SÉCURITÉ DES SERVEURS ET DES APPLICATIONS

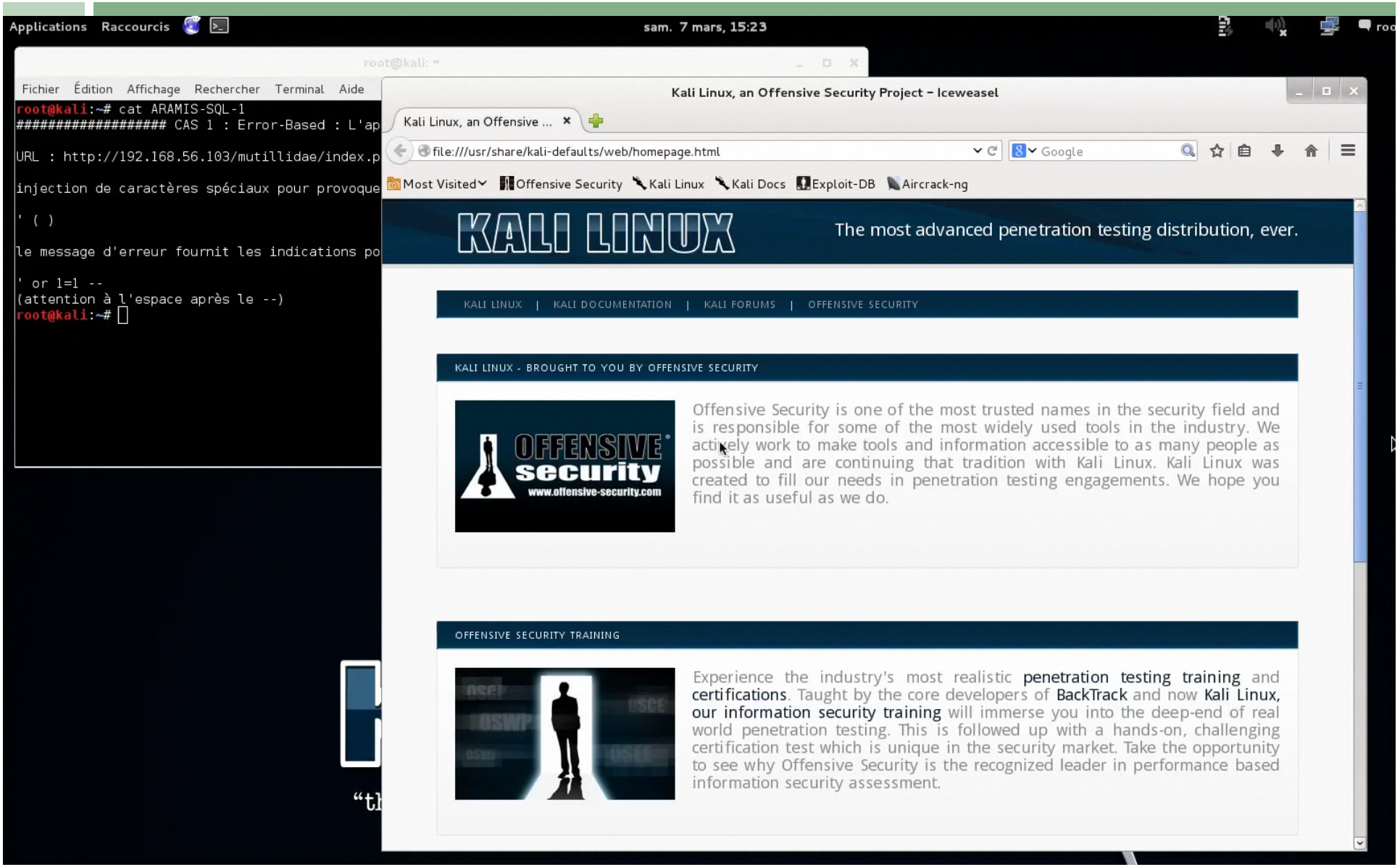
Injections SQL

K. Poutrain

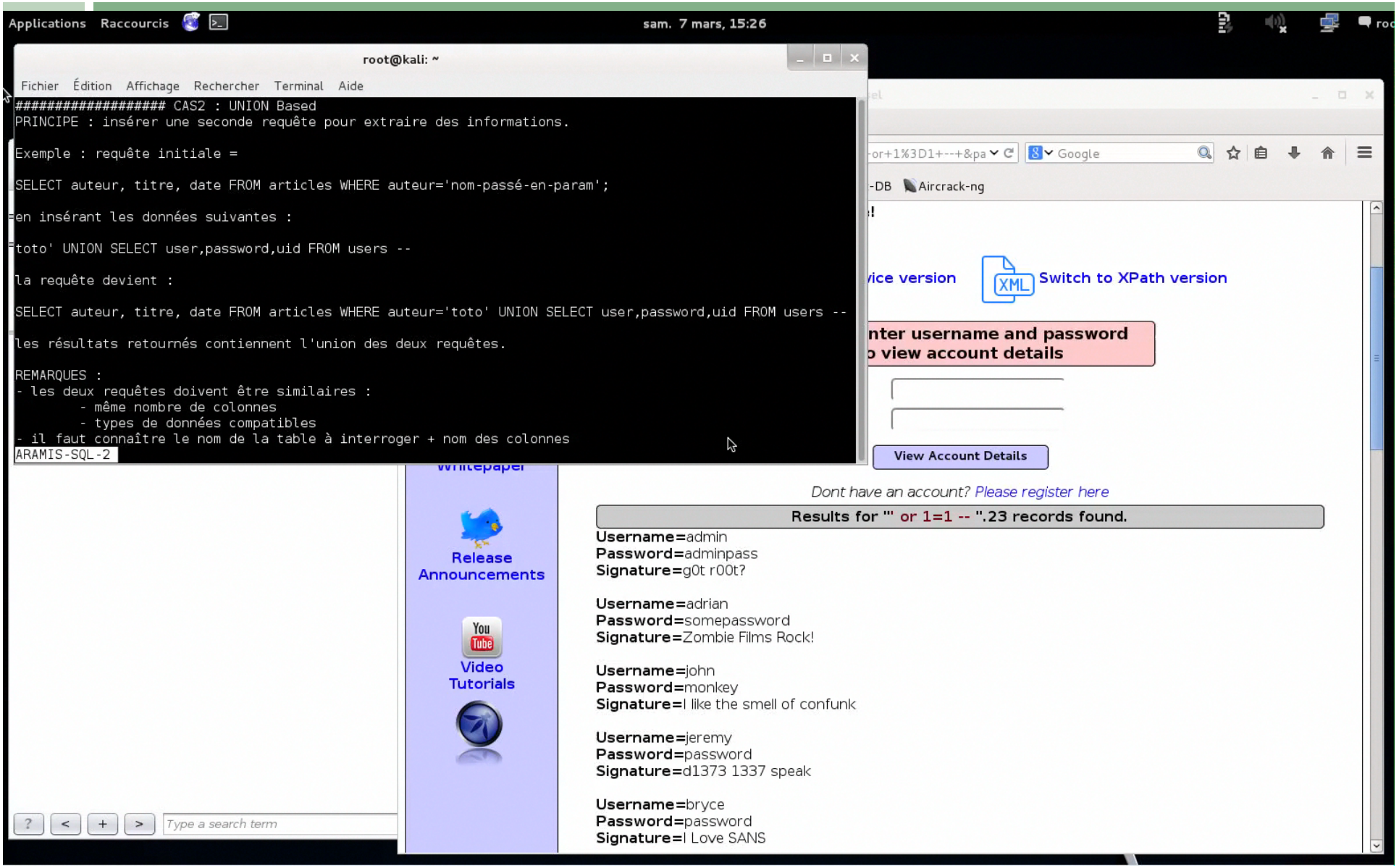
02/04/2015

7ème journée du réseau ARAMIS – Lyon

Injections SQL : ERROR-Based

