Université
De Boumerdes

Université
De Limoges

Département d'informatique
M2

Les différents types de vulnérabilités

Réalisé par : Dr RIAHLA
Docteur de l'université de Limoges (France)
Maitre de conférences à l'université de Boumerdes

Université
De Boumerdes

Université
De Limoges

Département de physique/Infotronique
IT/S6

Vulnérabilités applicatives

Réalisé par : Dr RIAHLA

2008/2009

Vulnérabilités applicatives

Beaucoup d'applications sont vulnérables dues à de la mauvaise programmation (par manque de temps, de motivation, …) ou volontairement (aménagement d'un point d'entrée, …).

- Services réseaux (daemons).
- Les applications téléchargées (applet java, …).
- Les applications web (scripts cgi, …).

Vulnérabilités applicatives

Les vulnérabilités peuvent être dues:

Backdoors: laissées volontairement ou involontairement sur un service par le programmeur

Erreurs de programmation

- Débordements de tampons (buffer overflow)
- Entrées utilisateurs mal validées
- Les problèmes de concurrence
- Chaînes de format

Université
De Boumerdes

Université
De Limoges

Département de physique/Infotronique
IT/S6

Buffer Overflow

Réalisé par : Dr RIAHLA

2008/2009

Buffer Overflow (Introduction)

```
int main (int argc, char **argv)
{
char buf [8] ;
strcpy (buf,argv [1]) ;
}
```

Exécution:

[root@austramine]$ *./demo aaaaaaaaaaaaaaaaaaaa*
Segmentation fault

Buffer Overflow (Introduction)

- La fonction principale d'un processeur est de traiter et de déplacer des données.

- Lors de ces traitements, le processeur a besoin d'un emplacement afin de sauvegarder rapidement les données traitées.

Buffer Overflow (Introcution)

- La taille des registres ne permet pas à ceux-ci de jouer ce rôle.

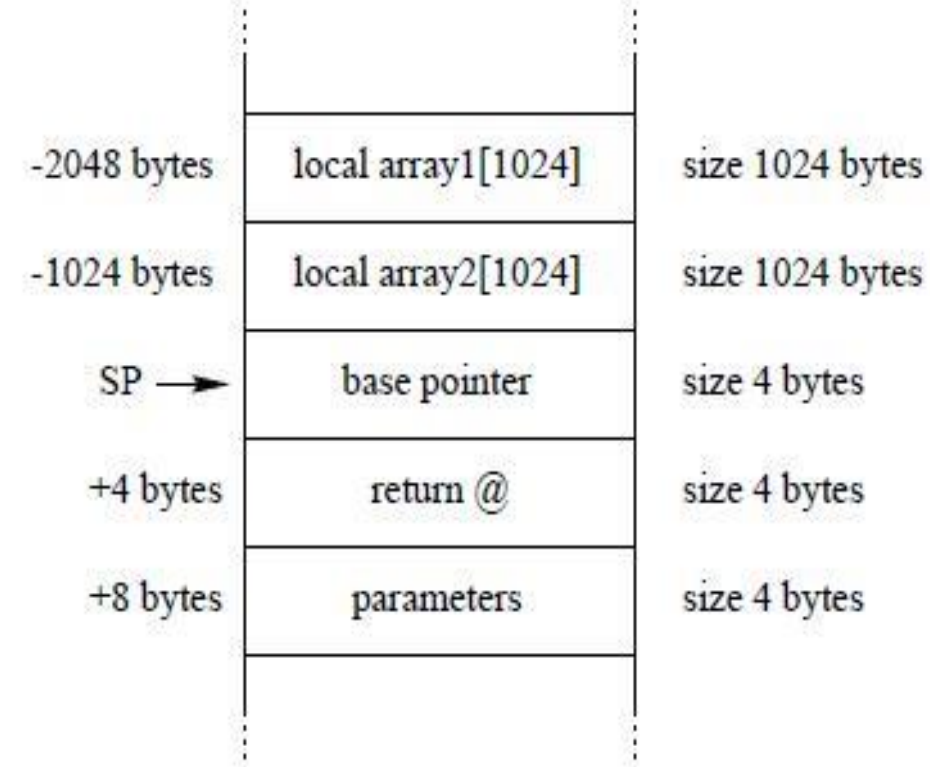
- Ces informations sont donc sauvées dans une zone mémoire appelées **pile**.

