La sécurité des sites web

Manuel Silvoso
François Thill

SMILE – home of:

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Économie
et du Commerce extérieur

AGENDA

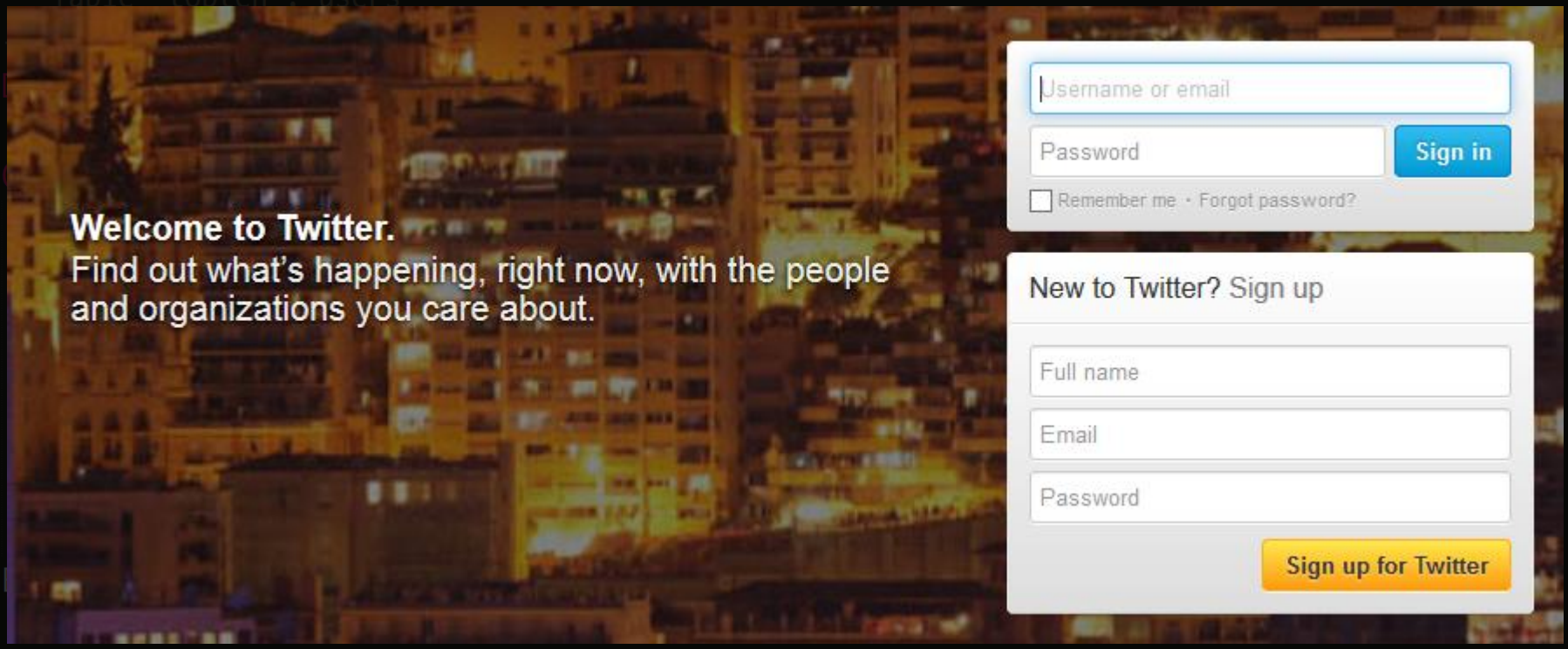
Vulnérabilités
Mesures à prendre

Sites de référence

https://owasp.org
https://www.cases.lu

```
SET @OLD_UNIQUE_CHECKS=@@UNIQUE_CHECKS, UNIQUE_CHECKS=0;
SET @OLD_FOREIGN_KEY_CHECKS=@@FOREIGN_KEY_CHECKS, FOREIGN_KEY_CHECKS=0;
SET @OLD_SQL_MODE=@@SQL_MODE, SQL_MODE='TRADITIONAL';

CREATE SCHEMA IF NOT EXISTS                                    SET utf8 COLLATE utf8_general_ci ;
USE `topten`;

-- -----------------------------------------------------
-- Table `topten`.`users`
-- -----------------------------------------------------

-- -----------------------------------------------------
-- Table `topten`.`threats`
-- -----------------------------------------------------
DROP TABLE IF EXISTS `topten`.`threats` ;
```

