Глава 10

Безопасность Joomla-сайта

В главе...

- Что делать, чтобы сайт не взломали
- Потенциально опасные директивы PHP
- Что делать, если сайт взломали
- Список ресурсов, посвященных безопасности Joomla

10.1. Несколько слов о безопасности сайтов

Беда всех стандартных (уже кем-то написанных, доступных для загрузки любому желающему) систем управления контентом (CMS) заключается в том, что они стандартно и взламываются. Причем для взлома сайта не нужно быть хакером высокого уровня — инструкции по взлому стандартных CMS опубликованы на многочисленных сайтах, и в большинстве случаев для их применения не нужно обладать какими-либо специальными знаниями, достаточно уметь использовать браузер. Не выполнить такие инструкции может лишь тот, кто не умеет читать. Помню, я администрировал сайт одной организации, построенный на базе CMS PHP-Nuke. Так вот, за три месяца этот сайт взламывали трижды. После последнего раза я закрыл сайт и написал для него собственную CMS. После этого (до сегодняшнего времени) — ни одного взлома. Секрет заключается в том, что в Интернете нет рекомендаций по взлому моей CMS. Взломать можно любую систему, и я не заявляю, что моя система была сверхзащищенной. Просто отсутствие готовых рекомендаций не позволит взломать ваш сайт любому школьнику.

К сожалению, Joomla — это одна из стандартных систем, которые легко могут быть взломаны. Однако, выполняя некоторые рекомендации и посещая сайты, посвященные безопасности Joomla, вы можете существенно снизить риск взлома вашего сайта. Пользователей Joomla очень много, вы один из них. Возможно, чей-то сайт уже был взломан, и информация о “дыре” уже известна разработчикам Joomla. На специальных сайтах (о них — чуть ниже) вы сможете найти

патчи (заплаты), закрывающие эту дыру. Вовремя установив заплату на свой сайт, вы обезопасите его на некоторое время, пока не будут найдены новые уязвимые места.

Если за полгода ваш сайт не взломали — радуйтесь. Но после того как отпразднуете это событие, обязательно обновите версию Joomla — к тому времени выйдет новая версия со всеми заплатами, и ваш сайт станет еще более недоступным для злоумышленников.

За два года использования Joomla на разных сайтах (если заказчик не хочет платить за разработку эксклюзивной CMS, устанавливается уже готовая, как правило — Joomla) был всего один факт взлома. Правда, взломали сайт, о котором я давно забыл и не присматривал за ним (не обновлял программное обеспечение). Разобравшись в причинах взлома, я выяснил, что проблема заключалась не только в Joomla, но и в настройках хостинга. После закрытия дыры взлом не повторился. Ведь безопасность сайта — это не только безопасность CMS. Нужно также учитывать безопасность хостинга и человеческий фактор (например, слишком простой пароль администратора).

Итак, приступим к рекомендациям, позволяющим обезопасить сайт.

10.2. Удаляем каталог installation

Если вы еще не сделали этого после установки Joomla, сделайте это сейчас. Ранние версии Joomla не запускались, если каталог `installation` не был удален. Версия 1.5 запускается, но на панели управления вы увидите соответствующее сообщение. Версии 2.5 и 3.0 не запускаются — вы не можете зайти ни на сайт, ни в панель управления, — и это правильно. Так никто не сможет переустановить вашу же Joomla.

10.3. Отключаем директиву register_globals

Самая примитивная в реализации, но и одна из самых эффективных защит Joomla заключается в отключении директивы `register_globals`. Если у вас есть доступ к файлу конфигурации `php.ini`, откройте его и отключите эту директиву:

```
register_globals = 0
```

Директива `register_globals` — это не дыра в PHP; просто некоторые разработчики, в том числе разработчики Joomla, не умеют правильно писать код с включенной директивой `register_globals`. Это я заявляю открыто, поскольку, если бы код был написан правильно, об этой проблеме не было бы упоминаний в каждом руководстве по Joomla-безопасности. В любом случае эту директиву лучше отключить.

