Безопасность

«ДокуВики» — это веб-приложение и оно часто используется на публичных серверах, доступных из интернета. Это означает, что есть бóльший риск подвергнуться нападению злонамеренных людей, чем, например, при применении на вашей настольной системе.

«ДокуВики» разработана с учётом требований безопасности. Мы пытаемся найти баланс между дружелюбием к пользователю и безопасностью, но предпочитаем безопасность пользе, когда компромисс не может быть найден.

Эта страница должна дать краткий обзор, на какие аспекты заострить внимание, чтобы удостовериться, что ваша «ДокуВики» безопасна.

Создание отчетов и уведомлений

Если обнаружена проблема безопасности в «ДокуВики», пожалуйста, сообщите нам. Предпочтительные способы:

- Предоставить отчет об ошибках
- Отправить сообщение в список рассылок
- Отправить приватное сообщение andi@splitbrain.org

Для небольших багов предпочтительнее первые два способа. Насчет очень серьезных ошибок, которые могут быть использованы для написания эксплойтов для «ДокуВики», рекомендуем пользоваться приватной перепиской.

Все предыдущие проблемы безопасности описаны в bugtracking system.

В зависимости от серьезности найденной проблемы безопасности, либо она будет исправлена в будущем выпуске (по очень незначительным проблемам), либо будет выпущен срочный bugfix-релиз. В последнем случае пользователи будут проинформированы через механизм проверки обновлений.

Вы должны **всегда** использовать самую последнюю версию «ДокуВики», поскольку старые версии никогда не исправляются.

Безопасность веб-доступа

«ДокуВики» хранит конфигурацию и статьи в файлах. Эти файлы никогда не должны быть доступны непосредственно из сети. Распространяемый tarball содержит ряд `.htaccess` файлов, которые указывают веб-серверу Apache закрыть доступ к определенным папкам.

Если вы не используете веб-сервер Apache, или ваш Apache не использует `.htaccess`-файлы, вы должны вручную защитить свою установку

Следующие папки **не должны** быть доступны из сети:

- `bin`
- `conf`
- `data`
- `inc` (хотя не особо и опасно)

Чтобы проверить, должны ли вы настроить права доступа попытайтесь получить доступ к `http://yourserver.com/dokuwiki/data/pages/wiki/dokuwiki.txt`. Вы не должны получить доступ к файлу по этому пути. Если вы видите исходный код - у вас проблема с безопасностью сервера.

Запрет доступа к папкам в Apache

Самый простой путь состоит в том, чтобы включить поддержку файлов `.htaccess` в вашей конфигурации Apache. Посмотрите учебник Apache по .htaccess.

«ДокуВики» поставляется с правильно сконфигурированными `.htaccess`-файлами. Содержимое файла `.htaccess` для блокировки доступа к папке, в которой он находится, должно быть следующим (корректно для версий 2.2 и 2.4):

```
<IfModule !mod_authz_core.c>
  Order deny,allow
  Deny from all
</IfModule>
<IfModule mod_authz_core.c>
  Require all denied
</IfModule>
```

Примечание: При использовании apache2 на Ubuntu файлы `.htaccess` будут работать только после активации 'mod_rewrite' в Apache2 (*sudo a2enmod rewrite && sudo service apache2 restart*)

Возможно, Apache2 в целом, либо по-особому в Ubuntu, настраивается несколько иначе, чем Apache1.x.

Нужно исправить в файле `/etc/apache2/sites-available/default` (или `default-ssl` в случае использования протокола HTTPS) AllowOverride в <Directory /var/www/> с **none** на **all** в следующем месте:

```
NameVirtualHost *
<VirtualHost *>
        ServerAdmin admin@site.com

        DocumentRoot /var/www/
        <Directory />
                Options FollowSymLinks
                AllowOverride None
        </Directory>
        <Directory /var/www/>
                Options Indexes FollowSymLinks MultiViews
                AllowOverride none
                Order allow,deny
```

```
                allow from all
        </Directory>
```

Сделайте */etc/init.d/apache2 reload* для обновления конфига Apache и файлы `.htaccess` будут работать.