Injection SQL



```
SET @OLD_UNIQUE_CHECKS=@@UNIQUE_CHECKS, UNIQUE_CHECKS=0;
SET @OLD_FOREIGN_KEY_CHECKS=@@FOREIGN_KEY_CHECKS, FOREIGN_KEY_CHECKS=0;
SET @OLD_SQL_MODE=@@SQL_MODE, SQL_MODE='TRADITIONAL';

CREATE SCHEMA IF NOT EXISTS `topten` DEFAULT CHARACTER SET utf8 COLLATE utf8_general_ci ;
USE `topten`;

-- -----------------------------------------------------
-- Table `topten`.`users`
-- -----------------------------------------------------
DROP TABLE IF EXISTS `topten`.`users` ;

CREATE  TABLE IF NOT EXISTS `topten`.`users` (
  `id_users` INT(11) NOT NULL AUTO_INCREMENT ,
  `login` VARCHAR(100) NOT NULL ,
  `password` VARCHAR(100) NOT NULL ,
  `admin` INT(1) NOT NULL ,
  `name` VARCHAR(100) NULL ,
  `organization` VARCHAR(255) NULL ,
  `email` VARCHAR(255) NULL ,
  PRIMARY KEY (`id_users`) )
ENGINE = MyISAM;


-- -----------------------------------------------------
-- Table `topten`.`threats`
-- -----------------------------------------------------
DROP TABLE IF EXISTS `topten`.`threats` ;
```

Quel est l’utilisateur qui a pour identifiant ‘utilisateur’ et pour mot de passe ‘mot de passe’?

```
SET @OLD_UNIQUE_CHECKS=@@UNIQUE_CHECKS, UNIQUE_CHECKS=0;
SET @OLD_FOREIGN_KEY_CHECKS=@@FOREIGN_KEY_CHECKS, FOREIGN_KEY_CHECKS=0;
SET @OLD_SQL_MODE=@@SQL_MODE, SQL_MODE='TRADITIONAL';

CREATE SCHEMA IF NOT EXISTS `topten` DEFAULT CHARACTER SET utf8 COLLATE utf8_general_ci ;
USE `topten`;

-- -----------------------------------------------------
-- Table `topten`.`users`
-- -----------------------------------------------------
DROP TABLE IF EXISTS `topten`.`users` ;

CREATE  TABLE IF NOT EXISTS `topten`.`users` (
  `id_users` INT(11) NOT NULL AUTO_INCREMENT ,
  `login` VARCHAR(100) NOT NULL ,
  `password` VARCHAR(100) NOT NULL ,
  `admin` INT(1) NOT NULL ,
  `name` VARCHAR(100) NULL ,
  `organization` VARCHAR(255) NULL ,
  `email` VARCHAR(255) NULL ,
  PRIMARY KEY (`id_users`) )
ENGINE = MyISAM;


-- -----------------------------------------------------
-- Table `topten`.`threats`
-- -----------------------------------------------------
DROP TABLE IF EXISTS `topten`.`threats` ;
```

Quel est l'utilisateur qui a pour identifiant 'PDupont' et pour mot de passe 'Secret'?

```
SET @OLD_UNIQUE_CHECKS=@@UNIQUE_CHECKS, UNIQUE_CHECKS=0;
SET @OLD_FOREIGN_KEY_CHECKS=@@FOREIGN_KEY_CHECKS, FOREIGN_KEY_CHECKS=0;
SET @OLD_SQL_MODE=@@SQL_MODE, SQL_MODE='TRADITIONAL';

CREATE SCHEMA IF NOT EXISTS `topten` DEFAULT CHARACTER SET utf8 COLLATE utf8_general_ci ;
USE `topten`;

-- -----------------------------------------------------
-- Table `topten`.`users`
-- -----------------------------------------------------
DROP TABLE IF EXISTS `topten`.`users` ;

CREATE  TABLE IF NOT EXISTS `topten`.`users` (
  `id_users` INT(11) NOT NULL AUTO_INCREMENT ,
  `login` VARCHAR(100) NOT NULL ,
  `password` VARCHAR(100) NOT NULL ,
  `admin` INT(1) NOT NULL ,
  `name` VARCHAR(100) NULL ,
  `organization` VARCHAR(255) NULL ,
  `email` VARCHAR(255) NULL ,
  PRIMARY KEY (`id_users`) )
ENGINE = MyISAM;


-- -----------------------------------------------------
-- Table `topten`.`threats`
-- -----------------------------------------------------
DROP TABLE IF EXISTS `topten`.`threats` ;
```

Quel est l'utilisateur qui a pour identifiant 'PDupont' et pour mot de passe '' ou 'toto'=toto'?

