La sécurité & Drupal

Tris Acatrinei

DRUPALCAMP
PARIS 2013

La notion de sécurité

- Disponibilité
- Intégrité
- Confidentialité

Authentification/Véracité

+

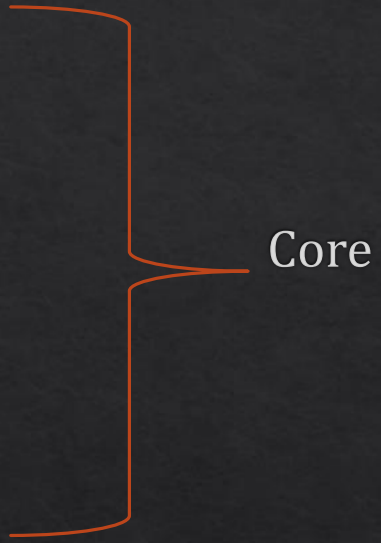
Non-répudiation

Les conséquences d'un défaut de sécurisation

- Impact sur les infrastructures informatiques
- Impact juridique
- Impact marketing/communication
- Impact financier

Premier niveau d'action : les utilisateurs

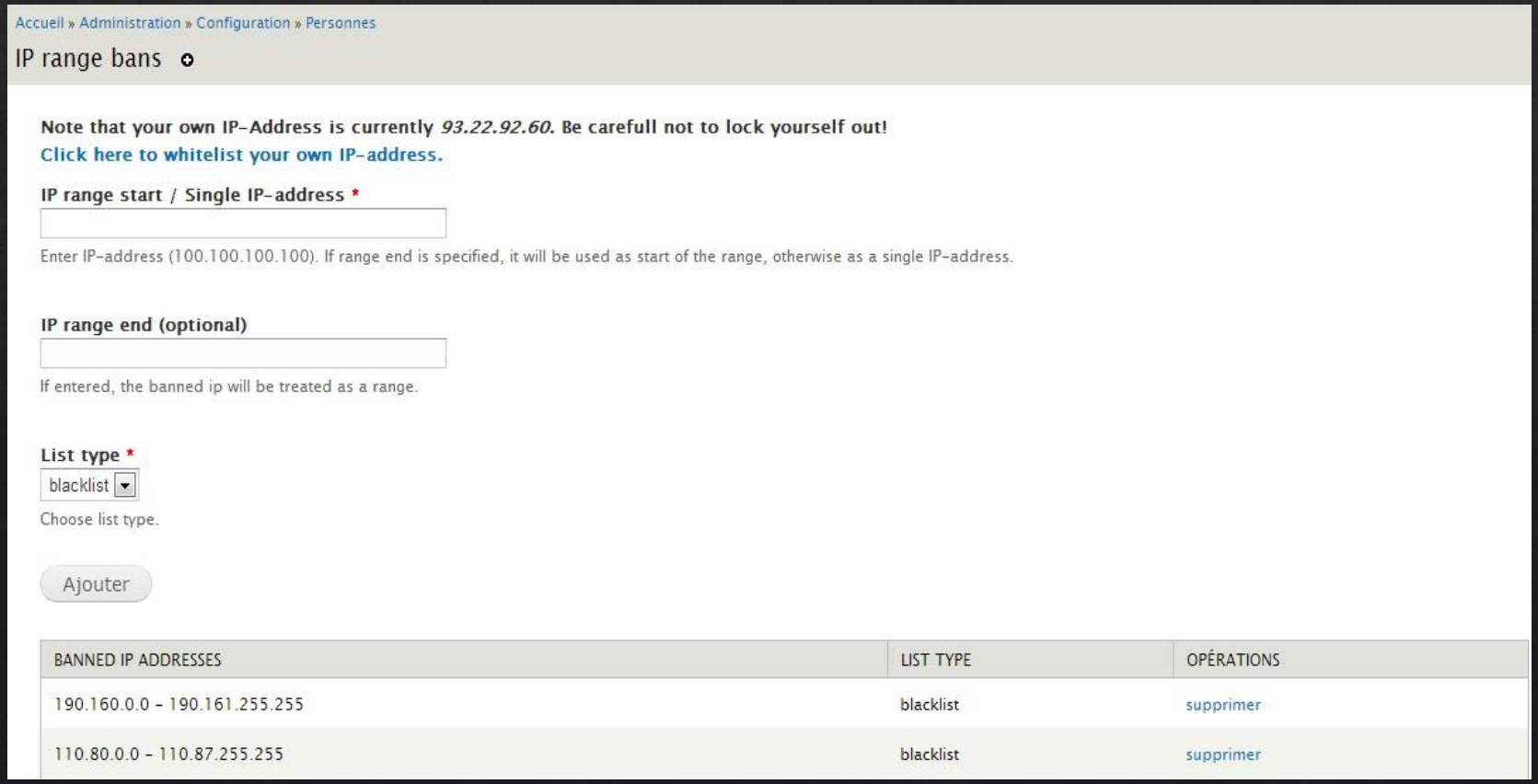
- Les formats
- L'administration des modules
- Les contenus et les commentaires



