

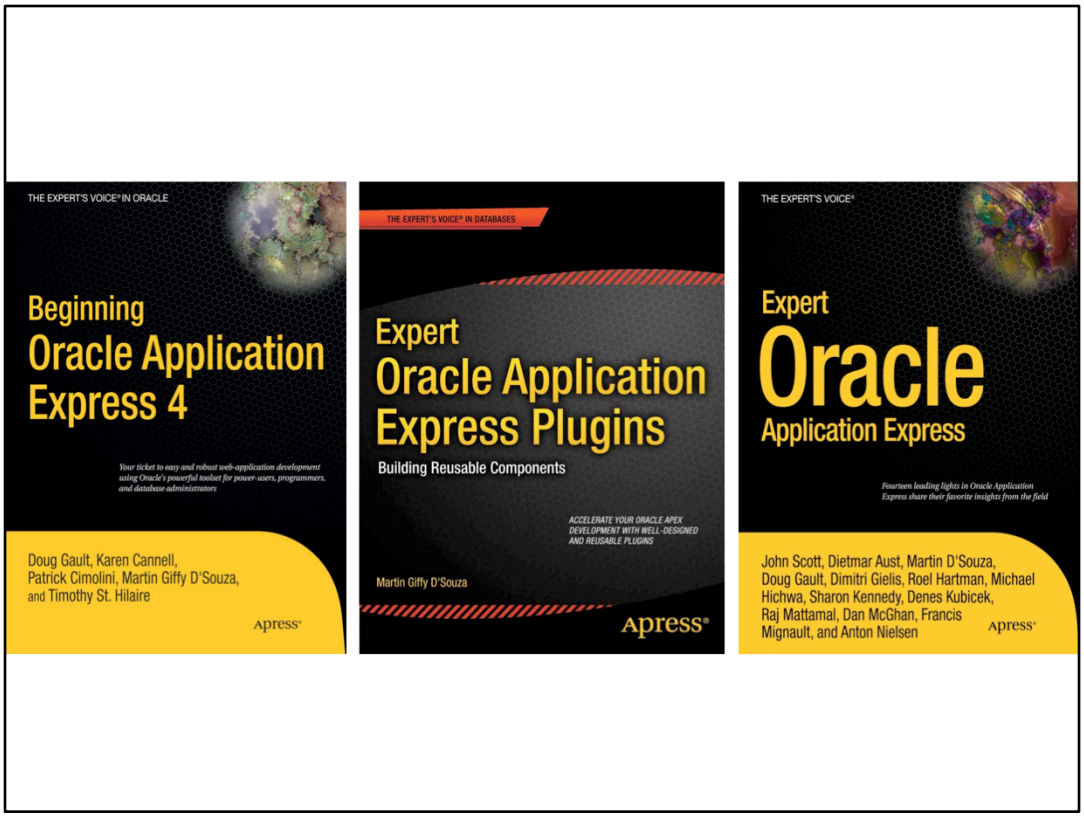
- Slides cover how to help protect your APEX application
- Some things to keep in mind
    - Security takes time, money, and effort so plan accordingly. Best to tackle biggest gaps and most important to your organization then move to smaller ones

Martin Giffy D'Souza



ORACLE ACE Director

- CTO and Co-founder at ClariFit: http://www.ClariFit.com
- Author of Oracle APEX blog: http://www.TalkApex.com
- Director for Oracle Development Tools User Group (ODTUG): http://www.odtug.com
- Oracle ACE Director