Démonstration

```
SET @OLD_UNIQUE_CHECKS=@@UNIQUE_CHECKS, UNIQUE_CHECKS=0;
SET @OLD_FOREIGN_KEY_CHECKS=@@FOREIGN_KEY_CHECKS, FOREIGN_KEY_CHECKS=0;
SET @OLD_SQL_MODE=@@SQL_MODE, SQL_MODE='TRADITIONAL';

CREATE SCHEMA IF NOT EXISTS `topten` DEFAULT CHARACTER SET utf8 COLLATE utf8_general_ci ;
USE `topten`;

-- -----------------------------------------------------
-- Table `topten`.`users`
-- -----------------------------------------------------
DROP TABLE IF EXISTS `topten`.`users` ;

CREATE  TABLE IF NOT EXISTS `topten`.`users` (
  `id_users` INT(11) NOT NULL AUTO_INCREMENT ,
  `login` VARCHAR(100) NOT NULL ,
  `password` VARCHAR(100) NOT NULL ,
  `admin` INT(1) NOT NULL ,
  `name` VARCHAR(100) NULL ,
  `organization` VARCHAR(255) NULL ,
  `email` VARCHAR(255) NULL ,
  PRIMARY KEY (`id_users`) )
ENGINE = MyISAM;


-- -----------------------------------------------------
-- Table `topten`.`threats`
-- -----------------------------------------------------
DROP TABLE IF EXISTS `topten`.`threats` ;
```

```
SET @OLD_UNIQUE_CHECKS=@@UNIQUE_CHECKS, UNIQUE_CHECKS=0;
SET @OLD_FOREIGN_KEY_CHECKS=@@FOREIGN_KEY_CHECKS, FOREIGN_KEY_CHECKS=0;
SET @OLD_SQL_MODE=@@SQL_MODE, SQL_MODE='TRADITIONAL';

CREATE SCHEMA IF NOT EXISTS `topten` DEFAULT CHARACTER SET utf8 COLLATE utf8_general_ci ;
USE `topten`;

-- -----------------------------------------------------
-- Table `topten`.`users`
-- -----------------------------------------------------
DROP TABLE IF EXISTS `topten`.`users` ;

CREATE TABLE IF NOT EXISTS `topten`.`users` (
  `id_users` INT(11) NOT NULL AUTO_INCREMENT ,
  `login` VARCHAR(100) NOT NULL ,
  `password` VARCHAR(60) NOT NULL ,
  `admin` INT(1) NOT NULL ,
  `name` VARCHAR(100) NULL ,
  `organization` VARCHAR(255) NULL ,
  `email` VARCHAR(255) NULL ,
  PRIMARY KEY (`id_users`) )
ENGINE = MyISAM;


-- -----------------------------------------------------
-- Table `topten`.`threats`
-- -----------------------------------------------------
DROP TABLE IF EXISTS `topten`.`threats` ;
```

Quelle est la liste de tous les articles qui contiennent ‘recherche’?

```
SET @OLD_UNIQUE_CHECKS=@@UNIQUE_CHECKS, UNIQUE_CHECKS=0;
SET @OLD_FOREIGN_KEY_CHECKS=@@FOREIGN_KEY_CHECKS, FOREIGN_KEY_CHECKS=0;
SET @OLD_SQL_MODE=@@SQL_MODE, SQL_MODE='TRADITIONAL';

CREATE SCHEMA IF NOT EXISTS `topten` DEFAULT CHARACTER SET utf8 COLLATE utf8_general_ci ;
USE `topten`;

-- -----------------------------------------------------
-- Table `topten`.`users`
-- -----------------------------------------------------
DROP TABLE IF EXISTS `topten`.`users` ;

CREATE TABLE IF NOT EXISTS `topten`.`users` (
  `id_users` INT(11) NOT NULL AUTO_INCREMENT ,
  `login` VARCHAR(100) NOT NULL ,
  `password` VARCHAR(100) NOT NULL ,
  `admin` INT(1) NOT NULL ,
  `name` VARCHAR(100) NULL ,
  `organization` VARCHAR(255) NULL ,
  `email` VARCHAR(255) NULL ,
  PRIMARY KEY (`id_users`) )
ENGINE = MyISAM;


-- -----------------------------------------------------
-- Table `topten`.`threats`
-- -----------------------------------------------------
DROP TABLE IF EXISTS `topten`.`threats` ;
```

