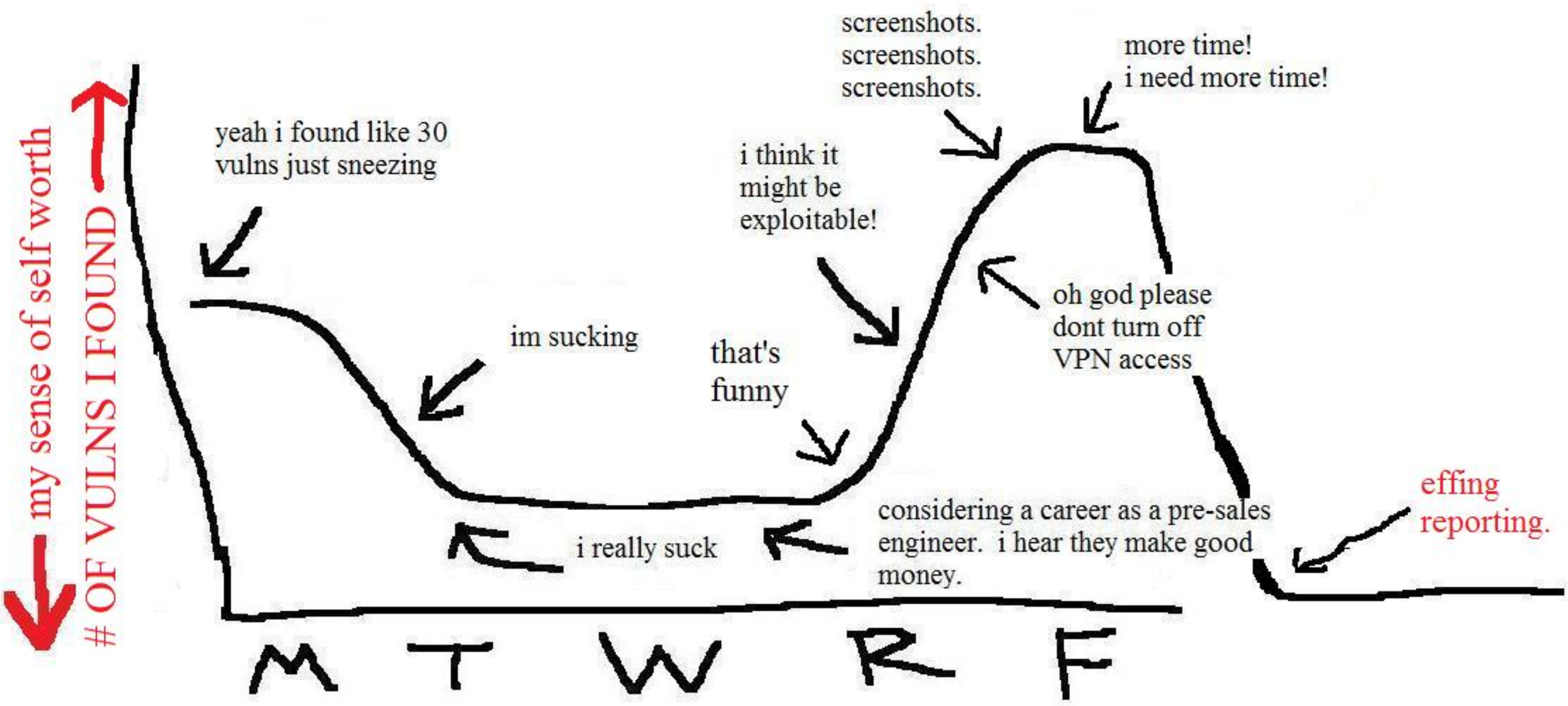
We Have…

1. Security focal
2. A couple bucks
3. (maybe a tool, maybe)

We (usually) Don't Have…

- Willing participants
- Policies, standards, guidelines, training

What is Code Review Like?


my sense of self worth
# OF VULNS I FOUND
yeah i found like 30 vulns just sneezing
im sucking
i really suck
that's funny
i think it might be exploitable!
screenshots. screenshots. screenshots.
more time! i need more time!
oh god please dont turn off VPN access
considering a career as a pre-sales engineer. i hear they make good money.
effing reporting.
M
T
W
R
F

Case Study: ACME Air

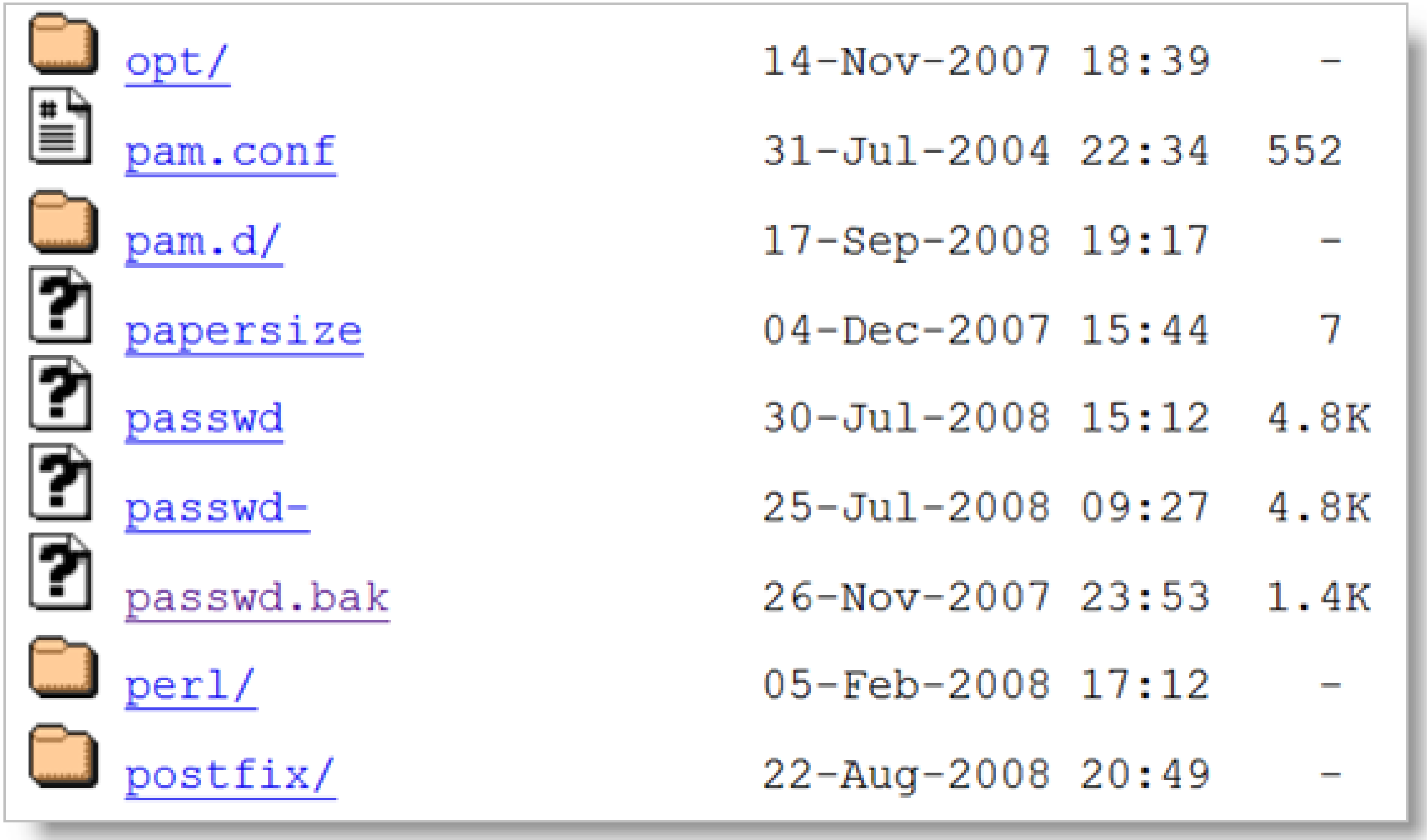
Background

- Portal with real-time communication

In-Flight Manager Application

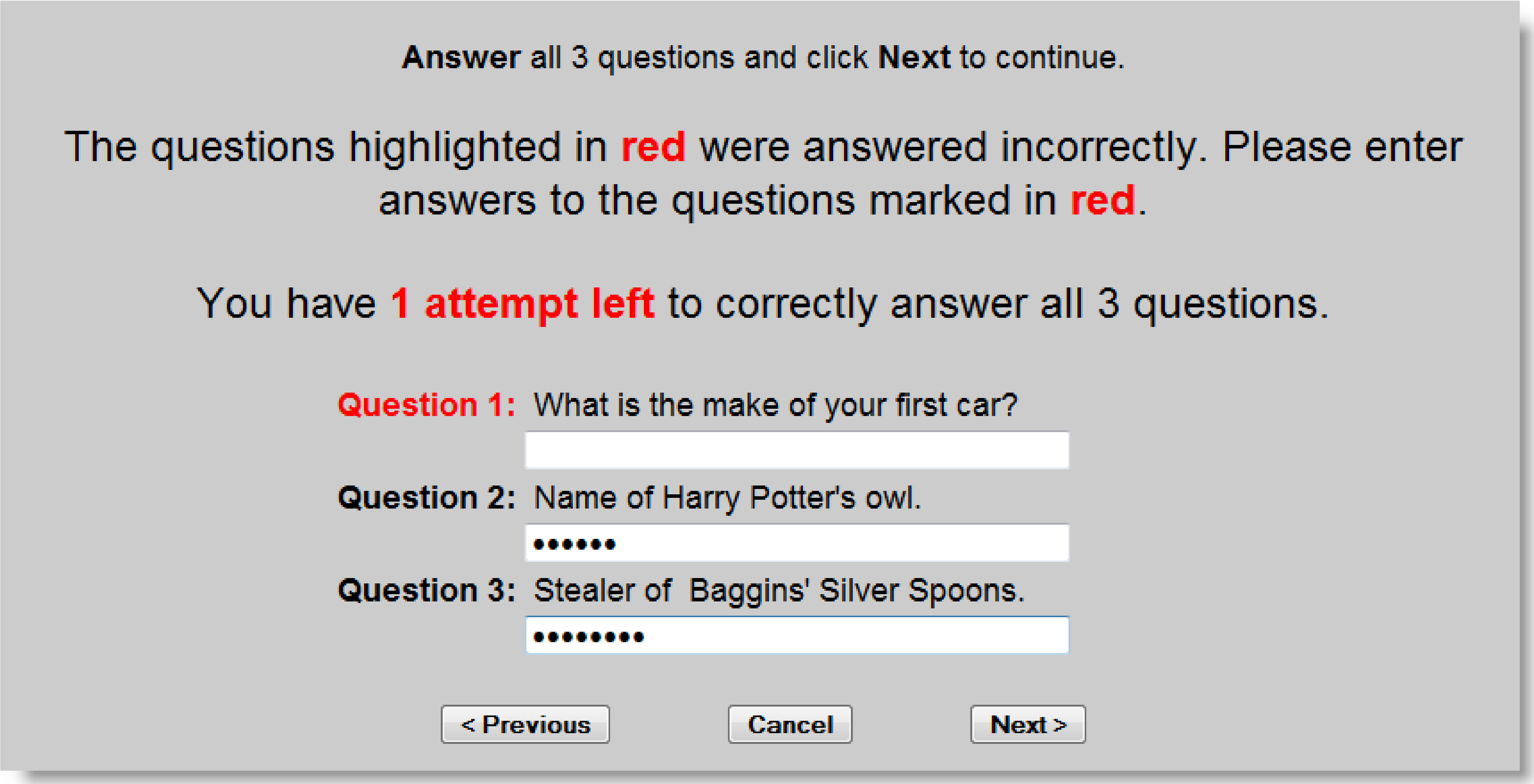
- Directory Indexing
- SQL Injection
- Security Questions

Directory Indexing



```
opt/         14-Nov-2007 18:39    -
pam.conf     31-Jul-2004 22:34  552
pam.d/       17-Sep-2008 19:17    -
papersize    04-Dec-2007 15:44    7
passwd       30-Jul-2008 15:12  4.8K
passwd-      25-Jul-2008 09:27  4.8K
passwd.bak   26-Nov-2007 23:53  1.4K
perl/        05-Feb-2008 17:12    -
postfix/     22-Aug-2008 20:49    -
```

Security Questions



Answer all 3 questions and click **Next** to continue.