(Полное обсуждение на http://ubuntuforums.org/showthread.php?t=47669)

[Эту поправку можно применить к отдельной папке с установленной ДокуВики, нп. `/var/www/путь-к-dokuwiki`, а не к глобальным настройкам всего сервера]

Другой путь состоит в использовании директивы *LocationMatch* внутри описания *VirtualHost*. Это немного более эффективно чем файлы `.htaccess`. Ниже директивы *Directory* добавьте:

```
<LocationMatch "/(data|conf|bin|inc)/">
    Order allow,deny
    Deny from all
    Satisfy All
</LocationMatch>
```

Загляните в секцию «What to use When» в http://httpd.apache.org/docs/2.0/sections.html#file-and-web для уточнения что директивы Location *не используются для защиты объектов файловой системы, а только для виртуальных (например, созданных базой данных) путей. По моему мнению (*прим. перев. *автора англоязычной статьи) если `.htaccess` недоступны или недостаточны, наиболее безопасный вариант - поместить папко-специфичные ограничения прямо в конфиг хоста. Здесь, кажется, верный подход - но это документ должен быть «каноническим».*

Вышеуказанное может вызвать проблемы, если у вас есть еще один «корень», что включает в себя папки `data|conf|bin|inc`. Например, другой вики-проект. Вы можете избежать этой проблемы путем расширения вашего *LocationMatch* в пределах папки (**тут неясно** You can avoid this problem by extending your LocationMatch within your wiki installation folder.).

```
        <Directory /var/www/dokuwiki>
            order deny,allow
            allow from all
        </Directory>

        <LocationMatch "/(data|conf|bin|inc)/">
            order allow,deny
            deny from all
            satisfy all
        </LocationMatch>
```

Запрет доступа к папкам в IIS

Доступ к упомянутым папкам может быть отключен в параметрах конфигурации IIS.

IIS 8+

(Windows 8(.1) и Servers 2012 или 2012R2):

1. Выберите «IIS Request Filtering»
2. Перейдите на вкладку «URL»
3. Щёлкните «Deny Sequence»
4. Введите «/data/» в появившееся окно
5. Повторите с остальными защищаемыми папками

IIS 7

1. Выберите «IIS Request Filtering»
2. Перейдите на вкладку «URL»
3. Щёлкните «Deny Sequence»
4. Введите «/data/» в появившееся окно
5. Повторите с остальными защищаемыми папками

Примечание: По умолчанию оснастка Консоли Управления для Internet Information Services 7 не имеет доступа интерфейса к секции «IIS Request Filtering». Это исправляется установкой «IIS Administration pack 1.0» через Web Platform Installer.

Ещё примечание: Убедитесь в точном вводе «/data/», а не «/data», иначе станут недоступны страницы, начинающиеся с «data...»

Альтернатива для IIS 7+

Если нет доступа к конфигу IIS (как обычно бывает на хостингах), можно использовать ещё пару методов на выбор:

Альтернатива 1:

Положите в корень вики следующий файл:

web.config

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
    <system.webServer>
        <security>
            <requestFiltering>
                <filteringRules>
                </filteringRules>
```

```
                <denyUrlSequences>
                    <add sequence="/data/" />
                    <add sequence="/conf/" />
                    <add sequence="/bin/" />
                    <add sequence="/inc/" />
                </denyUrlSequences>
            </requestFiltering>
        </security>
    </system.webServer>
</configuration>
```

Альтернатива 2:

Положите в закрываемые папки следующий файл:

web.config

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
    <system.webServer>
        <handlers accessPolicy="None" />
    </system.webServer>
</configuration>
```

IIS 6.5-

1. Откройте инструмент конфигурирования: Пуск → Настройки → Панель управления → Администрирование → Internet Information Services
2. Переместитесь к папке, которую вы хотите защитить: Local Computer → Web Sites → Default Web Site → *путь к папке data*
3. Щелкните правой кнопкой по папке и выберите Properties → Directory Security → IP address and domain name restrictions → Edit…
4. Выберите «By default, all computers will be: Denied access»
5. Повторите с остальными защищаемыми папками