Quelle est la liste de tous les articles qui contiennent ‘recherche’ et aussi le contenu du tableau utilisateurs tels que ‘toto’=‘toto’?

Démonstration

```
SET @OLD_UNIQUE_CHECKS=@@UNIQUE_CHECKS, UNIQUE_CHECKS=0;
SET @OLD_FOREIGN_KEY_CHECKS=@@FOREIGN_KEY_CHECKS, FOREIGN_KEY_CHECKS=0;
SET @OLD_SQL_MODE=@@SQL_MODE, SQL_MODE='TRADITIONAL';

CREATE SCHEMA IF NOT EXISTS `topten` DEFAULT CHARACTER SET utf8 COLLATE utf8_general_ci ;
USE `topten`;

-- -----------------------------------------------------
-- Table `topten`.`users`
-- -----------------------------------------------------
DROP TABLE IF EXISTS `topten`.`users` ;

CREATE  TABLE IF NOT EXISTS `topten`.`users` (
  `id_users` INT(11) NOT NULL AUTO_INCREMENT ,
  `login` VARCHAR(100) NOT NULL ,
  `password` VARCHAR(100) NOT NULL ,
  `admin` INT(1) NOT NULL ,
  `name` VARCHAR(100) NULL ,
  `organization` VARCHAR(255) NULL ,
  `email` VARCHAR(255) NULL ,
  PRIMARY KEY (`id_users`) )
ENGINE = MyISAM;


-- -----------------------------------------------------
-- Table `topten`.`threats`
-- -----------------------------------------------------
DROP TABLE IF EXISTS `topten`.`threats` ;
```

Sécurité des mots de passe

Password Popularity – Top 20

Rank	Password	Number of Users with Password (absolute)
1	123456	290731
2	12345	79078
3	123456789	76790
4	Password	61958
5	iloveyou	51622
6	princess	35231
7	rockyou	22588
8	1234567	21726
9	12345678	20553
10	abc123	17542

Rank	Password	Number of Users with Password (absolute)
11	Nicole	17168
12	Daniel	16409
13	babygirl	16094
14	monkey	15294
15	Jessica	15162
16	Lovely	14950
17	michael	14898
18	Ashley	14329
19	654321	13984
20	Qwerty	13856