The questions highlighted in **red** were answered incorrectly. Please enter answers to the questions marked in **red**.

You have **1 attempt left** to correctly answer all 3 questions.

Question 1: What is the make of your first car?

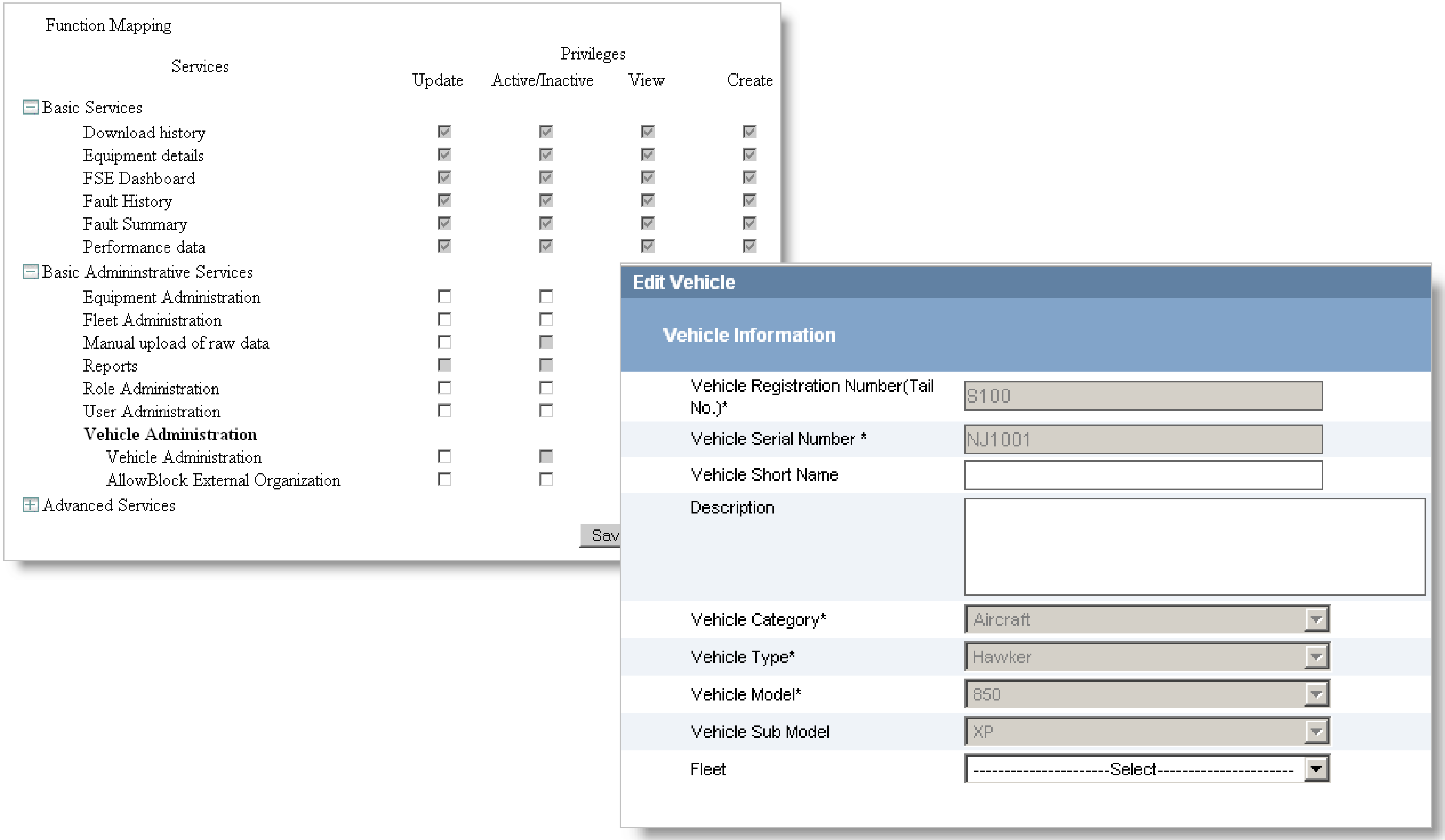
Question 2: Name of Harry Potter's owl.

●●●●●●

Question 3: Stealer of Baggins' Silver Spoons.

●●●●●●●●

SQL Injection in Workflow



Function Mapping

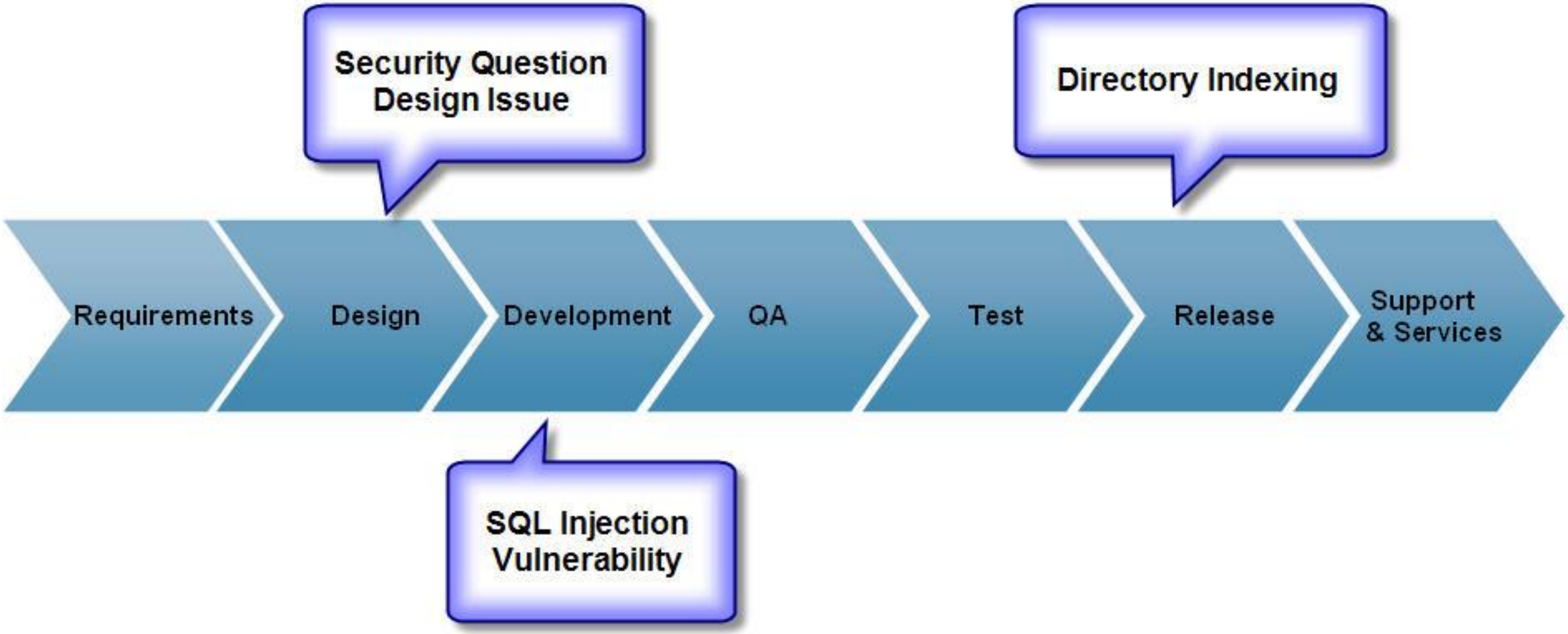
Services	Update	Active/Inactive	View	Create
⊟ Basic Services				
Download history	☑	☑	☑	☑
Equipment details	☑	☑	☑	☑
FSE Dashboard	☑	☑	☑	☑
Fault History	☑	☑	☑	☑
Fault Summary	☑	☑	☑	☑
Performance data	☑	☑	☑	☑
⊟ Basic Admininstrative Services				
Equipment Administration	☐	☐		
Fleet Administration	☐	☐		
Manual upload of raw data	☐	☐		
Reports	☐	☐		
Role Administration	☐	☐		
User Administration	☐	☐		
Vehicle Administration				
Vehicle Administration	☐	☐		
AllowBlock External Organization	☐	☐		
⊞ Advanced Services				

Edit Vehicle

Vehicle Information

Vehicle Registration Number(Tail No.)*	S100
Vehicle Serial Number *	NJ1001
Vehicle Short Name	
Description	
Vehicle Category*	Aircraft
Vehicle Type*	Hawker
Vehicle Model*	850
Vehicle Sub Model	XP
Fleet	---------------------Select---------------------

