

How to secure APEX applications

- Vidar Andersen
Espen Brækken

Senitel Consulting AS
<http://www.senitel.no>

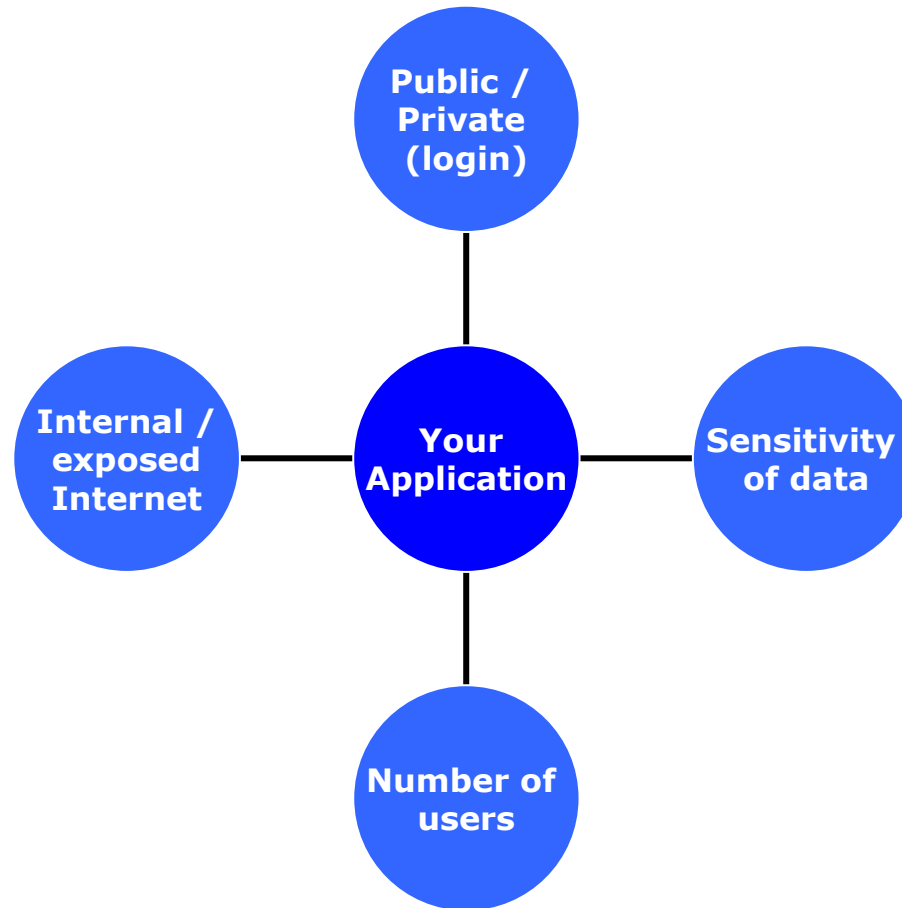
AGENDA

- Introduction – Senitel Consulting
- Consider your needs
- Authorization schemas
- Session State Protection
- Validations (Client/Server)
- Handling user input
- Virtual Private Database (VPD)
- Apex exports – Not only backup
(APEXExport Utility, SVN combination)

Senitel Consulting AS

- Established 1996 with focus on Oracle
- Owned by employees
- Focus
 - Web development (Oracle Application Express)
 - Data warehouse / BI solutions
 - Database
 - Training and workshops
 - Oracle licensing

Consider your needs



Authorization schemas

- What are they
- How to use them
- Where to use them
- Why are they so important
(*e.g. javascript:doSubmit('DELETE');*)

Demonstration

Session State Protection

- Used to prevent URL tampering
- How?