- Elle est stockée en mémoire à une adresse spécifique

Buffer Overflow (la pile)

Lors de l'exécution d'un programme qui fait appel a une procédure, le processeur sauve l'adresse de retour dans la pile, lorsque la procédure se terminera le processeur retournera à l'adresse spécifiée et continuera son travail...

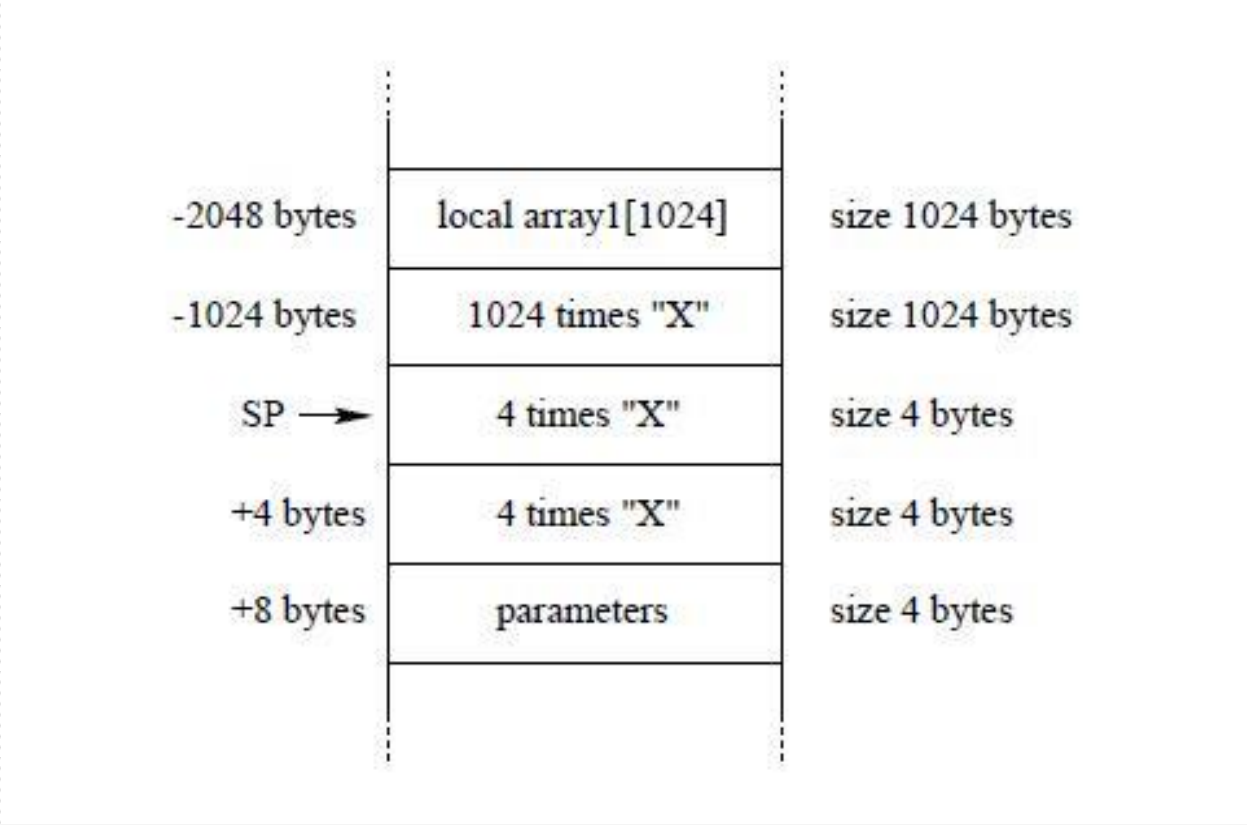
Buffer Overflow (Structure de la pile)



Buffer Overflow (Abuser l'adresse de retour)

Si (par hasard !) une procédure écrivait plus d'octets (bytes) dans une variable locale afin que la taille nécessaire à son stockage dans la pile dépasse celle de l'adresse de retour, on appellerait ceci un **Buffer Overflow**.