All Together


Security Question Design Issue

Directory Indexing

Requirements

Design

Development

QA

Test

Release

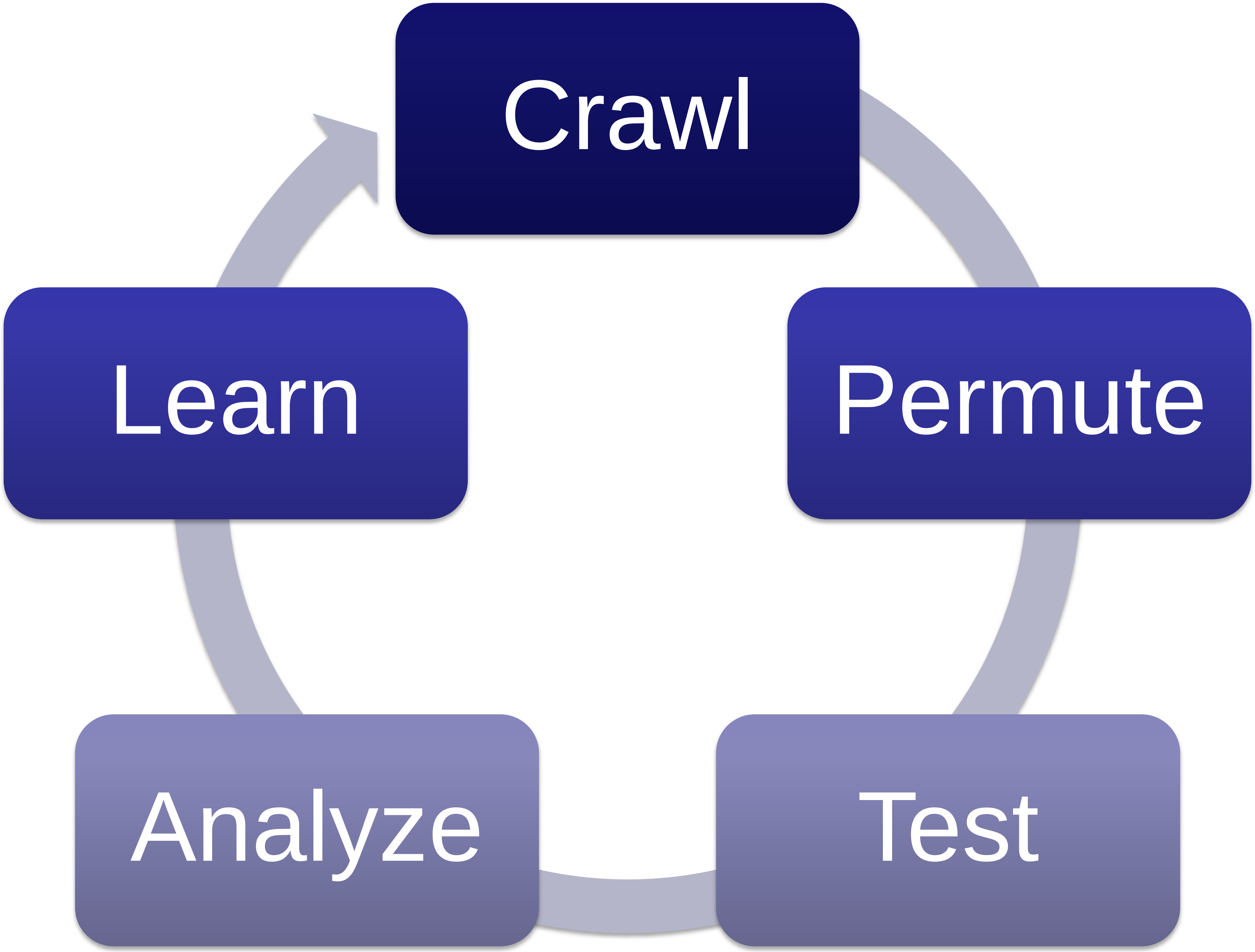
Support & Services

SQL Injection Vulnerability

STACH&LIU

Black Box Scanning

Black Box Scanning



Crawl

Permute

Test

Analyze

Learn

Black Box Scanning

Crawling Quickly

Basic Intelligent Fuzzing

Predictable Resource Locations

Brute-forcing Things

Finding Known Vulnerabilities

Directory Indexing

Identifying Entry Points in Apps

Middleware Misconfigurations

GOOD

Advanced Injection Attacks

Workflow Related Issues

Login Boxes

Single Sign-on Systems

Very Large Sites

Portals, SAP, WebSphere

AJAX Anything

JavaScript

BAD

Design Issues

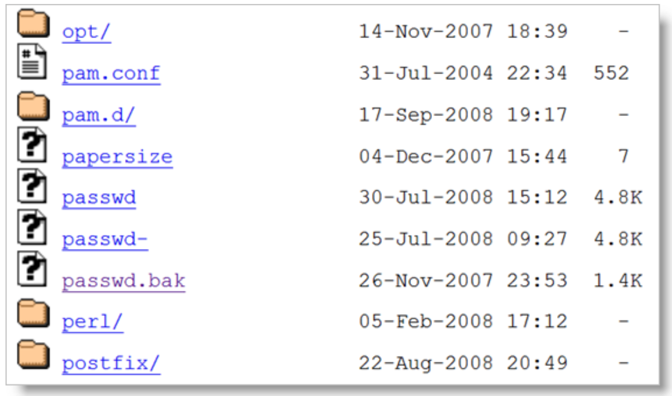
Contextually Sensitive

Attack Chaining

Anything with abnormal or delicate session management

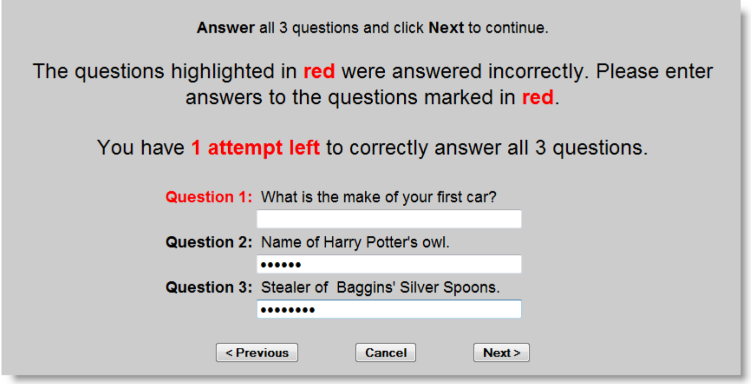
FAILWHALE

Black Box Scanning Results



```
opt/                 14-Nov-2007 18:39    -
pam.conf             31-Jul-2004 22:34  552
pam.d/               17-Sep-2008 19:17    -
papersize            04-Dec-2007 15:44    7
passwd               30-Jul-2008 15:12  4.8K
passwd-              25-Jul-2008 09:27  4.8K
passwd.bak           26-Nov-2007 23:53  1.4K
perl/                05-Feb-2008 17:12    -
postfix/             22-Aug-2008 20:49    -
```

✓



Answer all 3 questions and click **Next** to continue.

The questions highlighted in **red** were answered incorrectly. Please enter answers to the questions marked in **red**.

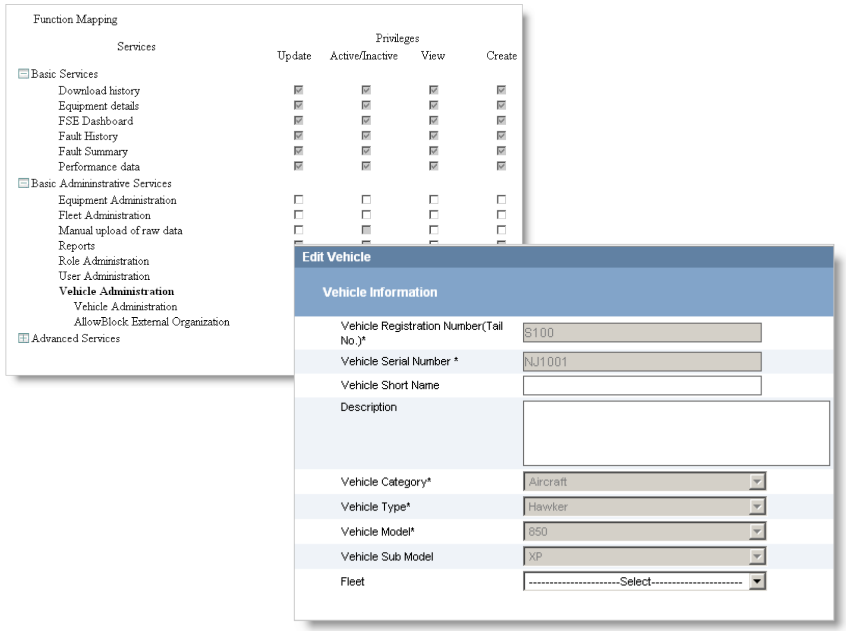
You have **1 attempt left** to correctly answer all 3 questions.

Question 1: What is the make of your first car?

Question 2: Name of Harry Potter's owl.
••••••

Question 3: Stealer of Baggins' Silver Spoons.
••••••••

🚫



Function Mapping

Services	Privileges Update	 Active/Inactive	 View	 Create
⊟ Basic Services				
Download history	☑	☑	☑	☑
Equipment details	☑	☑	☑	☑
FSE Dashboard	☑	☑	☑	☑
Fault History	☑	☑	☑	☑
Fault Summary	☑	☑	☑	☑
Performance data	☑	☑	☑	☑
⊟ Basic Admininstrative Services				
Equipment Administration	☐	☐	☐	☐
Fleet Administration	☐	☐	☐	☐
Manual upload of raw data	☐	☐	☐	☐
Reports				
Role Administration				
User Administration				
Vehicle Administration				
Vehicle Administration				
AllowBlock External Organization				
⊞ Advanced Services				

Edit Vehicle

Vehicle Information

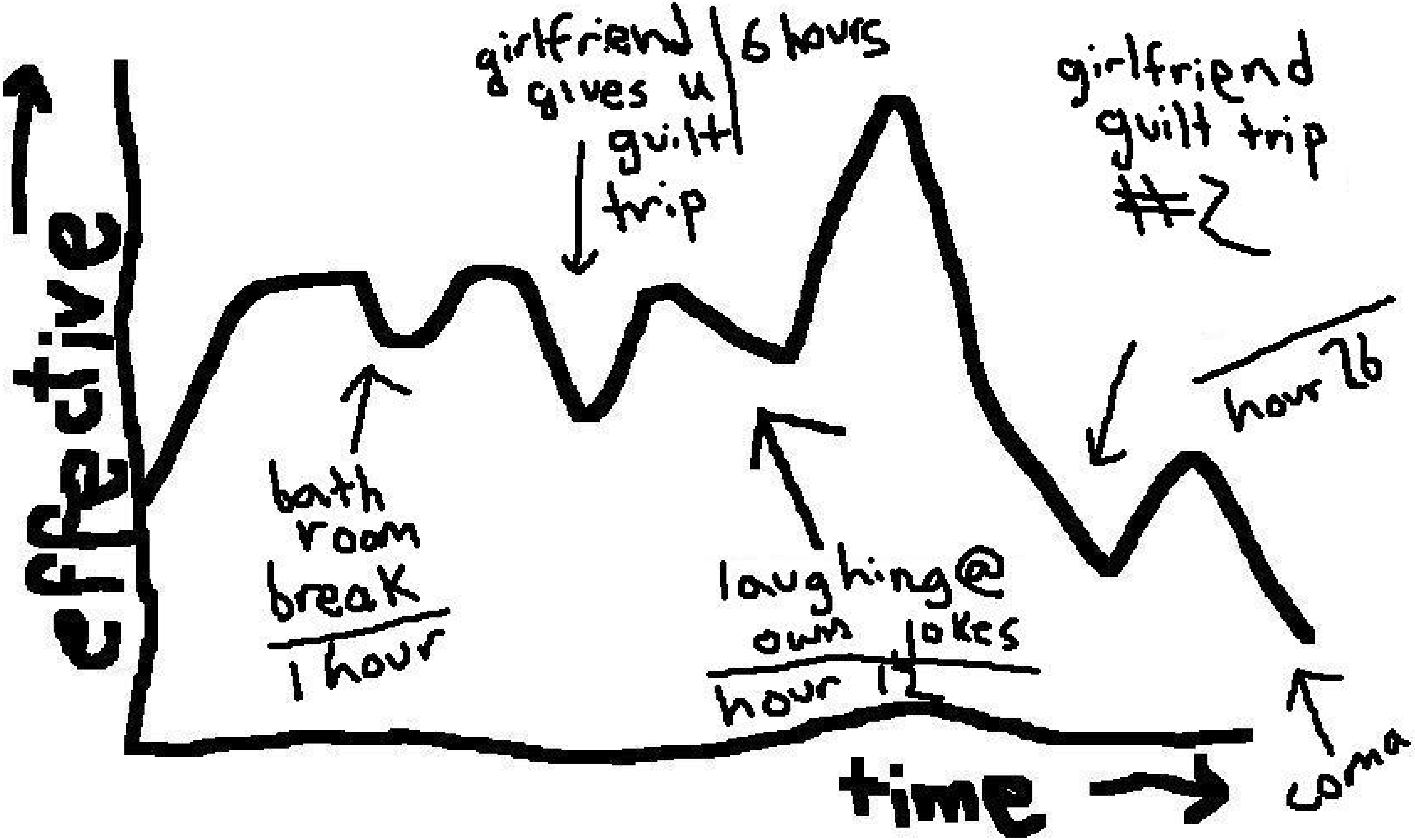
Vehicle Registration Number(Tail No.)*	S100
Vehicle Serial Number *	NJ1001
Vehicle Short Name	
Description	
Vehicle Category*	Aircraft
Vehicle Type*	Hawker
Vehicle Model*	850
Vehicle Sub Model	XP
Fleet	--------------------Select--------------------