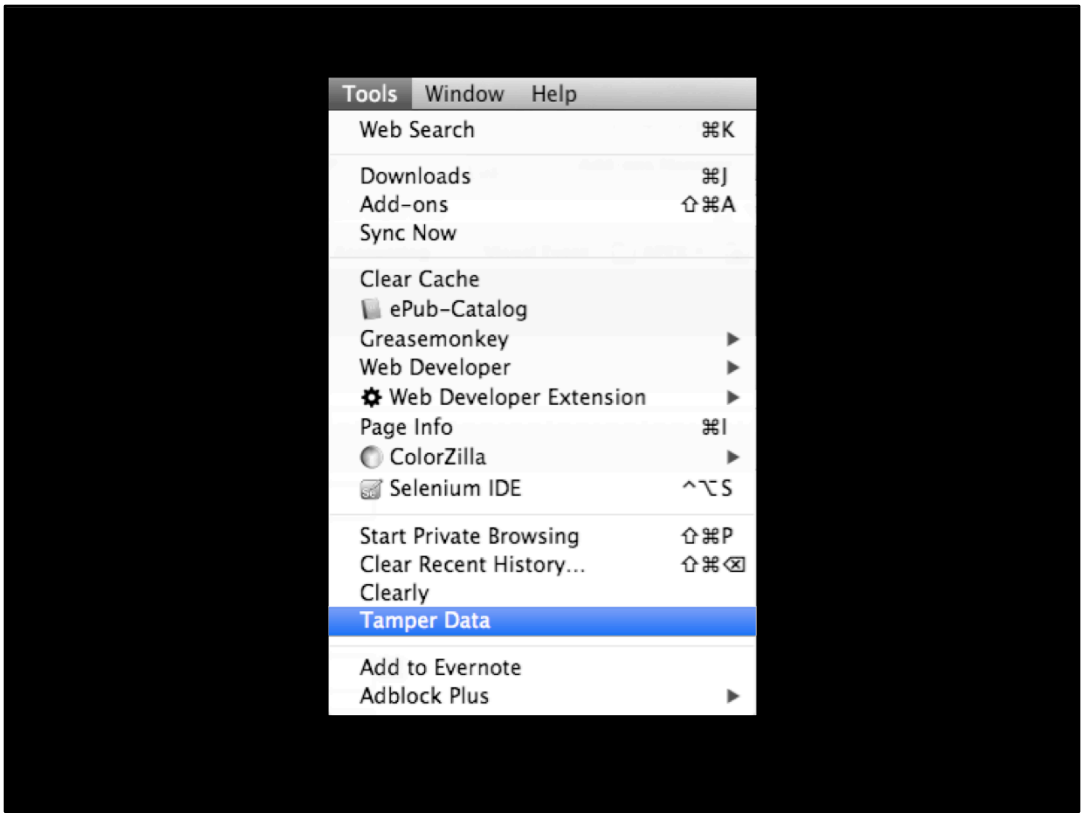
- Beginning Oracle Application Express 4: http://goo.gl/NxHoF
- Expert Oracle Application Express: http://goo.gl/tXm3P
    - More info about this book: http://jes.blogs.shellprompt.net/2011/03/30/expert-oracle-application-express
- Expert Oracle Application Express Plugins: http://goo.gl/089zi



- ClariFit is a Oracle APEX and PL/SQL consulting and training firm based out of Calgary, Alberta, Canada
- For more information please visit http://www.ClariFit.com or email: info@ClariFit.com

Session State Protection (SSP)