Если у вас нет доступа к файлу `php.ini`, попросите администратора хостинга отключить ее или же создайте файл `.htaccess` и поместите его в корневой каталог Joomla. Файл `.htaccess` должен быть следующего содержания:

```
php_value register_globals 0
```

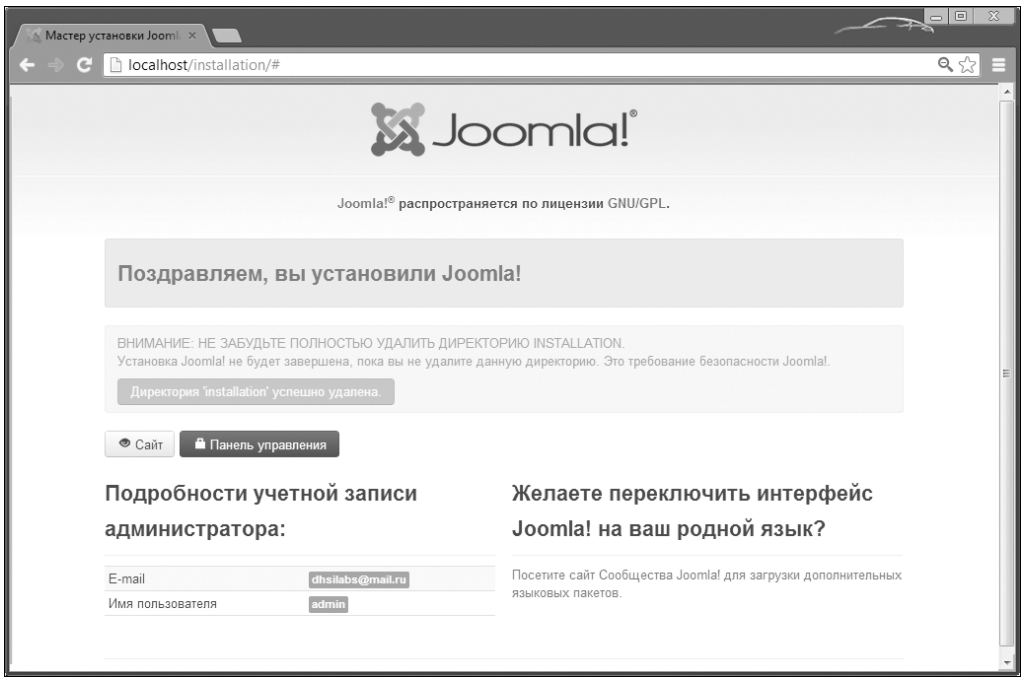

Рис. 10.1. *Каталог* `installation` *успешно удален*

10.4. Отключаем другие потенциально опасные директивы PHP

Директива `disable_functions` содержит список запрещенных PHP-функций. На хорошо защищенном хостинге этот список выглядит так:

```
disable_functions = show_source, system, shell_exec,
passthru, exec, phpinfo, popen, proc_open
```

Также нужно отключить директивы `safe_mode` и `allow_url_fopen`:

```
safe_mode = 0
allow_url_fopen = 0
```

Последние две директивы, если нет возможности редактировать файл `php.ini`, можно добавить в файл `.htaccess`:

```
php_value safe_mode 0
php_value allow_url_fopen 0
```

Также настоятельно рекомендуется (особенно для версии Joomla 3.0) выключить директиву `magic_quotes_gpc`. Если у вас есть доступ к файлу конфигурации, просто найдите следующие директивы и установите для них значение `off`:

```
magic_quotes_gpc = off
magic_quotes_runtime = off
magic_quotes_sybase = off
```

Если доступа к файлу `php.ini` у вас нет (т.е. у вас не собственный сервер, а купленный хостинг), добавьте в файл `.htaccess` строку

```
php_flag magic_quotes_gpc off
```

Если после этого ваши сценарии перестали запускаться и вы видите ошибку 500 в браузере, попросите хостинг-провайдера отключить `magic_quotes` через файл `php.ini`. Вам отказали в вашей просьбе? Тогда задумайтесь о смене провайдера.