Hashage
Transformation cryptographique irréversible


MD5
super-secret
0682f007844a0266990df1b2912f95bc

Méthodes de hashage de mots de passe

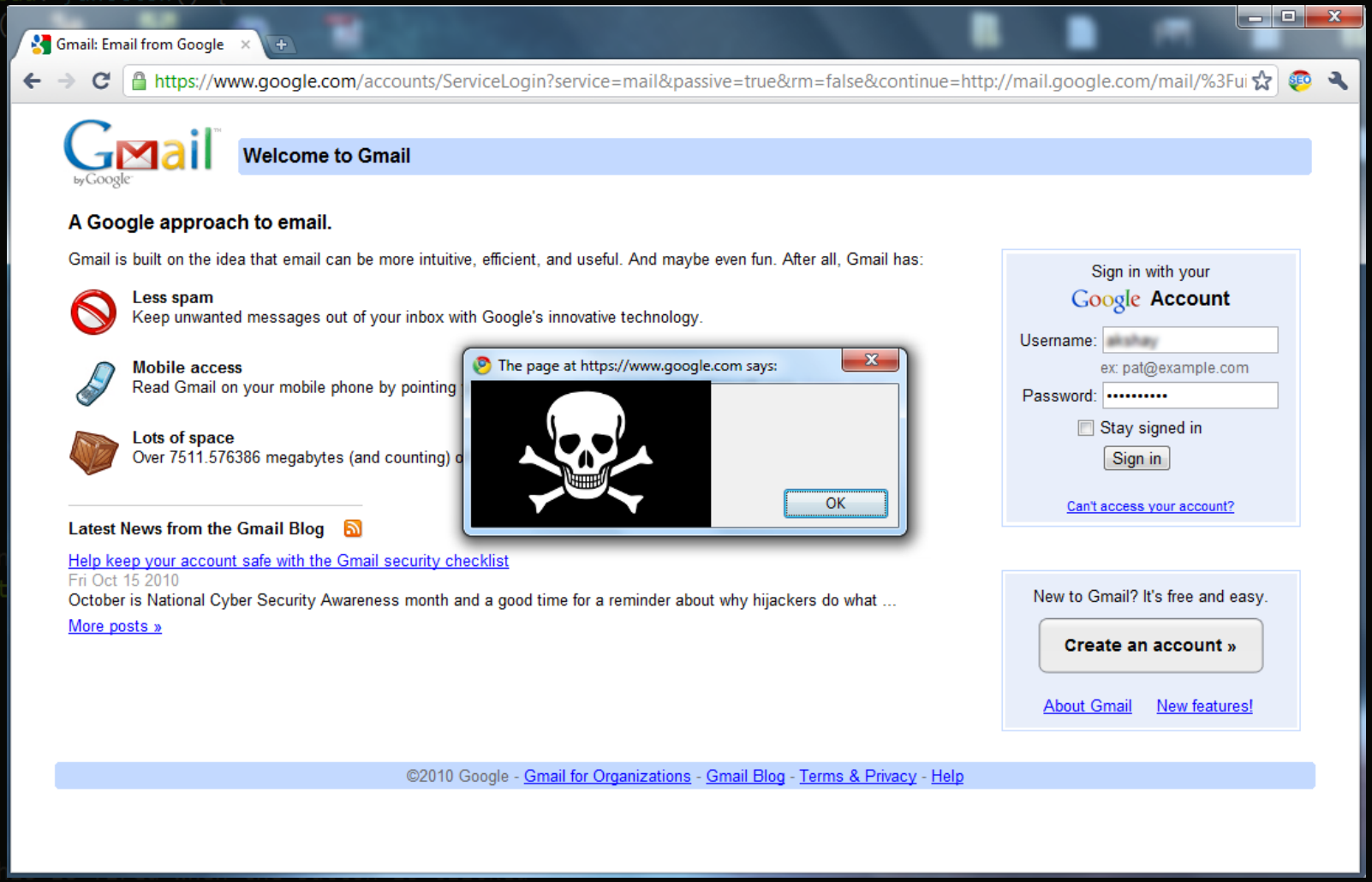
bcrypt, scrypt

Une pincée de sel

Sel aléatoire en base de donneés

Sel fixe et secret dans la fichier configuration

XSS


Gmail: Email from Google
https://www.google.com/accounts/ServiceLogin?service=mail&passive=true&rm=false&continue=http://mail.google.com/mail/%3Fui
Gmail by Google
Welcome to Gmail
A Google approach to email.
Gmail is built on the idea that email can be more intuitive, efficient, and useful. And maybe even fun. After all, Gmail has:
Less spam
Keep unwanted messages out of your inbox with Google's innovative technology.
Mobile access
Read Gmail on your mobile phone by pointing
Lots of space
Over 7511.576386 megabytes (and counting)
The page at https://www.google.com says:
OK
Latest News from the Gmail Blog
Help keep your account safe with the Gmail security checklist
Fri Oct 15 2010
October is National Cyber Security Awareness month and a good time for a reminder about why hijackers do what ...
More posts »
Sign in with your Google Account
Username:
ex: pat@example.com
Password:
Stay signed in
Sign in
Can't access your account?
New to Gmail? It's free and easy.
Create an account »
About Gmail
New features!
©2010 Google - Gmail for Organizations - Gmail Blog - Terms & Privacy - Help

