



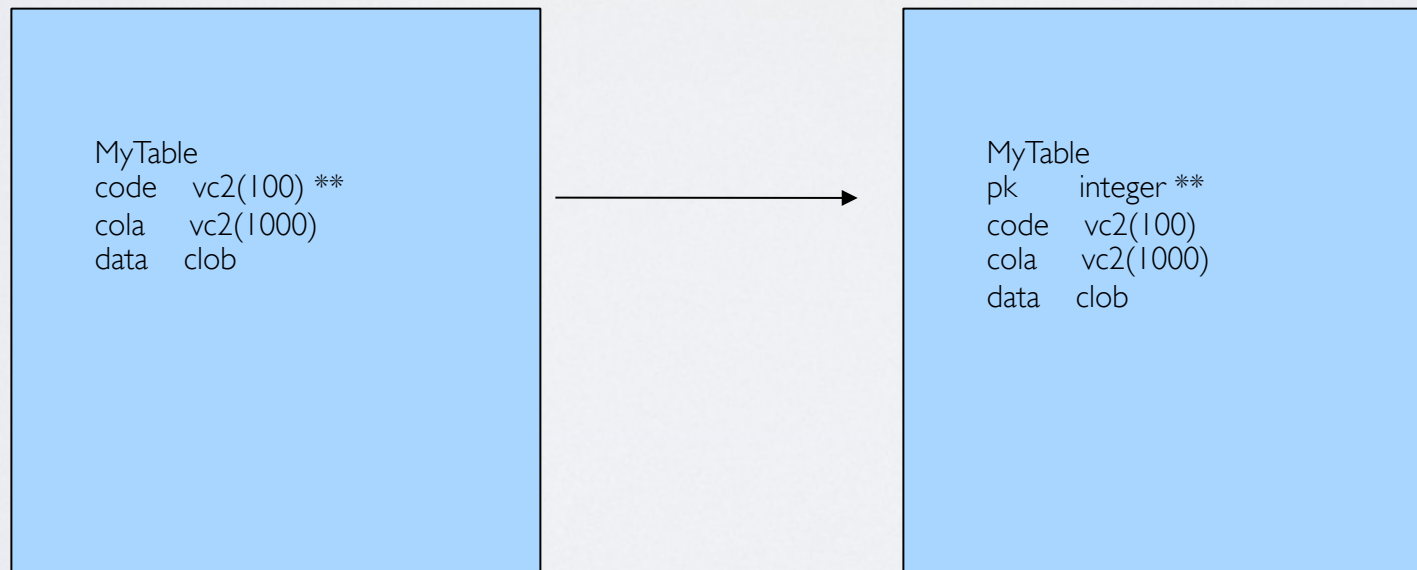
Building Secure Multimedia Web Applications: Tips and Techniques

Marcel Kratochvil
Piction CTO



- Image in the database or not?
- What is the real security threat?
 - Hacking
 - Unauthorised Access (un/pw)
 - Data Protection (be able to recover)
 - DRM – subsequent access
 - Social Engineering
 - Management
- Paranoia vs flexibility

- Code Injection
- Primary Key
- URL Encryption



Code Example

```
function encrypt_data( input_string in integer )
  return varchar2
as
  raw_input          raw(256);
  raw_key             raw(256);
  encrypted_raw       raw(2048);

  begin
    raw_key := utl_raw.cast_to_raw('MYKEY012');
    raw_input := utl_raw.cast_to_raw(substr(rpad(to_char(input_string),16,'
'),1,16));
    dbms_obfuscation_toolkit.desencrypt(input => raw_input, key => raw_key,
encrypted_data => encrypted_raw );
    return( rawtohex(encrypted_raw) );

  exception
  when others
  then
    return( NULL );
end encrypt_data;
```





WebServer

- DAD Configuration
- Embedded Gateway
- SSL
- SSO
 - LDAP

Example

Embedded Gateway

```
alter user anonymous ACCOUNT UNLOCK;

select * from dba_role_privs where granted_role = 'XDBADMIN';

DECLARE
  v_cfg XMLType;
BEGIN
  SELECT updateXML(DBMS_XDB.cfg_get(),
    '/xdbconfig/descendant::ftp-port/text()', '2121',
    '/xdbconfig/descendant::http-port/text()', '80')
    INTO v_cfg FROM DUAL;
  DBMS_XDB.cfg_update(v_cfg);
  COMMIT;
END;
/
```

```
exec dbms_epg.drop_dad( 'PICTION' );
```

```
exec dbms_epg.create_dad( 'PICTION','/w2k10g/*' );
```

```
exec dbms_epg.set_dad_attribute( 'PICTION','database-username'
```

```
exec dbms_epg.set_dad_attribute( 'PICTION','authentication-mo
```

```
exec dbms_epg.set_dad_attribute( 'PICTION','error-style','Dek
```

```
exec dbms_epg.set_dad_attribute( 'PICTION','session-state-mar
```

```
'StatelessWithFastResetPackageState');
```

```
exec dbms_epg.set_dad_attribute( 'PICTION','exclusion-list','
```

```
exec dbms_epg.set_dad_attribute( 'PICTION','exclusion-list','
```

```
exec dbms_epg.set_dad_attribute( 'PICTION','exclusion-list','
```

```
exec dbms_epg.set_dad_attribute( 'PICTION','exclusion-list','
```

```
exec dbms_epg.set_dad_attribute( 'PICTION','exclusion-list','
```

```
exec dbms_epg.set_dad_attribute( 'PICTION','exclusion-list','
```

```
exec dbms_epg.set_dad_attribute( 'PICTION','exclusion-list','
```

```
exec dbms_epg.set_dad_attribute( 'PICTION','document-table-na
```

```
'APACHE_OWS_CONTENT');
```

```
exec dbms_epg.authorize_dad( 'PICTION','WEBSYS');
```

```
commit;
```

