KYIV 09 DRUPAL CAMP

Drupal.ru

Drupal для параноиков: безопасность сайта и системного окружения VPS и выделенных серверов

А.Графов <axel@drupal.ru>

KYIV 09 DRUPAL CAMP

Drupal.ru

Проблемы

- Нежелательный контент (спам, трояны)
- Изменение кода сайта (кража данных пользователей, вставка нежелательного контента — показ скрытой рекламы, перенаправление на другой ресурс)
- Несанкционированное использование ресурсов сервера (рассылка спама и др.)

KYIV 09 DRUPAL CAMP

Drupal.ru

Причины проблем

- Сеть:
  - Скрипты сайта
  - Вебсервер
  - Другие сетевые службы (ftp, ssh, СУБД...)
- Локальный доступ:
  - Пользователи имеющие доступ (ssh, ftp)
  - Или получившие доступ к серверу при успешной атаке по сети
- Физический доступ к серверу:
  - Данные на жёстких дисках

KYIV 09 DRUPAL CAMP

Способы защиты

- Контроль работы скриптов
- Защита сетевых сервисов
- Разграничение прав между пользователями на исполняемые процессы
- Разграничение прав на доступ к файловой систему
- Ограничение доступа к сетевым сервисам
- Защита данных хранимых на жёстком диске

Drupal.ru

KYIV 09 DRUPAL CAMP

Drupal: защита изнутри

- Обновления ядра и модулей
  - Модуль **update status**
- Фильтр исполнения PHP
- Лишние модули
- Пользователь №1
- Модуль paranoia
  - Блокирует создание форматов включающих исполнение PHP
  - Блокирует изменения аккаунта №1
  - Блокирует отключение модуля paranoia

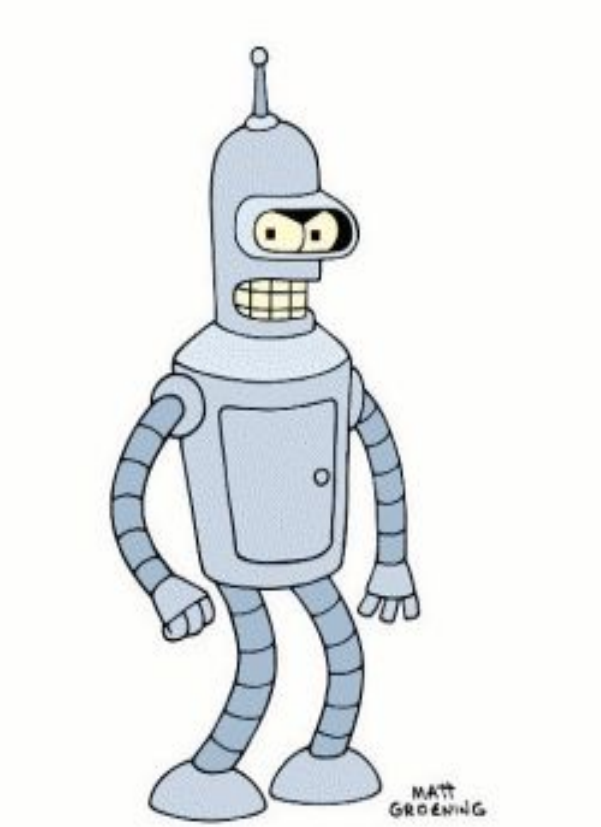
Drupal.ru

Drupal + HTTPS

- Вариант использования:
  - http://example.com/* - контент пользователям
  - Запрет доступа к http://example.com/admin*
  - Доступ к админке https://example.com only!
- Как сделать? Нам поможет:
  - `custom_url_rewrite_inbound( &$result, $path, $path_language)`
  - Переменные например
    - `$_SERVER['HTTP_X_SSL_CONNECT']`
    - `$_SERVER['HTTP_X_FORWARDED_HOST']`
    - `$_SERVER['HTTP_HOST']` и др.