10.5. Устанавливаем правильные права доступа

Установите для файла конфигурации `configuration.php` права доступа в виде значения `444`. Правда, после этого вы не сможете изменять параметры Joomla (потребуется заново установить права `666`, затем изменить файл и опять установить права `444`):

```
chmod 444 configuration.php
```

На все файлы установите права доступа в виде значения `644` (кроме `configuration.php`), а на все каталоги — в виде значения `755`. Но это нужно сделать уже после того, как вы настроили сайт и установили все необходимые расширения. Права со значением `777` нужно установить только на следующие каталоги.

- `administrator/backups/`
- `cache/`
- `images/`
- `images/banners/`
- `images/stories/`

Желательно каталог `administrator` защитить паролем. Во многих панелях управления хостинга есть такая возможность, и реализовать защиту паролем можно за считанные секунды. За подробной консультацией обратитесь в службу технической поддержки хостера.

Я помогу вам разве что с панелью DirectAdmin, которую использую сам. На главной странице выберите команду Защита директорий (рис. 10.2), затем — команду Выберите папку для защиты, после чего перейдите в каталог, в который вы установили Joomla, и напротив каталога administrator щелкните на ссылке Protect (рис. 10.3), чтобы ввести пароль доступа

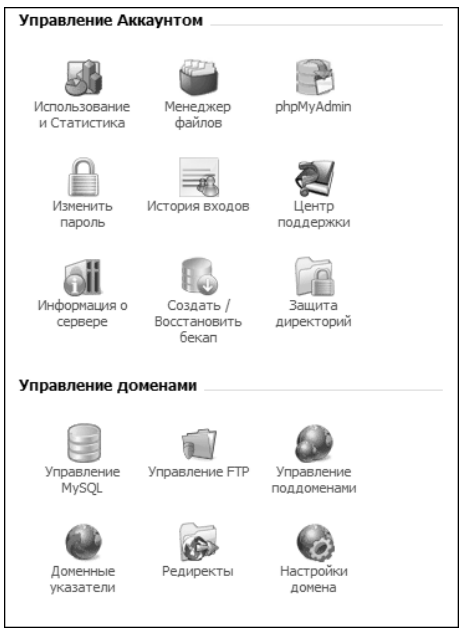

Рис. 10.2. *Щелкните на кнопке* Защита директорий

(рис. 10.4). Полный путь к своему каталогу `administrator` на рис. 10.4 я стер из соображений безопасности.

