HAVE I BEEN PWNED?

How Oracle APEX can help

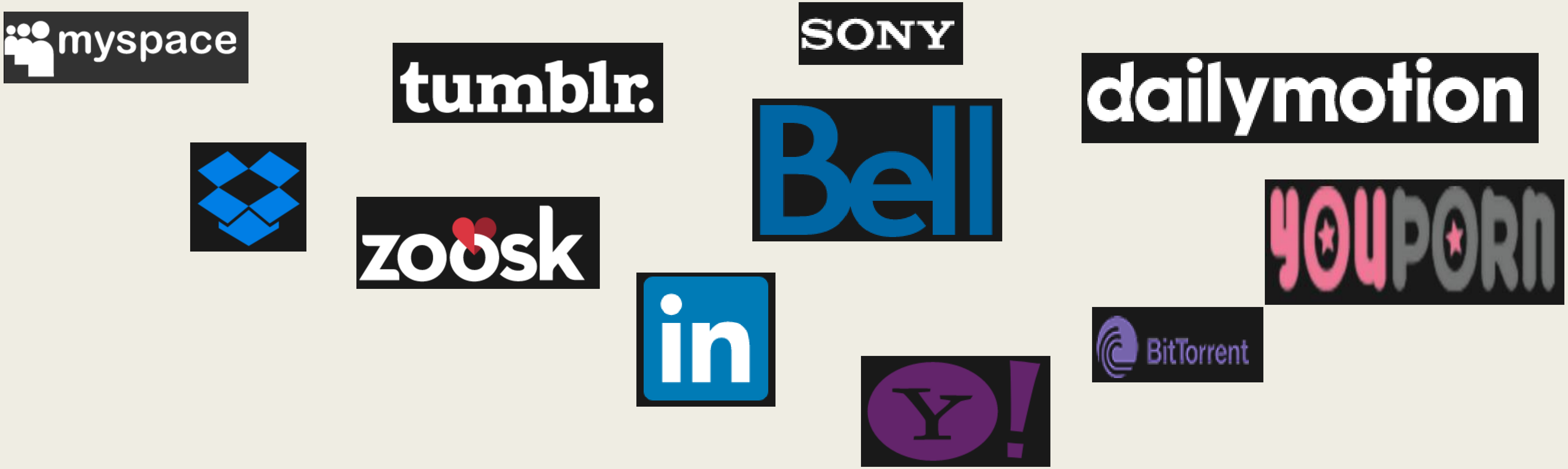
By Gaspar Gonzalez
Twitter: @gasparyyc

What is pwned??

- Pwn is a slang term derived from the verb “own”, as meaning to appropriate or to conquer to gain ownership.
  - *The term implies domination or humiliation of a rival*
- In jargon, pwn means to compromise or control, specifically another computer (server or PC), website, gateway device, or application.
  - *It is synonymous with one of the definitions of hacking or cracking, including jailbreaking.*

So? What’s the issue here?

- Multiple security breaches have made millions of passwords known to cybercriminals
  - *Yes, possibly **YOUR** password is known to cybercriminals..*



So the passwords are known, and?

- Not just passwords, recent breaches have confirmed emails, passwords, names, IP address and physical addresses have been stolen, also
- Usernames
- Dates of birth
- Genders
- Phone numbers

- Just what cybercriminals want for identify theft!

Really, how bad is it??

Passwords:

- Chances are that at least one of your passwords is already known to cybercriminals
- There are 306 million searchable passwords (2017)
- There are 501 million searchable passwords (March 2018)

Emails:

- On January 2017
  - *393 million unique email addresses were found*
- On August 2017,
  - *711 million unique email addresses were found*

Where can I learn more about this?

- All the information provided came from Troy Hunt (https://www.troyhunt.com)
- Troy is the known expert for consolidating and informing about breached data.
- Troy has created the website https://haveibeenpwned.com/
  - *This website will let you search for email & passwords known to him*

What can I do?

- 1st get a password manager and learn how to use it.
  - *1password.com, keepass.org, etc..*
- 2nd Change your passwords across the board…
- 3rd Use this information to your advantage
  - *Show the users you're ahead of the game*
  - *Show the users you know what to do*
  - *Lead the change, be the expert at work*
  - *Don't forget Home & Family.. They need professional advise too…*

But how is this related to APEX?

- Thanks to Troy you can download the password files and using APEX you can check if your passwords have been known to cybercriminals..
- Also with a little bit of creativity we can allow our users to check if their password has been compromised already so they can change it..
  - *Or you could enforce a check that if its compromised then that password can’t be used in your application(s).*

Note: I emphasise this presentation & demo is for passwords only and not emails as they haven’t been published

So, how to do it from APEX?

- There are a few steps and you'll decide what works best in your case.
  - *These are steps I used to load and make it available via APEX.*

- I used three different approaches:

1. **Load data in database**
2. Load data in text files on the Operating System as regular text files
3. External tables – (is not viable as its way too slow to be productive)

So, how to do it from APEX?
Load data in database

- In my case I used Oracle XE and the amount of data exceeds the 11GB of user data available in that version.
- I decided to load just 50 million (including a non-unique index)
- Response time is fantastic, I mean databases are made for that stuff!
- In case you haven’t seen it this is the error when you exceed the capacity:
  ORA-12953: The request exceeds the maximum allowed database size of 11 GB

So, how to do it from APEX?

Load data in database

- Steps to load in Database
- 1. Download the files from Troy Hunt's website:
  - *I used CentOS so you adjust as needed based on your OS and/or distro*

Note: You'll need 45GB of free space for this space to complete successfully.

