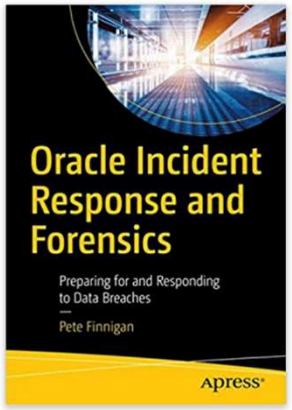
Oracle Database Vault in Real Life

Legal Notice

Oracle Database Vault in Real Life

Published by
PeteFinnigan.com Limited
Tower Court
3 Oakdale Road
York
England, YO30 4XL

PFCL
PETEFINNIGAN.COM LIMITED



Pete Finnigan – Background, Who Am I?

- Oracle Security specialist and researcher
- CEO and founder of PeteFinnigan.com Limited in February 2003
- Writer of the longest running Oracle security blog
- Author of the Oracle Security step-by-step guide and “Oracle Expert Practices”, “Oracle Incident Response and Forensics” books
- Oracle ACE for security
- Member of the OakTable
- Speaker at various conferences
  - UKOUG, PSOUG, BlackHat, more..
- Published many times, see
  - http://www.petefinnigan.com for links
- Influenced industry standards
  - And governments

Agenda

- Securing Oracle
- Three elements to secure
- Do you want to go further?
- Do it the hard way
- Use Database Vault to add better security
- Report and verify

Section

Securing Oracle

Secure Data

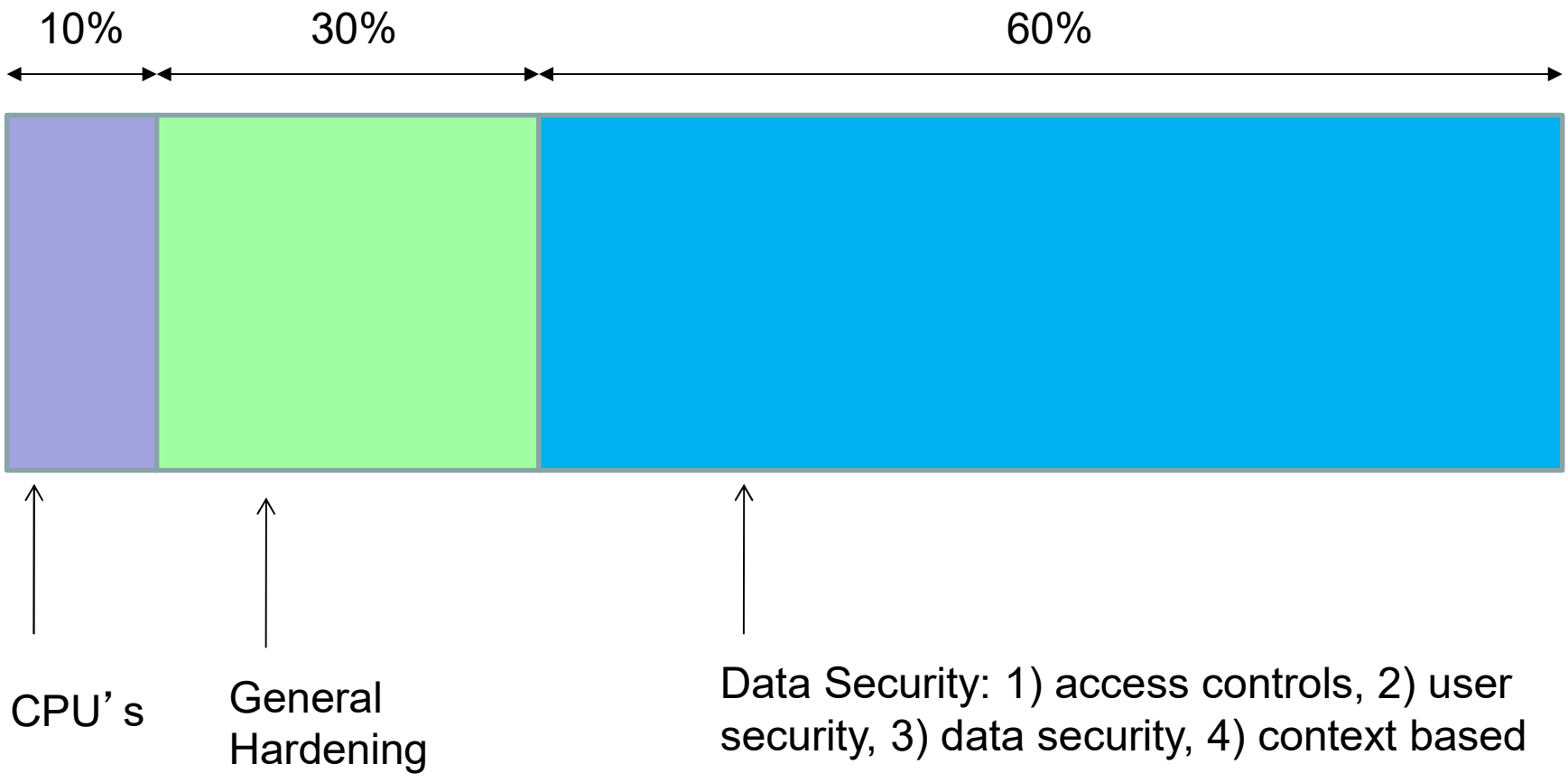
- The focus for us is to secure data and not "Oracle Security"
- We must use features of Oracle to secure our data BUT simply following a check list
- Securing to a list does not work as we must secure based on OUR data and OUR use of that data

- **We will keep this talk fairly high level**

Section

Three Elements to Secure

Compartmentalise Data Security?