🚫

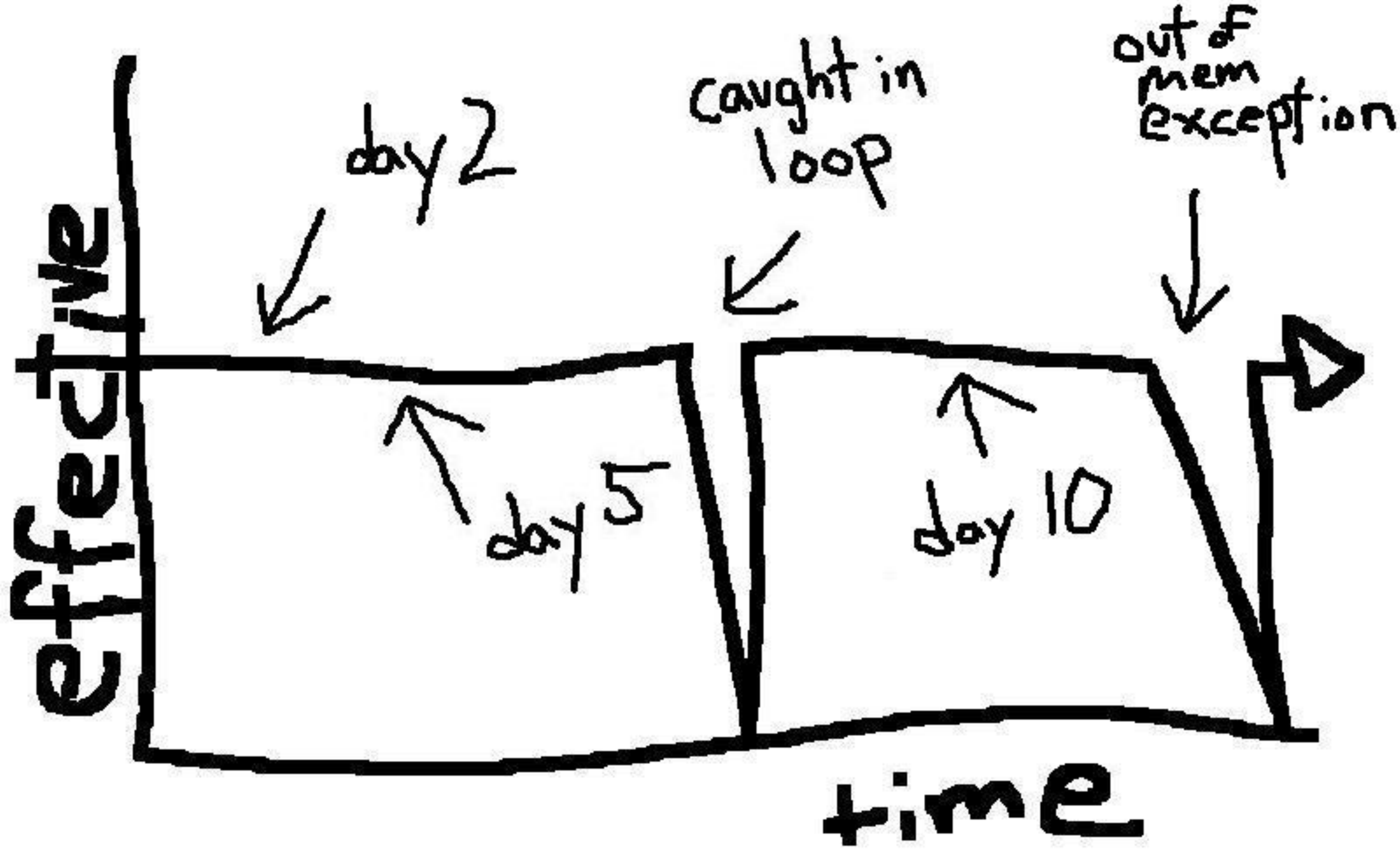
Reality Bites

“I find like 4x more bugs than scanners. Buy me not the tool. I am the Michael Jordan of code review.”

Human Productivity

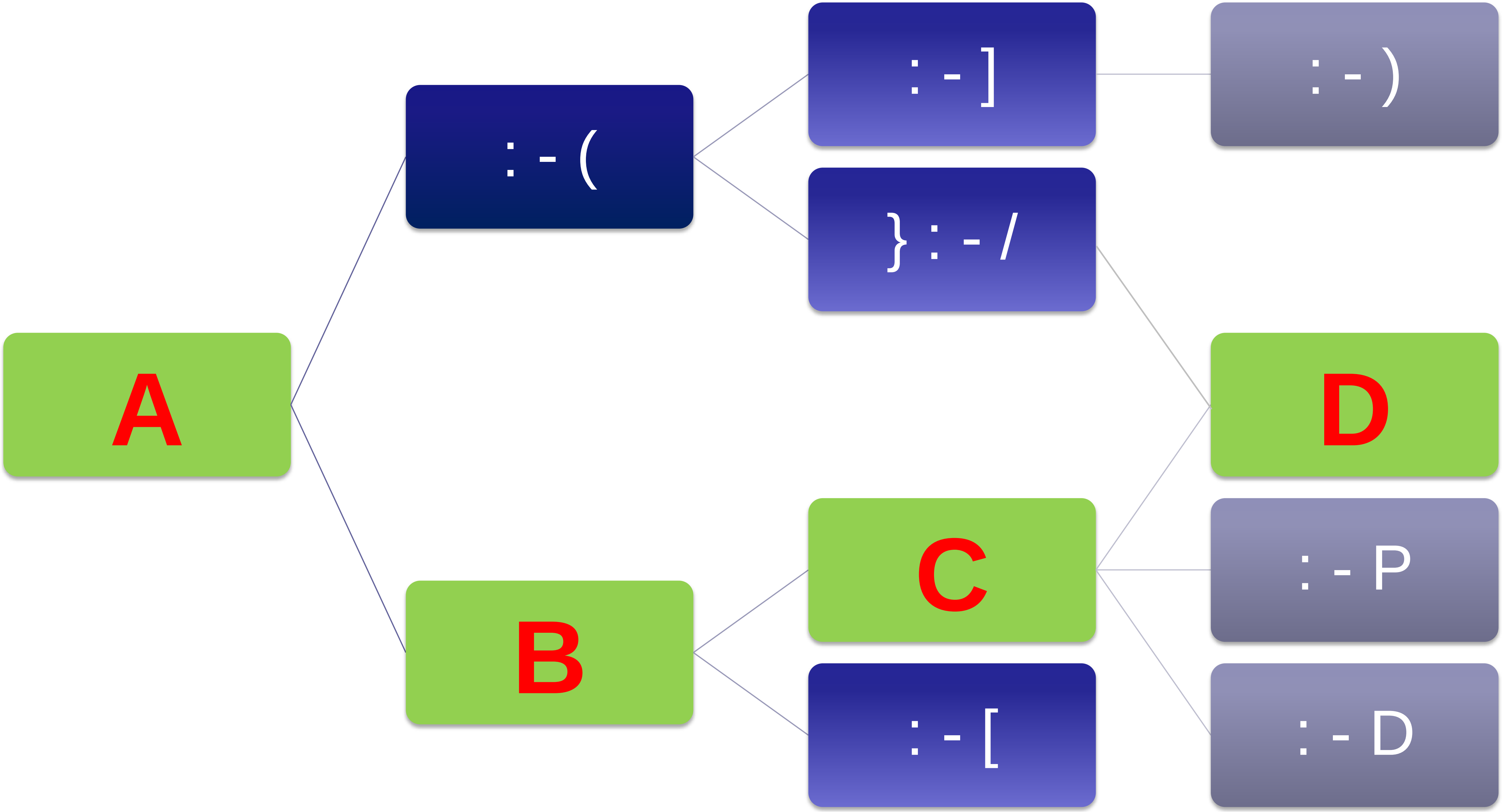

effective
girlfriend gives u guilt trip
6 hours
girlfriend guilt trip #2
hour 26
bath room break
1 hour
laughing@ own jokes
hour 12
time
coma