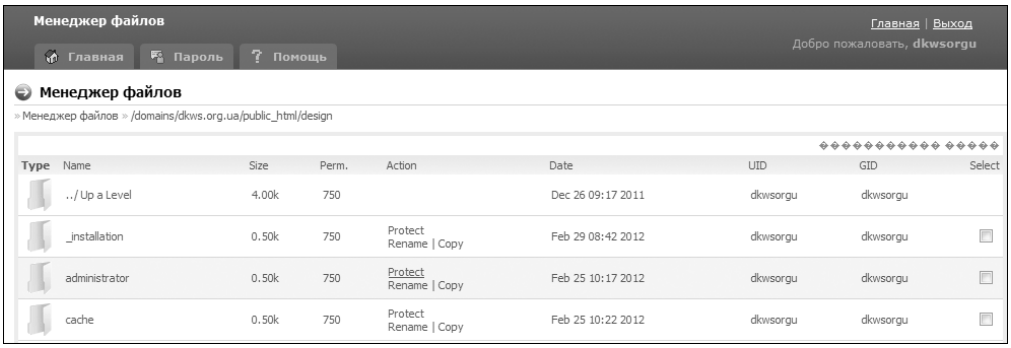

Рис. 10.3. *Выбор каталога для защиты паролем*

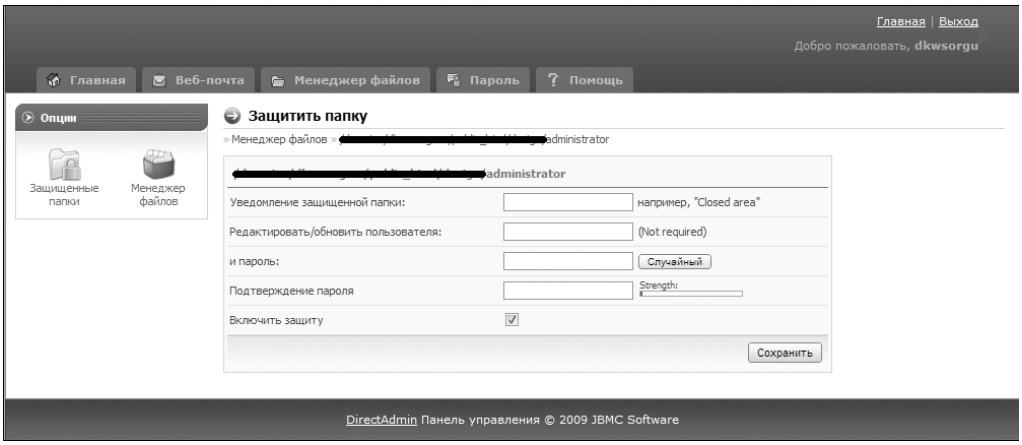

Рис. 10.4. *Установка пароля*

10.6. Обеспечиваем доступ к панели управления с определенных IP-адресов

Скорее всего, вы управляете сайтом с одной-двух подсетей, например с рабочего IP-адреса и с домашнего. Именно эти IP-адреса и нужно считать разрешенными, доступ со всех остальных адресов к панели управления нужно считать нелегальным.

Создайте файл `.htaccess` следующего содержания:

```
<Limit GET>
   Order Deny, Allow
   Deny from all
   Allow from 91.91.91.91, 91.91.91.92
</Limit>
```

Данный файл разрешает доступ к каталогу `administrator` только с IP-адресов `91.91.91.91` и `91.91.91.92`. Этот файл `.htaccess` нужно поместить в каталог `administrator`.

Что делать, если у вас динамический IP-адрес? Можно разрешить доступ всем IP-адресам из вашей подсети, но где вероятность, что вас не взломает кто-то из ваших "соседей" по сети? Существует одно не очень удобное, но очень безопасное решение. Если вы работаете в Windows, выполните команду меню Пуск⇨Выполнить, затем введите команду `cmd`, а в появившемся окне — команду `ipconfig`. Вы узнаете ваш IP-адрес. В Linux нужно открыть терминал и ввести команду `ifconfig`. Она также сообщит вам ваш IP-адрес. Далее нужно зайти по FTP-протоколу на сервер и изменить файл `.htaccess` из каталога `administrator`, прописав в нем свой IP-адрес.

Такую процедуру придется выполнять при каждом входе на сайт, но это самое безопасное решение. В некоторых случаях, например когда время аренды IP-адреса составляет 24 часа, данный способ не доставляет особых неудобств. Поскольку новый IP-адрес вам назначается раз в сутки, 24 часа вы можете заходить на панель управления без изменения файла `.htaccess`.

10.7. Я уезжаю в отпуск...

Вы боитесь оставить ваш Joomla-сайт без присмотра на время отпуска? Тогда зайдите по FTP на ваш сервер, перейдите в каталог `administrator`, откройте файл `.htaccess` и измените его следующим образом:

```
<Limit GET>
   Order Deny, Allow
   Deny from all
</Limit>
```

Теперь ни вы, ни кто-нибудь другой не сможет войти на панель управления. Когда ваш отпуск закончится, верните исходную версию файла `.htaccess`.

10.8. Проведем небольшой тест

Введите следующий URL:

`http://`*`ваш_сайт`*`/components/`

Если вы увидели сообщение о том, что доступ запрещен, значит, все нормально. А вот если сервер выдал список файлов и каталогов, значит, он настроен неправильно. Нужно отключить опцию `Indexes`, о чем следует уведомить администратора сервера. А пока он будет ее отключать, поместите в каждый каталог, в котором нет файла `index.html` или `index.php`, пустой файл `index.html`. Тогда вместо списка файлов и каталогов сервер выведет пустой файл (можете оставить в файле любое сообщение для злоумышленника — тогда он увидит его).

10.9. ЧПУ, файл .htaccess и резервные копии

Использование дружественных URL (ЧПУ) не только хорошо для поисковой оптимизации, но и помогает защитить ваш сайт от взлома. Включение ЧПУ существенно затрудняет взлом сайта. Так что не следует игнорировать поисковую оптимизацию — она, помимо всего прочего, помогает и защитить сайт.