Se débarrasser des nuisibles

- Identifier les nuisibles
- Adapter la réponse en fonction du nuisible
- Réponse la plus rapide = blocage d'IP

- Réponse plus radicale = blocage d'une plage d'IP



Accueil » Administration » Configuration » Personnes

IP range bans

Note that your own IP-Address is currently *93.22.92.60*. Be carefull not to lock yourself out!
Click here to whitelist your own IP-address.

IP range start / Single IP-address *

Enter IP-address (100.100.100.100). If range end is specified, it will be used as start of the range, otherwise as a single IP-address.

IP range end (optional)

If entered, the banned ip will be treated as a range.

List type *

blacklist

Choose list type.

Ajouter

BANNED IP ADDRESSES	LIST TYPE	OPÉRATIONS
190.160.0.0 - 190.161.255.255	blacklist	supprimer
110.80.0.0 - 110.87.255.255	blacklist	supprimer

Se débarrasser des spammeurs

- Honeypot : un module qui porte très bien son nom

La face cachée d'Honeypot

```
      <h2 class="title comment-form">Ajouter un commentaire</h2>
    <form class="comment-form user-info-from-cookie" action="/comment/reply/220" method="post" id="comment-form" accept-charset="UTF-8">
  <label for="edit-name">Votre nom </label>
 <input type="text" id="edit-name" name="name" value="" size="30" maxlength="60" class="form-text" />
</div>
<div class="form-item form-type-textfield form-item-mail">
  <label for="edit-mail">Courriel </label>
 <input type="text" id="edit-mail" name="mail" value="" size="30" maxlength="64" class="form-text" />
<div class="description">Le contenu de ce champ sera maintenu privé et ne sera pas affiché publiquement.</div>
</div>
<div class="form-item form-type-textfield form-item-homepage">
  <label for="edit-homepage">Page d'accueil </label>
 <input type="text" id="edit-homepage" name="homepage" value="" size="30" maxlength="255" class="form-text" />
</div>
<input type="hidden" name="form_build_id" value="form-S8RH7OCKty-E9VEZJzZpzcSSaL7nQgBNjueXpIlk3NA" />
<input type="hidden" name="form_id" value="comment_node_culture_du_hacking_form" />
<input type="hidden" name="honeypot_time" value="1366138562" />
<div class="form-item form-type-textfield form-item-subject">
  <label for="edit-subject">Sujet </label>
 <input type="text" id="edit-subject" name="subject" value="" size="60" maxlength="64" class="form-text" />
</div>
<div class="field-type-text-long field-name-comment-body field-widget-text-textarea form-wrapper" id="edit-comment-body"><div id="commen
  <label for="edit-comment-body-und-0-value">Comment <span class="form-required" title="Ce champ est obligatoire.">*</span></label>
 <div class="form-textarea-wrapper resizable"><textarea class="text-full form-textarea required" id="edit-comment-body-und-0-value" name
</div>
<fieldset class="[illegible]" id="edit-comment-body-und-0-format"><div class="fieldset-wrapper"><div class="filter-help
</div>
</div></div><div class="form-actions form-wrapper" id="edit-actions"><input type="submit" id="edit-submit" name="op" value="Enregistrer"
  <label for="edit-url">Leave this field blank </label>
<input autocomplete="off" type="text" id="edit-url" name="url" value="" size="20" maxlength="128" class="form-text" />
</div>
</div></div></form>  </div>
  </div>
```

Quelques modules en plus

- Tiny-IDS = détection et alerte en temps réel de l'activité malicieuse sur la plateforme.

- Fail2Ban = le module complémentaire à l'outil du même nom. Restriction => Serveur dédié

La sécurité, ce n’est pas que des outils !

