Правила безопасности для авторов плагинов

Создание плагинов для DokuWiki очень просто даже для начинающих программистов PHP. Чтобы убедиться, что ваш плагин не ставит под угрозу безопасность всей вики, на которой он установлен, вам следует следовать рекомендациям, изложенным на этой странице.

 Улучшение этой страницы всегда приветствуется. Она находится в очень сыром состоянии и должна быть расширена более подробной информацией, ссылками и примерами.

Краткое содержание

Список наиболее распространенных проблем безопасности и способы их избежания можно найти на этой странице. Краткое резюме:

- Межсайтовый скриптинг (XSS) — вставляет вредоносный код на веб-сайт для манипулирования сайтом в браузере пользователя.
- Подделка межсайтовых запросов (CSRF) — уловки, позволяющие вам совершать неосознанные вредоносные действия на вашем сайте.
- Удаленное включение кода – включает код на сервере, который там выполняется.
- Утечка информации – отображается слишком много информации
- SQL-инъекция – можно выполнить нежелательные запросы к вашим данным

Также добавлено примечание о необходимости сообщать о проблемах безопасности .

Межсайтовый скриптинг (XSS)

Это, вероятно, самая распространенная уязвимость, встречающаяся в плагинах DokuWiki.

Cross Site Scripting относится к атаке, при которой вредоносный код JavaScript внедряется на веб-сайт. Это может использоваться для перенаправления невинных пользователей на вредоносные веб-сайты или для кражи аутентификационных cookie-файлов.

Механизм плагинов DokuWiki дает разработчикам плагинов большую гибкость. В случае с плагинами синтаксиса, в частности, фреймворк дает плагинам возможность работать с сырым необработанным выводом. Это означает, что данные страницы вики, которые достигают вашего плагина, вообще не были обработаны. И не будет никакой дальнейшей обработки вывода после того, как он покинет ваш плагин.

Выход из режима экранирования

Как минимум, плагин должен гарантировать, что все выходные необработанные данные будут содержать все специальные символы HTML , преобразованные в сущности HTML с помощью

функции htmlspecialchars(). DokuWiki предоставляет удобный ярлык hsc() для этой функции. Значения URL-адресов следует экранировать с помощью rawurlencode().

Кроме того, следует с подозрением относиться к любым данным вики, извлеченным и используемым внутри компании (например, именам пользователей).

Проверка входных данных

Всегда проверяйте все ваши входные данные. Используйте белые списки, фильтры, преобразования в точный тип данных, который вы имеете в виду, например, из числа, введенного как смешанное значение php, в целое число и т. д., чтобы убедиться, что у вас есть только разрешенные вами данные.

Также ознакомьтесь с нашей главой об обработке переменных запросов, таких как _GET, _POST или _SERVER.

Смотрите также:

- Межсайтовый скриптинг
- Шпаргалка по XSS

Типичные примеры уязвимостей

Ниже показаны некоторые очень распространенные проблемы. Примеры очень просты, чтобы сделать общую проблему понятной. Ваш плагин, вероятно, сложнее, но вам нужно отслеживать те же уязвимости.

Синтаксис Тела

Многие простые плагины синтаксиса принимают часть введенных пользователем данных и форматируют их в виде пользовательского HTML .

Пример: Вот плагин сокращенного синтаксиса, позволяющий выделить заданный ввод жирным шрифтом.

```
class syntax_plugin_bold extends DokuWiki_Syntax_Plugin {
    // общие функции плагина опущены

    public function connectTo($mode) {
        $this->Lexer->addSpecialPattern('!!!.*?!!!', $mode, 'plugin_bold');
    }

    public function handle($match, $state, $pos, Doku_Handler $handler){
        return [substring($match, 3, -3)];
    }

    public function render($format, Doku_Renderer $renderer, $data) {
        if($format != 'xhtml') return false;
        $renderer->doc .= '<b>' . $data[0] . '</b>';  // без экранирования
    }
}
```

Как вы можете видеть, необработанные входные данные, захваченные в шаблоне лексера, просто передаются в метод рендеринга, где экранирование вообще не выполняется. Злонамеренные пользователи могут вводить любой код JavaScript и HTML , который они хотят.