PFCL
PETEFINNIGAN.COM LIMITED

Splitting Up Data Security in Oracle

- (1) - 10% - Patching
- (2) - 30% - Hardening
- (3) - 60% - Data Security design
  - Data design
    - (1) - Access controls
    - (2) - User security
    - (3) - Data access controls
  - Audit trails
  - Secure coding
  - Context based security
    - Either products from Oracle such as DV, OLS, VPD, TSDP,…
    - Home grown

Context Based Security

- Enhance other layers of security
- Allows detailed level security
  - Allow pete to access credit cards from JDE and only from the office and on a PC in the accounts department
- How?
  - Limit the database user, limit the application, limit the location, Limit by machine domain, limit by application roles of context / info / etc,

Section

Do you Want to go Further?

We Want to Achieve Better Security

- We must use context
  - That context must be secure and trusted
- Can do some things with VPD, …
- Can do by hand with
  - PL/SQL code, triggers, secure application roles, views and more
- Why is this an issue to do by hand?
  - Lots of code, Design the framework yourself
  - Can be bypassed as Oracle is complex

Section

Do if the Hard Way

Context: View Based Security

- We can create VIEW BASED security to limit access to read data
  - A PL/SQL function allows tests to be made to check whether access is allowed or not
  - We could also check in this PL/SQL whether the privilege used is SELECT ANY by checking the users actual rights
  - This can block some ANY privileges
- **BUT system ANY for select can access the base table. Solution:**
  - Revoke system ANY except for sys
  - Block SYSDBA access – The first versions of DV did this

Context: DML Based Security

- We can apply the same “Realm” type ideas to block DML with triggers
- This cannot be overridden as this is added to the base table and this is not view based
- Again we could check for System ANY in the PL/SQL code by looking at the callers rights
- We can also make a mandatory realm – in part at least with context based code

Command Rule: Block SQL*Plus - Webserver

```
133     program,
134     os_user
135   ) values (lv_username,lv_ip_address,lv_program,lv_os_user);
136   commit;
137
138   if(lv_ip_address not in('192.168.56.91','192.168.56.89','192.168.56.1','192.168.56.85','192.168.56.90')) then
139     -- the IP adress is not allowed
140
141     insert into stk_login_error (login_date,error_line) values (sysdate,1);
142     commit;
143     RAISE_APPLICATION_ERROR(-20070,'NOT AUTHORISED FROM THIS HOST');
144
145   else
146     -- test for web server and not apache and not httpd
147     if( (lv_ip_address in('192.168.56.89')) and
148         (upper(lv_program)<>'HTTPD@OEL59ORABLOG.LOCALDOMAIN (TNS V1-V3)') and
149         (upper(lv_os_user)<>'APACHE')) then
150
151         -- web server and not httpd and not apache OS user
152         insert into stk_login_error (login_date,error_line) values (sysdate,2);
153         commit;
154         RAISE_APPLICATION_ERROR(-20071,'NOT AUTHORISED WITH THESE DETAILS');
155     else
156       -- we must be on the admin PC or the actual database server
157       insert into stk_login_error (login_date,error_line) values (sysdate,3);
158       commit;
159     end if;
160   end if;
161   -- record that we got here
162   insert into stk_login_error (login_date,error_line) values (sysdate,4);
163   commit;
164 exception
165   when others then
166     insert into stk_login_error (login_date,error_line) values (sysdate,5);
167     commit;
168     RAISE_APPLICATION_ERROR(-20073,sqlerrm);
169   --
170 end login_dba;
171 /
```

- We can perfectly replicate the protection we have in DV with a logon trigger
- We can also use valid node checking but this is not granular
- In this example the httpd still works but SQL*Plus from the webserver is blocked

Section

Use Database Vault to Add Better Security

What Is Database Vault?