Scanner Productivity

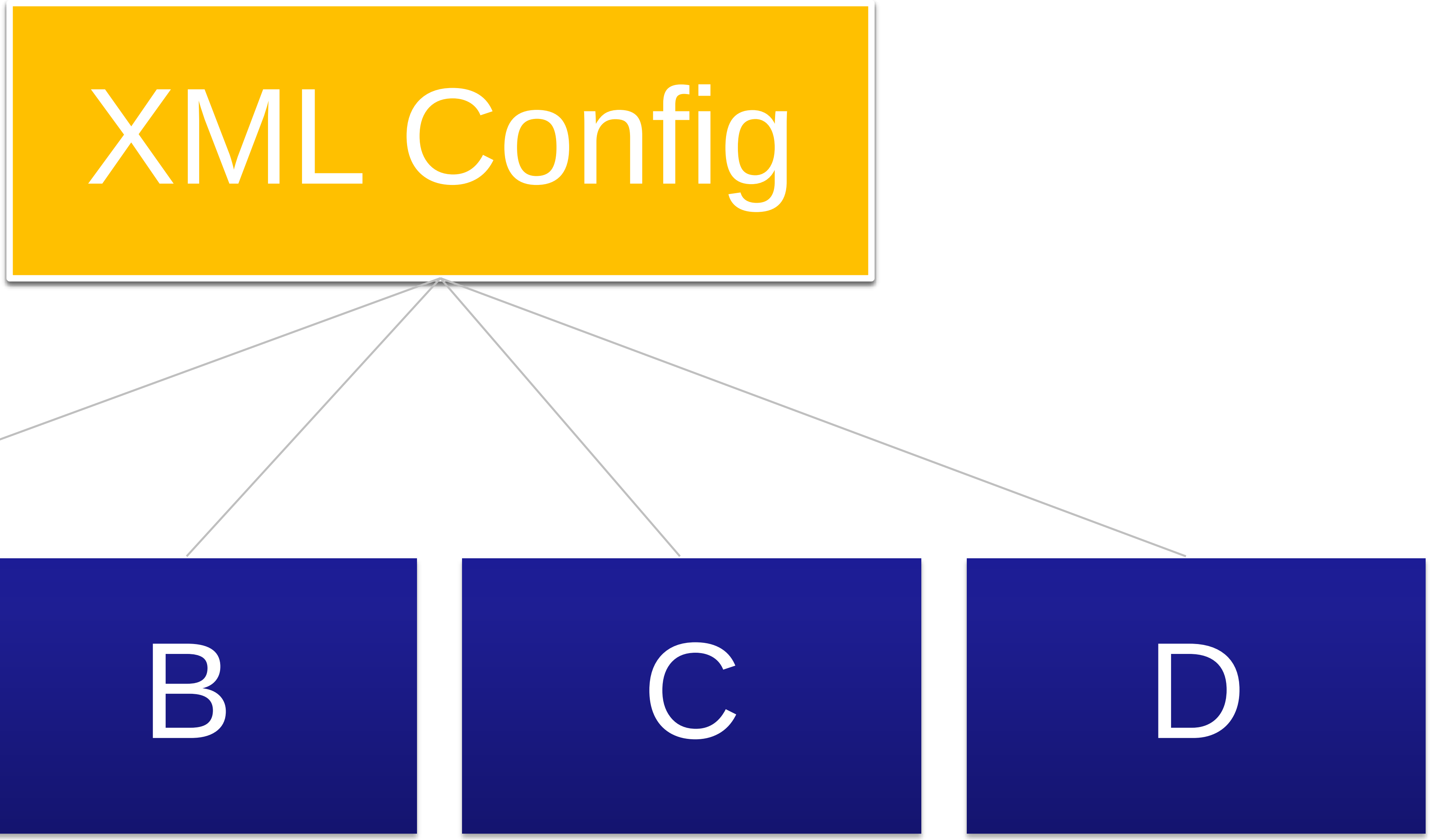


Static Code Analysis

Static Analysis Tools



Framework Failure



XML Config

A

B

C

D

Data Flow Failure

```
                 ②                              ①
String sTreat = request.getParameter(“TREAT”);

if (!sTreat.equals(“snickerDoodle”)) {
    return;
}
              ④
String sQuery = “SELECT * FROM tastySnacks
                   WHERE treat = ‘” + \ sTreat + “’”;
                                          ③
executeQuery(sQuery);
                   ⑤
```

Static Analysis Tools

Basic Data Flow Analysis, e.g. SQLi, XSS, Log Forging

Workflow Related Issues, e.g. finding all data paths

Login Boxes

Improper API Usage

Identifying Entry Points in Code

Very Large Code Bases

Programming Bugs

GOOD

Very Large Code Bases

Single Sign-on Systems

Finding Known Vulnerabilities

Middleware Misconfiguration

Identifying Proper Filtering

Reporting

BAD

Design Issues

Frameworks, e.g. Spring

Contextually Sensitive

Control Flow

Predictable Resource Locations

Brute-forcing Things

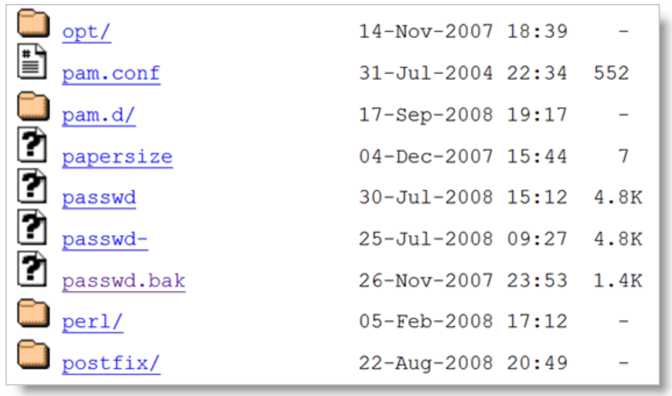
Attack Chaining

3rd Party Libraries

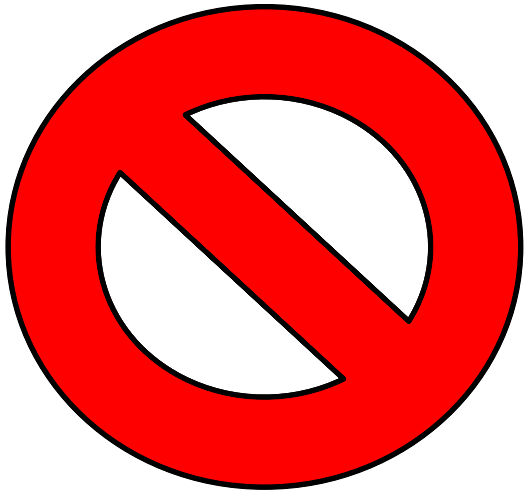
Wrapped Functions

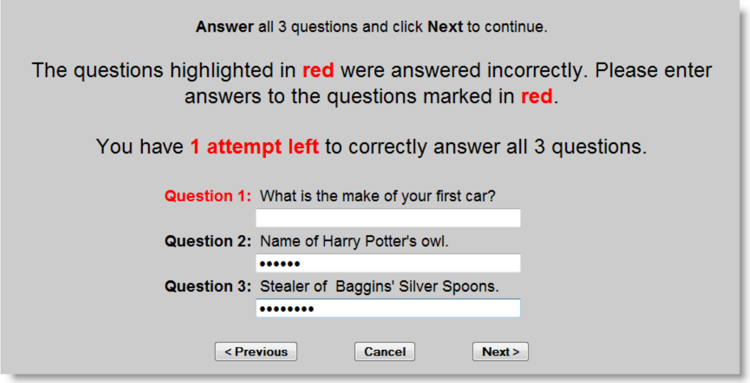
FAILWHALE

Static Analysis Results



```
opt/          14-Nov-2007 18:39    -
pam.conf      31-Jul-2004 22:34  552
pam.d/        17-Sep-2008 19:17    -
papersize     04-Dec-2007 15:44    7
passwd        30-Jul-2008 15:12  4.8K
passwd-       25-Jul-2008 09:27  4.8K
passwd.bak    26-Nov-2007 23:53  1.4K
perl/         05-Feb-2008 17:12    -
postfix/      22-Aug-2008 20:49    -
```





Answer all 3 questions and click **Next** to continue.

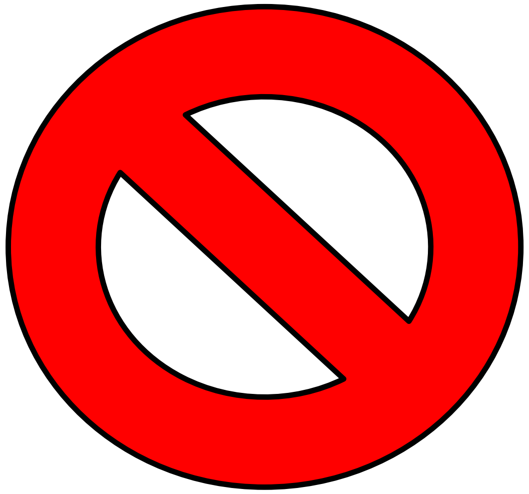
The questions highlighted in **red** were answered incorrectly. Please enter answers to the questions marked in **red**.

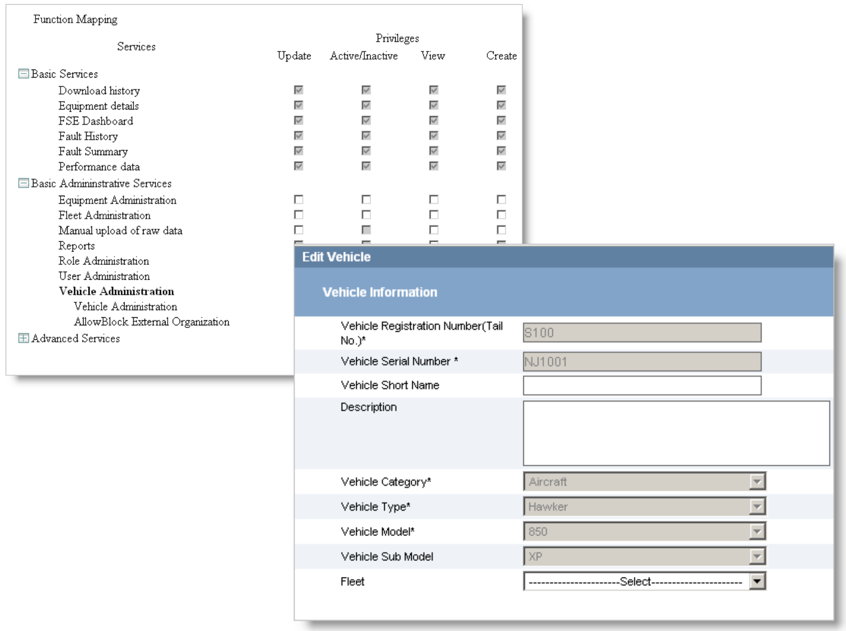
You have **1 attempt left** to correctly answer all 3 questions.

Question 1: What is the make of your first car?

Question 2: Name of Harry Potter's owl.
••••••

Question 3: Stealer of Baggins' Silver Spoons.
••••••••





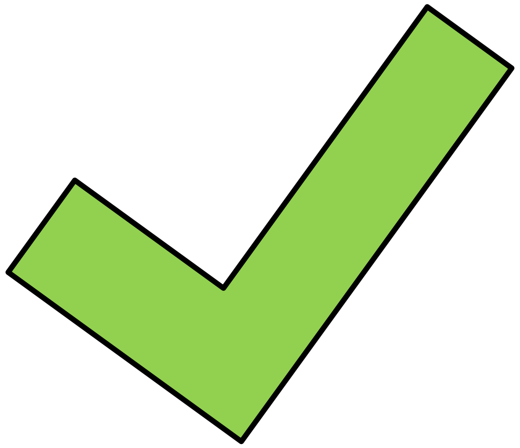
Function Mapping

Services	Privileges Update	Active/Inactive	View	Create
⊟ Basic Services				
Download history	☑	☑	☑	☑
Equipment details	☑	☑	☑	☑
FSE Dashboard	☑	☑	☑	☑
Fault History	☑	☑	☑	☑
Fault Summary	☑	☑	☑	☑
Performance data	☑	☑	☑	☑
⊟ Basic Admininstrative Services				
Equipment Administration	☐	☐	☐	☐
Fleet Administration	☐	☐	☐	☐
Manual upload of raw data	☐	☐	☐	☐
Reports				
Role Administration				
User Administration				
Vehicle Administration				
Vehicle Administration				
AllowBlock External Organization				
⊞ Advanced Services				

Edit Vehicle

Vehicle Information

Vehicle Registration Number(Tail No.)*	S100
Vehicle Serial Number *	NJ1001
Vehicle Short Name	
Description	
Vehicle Category*	Aircraft
Vehicle Type*	Hawker
Vehicle Model*	850
Vehicle Sub Model	XP
Fleet	---------------------Select---------------------



Another One Bites the Dust!