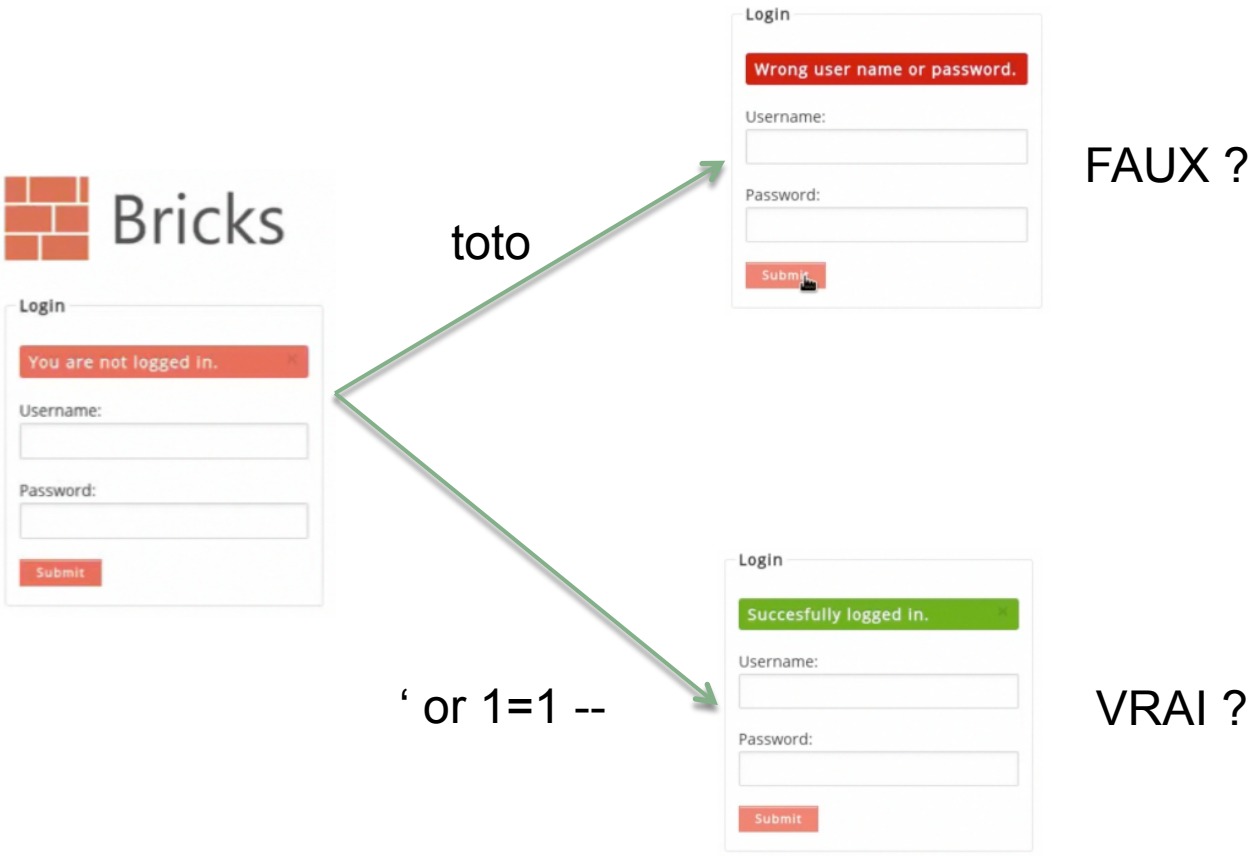


Injections SQL : UNION



Injections SQL : BOOLEAN BLIND

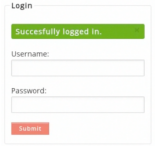
Aucun affichage de données utilisateur : injection aveugle.



Injections SQL : BOOLEAN BLIND

Confirmation du comportement booléen de l'application :

```
' or ascii(mid('abc',1,1)) = 97 --
```



VRAI !

```
' or ascii(mid('abc',1,1)) = 98 --
```

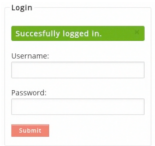
FAUX !

Premier caractère du nom de la base ?

```
' or ascii(mid(database(),1,1)) = 97 --
```