- Le plus difficile ? L’acquisition de bonnes pratiques
- Documentation
- Monitoring
- Sauvegarde

Monitorer un Drupal

- Lire ses logs !
- Connaître les différents niveaux de sévérité => se documenter !
- Mettre en place un système de log-management
- Être capable de retracer qui a modifié quoi

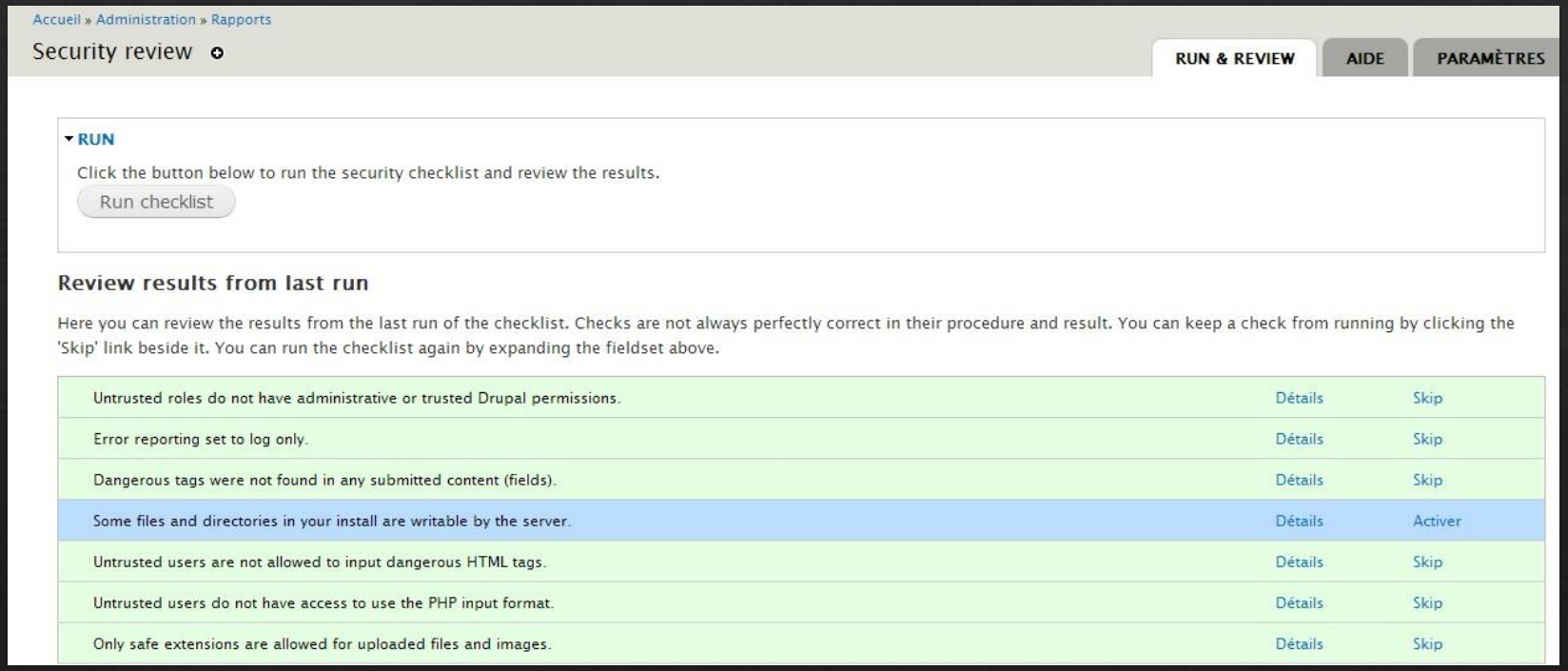
Apprendre à lire un log

Les niveaux de sévérité

La catégorie	Le niveau
Débogage	1
Info	2
Notice	3
Warning	4
Erreur	5
Critique	6
Urgence	7

Qui a bricolé quoi ? Le module Hacked!

Security Reviews : le module pour étourdi



Les dossiers et les fichiers

- Passer en revue les fichiers et éléments à supprimer
- Vérifier les droits d’accès
- Vérifier la récursivité
- Jamais de 777 !

Identification & authentification

- Certificat SSL
- Authentification des utilisateurs : s'assurer qu'ils sont bien qui ils prétendent être
- Authentification des utilisateurs : s'assurer qu'ils ne prennent pas la sécurité à la légère
- *Quid* des authentifications Oauth ?

La préproduction

- Vérifier le code !
- Tester la structure
- Auditer la structure

La documentation

- Le livrable est disponible à cette adresse :

http://www.hackersrepublic.org/outils/la-securite-et-drupal