Buffer Overflow (Abuser l'adresse de retour)



1032 fois le caractère "X" dans le tableau local "array2"

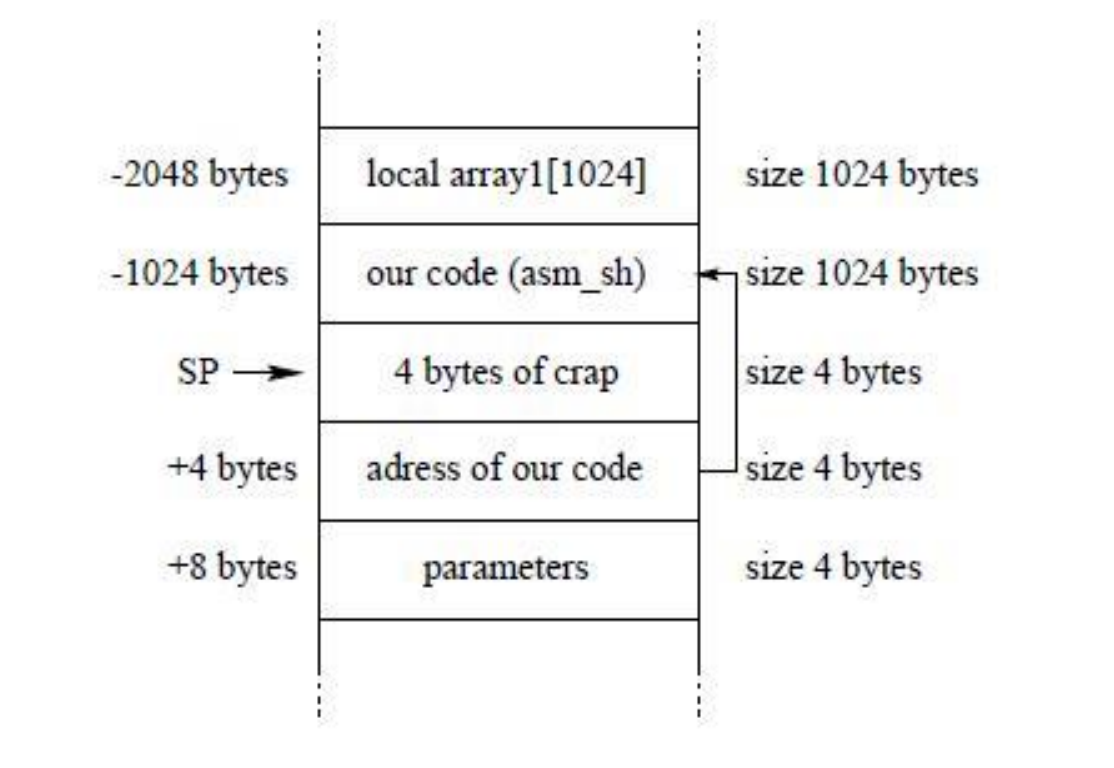
Buffer Overflow (Exploitation)

- Il est possible donc d'indiquer au programme une nouvelle adresse de retour contenant **un code totalement différent (code pirate).**

- Le programme sautera alors automatiquement à l'adresse spécifiée. . .

- Forcer le programme à sauter vers une adresse ou est situé un code assembleur destiné par exemple à exécuter un shell UNIX (**/bin/sh**).

Buffer Overflow (Exploitation)



Buffer Overflow (Pourquoi le langage C ?)

Beaucoup d'applications écrites en langage C sont vulnérables car la simplicité et l'efficacité de ce langage ont prévalu sur les contrôles d'intégrité laissés à la responsabilité du programmeur. Mais le problème existe également dans d'autres langages de programmation.

Université
De Boumerdes

Université
De Limoges

Département de physique/Infotronique
IT/S6

Attaques sur les applications web

Réalisé par : Dr RIAHLA

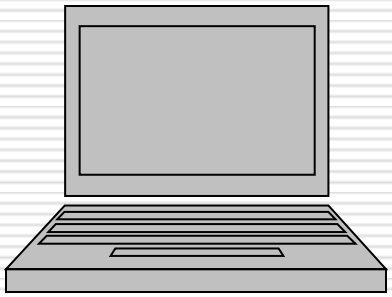
2008/2009

Attaques sur les applications web (Sites Web)

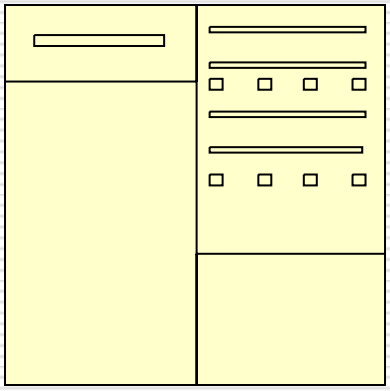
- Le nombre de sites web croît exponentiellement d'année en année : on compterait aujourd'hui plus de 185 millions de sites web à travers le monde,

- Les sites internet s'exposent naturellement aux attaques qui croient d'année en année.