- Declarative security framework to allow fine grained access to database objects (tables, views, procedures…) grouped into realms
- Literally unlimited context based security rules can be added to control access to any (well almost any) database object or command
- Default use is to protect against **SYSTEM ANY** privileges
- Because it is “built-in” to the database kernel it is harder to bypass
- Pre-built shipped settings protect risky parameter changes and the data dictionary and more
- Separation of duties are added by default by creation of a security administrator, user account manager and vault owner
- SYS, SYSTEM and DBA are restricted in value
- Most components / features have protections that can be used

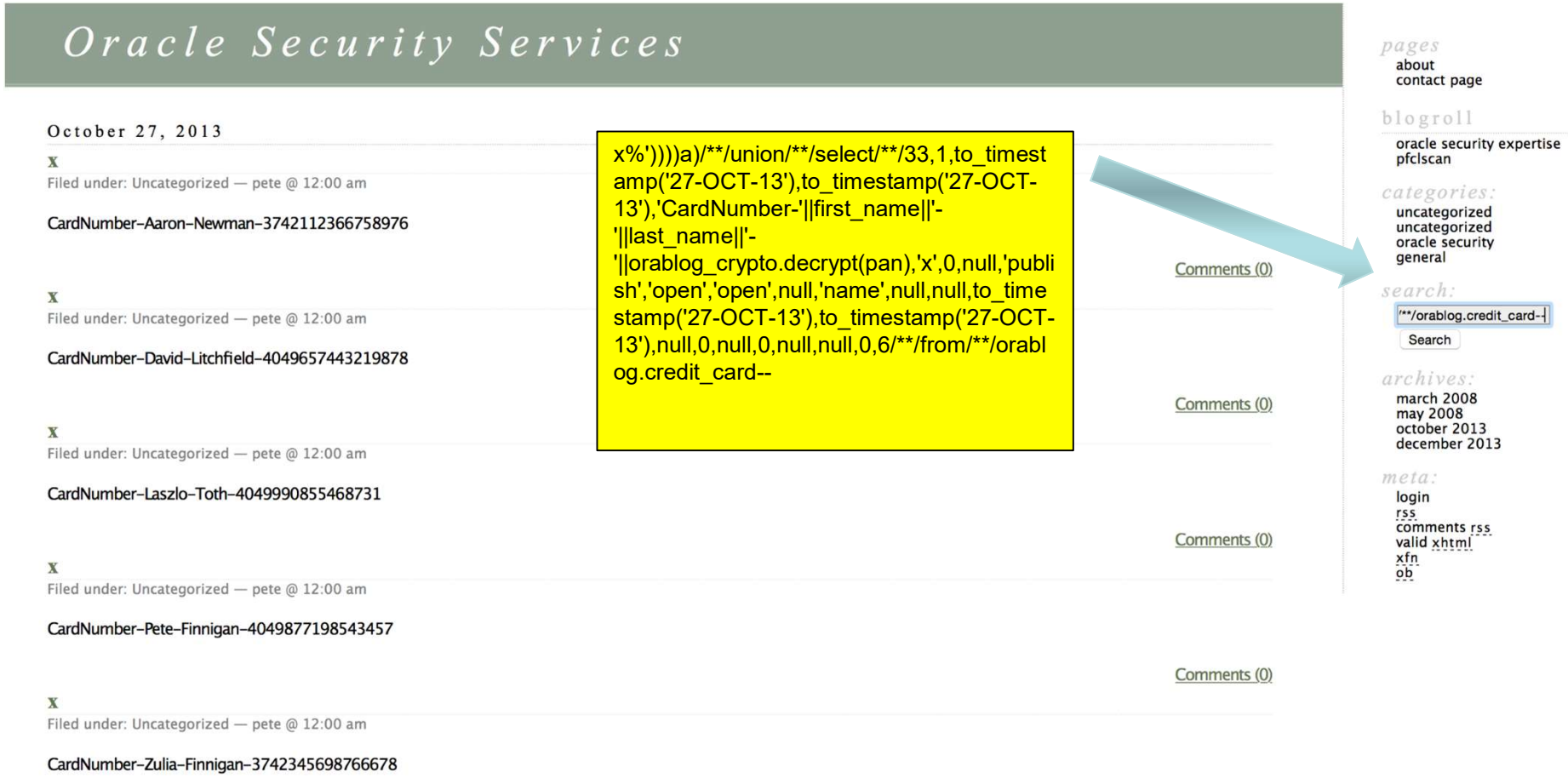
The Main DV Components

- Factors
  - Individual elements to use in rules (e.g. IP Address)
- Rules
  - True/False questions for the database
- Rule Sets
  - Groups of rules (Also results in True/False – with AND/OR)
- Realms
  - Protect database objects (uses rules, factors)
- Command Rules
  - Protect access to SQL commands (e.g. CONNECT) (uses rules, factors)
- Secure Application Roles (SAR)
  - Protective access to enable a role (uses rules, factors)