a

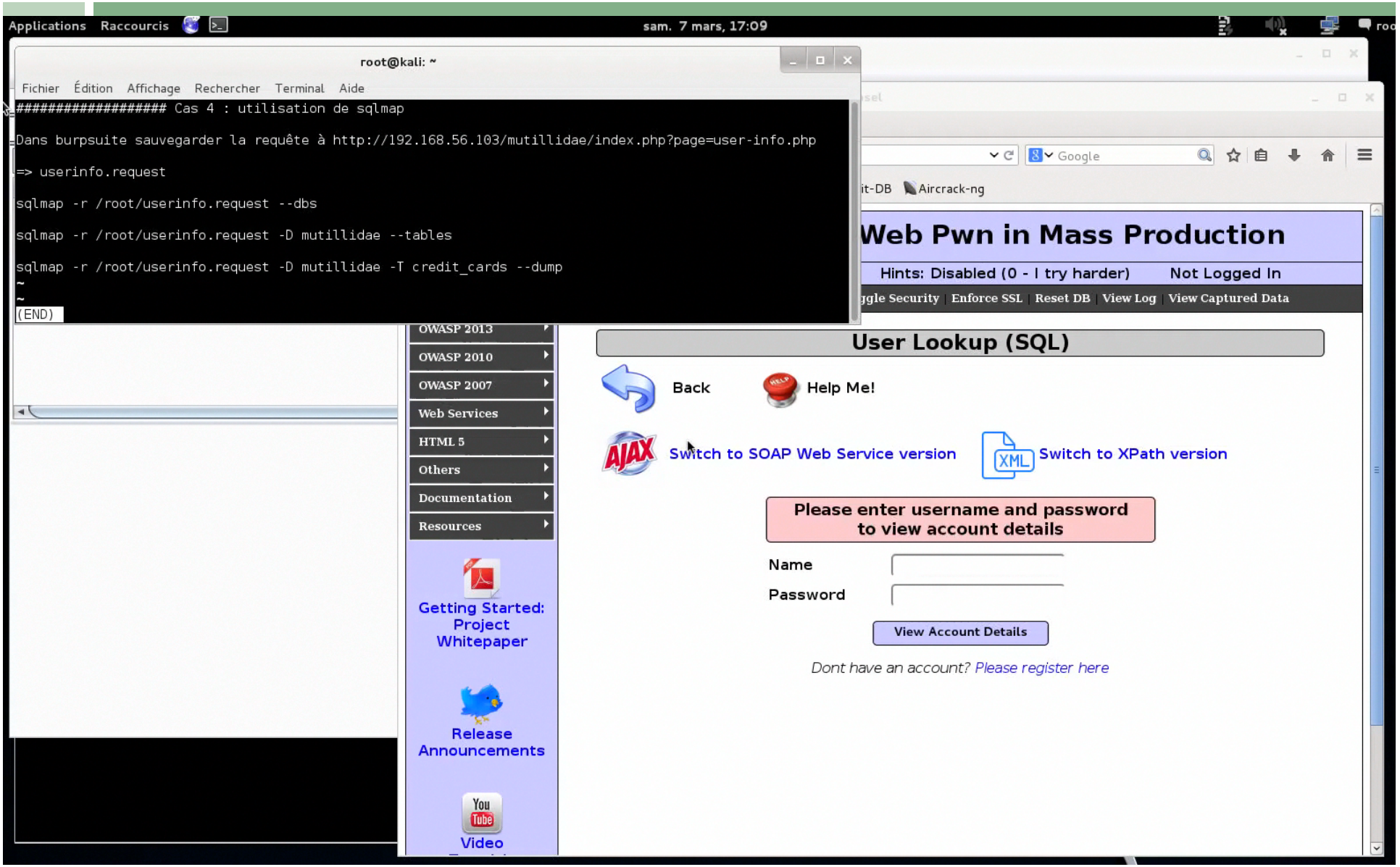
```
' or ascii(mid(database(),1,1)) = 98 --
```