Documentation:

http://download.oracle.com/docs/cd/E14373_01/apirefs.32/e13369/apex_util.htm#CDEIBCJD

```
http.p(APEX_UTIL.PREPARE_URL(
  p_url => 'f?p='
    || :APP_ID
    || ':10:'
    || :APP_SESSION
    || '::NO::P10_ITEM:NEW_VALUE');
```

Even easier (in SQL statements etc) - create your own function:

```
function makeUrlChecksum (
  p_page_id          varchar2 default null
  , p_item_name      varchar2 default null
  , p_value          varchar2 default null
) return varchar2 (...)
```

Demonstration

Validations (Client / Server)

- Client validations (JavaScript)
(also HTML "disabled" and CSS styles)
- Server validations (Apex validations, constraints)

Usage, Pros & Cons

Demonstration

Handling user input

- SQL Injection
 - Affecting dynamic queries
 - Bad handling of input may put entire db-schema at risk.

- Cross Site Scripting (XSS)
 - What is it
 - How to stop it

Demonstration

Virtual Private Database (VPD)

- Apply extra filtering conditions to a query, based on user logged in.
- License: Requires Enterprise Edition of DB.

Apex exports – not only backup

- Automate application exports with APEXExport java utility (bundled with APEX install)
`java APEXExport -db db01.database.no:1521:db_sid -user senitel -password pass123 -applicationid 103`
- Automatically check into e.g. SVN repository (*crontab, at* etc)
- Compare revisions of application exports.



Revision 874

11/38

Working Copy

<pre> p_field_alignment => 'LEFT', p_is_persistent=> 'Y', p_item_comment => '); end; / begin declare p varchar2(32767) := null; l_clob clob; l_length number := 1; begin p:=p 'begin' chr(10) ' ba_bonus_admin.keep_this_customer(' chr(10) ' p_kortnr => :P4_KORTNR' chr(10) ' ,p_kontonr => :P4_KONTONR);' chr(10) 'end;'; wwv_flow_api.create_page_process(p_id => 1138806346620093 + wwv_flow_api.g_id_offset, p_flow_id=> wwv_flow.g_flow_id, p_flow_step_id => 4, p_process_sequence=> 10, p_process_point=> 'AFTER_SUBMIT', p_process_type=> 'PLSQL', p_process_name=> 'Clean dupe', p_process_sql_clob => p, p_process_error_message=> '', p_process_when=> 'KEEPONE', p_process_when_type=> 'REQUEST_EQUALS_CONDITION', p_process_success_message=> '', p_process_is_stateful_y_n=> 'N', p_process_comment=> ''); end; null; end; / begin ----- -- ...updatable report columns for page 4 </pre>	<pre> 2642 2643 2644 2645 2646 2647 2648 2649 2650 2651 2652 2653 2654 2655 2656 2657 2658 2659 2660 2661 2662 2663 2664 2665 2666 2667 2668 2669 2670 2671 2672 2673 2674 2675 2676 2677 2678 2679 2680 2681 2682 2683 2684 2685 2686 2687 2688 2689 2690 2691 2692 </pre>	<pre> end; / begin declare p varchar2(32767) := null; l_clob clob; l_length number := 1; begin p:=p 'begin' chr(10) ' ba_bonus_admin.keep_this_customer(' chr(10) ' p_kortnr => :P4_KORTNR' chr(10) ' ,p_kontonr => :P4_KONTONR);' chr(10) 'end;' chr(10) ' chr(10) 'begin' chr(10) ' null;' chr(10) ' -- Code added shows up like this!' chr(10) 'end;'; wwv_flow_api.create_page_process(p_id => 1138806346620093 + wwv_flow_api.g_id_offset, p_flow_id=> wwv_flow.g_flow_id, p_flow_step_id => 4, p_process_sequence=> 10, p_process_point=> 'AFTER_SUBMIT', p_process_type=> 'PLSQL', p_process_name=> 'Clean dupe', p_process_sql_clob => p, p_process_error_message=> '', p_process_when=> 'KEEPONE', p_process_when_type=> 'REQUEST_EQUALS_CONDITION', p_process_success_message=> '', p_process_is_stateful_y_n=> 'N', p_process_comment=> ''); end; null; end; / begin ----- -- ...updatable report columns for page 4 </pre>
---	---	---

Q & A

Any questions?

Presentation, source code and demo
application available at

http://www.senitel.no/OUGN/apex_secure.zip