PFCL
PETEFINNIGAN.COM LIMITED

As an un-athenticated web user

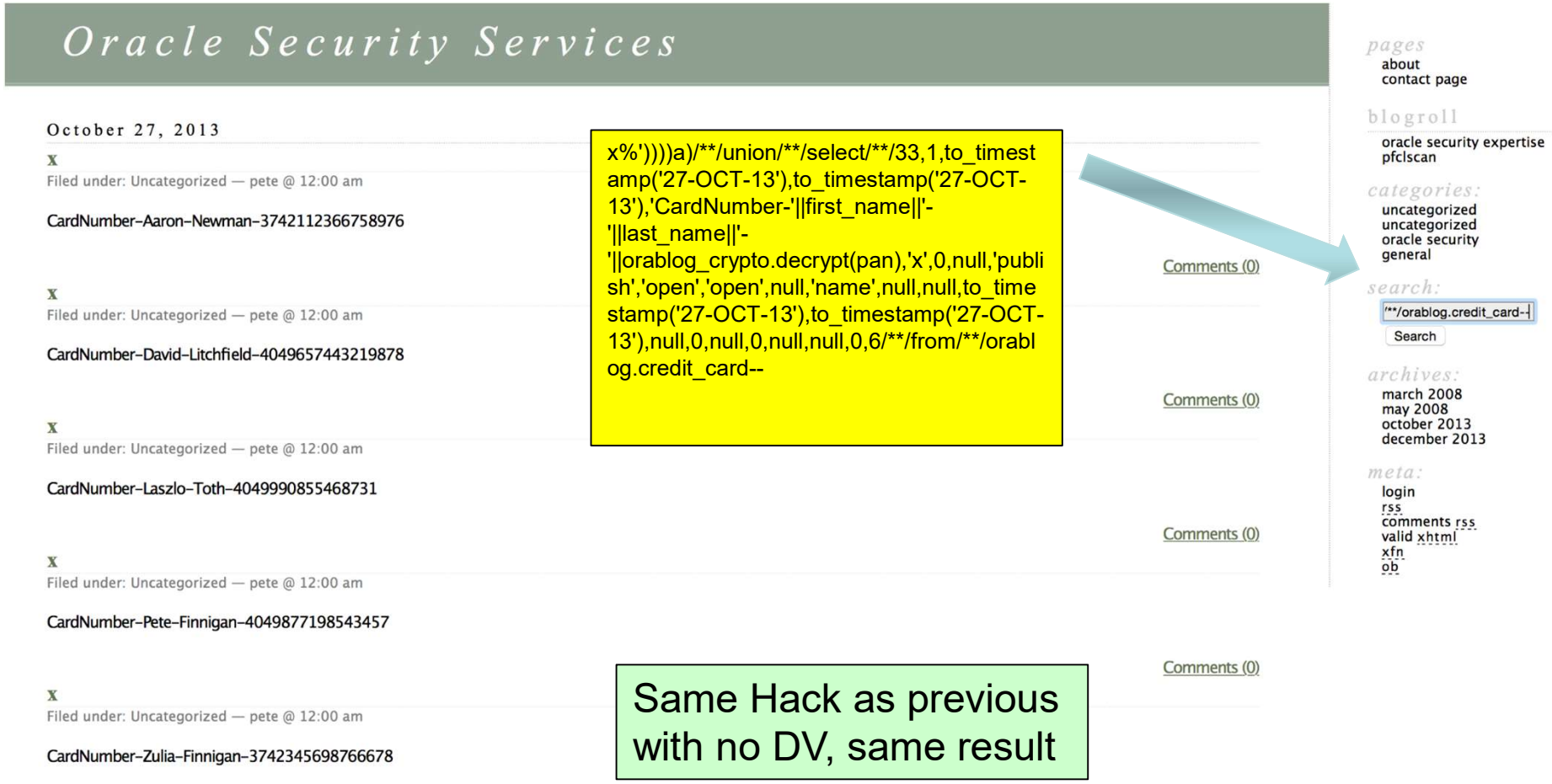
Hacking The Sample Database Before DV



PFCL
PETEFINNIGAN.COM LIMITED

As an un-athenticated web user

Hacking The Sample Database After DV OOTB



Same Hack as previous with no DV, same result

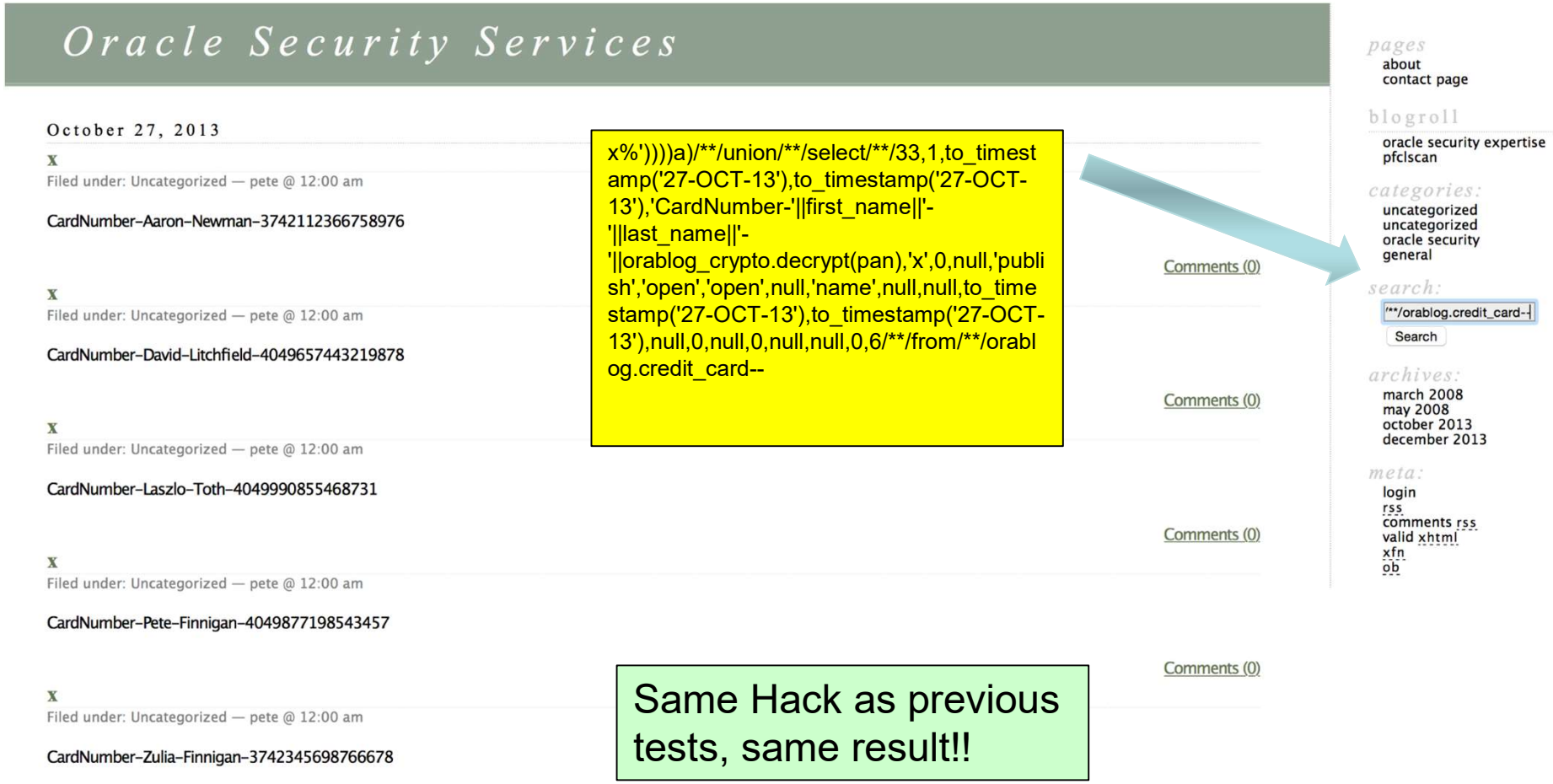
DV Add A Realm – Hack Again

```
SQL> -- create a simple realm for BOF
SQL> connect dvo/dvo@//192.168.56.94:1521/dvtst.localdomain
Connected.
SQL>
SQL> -- remove the realm to re-create
SQL> exec dbms_macadm.delete_realm('BOF Realm');

PL/SQL procedure successfully completed.

SQL>
SQL> -- create the BOF realm
SQL> begin
  2          dbms_macadm.create_realm(
  3          realm_name => 'BOF Realm',
  4          description => 'Protect BOF objects',
  5          enabled => dbms_macutl.g_yes,
  6          audit_options => dbms_macutl.g_realm_audit_fail,
