DRUPALCAMP LANNION

27-28-29 OCTOBRE 2017

Mon site est hacké! Que faire ?

Version 2017-2018: impact du RGPD

Frédéric G. MARAND

http://www.osinet.fr/

OSInet

Au programme

- 1 Intro : comme un lundi
- 2 Prendre un cliché de la situation
- 3 Maintenir une présence en ligne
- 4 Communiquer pendant la crise
- 5 Reconstruire, pas réparer
- 6 Enquêter
- 7 Revenir en production

1.1 Petite vérification préalable

1.1 Petite vérification préalable

- Dans cette pièce …
  - Qui a déjà été victime d'intrusion ?

1.1 Petite vérification préalable

- Dans cette pièce …
  - Qui a déjà été victime d'intrusion ?
  - Qui se sent prêt à faire face à un serveur hacké ?

1.1 Petite vérification préalable

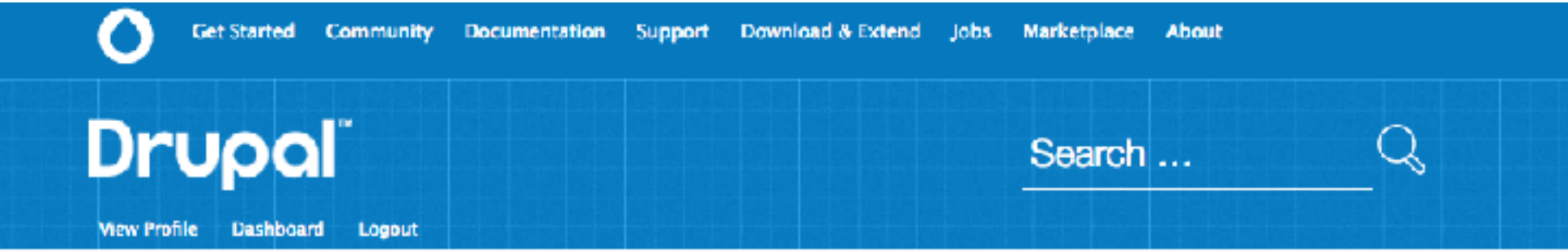
- Dans cette pièce …
  - Qui a déjà été victime d'intrusion ?
  - Qui se sent prêt à faire face à un serveur hacké ?
  - Qui a déjà un Plan de Reprise sur Incident en place ?

1.1 Petite vérification préalable

- Dans cette pièce …
  - Qui a déjà été victime d'intrusion ?
  - Qui se sent prêt à faire face à un serveur hacké ?
  - Qui a déjà un Plan de Reprise sur Incident en place ?
  - RGPD: qui sait quoi communiquer et à qui ?

1.1 Petite vérification préalable

- Dans cette pièce …
  - Qui a déjà été victime d'intrusion ?
  - Qui se sent prêt à faire face à un serveur hacké ?
  - Qui a déjà un Plan de Reprise sur Incident en place ?
  - RGPD: qui sait quoi communiquer et à qui ?
  - Qui a lu https://drupal.org/node/2365547 ?



Community Documentation

Community Docs Home | Develop for Drupal | Theming Guide | Glossary | Contribute to Docs

Your Drupal site got hacked. Now what?

View | View history

Last updated October 29, 2014. Created on October 29, 2014.
Edited by greggles, mlhess.

This information is useful should your Drupal site get compromised. Please report any details to the security team at security@drupal.org. The security team is unable to help with individual sites, but does like to keep track of compromised sites to see patterns.

Your Drupal site got hacked. Now what?

Ooops. The worst case scenario has come to pass: a vulnerability somewhere allowed a malicious individual (or bot, more likely) to take over your site. Some good news: you've noticed that they did it. Bad news: now you have to clean up.

This guide will give you a series of steps for how to deal with the situation. It may not be exhaustive. If you feel it's missing something, please contribute. The ideas are presented in chronological order. At each step, you will have to make decisions and take actions that are most appropriate for your situation.