Решение простое: правильный побег.

```
class syntax_plugin_bold extends DokuWiki_Syntax_Plugin {
    // общие функции плагина опущены

    public function connectTo($mode) {
        $this->Lexer->addSpecialPattern('!!!.*?!!!', $mode, 'plugin_bold');
    }

    public function handle($match, $state, $pos, Doku_Handler $handler){
        return [substring($match, 3, -3)];
    }

    public function render($format, Doku_Renderer $renderer, $data) {
```

```
        if($format != 'xhtml') return false;
        $renderer->doc .= '<b>' . htmlspecialchars($data[0]) . '</b>';
//экранирование
    }
}
```

Формы

Когда ваш плагин предоставляет форму, очень часто требуется проверить вводимые данные и повторно отобразить форму с полученными данными пользователя в случае возникновения ошибки проверки.

Пример: ниже показана форма, уязвимая для атаки XSS, поскольку она не экранирует правильно введенные пользователем данные:

```
<form action="" method="post">
    <input type="text" name="q" value="<?php echo $_REQUEST['q']?>" />
    <input type="submit" />                    //без экранирования
</form>
```

Предоставление данных `"><script>alert('bang')</script>` в качестве входных данных пользователя приведет к эксплуатации уязвимости.

Для исправления формы используйте функцию htmlspecialchars() или функцию DokuWiki shortcut hsc():

```
<form action="" method="post">
    <input type="text" name="q" value="<?php echo hsc($_REQUEST['q'])?>" />
    <input type="submit" />
//экранирование
</form>
```

В целом рекомендуется не создавать формы вручную, а использовать библиотеку форм DokuWiki .

Классы и другие атрибуты

Часто плагины принимают несколько параметров и опций, которые используются для изменения выходных данных плагина.

Представьте себе плагин, принимающий следующие входные данные для отображения окна сообщения:

```
<msg warning>Do not believe anything!</msg>
```

В методе рендеринга этого синтаксиса может быть такой код:

```
$renderer->doc .= '<div class="msg_' . $class . '">'  //$class может быть чем
```

```
угодно
                        . htmlspecialchars($message)
                . '</div>';
```

Как вы видите, само сообщение правильно экранировано, но класс — нет. Вместо экранирования может быть разумнее использовать белый список разрешенных классов с резервным вариантом по умолчанию::

```
$allowed = ['notice', 'info', 'warning', 'error'];    // белый список
if(!in_array($class, $allowed){
    $class = 'notice'; // неизвестный ввод, вернуться к разумному значению по
умолчанию
}
$renderer->doc .= '<div class="msg_' . $class . '">'
                        . htmlspecialchars($message)
                . '</div>';
```

входные URL-адреса

Когда плагин принимает URL-адреса в качестве входных данных, необходимо убедиться, что пользователи не смогут передать `javascript://` псевдо-протокол.

Вот пример того, как может выглядеть очень простая проверка, позволяющая убедиться, что используются только URL-адреса http и https.

```
// пустой URL при несоответствии протокола
if(!preg_match('/^https?:\/\//i', $url)) {
    $url = '';
}
```

Подделка межсайтовых запросов (CSRF)

Эта уязвимость часто появляется в плагинах из-за отсутствия понимания этой проблемы, ее часто путают с XSS.

Подделка межсайтовых запросов относится к атаке, при которой вредоносный сайт обманывает браузер жертвы, запрашивая страницу на уязвимом сайте для выполнения нежелательного действия. Атака предполагает, что браузер жертвы имеет учетные данные для изменения чего-либо на уязвимом сайте.

Добавление токена безопасности

DokuWiki предлагает функции, которые помогут вам бороться с атаками CSRF. getSecurityToken() создаст токен, который следует использовать для защиты любого аутентифицированного действия. Он должен быть включен в ссылки или формы, запускающие

это действие. Все формы, созданные с помощью библиотеки форм будут иметь автоматически добавленные токены безопасности, для форм, созданных вручную, можно использовать функцию formSecurityToken().

