

## **Сигурност на сайт базиран на Drupal CMS базов наръчник включващ принципни положения и модули за ползване**

1. Сигурността на един Интернет сайт е сходна с тази на вашия дом. Човек не взема предохранителни мерки, докато не се случи нещастие, а когато то се случи – времето за поправяне на щетите и похабените нерви са невъзвръщаем капитал. Какво да направим? Най-вече да бъдем разумни потребители (както сме и стопани на дома си) и да защитим нашия сайт.

### **2. Принципни положения със злонамерен достъп:**

- изтриване на информация или подмяна на страница с друга и компрометиращо съдържание;
- извличане на лични данни на потребителите в сайта;
- пренасочване при достъпване от референтен сървър, към сайт с компрометиращо съдържание.

Трите визирани по-горе случая са напълно реални, срещани в практиката и не може да се каже кой от тях е по-лошо да се случи. Всъщност най-добре е да подходим разумно и да направим нужните стъпки за да защитим нашия труд, информацията – наша или на клиента и да можем да реагираме и възстановим сайта, в случай на неправомерен достъп.

### **3. Основни методи за защита на информацията и сайта:**

- оторизиране пред системата (и контролния панел) чрез SSL криптиращ паролите и верифициращ сайта;
- даване акуратни права на потребители включително и филтрирани формати за въвеждане;
- ограничаване на потребителски роли / login по IP адрес;
- защитаване на формуляра за оторизация пред Drupal включително и известяване при проблем;
- следене на дневника за грешки и генериране на отчет за сигурността на системата;
- вграждане и регулярна употреба на модул за изнасяне на базата данни с цел архив;
- обновяване на Drupal и при нови версии на модулите, особено тези с критични новости за сигурността;
- периодичен архив на целия сайт.

\* \* \*

Друпал е сигурна система. Работейки с нея администраторът разбира гъвкавите възможности за управление на потребителите чрез ролите и съответните им права. Ако сте администратор на сайт с няколко нива на достъп, то след досадната настройка на правата за всяка роля, ще благодарите на системата че разполага точно с такива възможности. Лично не познавам друг CMS базиран на Отворен код и с подобна гъвкавост.

### *4. Когато нещастие се случи...*

За жалост напълно е възможно да сте взели предохранителни мерки прекалено късно и тогава се чудите какво да направите. Запазете духа си и проверете кога е бил последният злонамерен достъп в системата - разглеждайки файлове които са модифицирани и в които се намира злонамерен код. Не се оторизирайте пред Друпал като администратор, освен ако няма друг вариант за вход в системата. Преди да влезнете в системата проверете базата данни за злонамерен код, като я свалите и отворите с текстов редактор.

5. Ако има заменени файлове в коренната папка на споделения хостинг който ползвате, от злонамерен характер – препоръката е да смените паролите на FTP потребителите, както и на контролния панел. Изтрийте всички други приложения (ако има такива) намиращи се в каталога на Вашия Drupal сайт, даващи възможност за управление на файлове. Ако последните са чисти откъм злонамерен код, то уверете се че са максимално защитени в административната си част.

*Приложение – модули, примери от практиката, дискусия. Време на лекцията 45 мин / 1 час*

## 2) Основни концепции и методи за защита на Интернет сайт

Сигурността на Уеб приложението, независимо от своя характер, е работа на администратора на сайта. Тя е неделима част от неговото изграждане и би трябвало да се договаря с клиента, като перо за изработка или поддръжка – на вече изградена или бъдеща Интернет страница. За да бъдем спокойни за нашата информация е добре да спазваме правилото че **тя съществува, само ако е налична на три места.**

Методите за защита на информацията могат да бъдат разделени на три възлови момента – **сигурност при пренос на пароли, максимална сигурност на административния профил/роля, делегиране на акуратни права на потребителите.** В добрия случай инсталираме и настройваме сертификат за сигурна връзка SSL, криптиращ последната при пренос на данни. Можем да ползваме закупен такъв или да генерираме собствен, на нашия сървър. За двете операции е необходима заявка за статичен IP адрес.

Сигурност на административния профил. Препоръчително по IP адрес за управление на сайта. Варианти са достъп до профила на администратора чрез временно получения IP адрес, **който обаче може да бъде раздаден и на трета страна**, затова трябва динамично да се сменя за всяка сесия – което е досадно и отнема време. За професионално управляване на сайтове в Мрежата, задължително условие е статичен IP.