  7          realm_type => 0);
  8  end;
  9  /

PL/SQL procedure successfully completed.

SQL>
SQL> -- add the objects to the realm
SQL> begin
  2          dbms_macadm.add_object_to_realm(
  3          realm_name => 'BOF Realm',
  4          object_owner => 'ORABLOG',
  5          object_type => '%',
  6          object_name => '%');
  7  end;
  8  /

PL/SQL procedure successfully completed.
```

- Create a realm to effectively add the ORABLOG schema objects to that realm and so that System ANY is not able to be used on ORABLOG objects by any other user.
- Do the same hacks as before still work?
- The applications (Orablog and BOF) still work correctly even with the realm in place

As an un-athenticated web user

Hacking The Sample Database With Realm

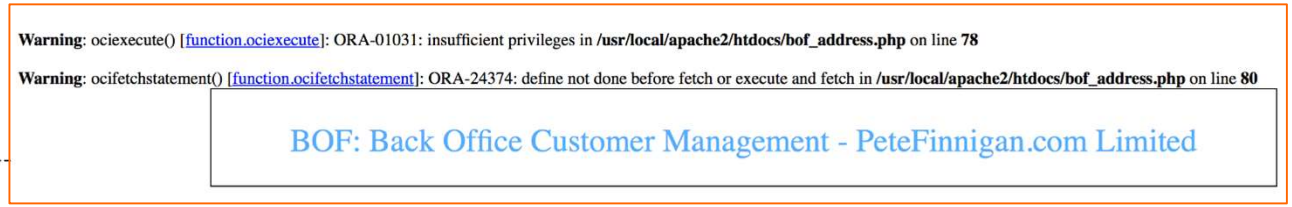


Same Hack as previous tests, same result!!