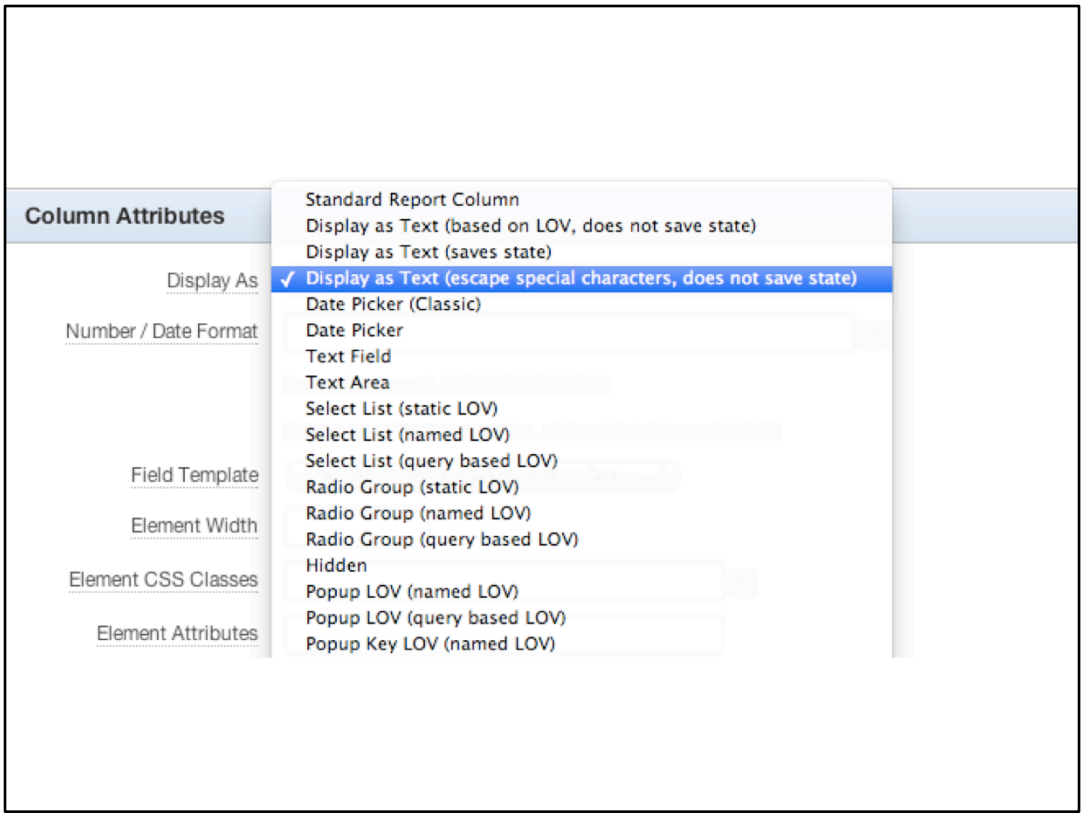
- Prevents URL tampering only
    - URL Tampering is when someone modifies the URL to modify another record
- SSP Can't be enabled on all items. Any cascading LOVs can't have SSP as JS is used to set the value in Session State.
    - By default JS is considered non secure since anyone can access the source code
- See http://www.talkapex.com/2012/11/session-state-protection-in-detail.html for detailed infomation



- Just because you enable SSP doesn't mean your application is secure. Can easily modify the values on the page using tools like Firebug and Tamper Data
- Example: In a LOV just because you restrict the set of LOVs doesn't mean that someone can't edit the Select List and modify the values
    - Only way to ensure the data is correct is to validate It before you insert/ update your tables (i.e. don't trust anything coming from the front end)