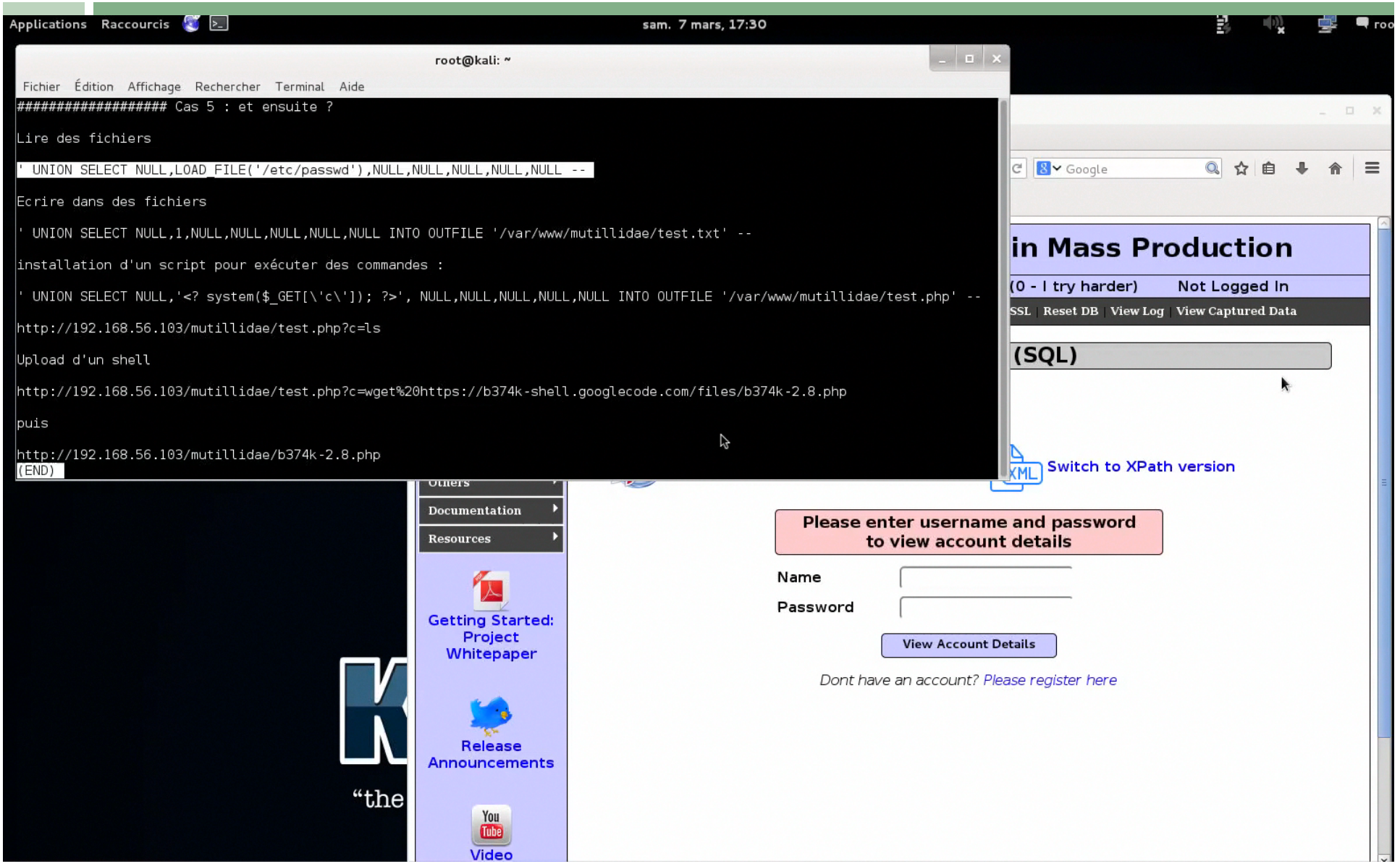
b

Etc... À automatiser

Injections SQL : SQLMAP



Injections SQL : et ensuite ?



CONCLUSION

Remarque : on s'est placé ici dans un contexte d'attaque idéal :

- Application vulnérable ;
- Distribution vulnérable ;
- Serveur WEB et SGBD sur la même machine ;
- Pas de filtrage en entrée/sortie.

CONCLUSION

Mais : en informatique il existe toujours plusieurs façons de réaliser les choses !

Injection SQL impossible ? wget non disponible ? Filtrage en sortie ?
=> formulaire d'upload... Ou autre...

CONCLUSION

A retenir :

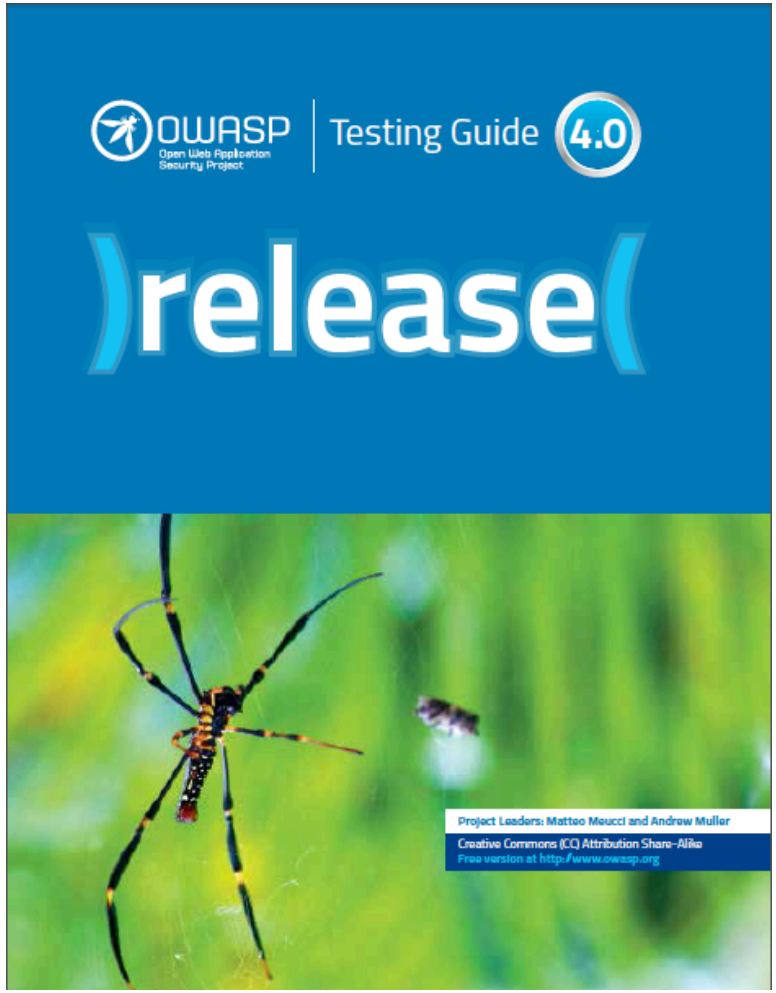
Un attaquant motivé sera méthodique, exhaustif.