Hmmm, the aps are now broken; we need to add ORABLOG to the realm but it defeats the object

Add Mandatory Realm – Hack Again

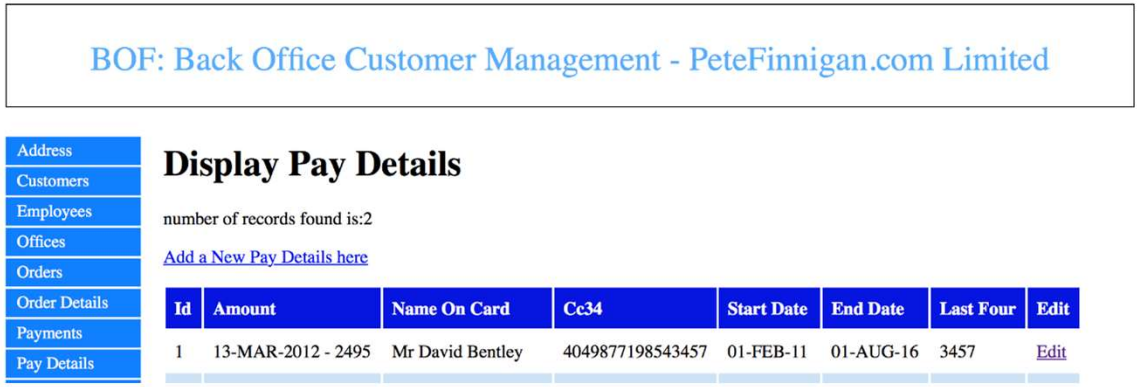
```
SQL> exec dbms_macadm.delete_realm('BOF Realm');

PL/SQL procedure successfully completed.

SQL>
SQL> -- create the BOF realm
SQL> begin
  2          dbms_macadm.create_realm(
  3          realm_name => 'BOF Realm',
  4          description => 'Protect BOF objects',
  5          enabled => dbms_macutl.g_yes,
  6          audit_options => dbms_macutl.g_realm_audit_fail,
  7          realm_type => 1);
  8  end;
  9  /

PL/SQL procedure successfully completed.

SQL>
SQL> -- add the objects to the realm
SQL> begin
  2          dbms_macadm.add_object_to_realm(
  3          realm_name => 'BOF Realm',
  4          object_owner => 'ORABLOG',
  5          object_type => '%',
  6          object_name => '%');
  7  end;
  8  /

PL/SQL procedure successfully completed.

SQL> select name,realm_type from dvsys.dba_dv_realm;

NAME
----------------------------------------------------------------
Oracle Database Vault
Database Vault Account Management
Oracle Enterprise Manager
Oracle Default Schema Protection Realm
Oracle System Privilege and Role Management Realm
Oracle Default Component Protection Realm
BOF Realm
```

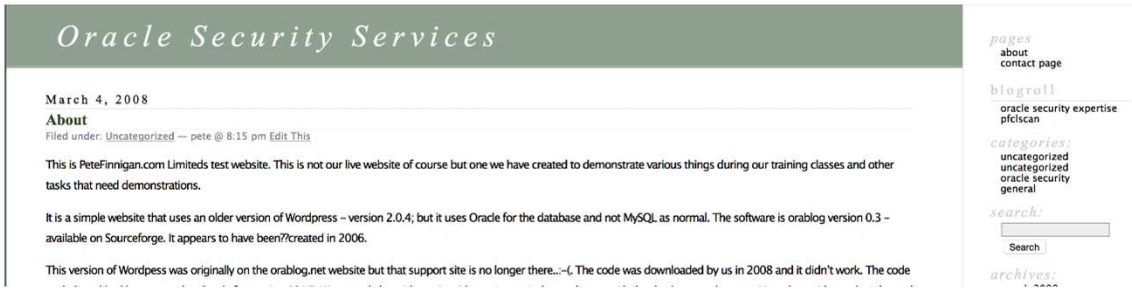


MANDATORY

Add Mandatory Realm – Fix The Realm Auth

```
SQL> -- remove the realm to re-create
SQL> exec dbms_macadm.delete_realm('BOF Realm');

PL/SQL procedure successfully completed.

SQL>
SQL> -- create the BOF realm
SQL> begin
  2          dbms_macadm.create_realm(
  3          realm_name => 'BOF Realm',
  4          description => 'Protect BOF objects',
  5          enabled => dbms_macutl.g_yes,
  6          audit_options => dbms_macutl.g_realm_audit_fail,
  7          realm_type => 1);
  8  end;
  9  /

PL/SQL procedure successfully completed.

SQL>
SQL> -- add the objects to the realm
SQL> begin
  2          dbms_macadm.add_object_to_realm(
  3          realm_name => 'BOF Realm',
  4          object_owner => 'ORABLOG',
  5          object_type => '%',
  6          object_name => '%');
  7  end;
  8  /

PL/SQL procedure successfully completed.

SQL>
SQL> -- add ORABLOG to the realm as a participant
SQL> begin
  2          dbms_macadm.add_auth_to_realm(
  3                  realm_name => 'BOF Realm',
  4                  grantee => 'ORABLOG',
  5                  rule_set_name => NULL,
  6                  auth_options => dbms_macutl.g_realm_auth_participant);
  7  end;
  8  /

PL/SQL procedure successfully completed.
```

