Учебник по PHP

XSS-уязвимости и защита

Динамические веб-сайты активно работают с данными, полученными от пользователей. То есть по сути, почти вся информация на сайте была добавлена туда самими пользователями. Хороший пример такого сайта — это форум. Любой форум на 99.9% состоит из опубликованной там пользователями информации.
Но каждый раз, когда пользователям предоставляются какие-либо возможности, нужно быть готовыми к использованию этих возможностей не по назначению. Так, формы для публикации контента могут использовать не для отправки безобидных текстов, а для заражения вашего сайта вредоносным кодом.

Фильтрация данных

Любую информацию, полученную от пользователя, обязательно надо фильтровать перед выводом в шаблоне! Фильтрация означает применение к этой информации набора правил, которые очистят и подготовят её к публикации на сайте. Мы фильтруем информацию, чтобы недопустить появления на нашем сайте XSS-уязвимости.

XSS-уязвимость

XSS — это вид уязвимости, которая свойственна веб-приложениям.
Данная атака на сайт состоит в том, что в выдаваемую страницу внедряется вредоносный JS-код. Это становится возможным из-за недостаточной фильтрации данных, полученных от пользователя.

Принцип атаки

1. На сайте есть форма для публикации сообщения.
2. Через эту форму хакер вместо простого текста отправляет JS-код.
3. Сообщение публикуется на странице, которая доступна всем посетителям.

4. Вредоносный код выполняется для каждого посетителя этой страницы.
5. Вредоносный скрипт вредит пользователям сайта. Например, крадёт их куки.

Замена опасных символов

Проблема ясна. Надо обезопасить страницу, отфильтровав информацию из формы.
Но как фильтровать, чтобы не потерять текст, но при этом лишить хакера возможности нам навредить?
Тут помогут HTML-мнемоники.
Мнемоника — это кодовое представление символа в HTML, который начинается со знака амперсанда «&» и завершается точкой с запятой «;».
Теги `<script>` состоят из треугольных скобок, а значит, если их заменить на мнемоники, то такой текст больше не будет трактоваться браузером как HTML-тег. Мнемоники часто используются, когда надо показать пользователю фрагмент с HTML-кодом на странице. Заглянув в исходный код такой страницы можно увидеть, что вместо кавычек и скобок в этом HTML-коде находятся мнемоники.

Есть и другой вариант фильтрации: попросту вырезать все теги из текста. Нет тегов — нет проблемы.

Функция фильтрации htmlspecialchars

Перейдём к практике. В PHP-сценарии добавим вызов функции, которая для переданной строки выполнит фильтрацию и заменит все опасные символы в ней на подходящие HTML-мнемоники. Такая функция называется `htmlspecialchars`.
Вот как выглядит её работа:

```
<?php
$text = "<script><script>"; // эту строку мы получили от пользователя
$safe_str = htmlspecialchars($text); // отфильтрованная, безопасная строка

print($safe_str); // узнаём, что получилось
```

Результат работы этого сценария: `<script></script>`

Никогда не забывайте использовать функцию `htmlspecialchars` при выводе информации от пользователей в шаблоне!

Поделиться

Вконтакте

Твитер

Телеграм

Одноклассники

Соглашение

Конфиденциальность

Сведения об образовательной организации

Лицензия № 3026

Sk Участник