XSS

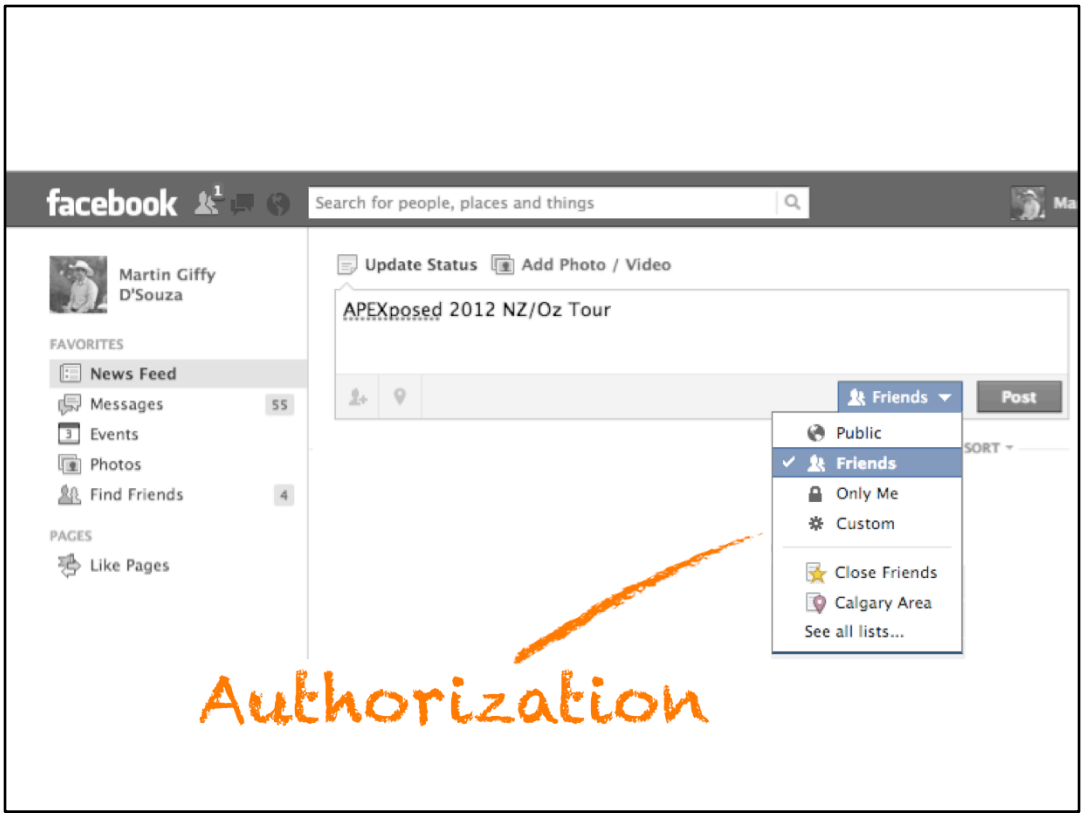
- Cross Site Scripting (XSS) is when a malicious enters embeds some JS code into your application for malicious purposes
    - http://en.wikipedia.org/wiki/Cross-site_scripting
- Example: Instead of their name they enter in: <script type="text/javascript">window.alert('this is annoying');</script>
    - By doing so when their name is displayed the user will see a popup message.
    - Instead of annoying message users can put in some malicious code to send them cookies about your session, scrape the screen, etc
- Can prevent this several ways:
    - Displaying data (report columns, display only, etc)
        - Set the Display As attribute to: Display as Text (escape special characters, does not save state)
        - Explicitly escape with the following packages/functions
            - All: `SYS.HTF.ESCAPE_SC`
            - 4.1: `APEX_PLUGIN_UTIL.ESCAPE`
            - 4.2: `APEX_ESCAPE`
    - Input:
        - Starting in APEX 4.2 on input items you prevent restricted characters by editing the item > Security > Restricted Characters


Column Attributes
Display As
Number / Date Format
Field Template
Element Width
Element CSS Classes
Element Attributes
Standard Report Column
Display as Text (based on LOV, does not save state)
Display as Text (saves state)
✓ Display as Text (escape special characters, does not save state)
Date Picker (Classic)
Date Picker
Text Field
Text Area
Select List (static LOV)
Select List (named LOV)
Select List (query based LOV)
Radio Group (static LOV)
Radio Group (named LOV)
Radio Group (query based LOV)
Hidden
Popup LOV (named LOV)
Popup LOV (query based LOV)
Popup Key LOV (named LOV)

Authorization

- Authorization allows you to control in-app security privileges on all APEX objects
    - Common use is for “Is Admin” options where only admins can use/view certain pages.


facebook
Email or Phone
Password
Log In
Keep me logged in
Forgot your password?
Sign Up
Connect and share with the people in your life.
Authentication


facebook
Search for people, places and things
Martin Giffy D'Souza
FAVORITES
News Feed
Messages 55
Events
Photos
Find Friends 4
PAGES
Like Pages
Update Status
Add Photo / Video
APEXposed 2012 NZ/Oz Tour
Friends
Post
Public
Friends
Only Me
Custom
Close Friends
Calgary Area
See all lists...
SORT
Authorization