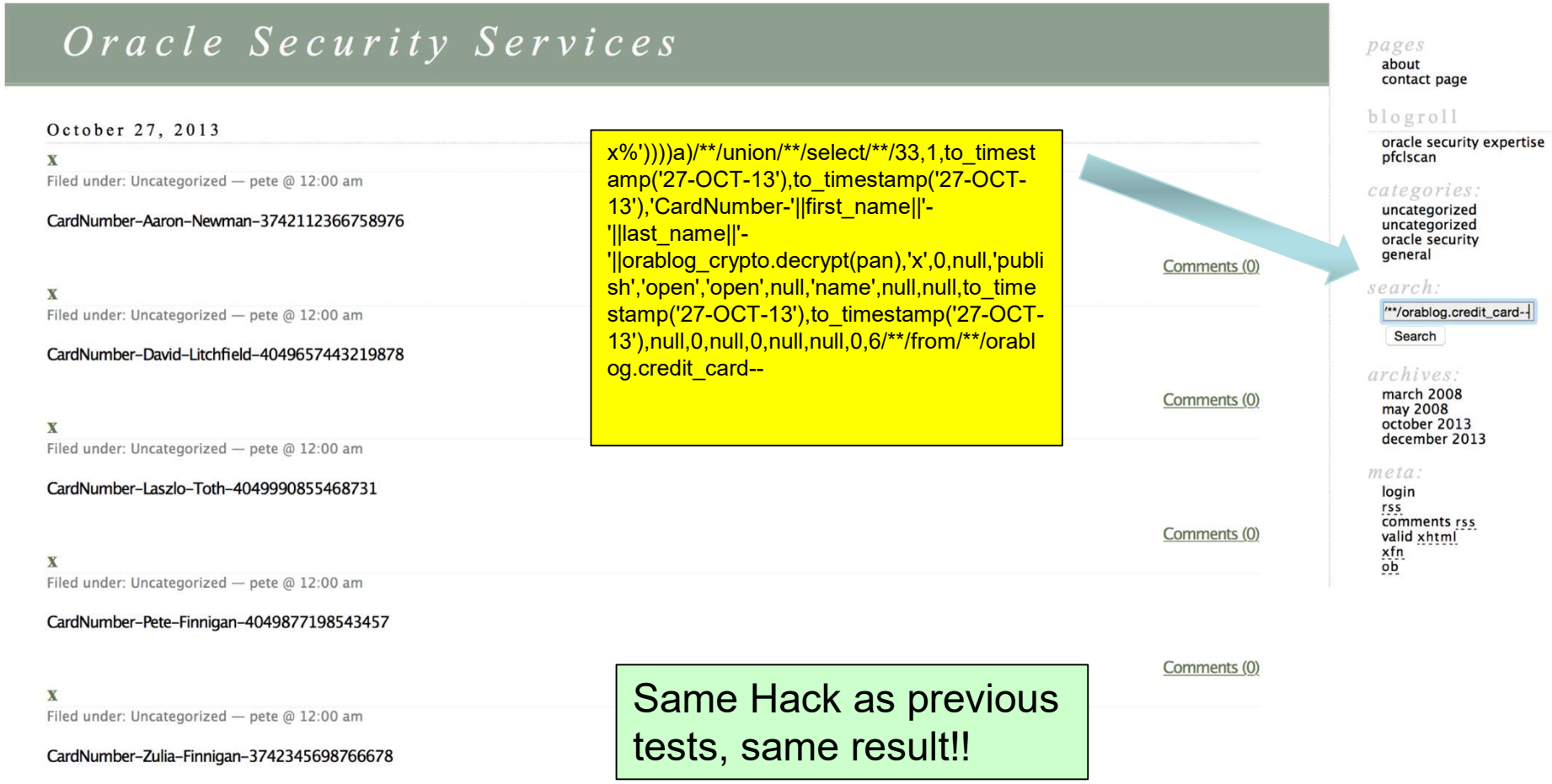




PFCL
PETEFINNIGAN.COM LIMITED

As an un-athenticated web user

Hacking The Sample Database With Mandatory Realm



Same Hack as previous tests, same result!!

PFCL
PETEFINNIGAN.COM LIMITED

DV Command Rule – Create the Rules

```
21 -- create the factor
22 begin
23   dbms_macadm.create_factor(
24   factor_name => 'PFCLProgramName',
25   factor_type_name => 'Application',
26   description => 'Locate the program name from the session',
27   rule_set_name => NULL,
28   validate_expr => NULL,
29   get_expr => 'UPPER(SYS_CONTEXT(''USERENV'',''MODULE''))',
30   identify_by => DBMS_MACUTL.G_IDENTIFY_BY_METHOD,
31   labeled_by => DBMS_MACUTL.G_LABELED_BY_SELF,
32   eval_options => DBMS_MACUTL.G_EVAL_ON_SESSION,
33   audit_options => DBMS_MACUTL.G_AUDIT_ON_GET_ERROR,
34   fail_options => DBMS_MACUTL.G_FAIL_SILENTLY);
35 end;
36 /
37 -- create the rule set
38 begin
39   dbms_macadm.create_rule_set(
40   rule_set_name => 'Enforce ORABLOG Webserver',
41   description => 'Ensure that ORABLOG can only connect with Apache from the webserver',
42   enabled => DBMS_MACUTL.G_YES,
43   eval_options => DBMS_MACUTL.G_RULESET_EVAL_ANY,
44   audit_options => DBMS_MACUTL.G_RULESET_AUDIT_OFF,
45   fail_options => DBMS_MACUTL.G_RULESET_FAIL_SHOW,
46   fail_message => 'SQL*Plus not allowed for ORABLOG from the Webserver',
47   fail_code => 20403,
48   handler_options => DBMS_MACUTL.G_RULESET_HANDLER_OFF,
49   handler => NULL,
50   is_static => FALSE);
51 end;
52 /
53 -- create the rules
54 begin
55   dbms_macadm.create_rule(
56     rule_name => 'Prevent ORABLOG Use of SQL*Plus From WebServer',
57     rule_expr =>'((UPPER (DVF.F$PFCLPROGRAMNAME) = ''HTTPD@OEL59ORABLOG12 (TNS V1-V3)'' AND UPPER (DVF.F$CLIENT_IP) in(
   .     ''192.168.56.97'')) OR (UPPER (DVF.F$CLIENT_IP) in( ''192.168.56.1'',''192.168.56.90'''))) AND DVF.F$SESSION_USER IN
   .     (''ORABLOG'')');
58 end;
```