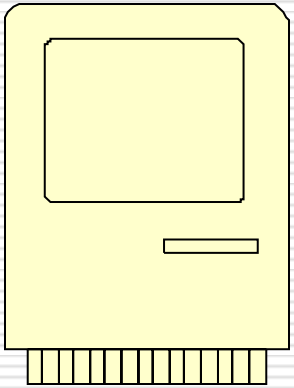
Attaques sur les applications web (Architecture 3 tiers)



Client



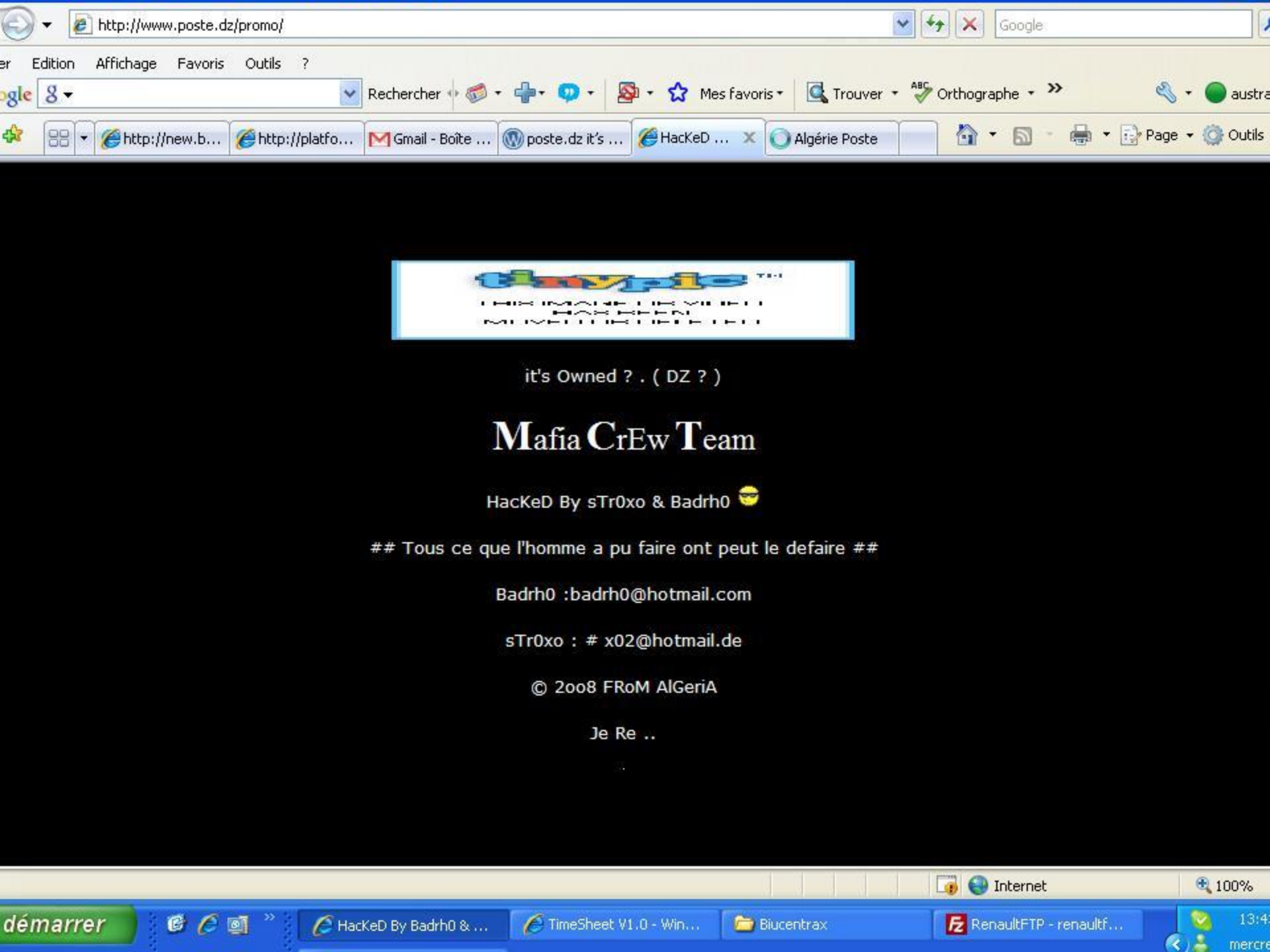
Server
D'application



Serveur de base de données

Attaques sur les applications web (Risques)