Page status

Report to moderator

About this page

Drupal version
Drupal 6.x, Drupal 7.x, Drupal 8.x

Audience
Contributors, Programmers, Site administrators, Site builders, Site users

Level
Intermediate

1.2 Comment dit on, déjà ?

I.A.N.A.L.

je ne suis ni avocat, ni juriste, ni conseil juridique, ceci ne constitue pas un conseil ou une offre de conseil juridique, mais uniquement une opinion personnelle sur un processus technique

Donc première étape: votre avocat !

1.3 Cela dit, côté technique…

- Sur Drupal org depuis 2005 (fgm)
- Consultant Drupal, pas agence web
- Intervenant d'urgence sur des sites en difficultés depuis 2008
    - Audits performance / qualité / sécurité
    - Résolution de problèmes techniques
    - Traitement des intrusions / pénétrations
- Surtout dans les média et le gouvernement (.fr)
- « Provisional member » de la Security Team

1.4 Comme un lundi

- 10:00 Le daily standup vient de commencer
- 10:01 Dring ! un appel signale que le site n'a pas l'air normal
- 10:02 Le buzz commence sur Twitter/Reddit
- 10:05 Cacophonie d'appels, de toute la chaîne hiérarchique comme des journalistes et blogueurs en mal de scoop
- Que faites-vous maintenant ?

1.5 Préparation

- Bloc 1 : journal d'observations
  - toutes les étapes du processus
  - toutes les observations / découvertes
  - horodatées, numérotées
- Bloc 2 : idées de corrections
  - références vers les numéros du bloc 1
  - toutes les idées pour corriger le problème
  - toutes les idées de durcissement à venir

2.1 Le cliché d'enquête

- Première tentation : restaurer et reprendre
  - Mais toujours vulnérable à la même pénétration
  - Donc il faut diagnostiquer et remédier
- Analyser implique de modifier
  - Donc préserve la « scène de crime »
  - Clichés de /tout/

2.2 Clichés: « débranche… »

- Pas d'interférences:
  - handlers d'arrêt, SIGPWR
  - code auto-destructeur à la perte de connectivité
- Facile à simuler sur des VMs

Mais…

- Serveurs physiques
- Pertes de données
  - Systèmes de fichiers journalisés
  - Bases de données
- Interruption de service

2.3 Clichés: de quoi ?

Pas que la DB principale:

- Reverse Proxy
- Frontaux web (Apache)
- Serveurs DB autres
- Serveurs de fichiers

Et aussi…

- Journaux tiers (SaaS)
- Transactions externes
- Journaux IDS/pare-feu

** Le site peut n'être qu'un vecteur d'attaque **

3.1 Rester en ligne 1

Comme si l'intrusion n'avait pas été détectée

- Pour
  - Ne pas alerter les intrus
  - Continuer la génération de valeur à court terme
- Contre
  - Dommages accrus
  - Résponsabilité
    - Légale
    - Financières
    - Morale

3.2 Workflows d'attaque

Evolué

- Pénétrer
- Chercher quoi exploiter
- Implanter un zombie
- Attendre l'archivage des versions zombie
- Activer
- Profiter

- **Alt : Need for Speed**
  - Exploiter sans tarder
  - Tant que ça dure
  - Pertes plus faibles
- **Alt : masquer l'acte**
  - Contenu valorisé
  - Données perso.
  - Fermer la porte

3.3 Rester en ligne 2

Mode de repli sécurisé

- Site statique limité
  - Travail préalable
  - Sous-ensemble minimal
  - Cache de RP
- Charge très faible: peut être servie par les RP seuls
- Site réel limité
  - Infra alternative
  - Tech alternative
- Mises à jour ?
  - Contenu créé durant le repli

3.4 Rester en ligne 3

Quand tout a échoué…

- Réseaux sociaux
  - Toujours là
  - Valeur d'autorité pour l'audience
- Préparation nécessaire :
  - Accès au(x) compte(s)
  - Les inclure dans le plan de communication à long terme

4.1 Communiquer: de la tech

- Parties prenantes
  - Jusqu'au CxO presque toujours
  - Ne pas trop anticiper
- Peur des représailles ? « Gag orders », « SLAPP »
- Protection
  - France : whistleblower protection (Sapin 2)
  - Italy : Dec. 385 01/09/93 sect 52bis (banks)
  - US : Anti-SLAPP