Apache Gateway

- Default security is built in

```
<Location /ram>
    SetHandler pls_handler
    Order deny,allow
    Allow from all
    AllowOverride None
    PlsqlDatabaseUsername          ram
    PlsqlDatabasePassword          @BfCDiK8XK
    PlsqlDatabaseConnectString    VNLB
    PlsqlAuthenticationMode       Basic
    PlsqlDefaultPage              ram.gl.default
    PlsqlDocumentTablename        ram.apache_ow
</Location>
```

dads.conf

httpd.conf

Alias /icons/ "P:\abc\images/"

```
<Directory "P:\abc\images/">  
    Options Indexes MultiViews  
    AllowOverride None  
    Order allow,deny  
    Allow from all  
</Directory>
```

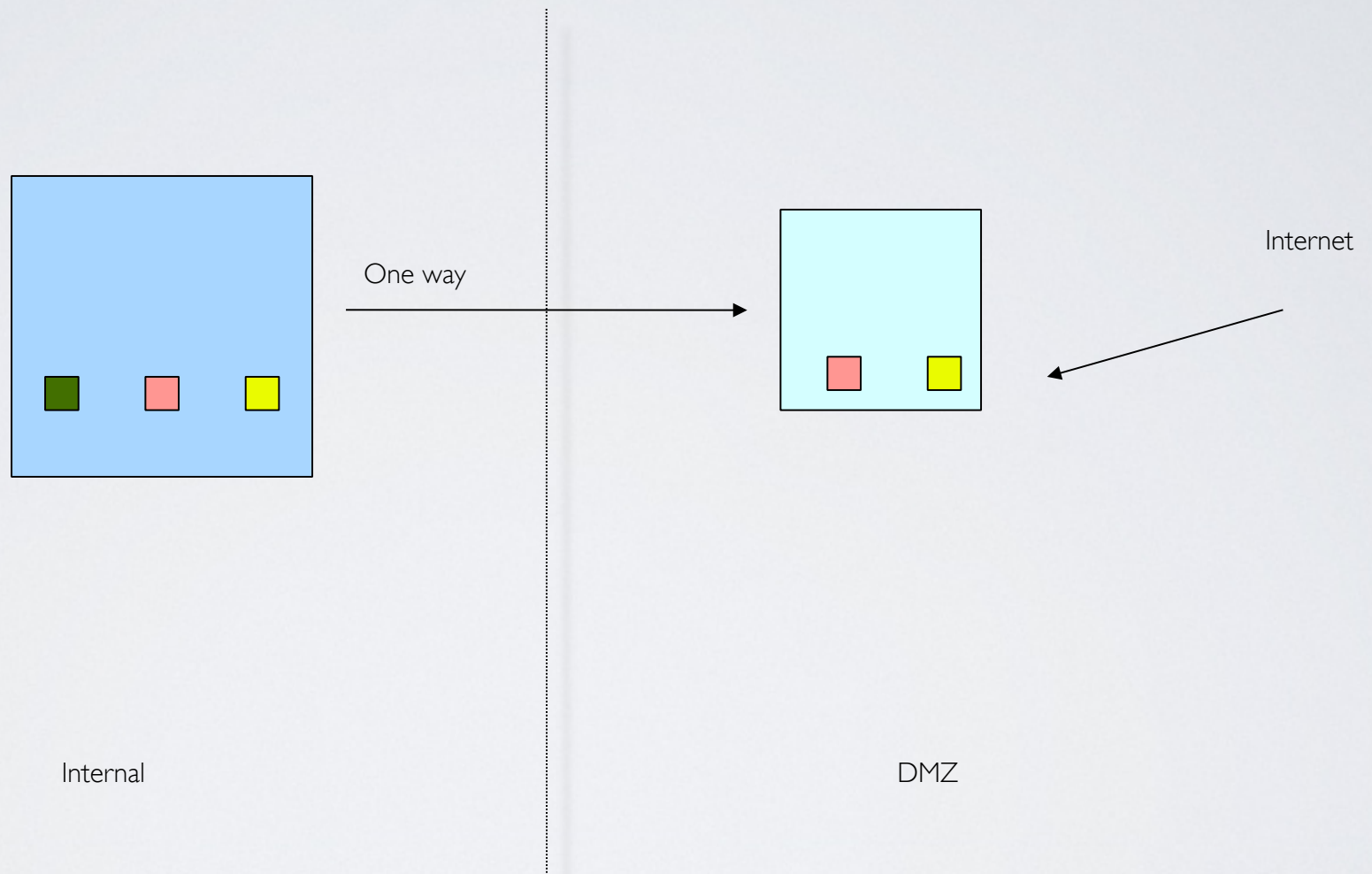


Database

- Replication
 - DMZ
- Loading
 - Ftp, ssh, firewalls
- Metadata
- Delivery
- Encryption
- Backups
 - rman



Example





Post Download

- DAM
- DRM
- Purchase
- Ownership
- Watermarking



Real World Review

- Experiences with Piction
- Photographers
- Museums
- Print Media
- Education
- Defence



VISION
DIGITAL IMAGE SYSTEMS



Further information:

marcel@piction.com

www.piction.com

www.eternal-donut.com