Вы как автор плагина несете ответственность за фактическую проверку токена перед выполнением авторизованных действий с использованием функции checkSecurityToken().

See also

- Подделка межсайтовых запросов
- Объяснение OWASP

Типичный пример уязвимости

Ниже приведен простейший пример для начала. У вас может быть более сложный плагин для защиты, вот простой пример на основе формы.

Представьте, что вы хотите узнать что-то, на что можно ответить «Да» или «Нет», у вас получится форма такого типа:

```
<form action="" method="GET">
    <input type="radio" name="yn" value="Yes" />
    <input type="radio" name="yn" value="No" />
    <input type="submit" value="Answer" />
</form>
```

Затем вы обрабатываете эту форму следующим образом:

```
global $INPUT;

if($INPUT->get->has('yn')){
    do_something_with_yn($INPUT->get->str('yn'));
}
```

Итак, пользователь подключен, чтобы ответить на этот вопрос, но он пока не знает ответа. Давайте уделим время размышлениям и просмотрим веб-страницы... Теперь пользователь посещает вредоносный веб-сайт, который знает или нет, что пользователь может быть подключен к вашему DokuWiki. На этом веб-сайте разработчик включил этот HTML- тег изображения:

```
<img src="http://your.dokuwi.ki/formpage?yn=Yes" />
```

Что тогда будет делать браузер пользователя?

Браузер обработает это изображение как любое другое и отправит запрос на этот URL . Ваш плагин увидит, что `$_GET['yn']` установлено, и вызовет `do_something_with_yn()` функцию.

Это один из примеров CSRF. Теперь, как исправить эту дыру в безопасности?

Предотвращение CSRF-атак

Помните вашу форму выше? Давайте добавим в нее ввод:

```
<form action="" method="GET">
    <input type="hidden" name="sectok" value="<?php getSecurityToken(); ?>"
/>
    <input type="radio" name="yn" value="Yes" />
    <input type="radio" name="yn" value="No" />
    <input type="submit" value="Answer" />
</form>
```

Видите первый ввод? Да? Хорошо. Теперь вам нужно проверить токен безопасности при получении формы, перед ее обработкой:

```
global $INPUT;

if($INPUT->get->has('yn') && checkSecurityToken()) {
    do_something_with_yn($INPUT->get->str('yn'));
}
```

Поскольку вредоносный веб-сайт никогда не найдет значение скрытого ввода «sectok», ваша форма больше не уязвима для CSRF.

Примечание: Если токен безопасности недействителен, `checkSecurityToken()` функция отображает сообщение, информирующее пользователя.

Удаленное включение кода

Эта атака позволяет злоумышленнику внедрить код (PHP) в ваше приложение. Это может произойти при включении файлов или использовании небезопасных функций операций, таких как eval() или system().

Всегда фильтруйте любые входные данные, которые будут использоваться для загрузки файлов или которые передаются в качестве аргумента внешним командам.

Утечка информации

Эта атака может привести к раскрытию файлов, которые обычно должны быть защищены ACL DokuWiki , или может раскрыть файлы на сервере (например, `/etc/passwd`).

Всегда фильтруйте любые входные данные, которые будут использоваться для загрузки файлов или которые передаются в качестве аргумента внешним командам.

Всегда используйте функции проверки ACL DokuWiki при доступе к данным страницы.

SQL-инъекция

Эта атака редко актуальна в DokuWiki, поскольку база данных не используется. Однако, если ваш плагин обращается к базе данных, всегда экранируйте все значения перед их использованием в операторах SQL.

Дополнительная информация:

- SQL-инъекция

Сообщение о проблемах безопасности

Если у вас возникли проблемы с плагином, сообщите об этом автору плагина по электронной почте, при желании указав Andi or the список рассылки on CC.

Дополнительно к данным на странице плагина `securityissue` следует добавить поле с кратким описанием проблемы . Это создаст красное предупреждающее поле и исключит плагин из основного списка плагинов.

После устранения проблемы и выпуска новой версии это поле следует снова удалить.