SQL Injection & APEX Advisor

- SQL Injection is when malicious users can start tampering with a SQL query because it wasn't coded properly
    - http://en.wikipedia.org/wiki/SQL_injection
- APEX Advisor (Utilities > Advisor > Select Security options) can detect any SQL injection areas you may have in your application
    - Should run this report before deploying

Mine APEX Logs

- Most security breaches happen internally
- Can mine the APEX_WORKSPACE_ACTIVITY_LOG to see if users who may be trying to download / access a lot more data then they should be (i.e. scraping it)

3rd Party Tools

- ApexSec by Recx
- eSert by Enkitec

VPD / FGAC

- Virtual Private Database (VPD) and Fine Grained Access Control (FGAC) are the exact same thing. Just different terms for marketing by Oracle
- See following slides for example

```
SELECT ename, job, deptno
FROM emp
```

- When applied converts a query like this

```
-- VPD Enabled
-- Login as MARTIN
-- Context set

SELECT ename, job, deptno
FROM emp
WHERE deptno = 30
```

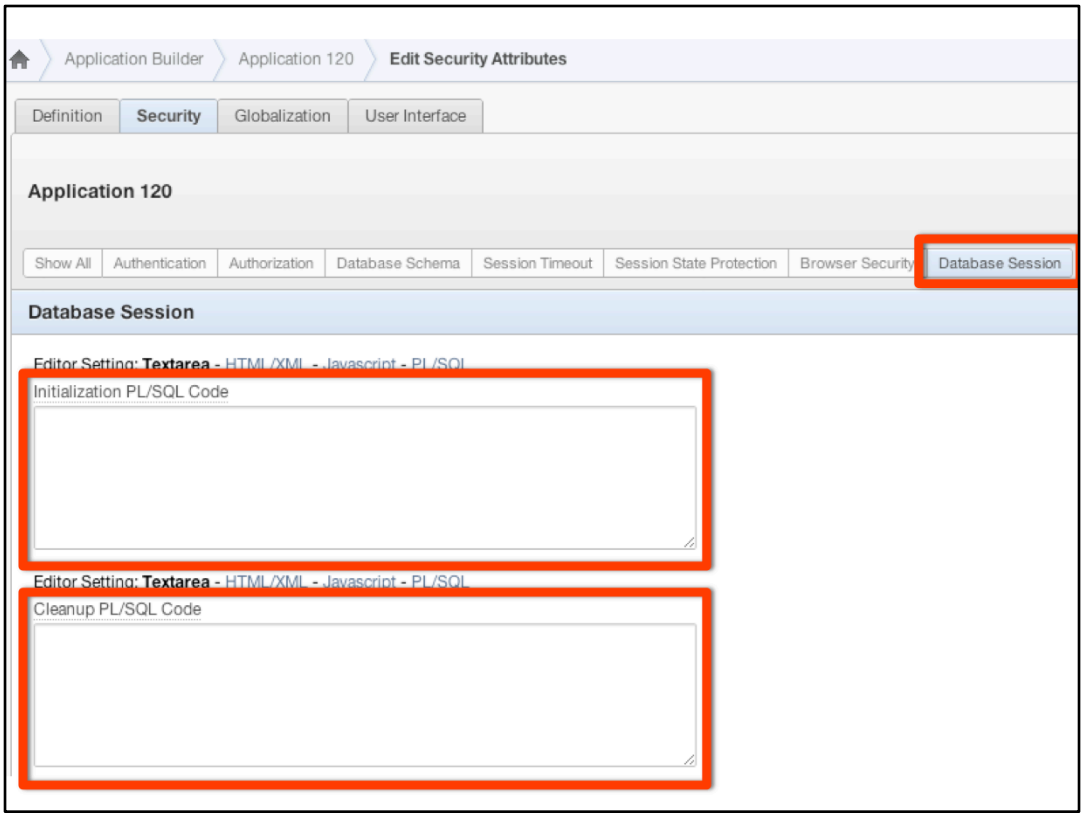
- To a something like this
- Note: you can define the predicate)
- No matter what the query is, the predicate (in red) will always be applied