4.2 : Communication : exécutif

- Conseil juridique / avocats (en premier)
- Spécialistes en gestion de crise
- Forces de l'ordre
  - EU: unités spécialisées« cybercrime »
  - France: ANSSI http://www.ssi.gouv.fr/
- Autres sites
  - Sur le même serveur
  - Sur le même réseau
  - Partenaires en ligne: clients/fournisseurs

4.3 Communication : privacy

- Dans la plupart des cas, des fuites de données personnelles sont incluses dans une intrusion
  - ou il ne sera pas possible de prouver qu'elles n'ont pas eu lieu
- Contraintes réglementaires
  - RGPD: obligation de diffusion (art 33.1)
  - Commerce : PCI/DSS (12 steps etc)
  - Health : (US) HIPAA Subtitle D E2.80.93
- Dégâts d'image publique. Un exemple français.

5.1 Refaire: garder, restaurer, ou ?

- Restaurer et redémarrer ?
  - Plus vulnérable qu'avant: faille connue
- Garder et corriger ?
  - temps et effort de la revue de code
  - Jamais totalement fiable: Drupal n'est qu'un maillon de la chaîne
- Jeter ?
  - Sites événementiels, anciennes lignes de produits, après-fusion/acquisition...
  - Pourquoi pas un simple site statique ?
  - Depuis les clichés RP: contenu récent seulement

5.2 Refaire : restaurer

- Sauvegardes antérieures à l'intrusion
  - Quand a-t-elle eu lieu ?
    - Indice: « workflows d'attaque »: « attendre »
  - GFS, incrémental continu, 15 min ?
  - Qu'est-il acceptable de perdre ?
- Solutions libres: Amanda, Bacula, maison
- Urgence sans préparation ?
  - Préproduction, images de CI…

5.3 Refaire : sources + export

- Développement dirigé par le code
  - Système fiables d'export des données déjà en place
    - Export en fichiers plats
    - Dépôts de contenus et assets
- Ajouter les correctifs
- Le délai peut être un problème sur les sites à fort trafic
  - Traitements par lot, chargement incrémental

5.4 Refaire : autres cas

- Reconstruction ad hoc « traditionnelle »
  - Plus long, moins fiable
  - Trop long pour en profiter pour améliorer le processus
- Ex nihilo
  - Fiable, mais presque toujours trop long
  - Complément utile après la réparation
  - Pas MAINTENANT

6 Enquête: changer de casquette

6.1 Enquête : d'abord, réfléchir!

- Comment avez-vous eu connaissance de l'intrusion ?
- Pourquoi a-t-elle pu réussir ?
  - Penser divergence, hors cadre
  - « Improbable » n'est pas « impossible »
- Priorités :
  - Les attaques les plus simples en premier
  - OWASP 10
  - Google : les motifs relevés sur le bloc 1

6.2 Enquête: garder en tête

- /tout/ peut avoir été effacé par l'intrus
  - Mais le plupart du temps /tout/ ne l'est pas
- Chaque action d'enquête ajoute ses traces
  - Travailler sur des copies des clichés
  - Permet de recommencer sur des copies fraîches autant de fois que nécessaire
- Il n'y a pas nécessairement eu une seule intrusion réussie

6.3 Enquête : les classiques

- Code source :
  - permissions trop étendues
  - failles de parcours de système de fichiers
  - Exécution distante de code téléversé
- Nginx sans durcissement complémentaire
  - .htaccess ne sert à rien
- PHP dans la base de données
  - Le module PHP
  - Code `eval`-ué

6.4 Enquête : hors Drupal

- Système de fichiers:
  - `<user>/www-data` hors de `/sites`
    - cibler `www-data/www-data`
    - Le bit x sur des fichiers sous docroot
  - horodatage
    - hors de `sites/*/files == install`
    - `exploits > install`
  - comparer avec un build frais à partir des sources
- Vérifier aussi hors de la docroot / racine de projet