Expert Analysis

Expert Analysis

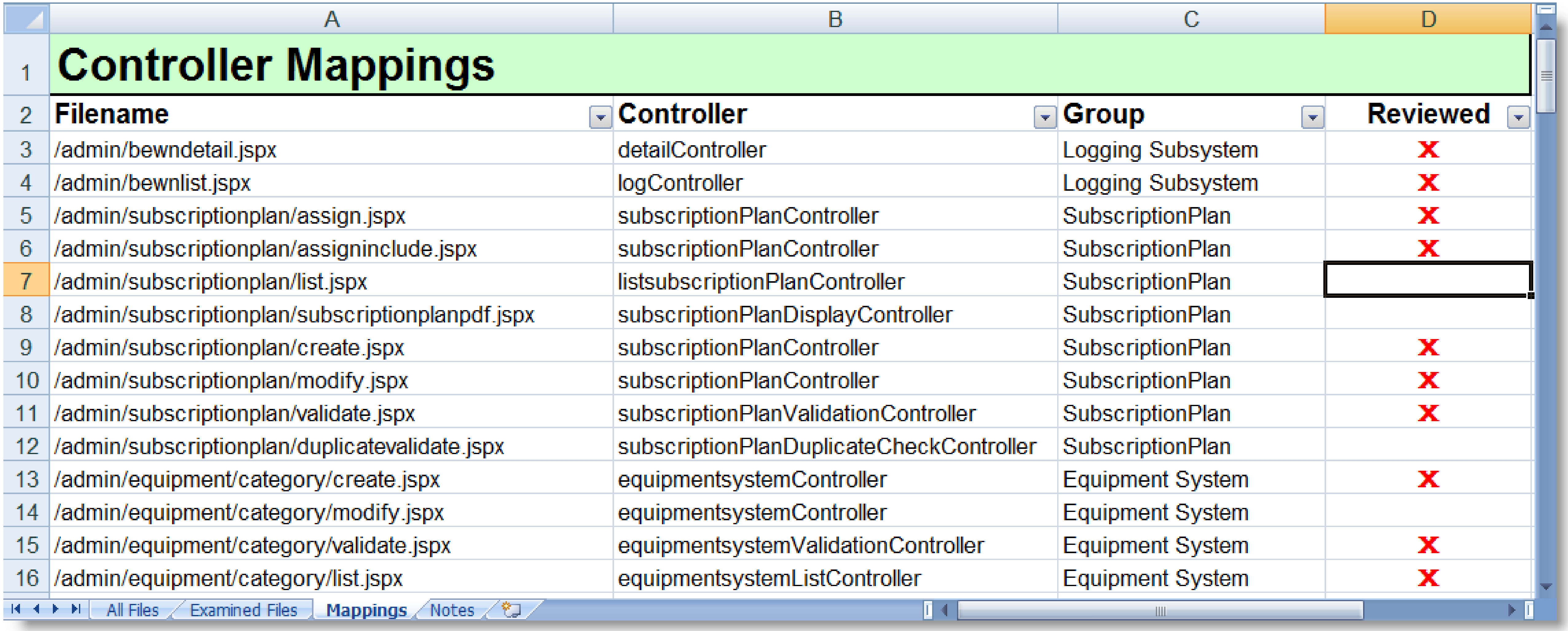
How does one review?

- Have brain, will work for food.
- Synthesis + Context

What’s the process?

- File by File
- Data Flow
- Control Flow

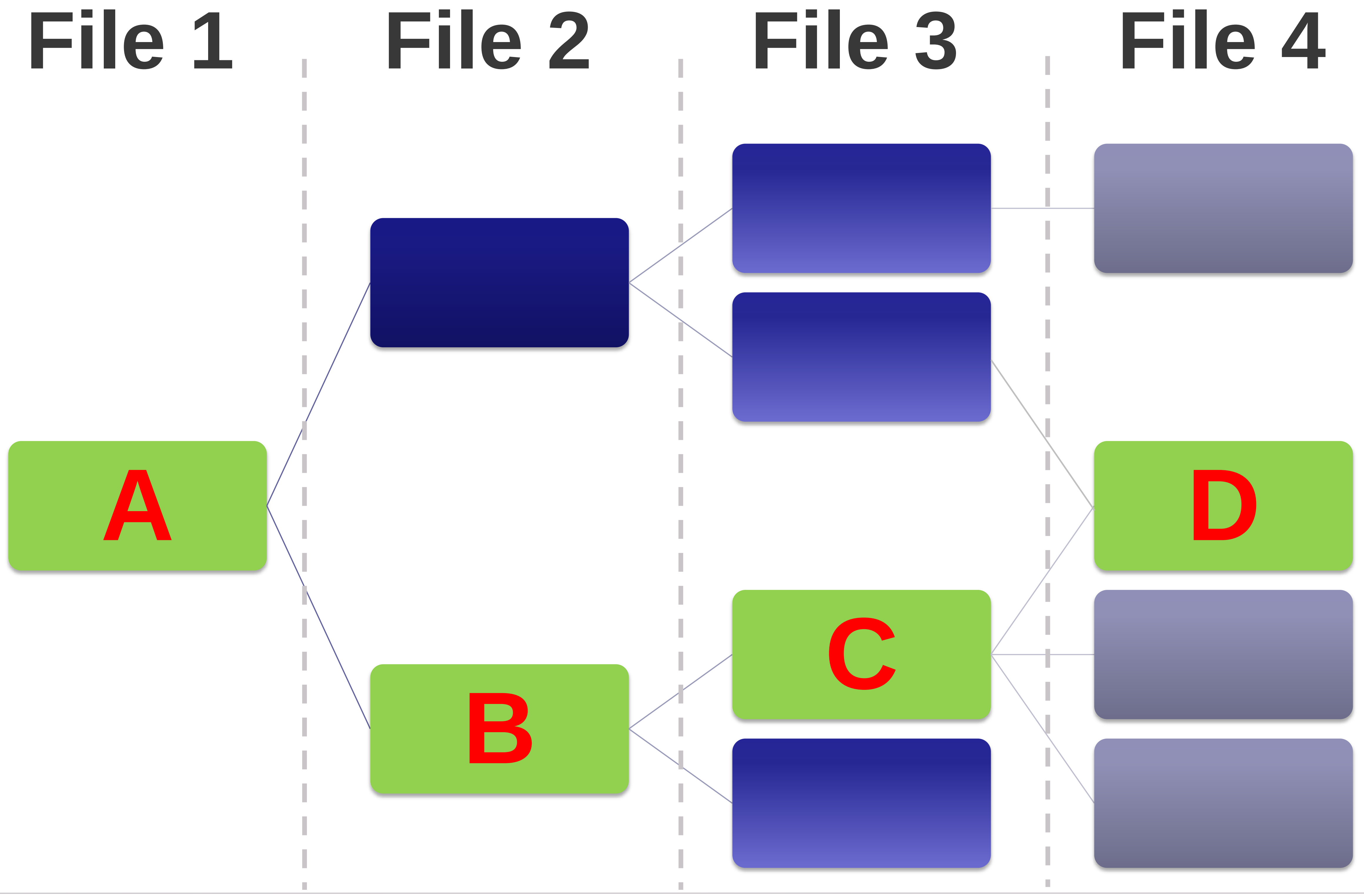
File by File Technique



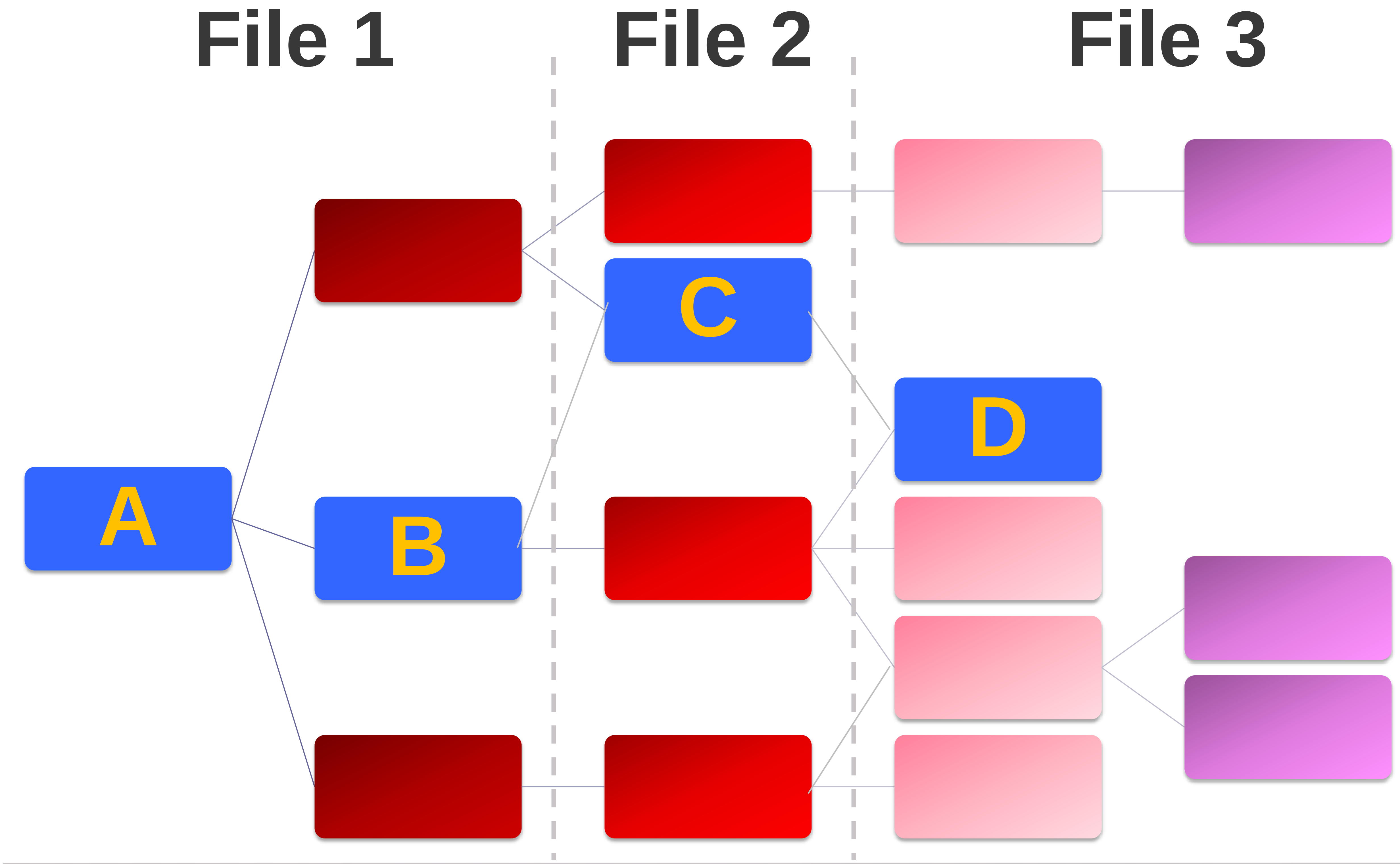
Controller Mappings

	Filename	Controller	Group	Reviewed
3	/admin/bewndetail.jspx	detailController	Logging Subsystem	X
4	/admin/bewnlist.jspx	logController	Logging Subsystem	X
5	/admin/subscriptionplan/assign.jspx	subscriptionPlanController	SubscriptionPlan	X
6	/admin/subscriptionplan/assigninclude.jspx	subscriptionPlanController	SubscriptionPlan	X
7	/admin/subscriptionplan/list.jspx	listsubscriptionPlanController	SubscriptionPlan	
8	/admin/subscriptionplan/subscriptionplanpdf.jspx	subscriptionPlanDisplayController	SubscriptionPlan	
9	/admin/subscriptionplan/create.jspx	subscriptionPlanController	SubscriptionPlan	X
10	/admin/subscriptionplan/modify.jspx	subscriptionPlanController	SubscriptionPlan	X
11	/admin/subscriptionplan/validate.jspx	subscriptionPlanValidationController	SubscriptionPlan	X
12	/admin/subscriptionplan/duplicatevalidate.jspx	subscriptionPlanDuplicateCheckController	SubscriptionPlan	
13	/admin/equipment/category/create.jspx	equipmentsystemController	Equipment System	X
14	/admin/equipment/category/modify.jspx	equipmentsystemController	Equipment System	
15	/admin/equipment/category/validate.jspx	equipmentsystemValidationController	Equipment System	X
16	/admin/equipment/category/list.jspx	equipmentsystemListController	Equipment System	X