- Pertes de données par des actes malveillants
- Publication de données confidentielles
- Vol d'identité permettant à un pirate d'avoir un accès administrateur ou sur une zone payante.
- Les abus de ressources qui pourraient ralentir les services du site.
- Détournement de site


http://www.poste.dz/promo/
Edition Affichage Favoris Outils ?
Rechercher
Mes favoris
Trouver
Orthographe
http://new.b...
http://platfo...
Gmail - Boîte ...
poste.dz it's ...
HacKeD ...
Algérie Poste
Page
Outils
it's Owned ? . (DZ ?)
Mafia CrEw Team
HacKeD By sTr0xo & Badrh0
Tous ce que l'homme a pu faire ont peut le defaire
Badrh0 :badrh0@hotmail.com
sTr0xo : # x02@hotmail.de
© 2oo8 FRoM AlGeriA
Je Re ..
Internet
100%
démarrer
HacKeD By Badrh0 & ...
TimeSheet V1.0 - Win...
Biucentrax
RenaultFTP - renaultf...
mercre

Université
De Boumerdes

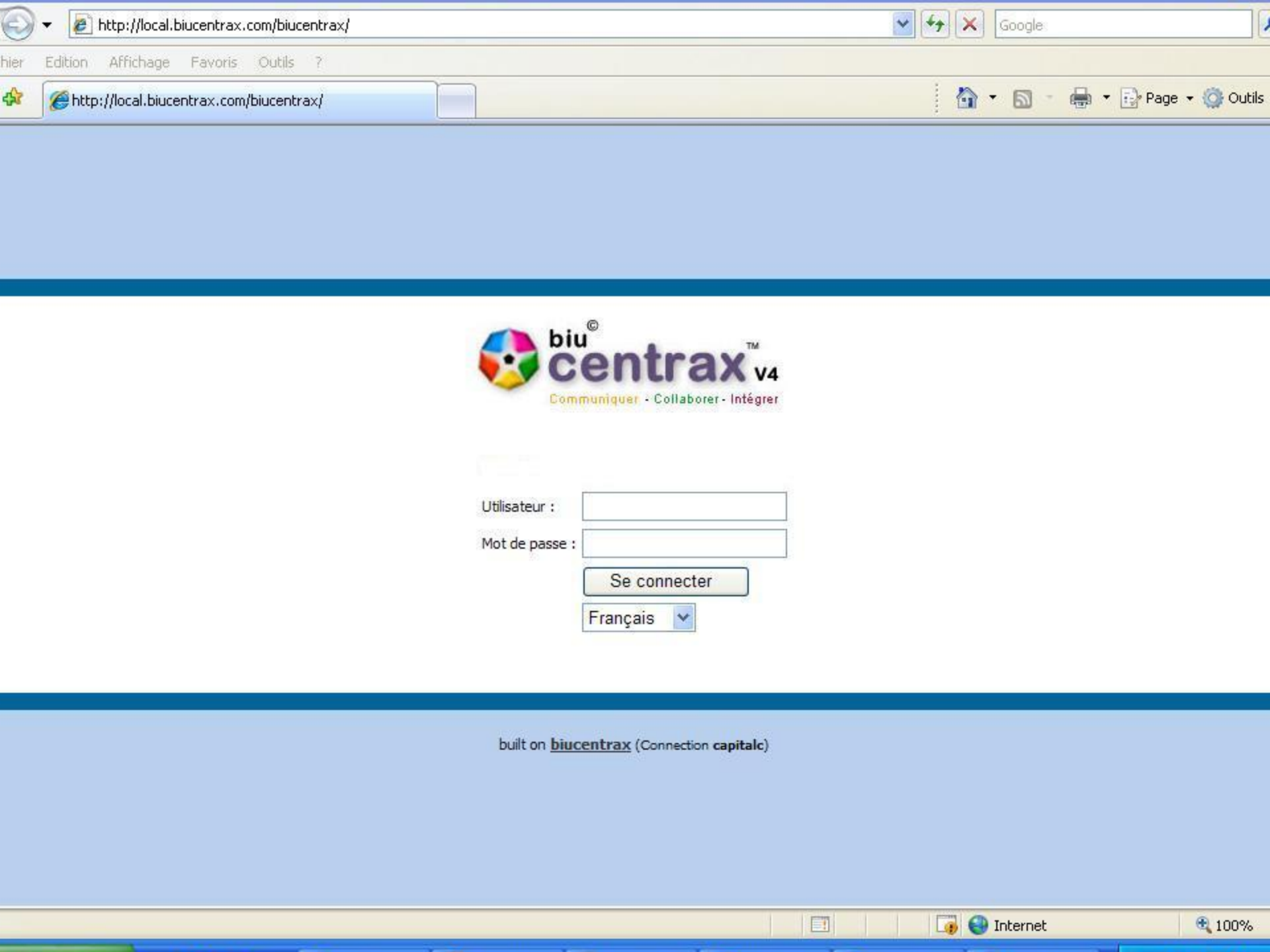
Université
De Limoges

Département de physique/Infotronique
IT/S6

SQL injection

Réalisé par : Dr RIAHLA

2008/2009


http://local.biucentrax.com/biucentrax/
Google
hier Edition Affichage Favoris Outils ?
http://local.biucentrax.com/biucentrax/
Page Outils
biu©
centrax™ V4
Communiquer - Collaborer - Intégrer
Utilisateur :
Mot de passe :
Se connecter
Français
built on biucentrax (Connection capitalc)
Internet
100%