As root:

```
yum install -y p7zip
mkdir /pwned
chown oracle:dba /pwned
cd /pwned
wget https://downloads.pwnedpasswords.com/passwords/pwned-passwords-ordered-2.0.txt.7z
7za e pwned-passwords-ordered-2.0.txt.7z
```

So, how to do it from APEX?
Load data in database

- Steps to load in Database
- 2. Prepare the database for SQLLoader:

Connect SYS as sysdba:

```
  @$ORACLE_HOME/rdbms/admin/catldr.sql
```

So, how to do it from APEX?

Load data in database

- Steps to load in Database
- 3. Create the table and non-unique index

Using SQLWorkshop in APEX:

```
CREATE TABLE  PWNED    (HASH CHAR(40), COUNTS NUMBER);

CREATE INDEX  PWNED_IDX1 ON  PWNED (HASH);
```

So, how to do it from APEX?

Load data in database

- Steps to load in Database
- 4. Prepare the SQLLoader control file, which is an Operating System program

Content of loader1.ctl:

```
LOAD DATA
INFILE 'xaa.dat'
TRUNCATE
INTO TABLE pwned
(HASH terminated by ':',COUNTS )
```

Note: File *xaa.dat* is a file with only 50m rows, created using ‘split’ command in Unix.
Replace with *pwned-passwords-ordered-2.0.txt* if you wish.

So, how to do it from APEX?

Load data in database

- Steps to load in Database
- 5. Load the data files using SQLLoader

```
$ sqlldr userid=schema/password control=loader1.ctl bad=loader1.bad direct=TRUE
```

So, how to do it from APEX?

Load data in database

- Steps to load in Database
- 6. Update the statistics

Trust me… you want this:

```
SQL> ANALYZE TABLE schema.pwned ESTIMATE STATISTICS;
SQL> ANALYZE TABLE schema.pwned ESTIMATE STATISTICS for all indexes;
```

*I could provide technical details and metrics if you're interested.. (not relevant for this presentation material)

So, how to do it from APEX?

- There are a few steps and you’ll decide what works best in your case.
- These are steps I used to load and make it available via APEX.

- I used two different approaches:

1. Load data in database
2. **Load data in text files on the Operating System** as regular text files
3. External tables – (is not viable as its way too slow to be productive)

So, how to do it from APEX?

Load data in text files on the Operating System

- The previous step you actually created the files that we'll search on
- 1. Download the files from Troy Hunt's website:
  - *I used CentOS so you adjust as needed based on your OS and/or distro*

Note: You'll need 45GB of free space for this space to complete successfully.

As root:

```
yum install -y p7zip
mkdir /pwned
chown oracle:dba /pwned
cd /pwned
wget https://downloads.pwnedpasswords.com/passwords/pwned-passwords-ordered-2.0.txt.7z
7za e pwned-passwords-ordered-2.0.txt.7z
```

So, how to do it from APEX?
Load data in text files on the Operating System

- Create the Script to search in the operating system
  - *(Full Script to be posted in Github)*
- Enable the database server to execute Operating System commands
- Make the appropriate calls from the APEX Application to execute OS Commands/Scripts
  - *All this will be part of a future meetup/blog*

So, how to do it from APEX?

Load data in text files on the Operating System

- Personally I prefer this way as it doesn't grow the database increasing the size of backups, recoveries and potentially flushing valuable cache in searching.
  - *This data is 100% static, seriously consider if you want it in the database*
- Response time is smoking fast!!
  - *501,636,842 rows in total*
  - *Time to search: ~180ms*
  - *Note: For the kind of search the data must be sorted, which it is.*
- You don't believe me??

  It's Demo time!

Summary

- It’s bad news that our email, password, etc. are available to cybercriminals
- Be positively reactive and get a password manager and change your passwords!
- For new accounts be proactive and create passwords from the password manager
- Help your users and Family
  - *We are all in this, cybercriminals will take advantage of anyone.*

With APEX I have shown you how to help your users identify if their passwords have been compromised.

External Tables

- Way too slow for this volume, we’re talking minutes per search
- Here are the steps if you’re really keen and need to prove your DBA wrong (cause you know they’ll ask if you tried external tables)

```
sqlplus sys as sysdba

SQL> grant create any directory to oos_user;    (oos_user is my schema owner in APEX)


sqlplus oos_user/password

SQL> create or replace directory pwned_dir as '/u01/app/oracle/pwned';
```

External Tables (cont.)

```
sqlplus oos_user/password



CREATE TABLE  pwned_ext
   (              hash CHAR(41), COUNTS NUMBER    )
ORGANIZATION EXTERNAL (
  TYPE ORACLE_LOADER
  DEFAULT DIRECTORY pwned_dir
  ACCESS PARAMETERS (
    RECORDS DELIMITED BY NEWLINE
  )
  LOCATION (‘pwned-passwords-ordered-2.0.txt')
)
PARALLEL 5
REJECT LIMIT UNLIMITED;
```

External Tables

- As oos_user

```
SQL> select * from oos_user.pwned_ext where hash like 'FFFFF4D7A686D1C2515B7A26A3B7E5E1FB802F4C%';

HASH

----------------------------------------

FFFFF4D7A686D1C2515B7A26A3B7E5E1FB802F4C
```

Elapsed: **00:02:25.61 <-This is pretty consistent as it has to read all 300+million rows**

This way too long..

Sequential Scan on 300+million rows via Oracle_OCI layer..

What did you expect??