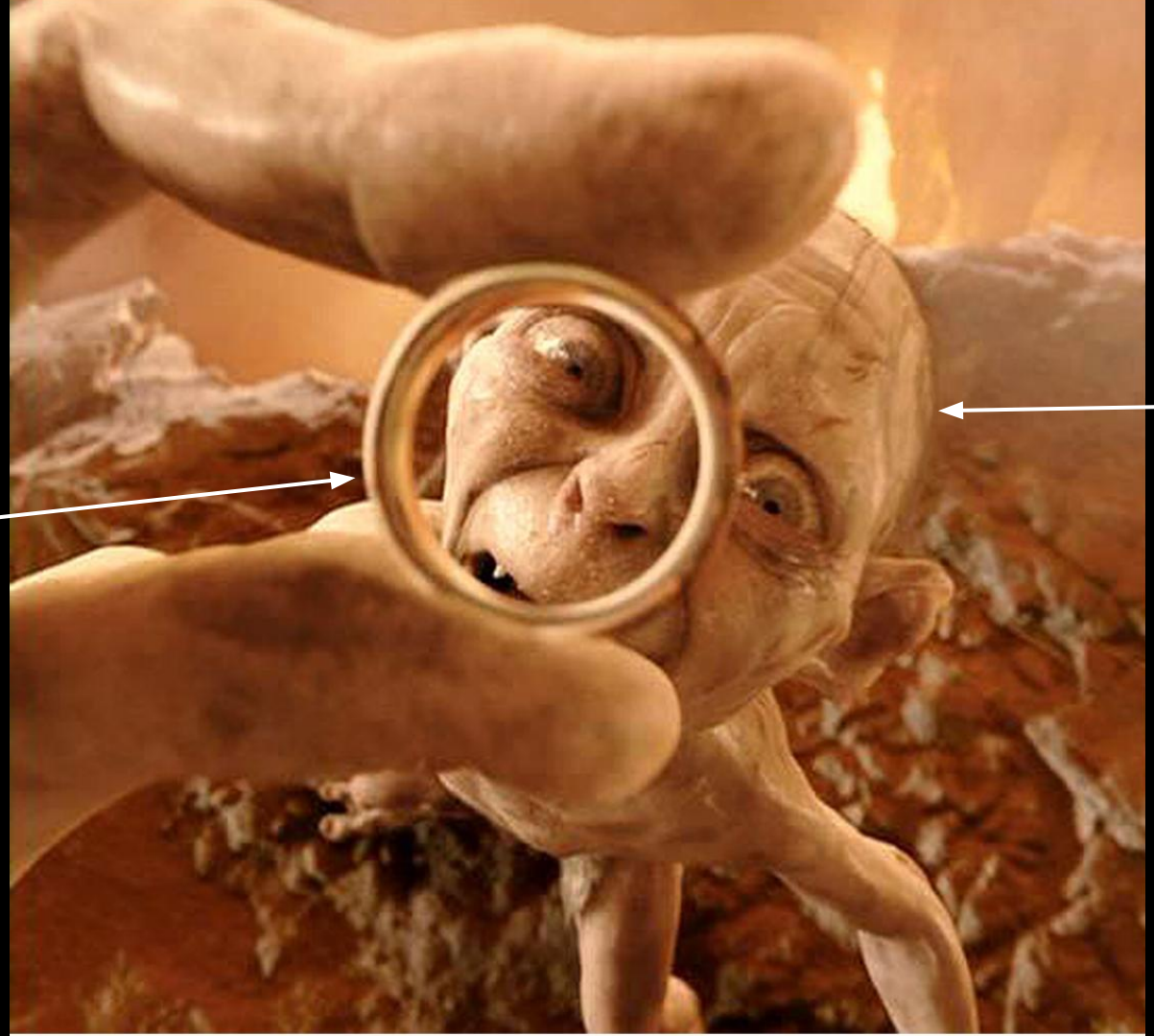
El Framework De La Muerte

Disclaimer

WIZACHA.COM

Benoit Viguier
@b_viguier


CTO
CEO


Framework
Agence
Web

Les bases

C’est le premier pas qui coûte

WDF Webkit Data Framework (?)

- *Méta* format pour la génération des fichiers
- Peut mélanger WDF, Php, Js et Html
- Analyse *offline* en bash > *Méta Php*
- Analyse *online* en Php > Php
- Pas de cache (jamais)

```
// Use common boxes code
@include(../Element.wdf)


#php
// Export fragment for script
$block->exportFragment("click");
$real_block_id = $block->getRealId();

if ( ! isset($link) )
{
    $link = "";
}

$extra_js = "";
if ( substr($link, 0, 3) == "js:" )
{
    $extra_js = substr($link, 3);
    $link = "#";
}
```

```
#js
$(function()
{
     // On click block
     $("#@{block->getRealId("-")}").click
(function()
     {
     // Call associated fragment
     //$block.callFragment("click");
     //$fragments["@{real_block_id."/click"}"]();
     $block = "@{real_block_id}";
          WebKit.Block.callFragment("@{block-
>getRealId()}", "click");

     @{extra_js}
     });
});

#html
@if(isset($class) && $class=="special-text-align-
right")
<p style="text-align: right;">
@end
```

Templating

- M(VC)
- Fichiers de contrôleurs inclus (procédural)
- Templating basé sur le système de fichier
- Importance des dossiers vides
- Des chemins de plus de 256 caractères
- Surcharge possible depuis un autre dossier

Base de données

La clé de voûte

" OR 1;#

Les bases

- Injection SQL
- Mots de passe non chiffrés
- Données échappées aléatoirement

évitons les banalités….

ORM

Objet

Parent

Child children[];

Child

...

SQL like

Parent

int parent_id

Child

int child_id
int parent_id

WDF

Parent

int parent_id;
string children;

Child

int child_id

On n’y pense pas assez...

- #address, #identifier
- Merchant@, Image@
- Messages[@], Roles[@]
- From, To

Gestion des connexions

```
public function execute($expression)
{
    $base = $this->getBase();
    $base->connect();
    $result = $base->sql($expression);
    $rets = array();
    while ( $row = mysql_fetch_assoc($result) )
    {
        $rets[] = $row;
    }
    $base->disconnect();
    return $rets;
}
```

Scalabilité

Le code

Le retour du roi

Polymorphisme

```
if ( $object instanceof Hook ) {
}
else if ( $object instanceof Service ){
}
else if ( $object instanceof Task ){
}
else if ( $object instanceof Page ){
}
else if ( $object instanceof Module ){
}
else if ( $object instanceof Site ){
}
else if ( is_array($object) ){
}
```

Eval

```
foreach ($parameters as $__key => $__value)
{
    $line = '$' . $__key . ' = ' . '$parameters["' . $__key .'"];' . "\n";
    eval($line);
}
```

Upload de fichiers

```
$fileParts     = pathinfo($_FILES['Filedata']['name']);
$fileType      = $_POST['fileType'];
$imageWidth    = $_POST['imageWidth'];
$imageHeight   = $_POST['imageHeight'];

$fileTypeExts = str_replace(array("*.", "", " "), "", $_POST['fileTypeExts']);
$fileTypes    = explode(";",$fileTypeExts);
if ( in_array($fileParts['extension'], $fileTypes) )
{
  $tempFile    = $_FILES['Filedata']['tmp_name'];
  move_uploaded_file($tempFile, $upload_df);
  //...
}
```

No Comment

Conclusion

Que faire ?

Destruction

“le cœur des hommes est aisément corruptible et l’anneau de pouvoir a sa volonté propre”

Merci !

Questions ?