Université
De Boumerdes

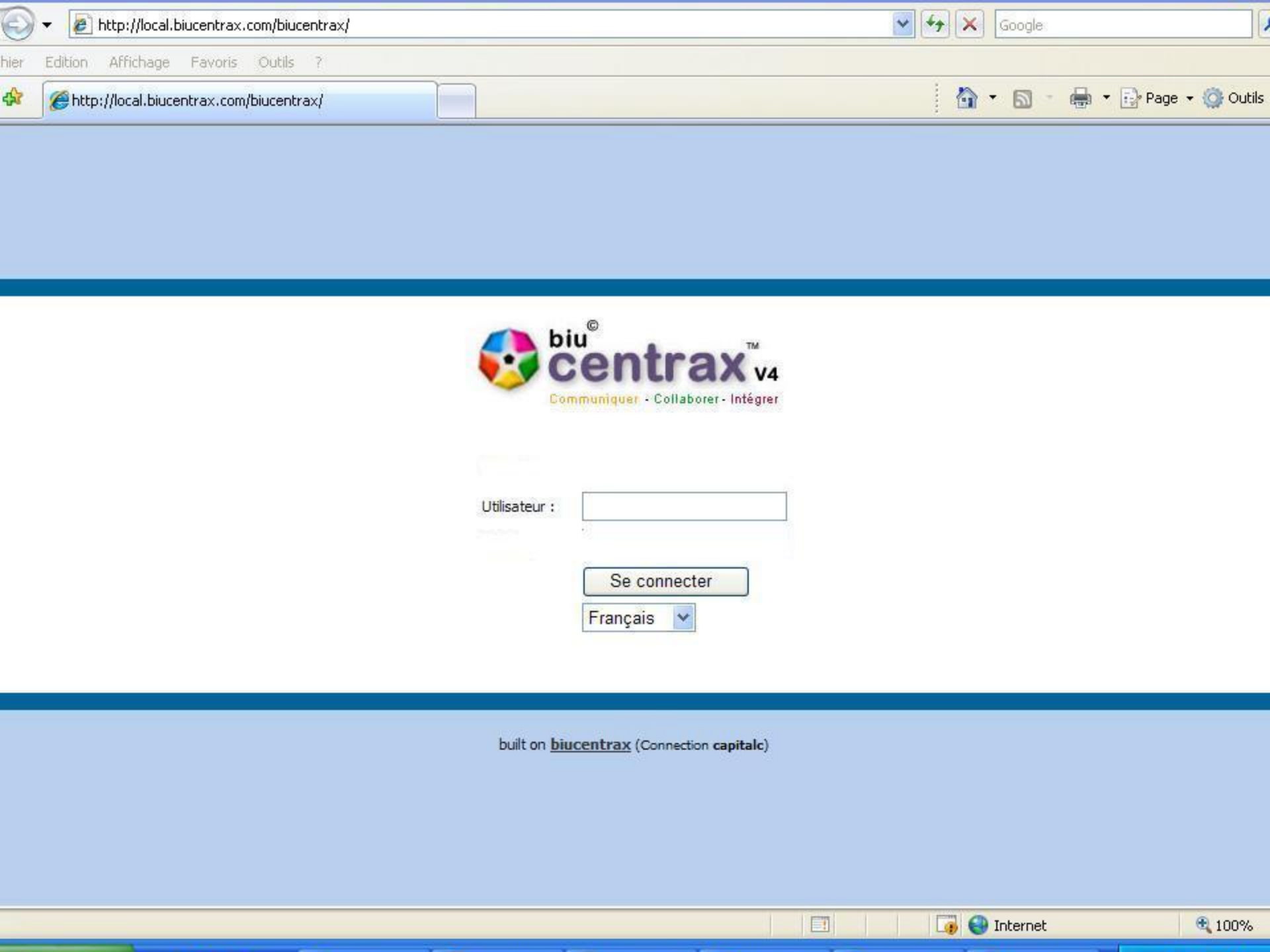
Université
De Limoges

Département de physique/Infotronique
IT/S6

Exemple 1

Réalisé par : Dr RIAHLA

2008/2009


http://local.biucentrax.com/biucentrax/
Google
hier Edition Affichage Favoris Outils ?
http://local.biucentrax.com/biucentrax/
Page Outils
biu©
centrax™ V4
Communiquer - Collaborer - Intégrer
Utilisateur :
Se connecter
Français
built on biucentrax (Connection capitalc)
Internet
100%

