La faille include.

```
Inutile en PHP5 si l'option "allow_url_fopen" est à "OFF". Le but est de controler
la présence d'un fichier include demandé dans le formulaire.

if(isset($_GET['page']) AND file_exists($_GET['page'].'.php'))
{  include $_GET['page'].'.php';
}
else
{  include 'accueil.php';
}
```

La faille SQL injection.

```
Il faut éviter qu'un champ puisse détourner une requete SQL (par ajout d'une
condition " or 1 = 1 ").

En premier, on inactive les guillemets magiques pour tout les objets reçus (Get /
Post / Cookie).

//
// -- Inactivation Magic Quotes
//
if(get_magic_quotes_gpc()===1)
{  if (isset($_POST['login'])) { $_POST['login'] = stripslashes($_POST['login']);
}
   if (isset($_POST['passe'])) { $_POST['passe'] = stripslashes($_POST['passe']);
}
}
Les données encapsulées dans un ordre SQL sont protégées.

//
// Préparation d'un ordre MySQL
//
..
$sql .= ", Var01 = '" . mysql_real_escape_string($Var01, $link) . "' " ;
$sql .= ", Var02 = '" . mysql_real_escape_string($Var02, $link) . "' " ;
$sql .= ", Var03 = '" . mysql_real_escape_string($Var03, $link) . "' " ;
$sql .= ", Var04 = '" . mysql_real_escape_string($Var04, $link) . "' " ;
..
```

La faille du code HTML et des formulaires.

```
Le code html présent dans des champs lus doit être inactivé.

echo '<tr>' ;
echo '<td>'.htmlentities($row['JourEVT']).'</td>'."\n"  ;
```

```
echo '<td>'.htmlentities($row['JourAlertEVT']).'</td>'."\n"   ;
echo '<td>'.htmlentities($row['Libelle']).'</td>'."\n"   ;
echo '<td>'.htmlentities($row['Type']).'</td>'."\n" ;
echo '</tr>' ;
```

Exemple réception de données (pour GET, POST, Cookie).

```
Exemple de réception de donnée alphanumérique sécurisé.

$variabl = '' ;
if (isset($_GET['variabl']))
{  $variabl = (get_magic_quotes_gpc()===1) ? stripslashes($_GET['variabl']) :
$_GET['variabl'] ;
   $variabl = trim($variabl) ;  // facultatif
}
Exemple de réception de donnée numérique sécurisé.

$variabl = '' ;
if (isset($_GET['variabl']))
{  $variabl = (get_magic_quotes_gpc()===1) ? stripslashes($_GET['variabl']) :
$_GET['variabl'] ;
   $variabl = intval(trim($variabl)) ;  // facultatif
}
```