Data Flow Review


File 1
File 2
File 3
File 4
A
B
C
D

Control Flow Review


File 1
File 2
File 3
A
B
C
D

Hybrid Approach

1. Track with the File by File
2. File by File for Non-compiled Files
3. Scan with Black Box
4. Use Static Analysis Tools
5. Validate the Static Analysis Tools
6. Perform a Manual Review of Data Flow + Control Flow + App Design

Expert Analysis

STACH&LIU

- **Design Issues**
- **Frameworks, e.g. Spring**
- **Contextually Sensitive**
- **Control Flow**
- **Advanced Injection Attacks**
- Identifying Entry Points, Weak Spots
- Third-Party Libraries
- Identifying Proper Filtering
- Reporting

GOOD

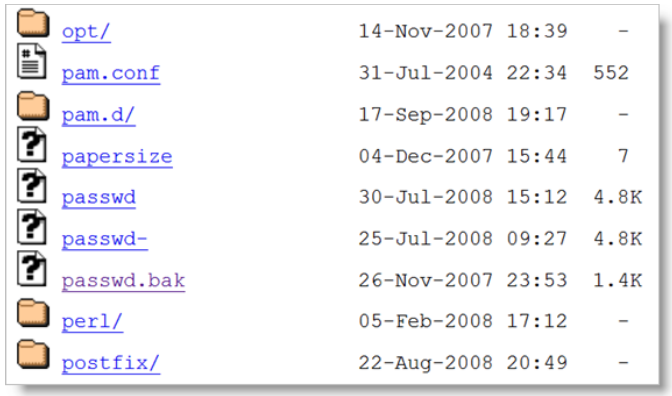
- Basic Data Flow Analysis, e.g. SQLi, XSS, Log Forging
- Workflow Related Issues, e.g. finding all data paths
- Login Boxes
- Portals, SAP, URL obfuscation
- Workflow Related Issues
- Single Sign-on Systems
- Directory Indexing

BAD

- Cost Cost Cost
- Time & Speed
- Predictable Resource Locations
- Very Large Code Bases
- Finding Known Vulnerabilities
- Middleware Misconfiguration
- Improper API Usage
- Brute-forcing Things

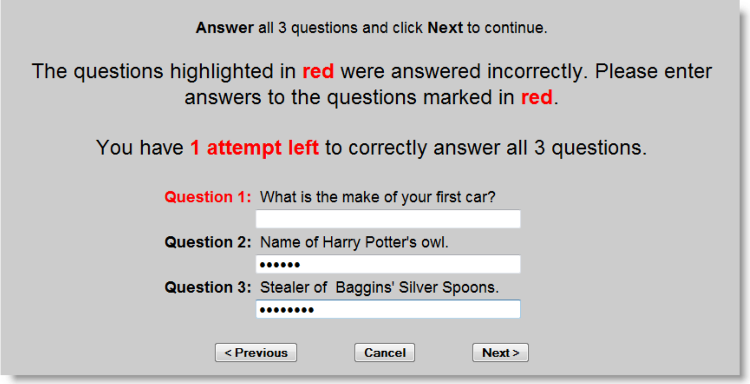
FAILWHALE

Expert Analysis Results



```
opt/                  14-Nov-2007 18:39    -
pam.conf              31-Jul-2004 22:34   552
pam.d/                17-Sep-2008 19:17    -
papersize             04-Dec-2007 15:44    7
passwd                30-Jul-2008 15:12   4.8K
passwd-               25-Jul-2008 09:27   4.8K
passwd.bak            26-Nov-2007 23:53   1.4K
perl/                 05-Feb-2008 17:12    -
postfix/              22-Aug-2008 20:49    -
```

✓



Answer all 3 questions and click **Next** to continue.

The questions highlighted in **red** were answered incorrectly. Please enter answers to the questions marked in **red**.

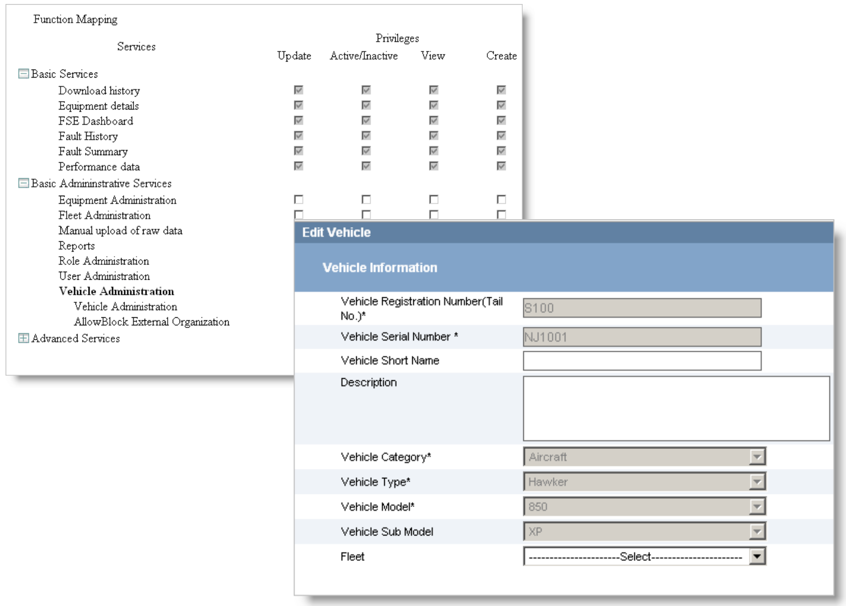
You have **1 attempt left** to correctly answer all 3 questions.

Question 1: What is the make of your first car?

Question 2: Name of Harry Potter's owl.
••••••

Question 3: Stealer of Baggins' Silver Spoons.
••••••••

✓



Function Mapping

Services	Privileges Update	Active/Inactive	View	Create
⊟ Basic Services				
Download history	☑	☑	☑	☑
Equipment details	☑	☑	☑	☑
FSE Dashboard	☑	☑	☑	☑
Fault History	☑	☑	☑	☑
Fault Summary	☑	☑	☑	☑
Performance data	☑	☑	☑	☑
⊟ Basic Admininstrative Services				
Equipment Administration	☐	☐	☐	☐
Fleet Administration	☐	☐	☐	☐
Manual upload of raw data				
Reports				
Role Administration				
User Administration				
Vehicle Administration				
Vehicle Administration				
AllowBlock External Organization				
⊞ Advanced Services				

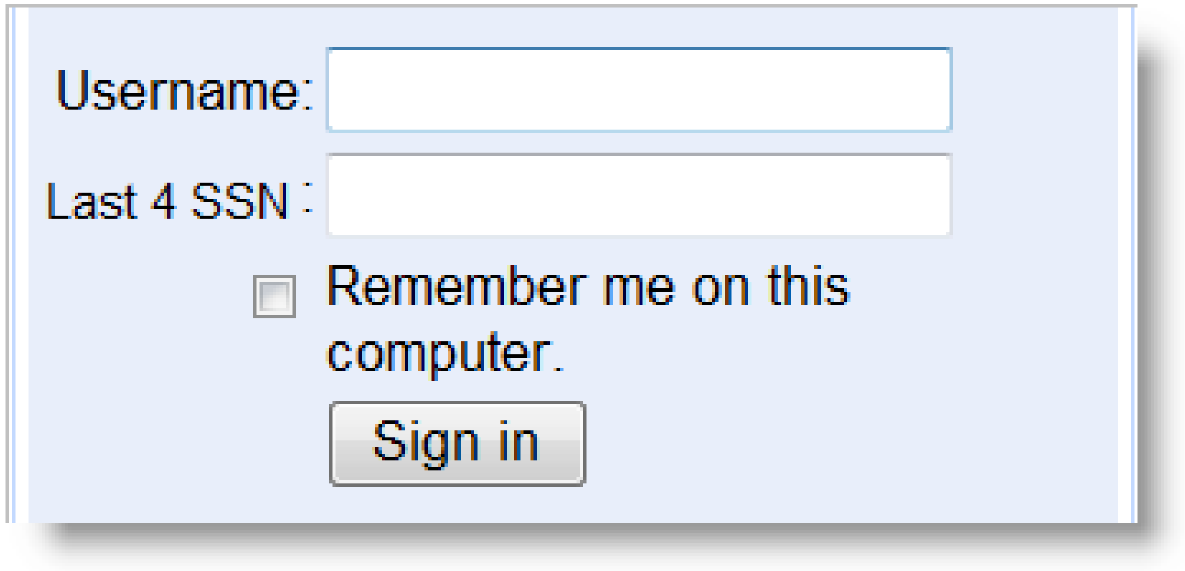
Edit Vehicle

Vehicle Information

Vehicle Registration Number(Tail No.)*	S100
Vehicle Serial Number *	NJ1001
Vehicle Short Name	
Description	
Vehicle Category*	Aircraft
Vehicle Type*	Hawker
Vehicle Model*	850
Vehicle Sub Model	XP
Fleet	--------------------Select--------------------