SQL Injection
Exemple 1

SELECT * FROM utilisateurs WHERE nom="$nom**";**

SELECT * FROM utilisateurs WHERE nom="toto**";**

Il suffit à un pirate de saisir un nom tel que:
toto" OR 1=1 OR nom ="titi

SELECT * FROM utilisateurs WHERE nom="toto" OR 1=1 OR nom ="titi**";**

Université
De Boumerdes

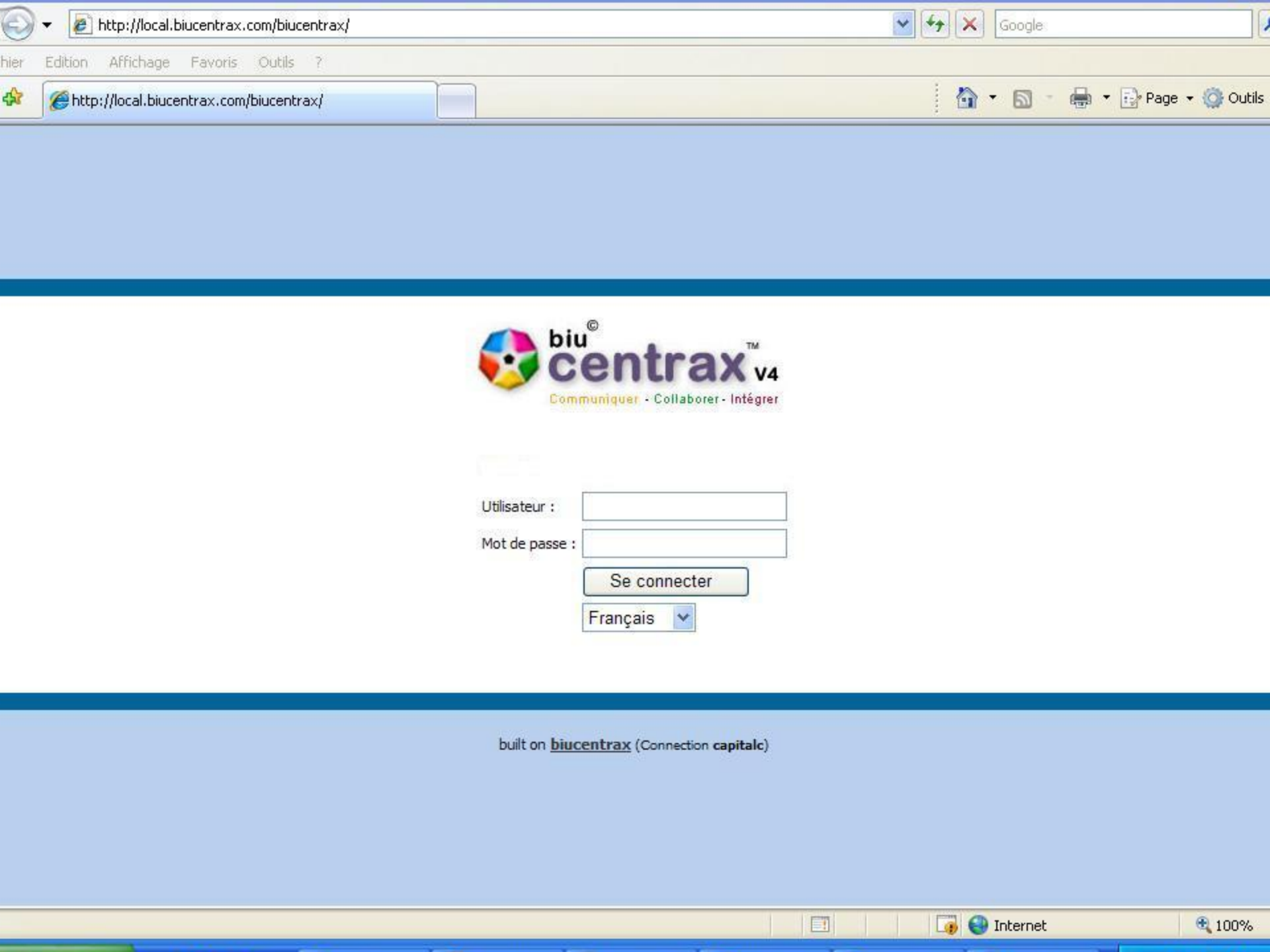
Université
De Limoges

Département de physique/Infotronique
IT/S6

Exemple 2

Réalisé par : Dr RIAHLA

2008/2009


http://local.biucentrax.com/biucentrax/
Google
hier Edition Affichage Favoris Outils ?
http://local.biucentrax.com/biucentrax/
Page Outils
biu©
centrax™ V4
Communiquer - Collaborer - Intégrer
Utilisateur :
Mot de passe :
Se connecter
Français
built on biucentrax (Connection capitalc)
Internet
100%

SQL Injection
Exemple 2

SELECT nom, pw FROM database WHERE nom= "'+$nom+'" AND password = "'+$pw+'"

SELECT nom, pw FROM database WHERE nom = " Titi" AND password = "Toto"

Pour de nom = admin "/* et pw = maison

SELECT nom, pw FROM database WHERE nom ="admin" /* " *AND pw = "maison"*

SQL Injection
Exemple 2

Pour de nom = **" OR True OR nom= "** et pw = bla

SELECT nom, pw FROM database WHERE nom = " " OR True OR nom= " " AND password = " bla"

SQL Injection
Precautions

- Vérifier le format des données saisies.
- Ne pas afficher la requête ou une partie de la requête.
- Supprimer les comptes utilisateurs non utilisées et les comptes par défaut
- Eviter les comptes sans mot de passe.
- Restreindre au minimum les privilèges des comptes utilisés

Université
De Boumerdes

Université
De Limoges