При *добре обмислено задаване права на потребителите* можете спокойно да редактирате информация или делегирате правомощия, като изключите административните функции и такива, които биха довели до възможен злонамерен пробив в системата. Сред тях са и форматите за въвеждане на информация – които трябва внимателно да бъдат настроени. В една отворена система като Форум или възможност за публикуване на коментари или попълване на Уеб формуляри, това е задължително.

В допълнение. Вие работите на споделен хостинг който обезпечава архив на информацията в рамките на 7-10 дни. Ако е извършен пробив в системата, то може *да не сте в състояние да възстановите сайта.* Задължително е да бъде обезпечено решение за извличане на базата данни и файловете от Уеб приложението, със същата условност – да копирате информацията *поне на три места.*

Друпал предлага възможности чрез модули за ръчно и автоматизирано архивиране на базата данни и част от сайта. Можете да настроите модула да съхранява информация на сървъра и дори да я препраща на електронна поща или отваря FTP сесия, в която да осъществи запис на друг сървър. Боравете внимателно с това приложение, в случай че правите запис при трета страна – *създайте специализиран каталог на другия сървър* само за тези архиви и задайте квота и права на потребител за тях.

**Сигурни пароли.** Както виждаме до момента, що касае управлението на сайта – паролите са последното нещо което е важно, но не съществено. Защо е така? Ако не ползваме сигурна връзка (SSL) последните се предават некриптирани в Мрежата и могат да бъдат прихванати от трета страна (man in the middle) която е на линията и подслушва трафика. Също така при злонамерен достъп до Вашия компютър, паролите могат да бъдат компрометирани, но няма как да бъде иззет вашият (статичен) IP адрес, освен ако не сте го включили в мрежа за прокси подобна на [TOR](#), като възможността да бъде получен е сравнително малка.

И все пак... **Ползвайте генератор на пароли** (виж приложението). Паролите които пишете са логични и предвидими. Повечето хора ползват подобни комбинации или замествания на букви със символи. В Друпал можете да вградите модул който да изисква минимален брой знаци, като още по-добре е да бъдат включени специализирани символи и букви, с различна капитализация.

*Отвъд параноята.* Ако искате абсолютно сигурен сайт, то последният трябва да се намира на Виртуален сървър или собствен хост. За средния потребител това е непосилна инвестиция или изисква умения надхвърлящи неговите способности. Можете да направите необходимото следвайки принципите по-горе и най-вече **своята Интуиция**, за обезпечаване информацията на клиента и Вашите лични данни.

В допълнение – абсолютно в реда на нещата е *да добавите стойност* за Вашата услуга по сигурността включваща в себе си и обновяване на Системата на сайта, при необходимост.

# ПРИЛОЖЕНИЕ

Връзки към полезна информация относно сигурността на Drupal и общата сигурност на данните а също и към някои от модулите които ползваме към момента.

## Обща информация

<http://drupal.org/security/secure-configuration>

<http://drupal.org/https-information>

[http://en.wikipedia.org/wiki/Session\\_hijacking](http://en.wikipedia.org/wiki/Session_hijacking)

[http://en.wikipedia.org/wiki/HTTP\\_cookie#Cookie\\_theft\\_and\\_session\\_hijacking](http://en.wikipedia.org/wiki/HTTP_cookie#Cookie_theft_and_session_hijacking)

<http://blamcast.net/articles/block-bots-hotlinking-ban-ip-htaccess>

<http://blog.superhosting.bg/good-vs-bad-bots.html>

[http://help.superhosting.bg/faq/31\\_208\\_bg.html](http://help.superhosting.bg/faq/31_208_bg.html)

## Модули

[http://drupal.org/project/security\\_review](http://drupal.org/project/security_review)

<http://drupal.org/project/schema>

[http://drupal.org/project/restrict\\_by\\_ip](http://drupal.org/project/restrict_by_ip)

[http://drupal.org/project/restrict\\_ip](http://drupal.org/project/restrict_ip)

[http://drupal.org/project/login\\_security](http://drupal.org/project/login_security)

<http://drupal.org/project/session443>

[http://drupal.org/project/backup\\_migrate](http://drupal.org/project/backup_migrate)

[http://drupal.org/project/backup\\_migrate\\_files](http://drupal.org/project/backup_migrate_files)

<http://drupal.org/project/logintoboggan>

[http://drupal.org/project/better\\_formats](http://drupal.org/project/better_formats)

<http://drupal.org/project/goaway>

## Друга информация свързана със сигурността на данни и полезни програми

<http://pwgen-win.sourceforge.net/>

<http://www.truecrypt.org/>

<http://www.gnupg.org/>

<http://code.google.com/p/dngrep/>