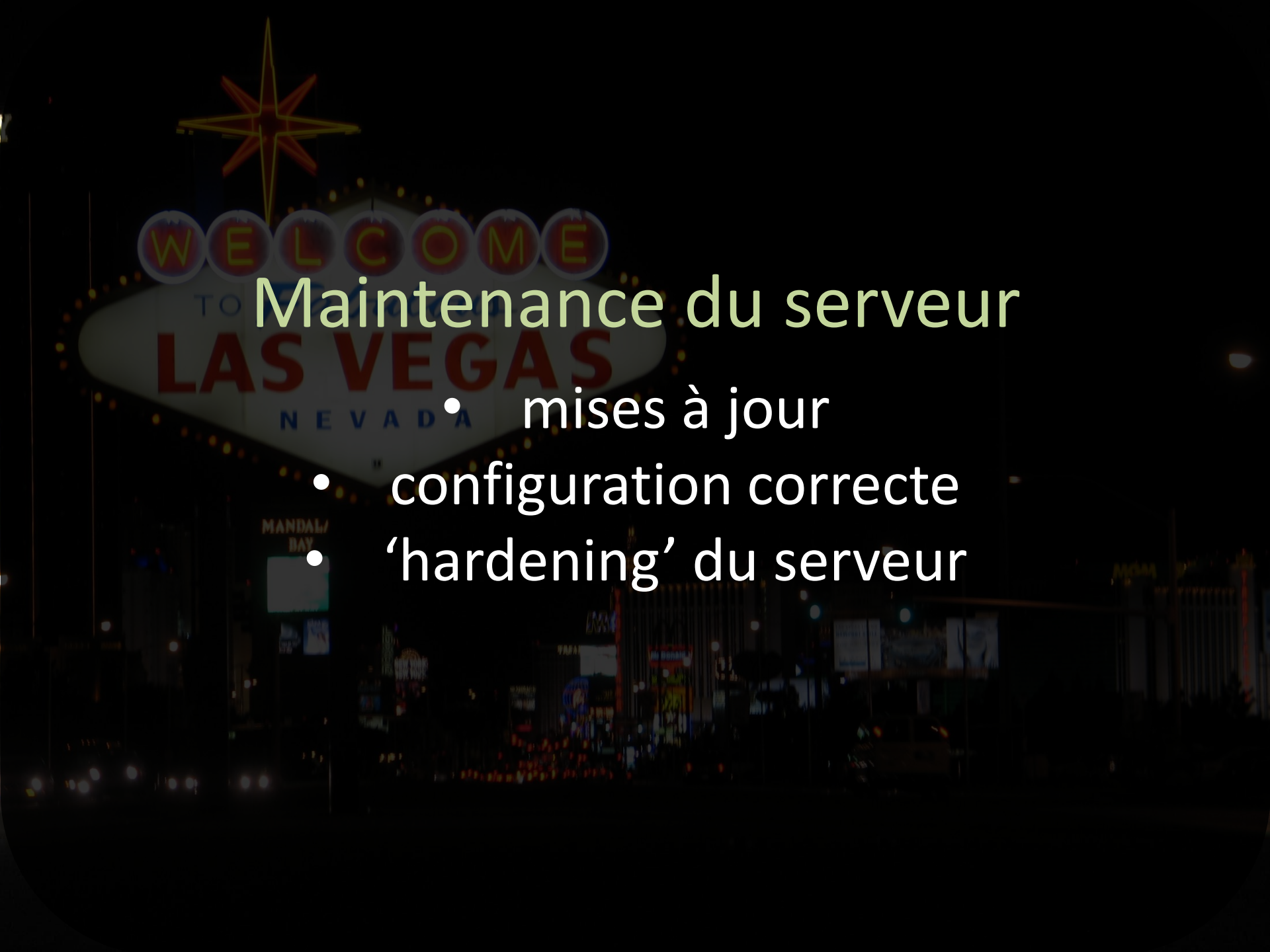
Démonstration

```
var ClickToPlayButtonMainClass = {
    prefs: Components.classes["@mozilla.org/preferences-service;1"].getService(Components.interfaces.nsIPrefBranch),
    firstRunPref: "extensions.clicktoplaybutton.firstRunDone",
    reloadPref: "extensions.clicktoplaybutton.reload",

    initialized: false,

    //Initialization (this should only be called once)
    onLoad: function() {
    if (!this.initialized) {
            this.initialized=true;
            var pref = this.prefs.getBoolPref("plugins.click_to_play");
            var button = document.getElementById("clicktoplayswitch");
            if (button) {
                button.setAttribute("label","Click to play");
                button.setAttribute("class","toolbarbutton-1 clickbutton");
            }
            this.prefs.setBoolPref("plugins.click_to_play", !pref);

            if (!this.prefs.prefHasUserValue(this.firstRunPref)) {
                this.prefs.setBoolPref(this.firstRunPref, true);
                this.installButton();
            }
        }
    },

    //install button in the toolbar
    installButton: function() {
        var toolbar = document.getElementById("nav-bar");
        if (!document.getElementById("clicktoplayswitch")) {
            toolbar.insertItem("clicktoplayswitch",null);
            toolbar.setAttribute("currentset", toolbar.currentSet);
            document.persist(toolbar.id, "currentset");
        }
    },

    //this is fired when the button is clicked
    onClick: function() {
        var pref = this.prefs.getBoolPref("plugins.click_to_play");
```