✓

Hacking Prepared SQL Statements

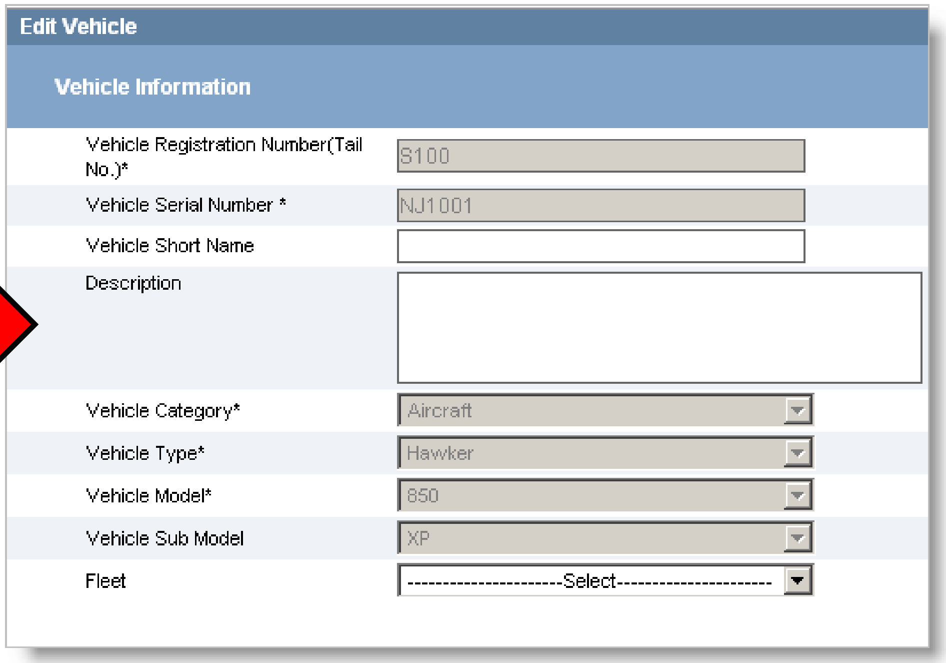

Username:
Last 4 SSN :
☐ Remember me on this computer.
Sign in

```
SELECT * FROM tblUsers
WHERE uName = ‘USERNAME’
AND ssn LIKE ‘%LAHLAHLAH’
```

Stealing Airplanes

Stealing an Airplane

Check A

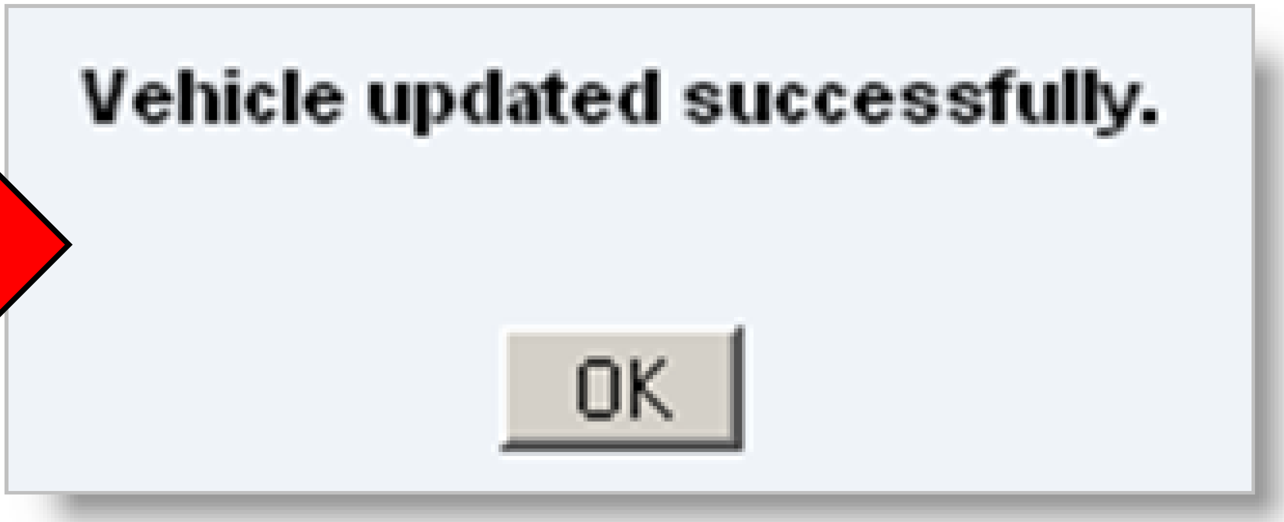


Edit Vehicle

Vehicle Information

Vehicle Registration Number(Tail No.)*	S100
Vehicle Serial Number *	NJ1001
Vehicle Short Name	
Description	
Vehicle Category*	Aircraft
Vehicle Type*	Hawker
Vehicle Model*	850
Vehicle Sub Model	XP
Fleet	----------------------Select----------------------

Check B



Vehicle updated successfully.

Check A

```
String airplaneID = request.getParameter(“airplaneID”);

request.getSession().setAttribute(“AID”, airplaneID);

if (haveAccessToPlane() != true) {
    return;
}

request.getSession().removeAttribute(“AID”);
```

Check B

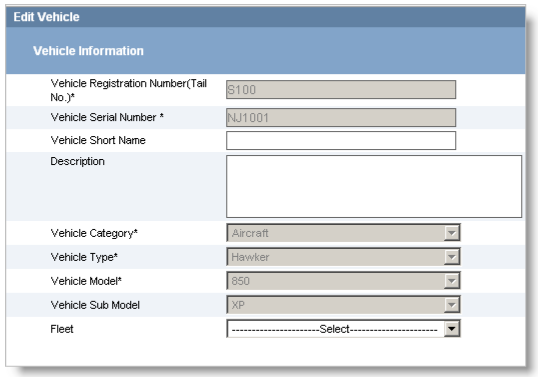
```
if (hasRight2Update() &&
   getAirplaneID.equals(
      request.getSession().getAttribute(“AID”)) {

          // allow submission and overwrite of data
}
```

Stealing an Airplane

← AirplaneID = 100
OwnerID = DarthVinnie

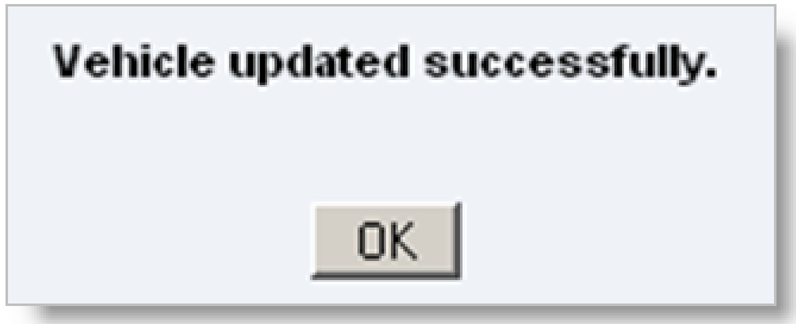
AirplaneID = 200 →
OwnerID = HanSolo



Edit Vehicle

Vehicle Information

Vehicle Registration Number(Tail No.)*	S100
Vehicle Serial Number *	NJ1001
Vehicle Short Name	
Description	
Vehicle Category*	Aircraft
Vehicle Type*	Hawker
Vehicle Model*	850
Vehicle Sub Model	XP
Fleet	--------------------Select--------------------

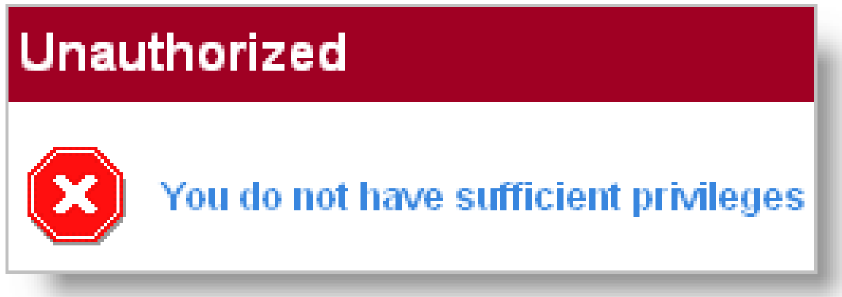


Vehicle updated successfully.

Browser Tab One

AID

200



Unauthorized

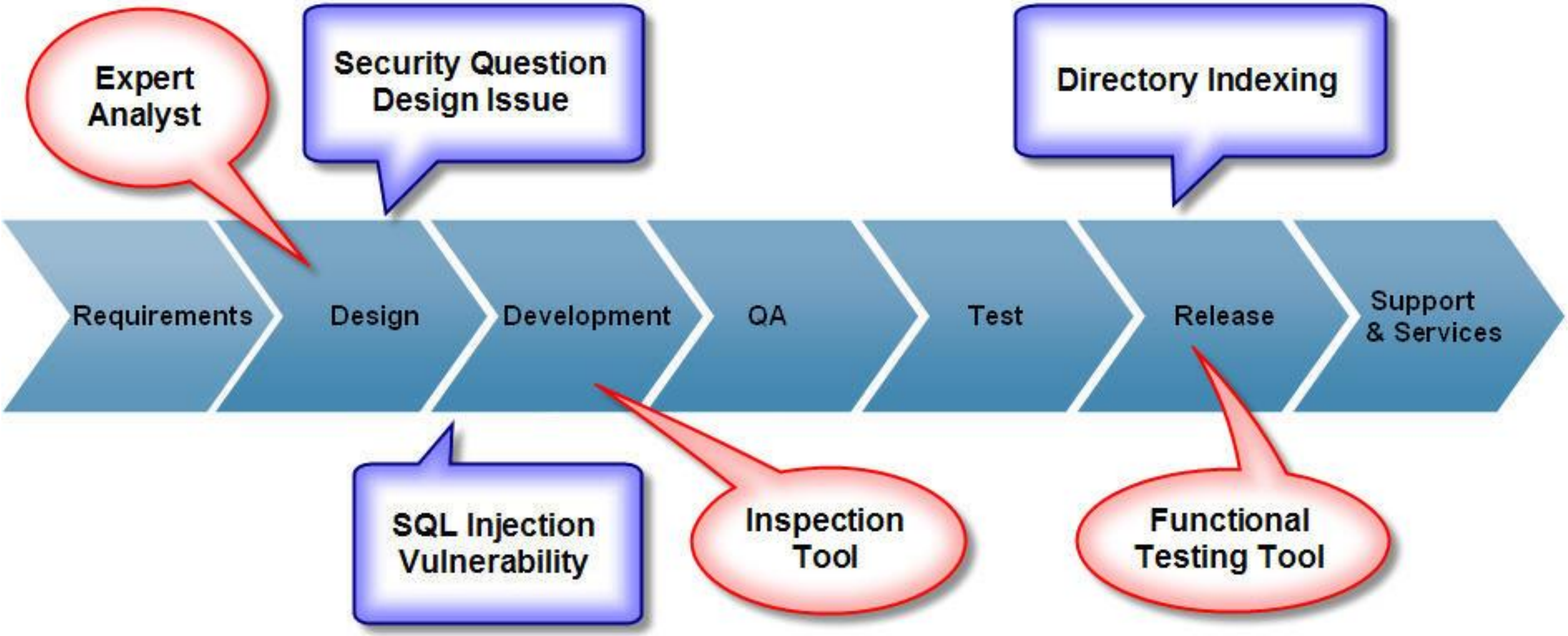
You do not have sufficient privileges

Browser Tab Two

Stealing an Airplane

0WN3D!

What Have We Learned?


Expert Analyst
Security Question Design Issue
Directory Indexing
Requirements
Design
Development
QA
Test
Release
Support & Services
SQL Injection Vulnerability
Inspection Tool
Functional Testing Tool

What Have We Learned?

Thanks!

Image Citations

- Hammer image courtesy of Keattikorn from FreeDigitalPhotos.net
- Airplane image courtesy of vectorolie from FreeDigitalPhotos.net
- Millennium Falcon image courtesy of from Wikimedia Commons