6.5 Enquête : modules Drupal

- Signature et comparaison de code:
  - `Hacked!`
  - D7 : `md5check`, `file_integrity`
- Trouver le PHP en base de données
  - OSInet QA (github)
- Divers
  - `security_review`

6.6 Enquêtes : base de données

- Coups d'oeil rapides :
  - `ufd.email != ufd.init`
  - contrôler d'abord les rôles et comptes à privilèges étendus
  - En corp., vérifier les domaines de `ufd.email`
  - associer les comptes aux données du SSO
- Comparer un cliché DB avec la base courante
  - D8: `router.route` / D7: `menu_router`
  - `file_put_contents`, `assert`
  - Altova DatabaseSpy pour comparer

6.7 Enquête : sessions

- Les sessions doivent être en stockage persistant
  - Souvenez-vous, vous avez débranché.
  - Et si vos sessions étaient dans Memcached ou un Redis mémoire seule ?
- `sessions.timestamp` vs `ufd` : `created / changed / access / login`
- en intranet : `sessions.hostname`

6.8 Enquêtes : journaux (logs)

- Vos logs sont bien hors site en écriture seule ?
  - Remote ELK, Loggly, Logmatic, Logsene, Logz.io, Papertrail, Scalyr….
  - RGPD: votre registre indique où (art 24/30)
- Sur site ?
  - `dblog {watchdog}`
  - `syslog` → suivre la chaîne de renvoi
  - `mongodb_watchdog`, `redis_watchdog`
- Journaux d'applications, services, APIs

6.9 Enquête : outils de police

- Logiciel
  - OpenText (Guidance Software) : Encase
  - AccessData : Forensic Toolkit (FTK)
- Consultants spécialisés, ANSSI

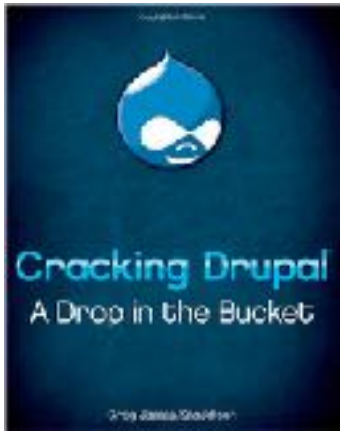
7.1 Retour vers la production

- Refaire une passe des anomalies du bloc 1 sur la nouvelle version
- Réinitialiser les mots de passe.
-
```
update users_field_data
   set pass = concat('ZZZ',
     sha(concat(pass, md5(rand()))))
);
```
- RGPD: rapport d'intrusion (art. 34)
- Préparer les rédactionnels pour le marketing et les réseaux sociaux

7.2 L8R: Préparer la suite

7.3 L8R : se préparer

- Education des développeurs à la sécurité dans le contexte Drupal
  - Security Team mailing list
  - https://twitter.com/drupalsecurity
  - https://www.drupal.org/security/rss.xml
  - http://crackingdrupal.com/



7.3 L8R : se préparer

- Éducation des développeurs à la sécurité en général
  - MOOC de l'ANSSI https://www.secnumacademie.gouv.fr/
  - 4 modules:
    - Panorama de la SSI
    - Sécurité de l'authentification
    - Sécurité sur Internet
    - Sécurité du poste de travail et nomadisme

7.4 L8R : se préparer

- Processus de sécurité
  - Analyser chaque release de sécurité pour comprendre ce qu'elle corrige et comment
  - Rechercher des failles similaires dans le code spécifique
  - Contribuer à Drupal core pour acquérir de l'expertise
- Processus
  - Revue de code croisée systématique
  - Maintenance et développement dirigés par le code
  - Contrôle automatique de qualité sur les chaînes CI
  - Planning des mises à jour de contribution

7.5 Amélioration continue

- On ne peut améliorer que ce qu'on mesure
  - Relever les métriques du bloc 1
- Construire un Plan de Reprise sur Incident à partir du bloc 2
- Planifier des simulations d'intrusion périodiques
  - RGPD: art 32.1.d: « une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement. »

Drupal, *plus rapide, plus sûr*

http://www.osinet.fr/