Mesures de protection

Techniques de programmation saines

- éducation adéquate des développeurs
- validation des entrées/sorties
- échappement des entrées/sorties
- paramétrages corrects
- standard de programmation
- revue de code



Maintenance du serveur

- mises à jour
- configuration correcte
- ‘hardening’ du serveur

CMS, projet opensource, projets tiers:

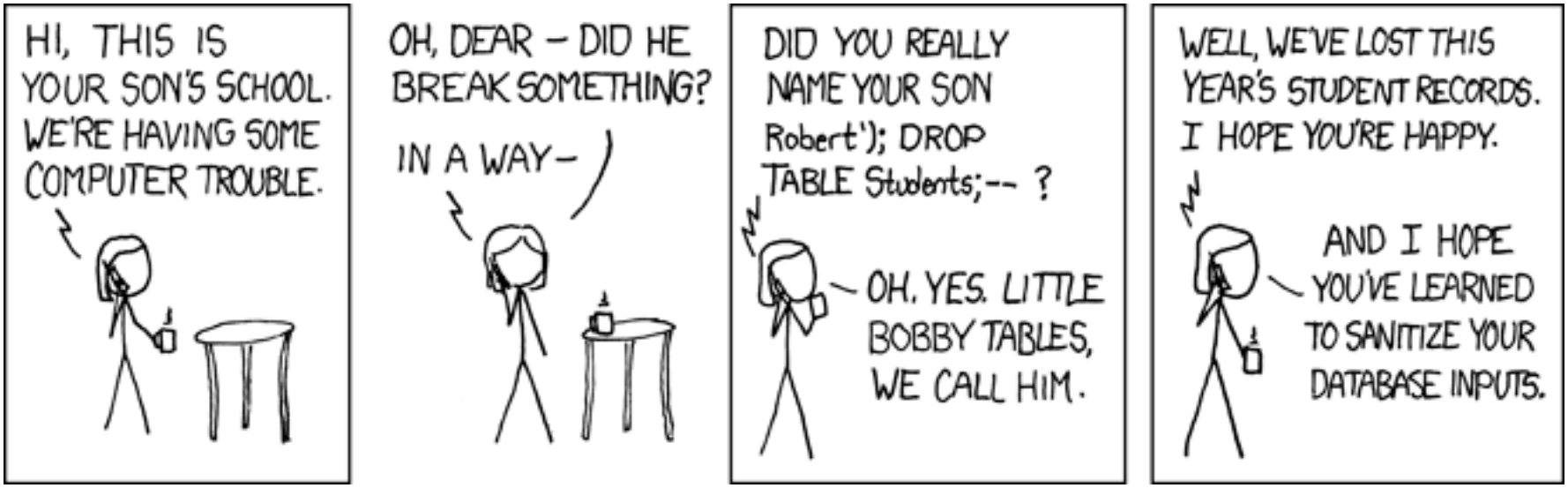
- mises à jour
- attention aux développements sauvages
- ne pas installer n’importe quel ajout

Contremesures

- firewalls applicatifs
- fosse de goudron
- protection contre le déni de service

Comic de remerciement

manuel.silvoso@eco.etat.lu
francois.thill@eco.public.lu



SMILE – home of:

BEE SECURE

CASES
SECURITY MADE IN LETZEBUERG

CIRCL
Computer Incident Response Center Luxembourg
SECURITY MADE IN LETZEBUERG

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Économie
et du Commerce extérieur