Département de physique/Infotronique
IT/S6

CSS/XSS (Cross Site Scripting)
Regard suisse

Réalisé par : Dr RIAHLA

2008/2009

CSS/XSS (Cross Site Scripting) Principe

- l'une des attaques les plus utilisées par les pirates.

- **Objectif**: pénétrer dans les applications Web.

- **Principe**: Consiste à forcer un site web à exécuter du code HTML ou des scripts saisis par l'utilisateur dans un champ d'un formulaire ou à travers un lien d'un site web.

CSS/XSS (Cross Site Scripting)
Cas 1

- Afficher les messages déposés par les internautes
- Un pirate dépose un script qui dirige les internautes vers un autre serveur
- Game over

CSS/XSS (Cross Site Scripting)
Cas 2

- Envoyer un courrier électronique a une victime qui contient un code dans le **sujet**
- Récupérer les cookies de l'internaute
- Lire le courrier jusqu'à l'expiration du cookie
- Game over

CSS/XSS (Cross Site Scripting)
Cas 3

- Envoi d'un courrier à la victime lui demandant de se rendre à une URL.
- (ex: site de banque en ligne de la victime).
- URL Fausse.
- Le serveur renvoi une erreur en réaffichant L'URL
- L'URL redirige la victime à une page semblable
- Game Over (récupéré les mots de passes)

phishing


LES CHEVAUX DE TROIE ET LE PHISHING SUPPLANTENT LES VIRUS
CHACUN SES MÉTHODES...
HÉHÉ
INTERNAUTUS VULGARIS
e-mail

Université
De Boumerdes

Université
De Limoges

Département de physique/Infotronique
IT/S6

Autres Attaques

Réalisé par : Dr RIAHLA

2008/2009

Autres attaques

- Les fichiers générés en cache
- Publication de code source
- Les fichiers logs
- L'inclusion en PHP
- le CSRF