Utilisera toutes les informations disponibles.

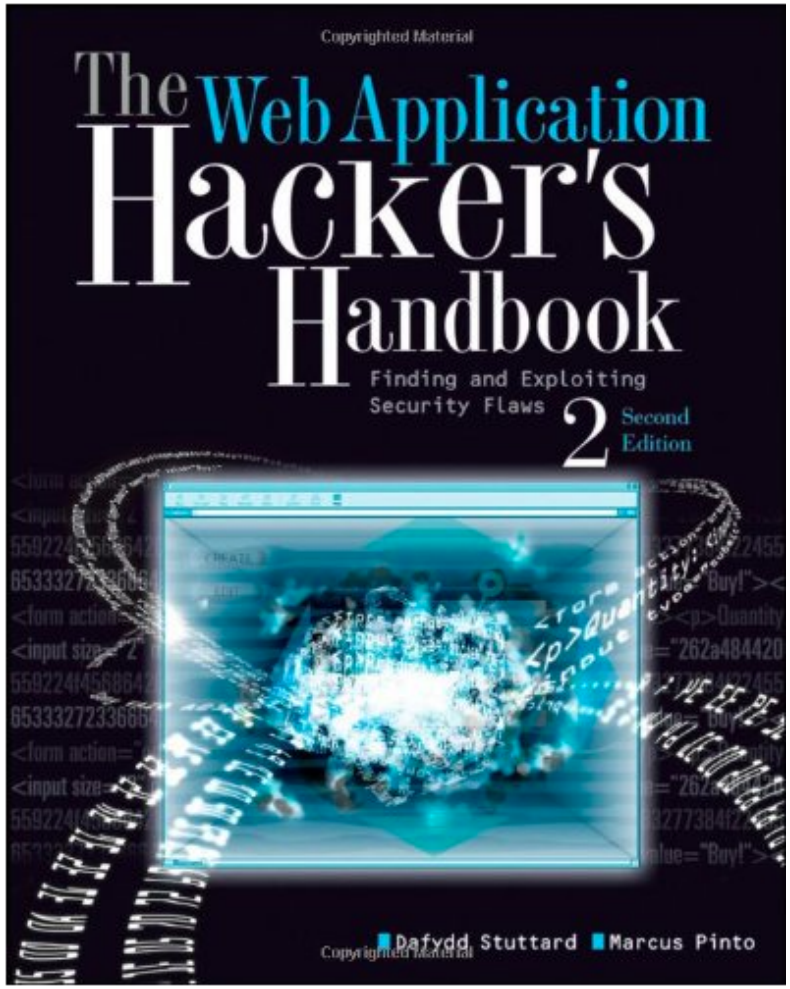
Exploitera la moindre faille.

Les conséquences ne se limitent pas à la vulnérabilité elle-même.

Références



https://www.owasp.org/index.php/Category:OWASP_Testing_Project



Rappel…

Vous êtes responsables de ce que vous faites…

But : connaître les attaques pour mieux se protéger.

N’attaquez que les serveurs dont vous êtes propriétaire, administrateur, hébergeur.

Attention : n’utilisez pas les techniques et outils d’attaque sur vos serveurs en production tant que vous ne maîtrisez pas leurs conséquences !

Merci ! Questions ?