ENAME	JOB	DEPTNO
CLARK	MANAGER	10
MILLER	CLERK	10
KING	PRESIDENT	10
FORD	ANALYST	20
SCOTT	ANALYST	20
JONES	MANAGER	20
SMITH	CLERK	20
ADAMS	CLERK	20
WARD	SALESMAN	30
MARTIN	**SALESMAN**	**30**
TURNER	SALESMAN	30
JAMES	CLERK	30
ALLEN	SALESMAN	30
BLAKE	MANAGER	30

- Without VPD result set would look like this

ENAME	JOB	DEPTNO
CLARK	MANAGER	10
MILLER	CLERK	10
KING	PRESIDENT	10
FORD	ANALYST	20
SCOTT	ANALYST	20
JONES	MANAGER	20
SMITH	CLERK	20
ADAMS	CLERK	20
WARD	SALESMAN	30
MARTIN	SALESMAN	30
TURNER	SALESMAN	30
JAMES	CLERK	30
ALLEN	SALESMAN	30
BLAKE	MANAGER	30

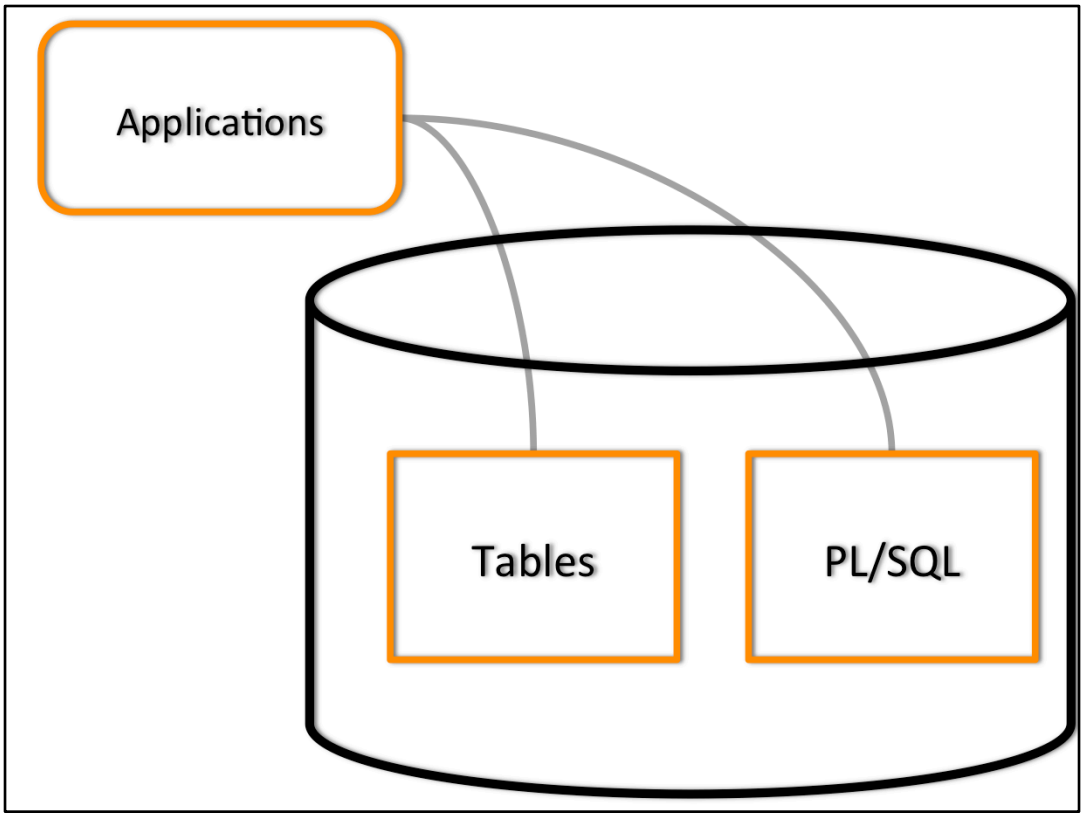
- After VPD result set looks like this
  - Note: greyed out areas aren't actually returned