Запрет доступа к папкам в Lighttpd

Используя URL re-write вы можете закрыть доступ к вышеупомянутым папкам. В файле `lighttpd.conf` добавьте нижеследующее правило подстановки URL, достаточное, чтобы не пускать людей. Пример предполагает, что ваша «ДокуВики» установлена в http://yourwebsite.tld/dokuwiki/. Не забудьте раскомментировать «mod_rewrite» в разделе server.modules.

```
url.rewrite-once = ( "^/dokuwiki/(data|conf|bin|inc)/+.*" =>
"/nonexistentfolder" )
```

Запрет доступа к папкам в Nginx

Доступ к вышеупомянутым папкам может быть отключен в разделе конфига Nginx, касающегося сервера DokuWiki. Добавьте нижеследующие локации в файл `nginx.conf`.


Эта инструкция слегка вводит в заблуждение. На самом деле нужно отредактировать файл `/etc/nginx/sites-available/default`. Не забудьте сначала создать резервную копию: *cp /etc/nginx/sites-available/default /etc/nginx/sites-available/default.bak*

```
    location ~ /(data|conf|bin|inc)/ {
      deny all;
    }
```

Примечание: При использовании xsendfile вышеуказанное правило ломает функционал sendfile. Необходимое уточнение:

```
    location ~ /(conf|bin|inc)/ {
        deny all;
    }
    location /data/ {
        internal;
    }
```

Также рекомендуется запретить доступ к файлам `.htaccess`:

```
    location ~ /\.ht {
      deny  all;
    }
```

(Коммент: nginx не пользуется `.htaccess`, так что это бессмысленно)

Запрет доступа к папкам в Cherokee

При использовании Cherokee запретить доступ к папкам относительно легко. В *cherokee-admin* выберите виртуальный сервер, где установлена «ДокуВики» и выберите управление правилами, добавьте новое правило «Регулярное выражение» и вставьте туда (считается, что вики находится в корневой папке):

```
   /(data|conf|bin|inc)/
```

Не забудьте поставить «NON FINAL», в ином случае некоторый код в этих папках может быть выполнен при определенных обстоятельствах (правилом «Extensions php» как «NON FINAL», например).

Затем зайдите в секцию «Обработчик» и выберите HTTP Error и в нём – «403 Forbidden».

Переименование папки data

Защита папки `data` очень важна. Если вы не можете переместить папки из веб-сервера (см. описание ниже) или не можете сконфигурировать свой веб-сервер, чтобы запретить доступ (см. выше), то вы должны, по крайней мере, усложнить получение имени папки данных.

Чтобы сделать так, переименуйте свою папку данных на что-то сложное (например, длинную строку букв и чисел) и переконфигурируйте опцию savedir в вашем файле `conf/local.php` (лучше через FTP, а не веб-форму *Управление/Настройки вики*).

Перемещение папок из корневой папки

Самый безопасный способ избежать любого доступа к упомянутым папкам состоит в том, чтобы переместить их из корневой папки веб-сервера.

Предупреждение: Установщик вики работает с жёстко заданными оригинальными именами папок и вы должны применить его прежде, чем сделаете перемещения. Иначе выполнить установку вики не получится.

Папка data

1. Переместите папку `data` (и всё её содержимое) из корневой папки
2. Отредактируйте настройку savedir, чтобы указать на новое расположение папки `data`.

Например, если папка `data` перемещена в `.home/yourname/data`, добавьте следующую строку в `conf/local.php`:

```
$conf['savedir'] = '/home/yourname/data';
```

Папка conf

1. Переместите папку `conf` (и всё её содержимое) из корневой папки
2. Создайте в папке `inc` файл `preload.php` и переустановите там переменную *DOKU_CONF* на новое расположению папки `conf`.