DV Command Rule – Code Continued

```
begin
  dbms_macadm.create_rule(
    rule_name => 'Allow All Other Users Access',
    rule_expr =>'DVF.F$SESSION_USER NOT IN (''ORABLOG'')');
end;
/
-- add the rules to the rule set
begin
  dbms_macadm.add_rule_to_rule_set(
    rule_set_name => 'Enforce ORABLOG Webserver',
    rule_name => 'Prevent ORABLOG Use of SQL*Plus From WebServer',
    rule_order => 1);
end;
/
begin
  dbms_macadm.add_rule_to_rule_set(
    rule_set_name => 'Enforce ORABLOG Webserver',
    rule_name => 'Allow All Other Users Access',
    rule_order => 1);
end;
/

-- create the connect command rule
begin
  dbms_macadm.create_command_rule(
    command => 'CONNECT',
    rule_set_name => 'Enforce ORABLOG Webserver',
    object_owner => '%',
    object_name => '%',
    enabled => DBMS_MACUTL.G_YES);
end;
/
```

DV Command Rule - Results

```
SQL> connect orablog/orablog@//192.168.56.94:1521/dvtst.localdomain
ERROR:
ORA-47306: 20403: SQL*Plus not allowed for ORABLOG from the Webserver


SQL> !hostname
oel59orablog12
```

```
SQL> connect orablog/orablog@//192.168.56.94:1521/dvtst.localdomain
Connected.
SQL> !hostname
Peters-MBP
```

- The rules are not perfect as we have implemented properly only for Orablog and not BOF but BOF has no client tools installed
- The client_program_name is not set from the server so we have used instead Module – but it would be better to use the hash
- Implementing factors, rules, rule sets and command rules or rule sets for realms is a large task when a lot of controls are needed

Do Not Use DV

- Don’t use Database Vault if you do not have normal database security
- Even then
  - Use standard database security first
  - Achieve some of DV with standard features – i.e. do not use DBA, SYS and SYSTEM, revokes, %ANY% remove,…
- Secure DV
- Then use DV to enhance existing data security

TDE Would Benefit from Database Vault

- TDE can be used to protect data at rest
- In a typical database data in datafiles is visible on the OS to “oracle” Unix user only
- If TDE is used then it protects the datafiles at rest on tape or other media
- The “oracle” user can connect “/ as sysdba” and see any TDE protected data
- Database Vault can be used to protect the access to the TDE data when connected

Choose the Correct DV Solution

- Keep the Database Vault set up as simple as possible
- Use simple rules / rule sets that can be verified
- Use designs not random code
- Use the right solution; command rule, SAR, Realm based on the requirement
- Enrich realms with command rules

Do Not Mix

- If an object must appear in multiple realms
  - use one realm and more complex rules
  - Or multiple realms and simpler rules
  - Don’t cross over in rules
- Layer command rules on realms if necessary
- Design and create simple rules and rule sets
- Design necessary factors and ensure they are secure

PFCL
PETEFINNIGAN.COM LIMITED

Section

Report and Verify

Check The DV Security

- Run sc_dv.sql
- >20k lines O/P
- Check rules

```
--------------------------------------------------------------------------------
              Oracle Database Vault Configuration Report
--------------------------------------------------------------------------------


PL/SQL procedure successfully completed.

DBID           : 1405253007
Name           : FREE
Container Name: FREEPDB1


PL/SQL procedure successfully completed.

Oracle Database Vault is Not Enabled


PL/SQL procedure successfully completed.


~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
        Database Vault Status
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~


PL/SQL procedure successfully completed.


DV_CONFIGURE_STATUS   FALSE
DV_ENABLE_STATUS      FALSE
DV_APP_PROTECTION     NOT CONFIGURED
```

Conclusions

- Database Vault is complex
- Its use MUST be on top of hardened database with designed data security
- Do not mix
- Secure DV
- Use DV to enhance data security not replace standard security

Questions

?

If Anyone has questions, please ask now or catch me during the event!!

Oracle Database Vault in Real Life