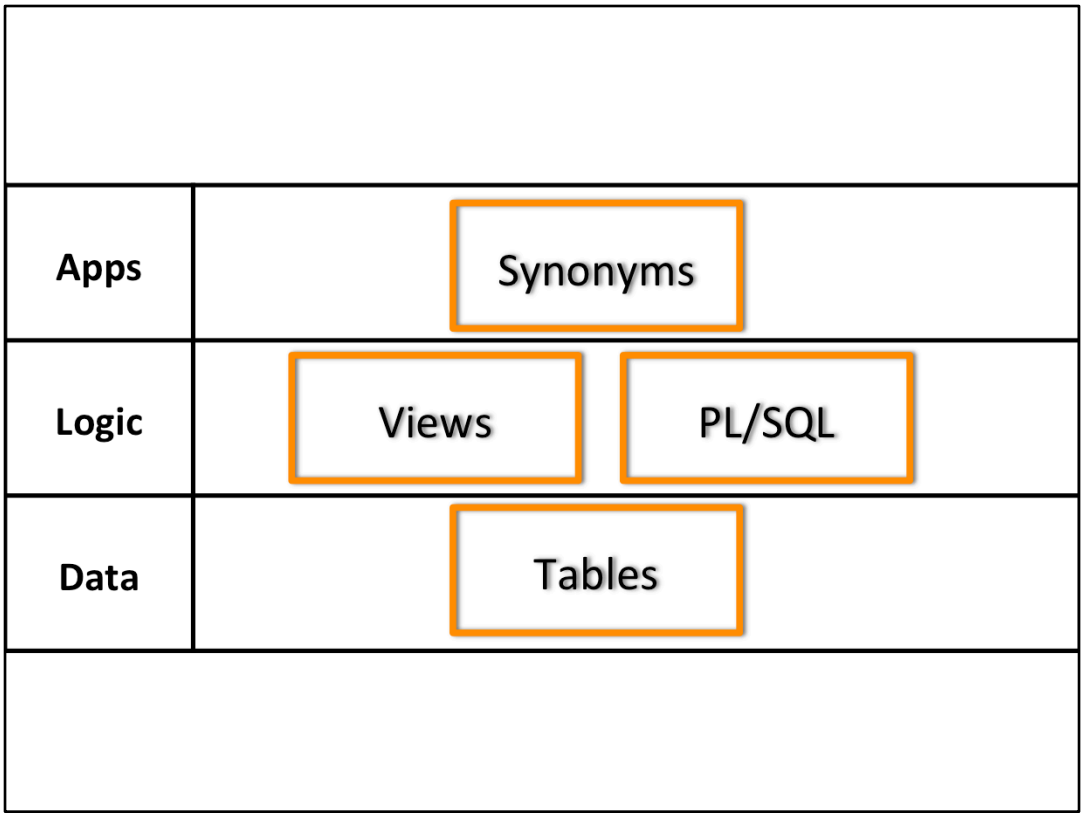
- To set VPD (context values) go to Shared Components > Edit Application > Security > Database Session
    - Pre-4.2 this area used to be called “VPD”

Database Design

- Database design can also affect your security



- Most applications run directly against the schema where the data is stored



- Instead can create a multi-layer approach where you only explicitly give access to what developers can have access to
- If the application is ever compromised this can help minimize the damage
- Another way to think of this is creating an “API” layer



- Email: Martin@ClariFit.com
- Twitter: @martindsouza
- Blog: http://www.TalkApex.com
- Presentation: http://presentations.ClariFit.com