Например, если папка `conf` перемещена в `/home/yourname/conf`, создайте следующую запись в `inc/preload.php`:

inc/preload.php

```
<?php
// Не используйте закрывающий  php  тег. Это вызывает проблему с каналами, помимо прочего.
// Для получения дополнительной информации по этой проблеме, пожалуйста, см:
//  http://www.dokuwiki.org/devel:coding_style#php_closing_tags
```

```
define('DOKU_CONF','/home/yourname/conf/');
```

Папка bin

Папка `bin` содержит CLI инструменты. Если у Вас нет доступа к шеллу на вашем сервере, вы можете просто удалить эту папку и её содержимое. Иначе переместите её из корневой папки. Никакая дальнейшая конфигурация не нужна.

Папка inc

В настоящий момент нет никакого легкого способа переместить эту папку из корневой папки. Но так как она не содержит уязвимых данных, не стоит прилагать каких-то усилий для этого.

Примечание: Однако, если перемещалась папка `conf`, файл `inc/preload.php` может навести на её расположение, а оттуда может стать известным новое имя и расположение папки `data`, что делает всю затею с перемещениями довольно бессмысленной. Постарайтесь договориться с хостером вашего сервера о защите папок методами, что описаны выше для различных видов серверов.

Параметры конфигурации «ДокуВики»

«ДокуВики» содержит несколько параметров конфигурации, которые оказывают влияние на различные аспекты безопасности установки. Пожалуйста, изучите документацию по каждой настройке, чтобы понять, что они делают и каковы их параметры по умолчанию.

- allowdebug — отключает отладочную информацию во избежание системной утечки информации 
- fmode, dmode — устанавливает права на файлы, создаваемые «ДокуВики»; также читайте информацию об установке прав;
- fetchsize — настраивает кэширование внешних данных;
- fullpath — показывает полные пути страниц;
- auth — виды аутентификации;
- usewordblock — предотвращает спам с помощью «чёрного списка»;
- mailguard — кодирует e-майлы для защиты от спамоботов - сборщиков адресов;
- iexssprotect — занимается защитой от проблем в XSS в пределах Internet Explorer’а;
- htmlok — включает парсинг вставляемого HTML-кода;
- phpok — включает парсинг вставляемого PHP-кода;
- hidepages — скрывает определённые страницы от индексации и поиска;
- safemodehack (англ.) — занимается работой при ограничениях безопасного режима;
- disableactions — отключает некоторые функции, например, регистрацию или просмотр исходников.

Безопасность плагинов

DokuWiki имеет много разрабатываемых сообществом плагинов. Плагины добавляют новую функциональность к DokuWiki, расширяя её код. Это означает, что у них есть фактически полный доступ к Вашему серверу. Кроме того, плагины распространяются отдельно от DokuWiki, иногда довольно специфичными способами. Они не подвергаются столь тщательной проверке, как кодовая база DokuWiki. Таким образом, необходимо принять необходимые меры безопасности до установки плагинов.

Вот некоторые подсказки, чтобы помочь вам с выбором плагинов, которые вы устанавливаете.

- Если понимаете языки программирования, ознакомьтесь самостоятельно с исходными кодами плагина - *до* его установки.
- Если сомневаетесь, спросите в списке рассылки.
- Плагины устанавливаются в DokuWiki в папку «lib», которая напрямую доступна извне. Необходимо очень внимательно просматривать код таких плагинов и закрывать доступ к ним через файл `.htaccess`.
- Плагины созданы разработчиками, напрямую не связанными с проектом DokuWiki - они могут быть неопытными, иметь злые намерения или могут разместить исходный код плагина на сервер, который был скомпрометирован. Будьте осторожны в доверии!
- Просмотрите страницу плагина для выявления упомянутых предупреждений безопасности и обновляйте плагин, когда его новый выпуск станет доступным.

См. также: Как сообщить о проблеме безопасности в плагине

Контроль доступа

С помощью средств управления доступом можно указать, какие папки и файлы сайта будут доступны через браузер, каким группам и пользователям, и с какой степенью свободы.

Дополнительное чтение

Вот еще несколько внутренних и внешних страниц, связанных с безопасностью.

- Принудительное использование HTTPS при авторизации
- Настройка PHP для «ДокуВики»
- Удаление правил ACL для удаленных страниц
- Apache Security - Глава 3: Locking down PHP (англ.)
- Как полностью скрыть несанкционированные страницы (англ.)

security-old