KYIV 09 DRUPAL CAMP
Drupal.ru

Фильтруем контент: технические средства



- «Фейсконтроль» сайта — роботам вход воспрещён: captcha
- Самобучающиеся фильтры
  - Модуль Spam на алгоритме Байеса
  - Правила для URL в модуле Spam
- Публичные спамбазы и блоклисты
  - Mollom — проект Дриса

KYIV 09 DRUPAL CAMP

Drupal.ru

Фильтруем контент: организационные методы

- Общественная модерация
  - Премодерация
  - Постмодерация
  - Пример вики-модерации на drupal.ru
    - Ничего не удаляется!
    - Больше 100 модераторов
    - Легкость внесения правок
    - Бан одним кликом
- Тем эффективнее, чем больше человек задействовано в модерации

KYIV 09 DRUPAL CAMP

Apache mod_security

- mod_security — «файрвол для вебприложений»
  - Проверка GET и POST
  - Фильтрация подозрительного содержимого (ввод-вывод) на основе правил
    - SQL injections
    - XSS
    - Команды ОС
  - Обнаружение троянов
  - Аномалии HTTP-запросов

Drupal.ru

KYIV 09 DRUPAL CAMP

Drupal.ru

Установка **PHP**

- mod_php в Apache — один пользователь на все процессы
- open_base_dir — можно указывать для каждого виртуального хоста
- FastCGI в Apache и NGINX — можно легко разделить пользователей виртуальных хостов
- Suhosin — патч и модуль расширения к PHP

Средства ОС

- Кража паролей — самый частый способ «взлома»
- FTP на продуктиве лучше отключать (use SFTP)
- Защита от последствий украденного пароля на VPS/сервере:
  - Права владения на скрипты сайта передаются другому пользователю (например root)
  - Папки files и tmp — единственные места, куда Drupal требует прав на запись
  - Совет: index.html с правами на запись

Drupal.ru

Средства ОС

- POSIX ACL на файловой системе:
  - Более гибкая схема, чем механизм user:group:other – rwx
  - Упрощённо говоря ACL задавать отдельные права на файл для нескольких пользователей и групп
  - Пакет acltools: getfacl/setfacl

Drupal.ru

Блокировка перебора паролей

- Можно сделать в друпале через hook_user()
- Fail2ban — защита от перебора паролей и от DOS
  - Защита входов SSH и FTP
  - Защита авторизационных форм вебсервера
  - Защита авторизации Drupal:

```
failregex = \|user\|<HOST>\|.*\|Login
 attempt failed (.+)\.$
```

  - Блокирует IP или производит другие действия

KYIV 09 DRUPAL CAMP
Drupal.ru

KYIV 09 DRUPAL CAMP

Сетевой файрвол

- Ограничения доступа на уровне сетевых протоколов и портов
- Не всем приложениям нужен доступ отовсюду из сети: ограничения по IP
- Всегда ли нужен файрвол?

Drupal.ru

KYIV 09 DRUPAL CAMP

Последний рубеж

- ФС в файле через loopback-интерфейс
- Или ФС в отдельном разделе
- Включить поддержку криптографии в ядре
  - AES, Blowfish, DES...
- Критичные данные на шифрованном разделе

```
Cryptographic options  --->
  <M> DES and Triple DES EDE cipher algorithms
  <M> Blowfish cipher algorithm
  <M> AES cipher algorithms (i586)
```

- Пример для Linux:

```
$ cryptsetup -c aes -y create mycrypt /dev/vg/storage
$ mkfs.ext4 /dev/mapper/mycrypt
$ mount /dev/mapper/mycrypt /var/lib/mysql/secured
```

или

```
$ losetup -e aes /dev/loop0 /mnt/secured
```

Drupal.ru

KYIV 09 DRUPAL CAMP

Drupal.ru

Мониторинг работы

- Мониторинг работы основных сервисов локально и перезапуск при необходимости (вебсервер, СУБД, PHP)
- Комплексный мониторинг (Zabbix, ZenOSS)
  - CPU
  - Память
  - Место на ФС
  - Доступность сетевых сервисов
  - Уведомления по почте, СМС
  - Вебинтерфейс с таблицами и графиками

KYIV 09 DRUPAL CAMP

Ссылки на самое вкусное

- Коды примеров и файлов конфигурации можно скачать:
- Ссылки на п/о:
  - http://fail2ban.org
  - http://modsecurity.org
  - http://suhosin.org
  - http://zabbix.com
- Статьи по теме:
  - www.drupal.ru/node/31163 - fail2ban + Drupal
  - http://tr.im/x5cQ - настройка шифрования ФС

Drupal.ru

Drupal.ru

Drupal.ru

Drupal.ru

Drupal.ru

Презентация подготовлена в OpenOffice

Использована иллюстрация из мультсериала Futurama

Вопросы?

А.Графов <axel@drupal.ru>