В корневом каталоге Joomla находится файл `htaccess.txt`. На сервере переименуйте его в файл `.htaccess`. Это также повысит безопасность сайта.

Регулярно делайте резервные копии файлов сайта и его базы данных. Если ваш сайт обновляется не очень часто, вполне достаточно будет создавать резервные копии раз в неделю. Для часто обновляемых сайтов, обладающих высокой посещаемостью, будет полезно создавать резервные копии несколько раз в сутки (хотя бы, например, в 12:00 и 00:00 или в 08:00 и 22:00). Как правило, на панели управления сайтом (доступ к ней предоставляется хостером) есть возможность создания расписания для процедуры создания резервной копии. Если такой возможности нет, уточните у хостера, когда создаются резервные копии и как можно изменить расписание, чтобы оно соответствовало вашим требованиям. На моем хостинге копии создаются автоматически самим хостером один раз в сутки, чего для моего ресурса вполне достаточно.

В случае взлома резервная копия вам очень пригодится. С ее помощью вы сможете быстро восстановить работоспособность сайта. Однако мало восстановить сайт. Нужно найти и устранить причину взлома, а вот об этом мы как раз и поговорим в следующем разделе.

10.10. Что делать в случае взлома

Первым делом нужно просмотреть журналы сервера на предмет следующих строк:

```
mosConfig
http://
wget
perl
_REQUEST
```

Чаще всего наличие таких строк в журналах сервера указывает на факт взлома. По содержимому подобных строк попробуйте определить IP-адрес злоумышленника и закройте доступ к вашему серверу с его подсети. Это не панацея, так как завтра вас могут взломать из другой точки земного шара, но как временное решение — вполне нормально.

Восстановите систему Joomla и сайт из резервной копии. После этого измените следующие пароли:

- пароль администратора Joomla;
- пароли всех дополнительных администраторов, если таковые есть на вашем сайте;

- пароль учетной записи FTP;
- пароль пользователя MySQL (после этого требуется изменить файл `configuration.php`, чтобы "прописать" в нем новый пароль, иначе Joomla перестанет открываться);
- пароль для доступа к панели управления хостингом.

После того как сайт будет восстановлен, посетите сайт `www.joomla.org`. Возможно, уже доступна новая версия Joomla. Если это так, обновите Joomla. Затем просмотрите, какие нестандартные расширения (т.е. те, которые вы устанавливали сами) у вас установлены. Посетите сайты их разработчиков: возможно, есть обновления и расширений. Обязательно обновите все используемые расширения. В большинстве случаев обновление помогает закрыть текущие дыры.

10.11. Список ресурсов

Сейчас мы рассмотрим список ресурсов, посвященных безопасности Joomla. Эти ресурсы нужно периодически посещать, чтобы обеспечить максимальную защиту вашего сайта.

Первым делом нужно ознакомиться с контрольным списком безопасности. Надеюсь, вы знаете английский язык, потому что на русском такого списка пока нет:

`http://docs.joomla.org/Joomla_Administrators_Security_Checklist`

Затем прочитайте краткое руководство администратора по обеспечению безопасности Joomla-сайта. Благо оно на русском языке:

`http://www.joomla-docs.ru/Безопасность`

Список уязвимых мест и способов защиты от взлома сайта через них них можно найти на сайте Joomla-портала в категории Безопасность:

`http://joomlaportal.ru/content/blogcategory/15/88/`

И не забывайте об обновлениях! К счастью, теперь Joomla сама уведомляет о выходе новой версии — в панели управления вы найдете кнопки уведомлений о выходе новой версии CMS и ее расширений. К сожалению, полностью защитить сайт невозможно. Даже если разработчики Joomla создадут абсолютно безопасную систему, никто не даст вам гарантии, что устанавливаемые расширения сторонних разработчиков будут абсолютно безопасны. Очень часто система взламывается из-за бреши не в ней самой, а в каком-то расширении. Поэтому следует внимательно относиться к устанавливаемым расширениям и перед установкой расширения почитать отзывы о нем. Наверняка в Интернете уже есть сведения о том, что устанавливаемое расширение небезопасно (или, наоборот, безопасно).