Веб уязвимости

Подготовил: Муковкин Дмитрий

Содержание курса

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

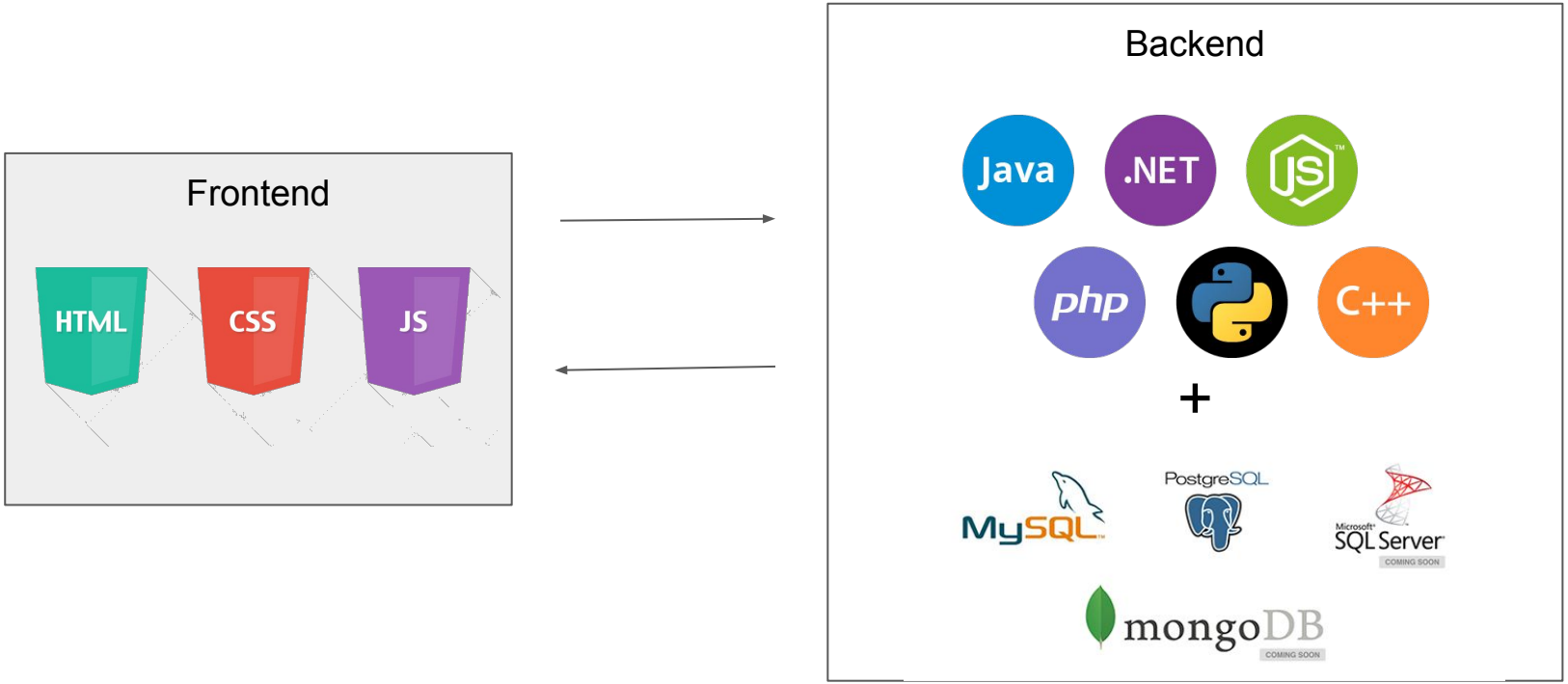
Содержание

В этой лекции будут рассмотрены основные моменты архитектуры веб приложений.

Программы обработчики

- PHP
- Python
- NodeJS
- C++
- Java
- Ruby
- …

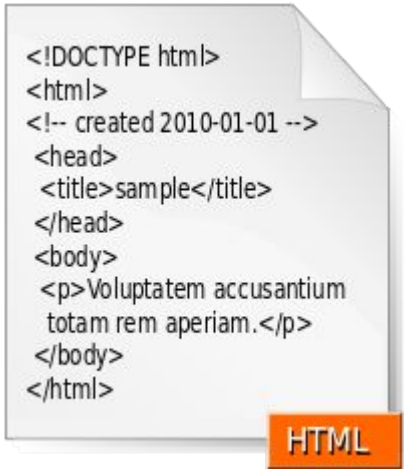
Из чего состоит сайт?



HTML

HyperText Markup Language — «язык гипертекстовой разметки»

Актуальная версия - HTML5



HTML

Любой документ на языке HTML представляет собой набор элементов, причём начало и конец каждого элемента обозначается специальными пометками — тегами.

Элементы могут быть пустыми, то есть не содержащими никакого текста и других данных (например, тег перевода строки
). В этом случае обычно не указывается закрывающий тег. Кроме того, элементы могут иметь атрибуты, определяющие какие-либо их свойства. Атрибуты указываются в открывающем теге. Вот примеры фрагментов HTML-документа:

HTML

Примеры основных тегов:

- `<a href="http://vk.com">VK.com</a>`
- `<div class="block1" id="id1">Lorem ipsum.</div>`
- `Текст<br> текст`
- `<img src="URL" alt="альтернативный текст">`

Полный список тегов http://htmlbook.ru/html

CSS

CSS используется создателями веб-страниц для задания цветов, шрифтов, расположения отдельных блоков и других аспектов представления внешнего вида этих веб-страниц. Основной целью разработки CSS являлось разделение описания логической структуры веб-страницы (которое производится с помощью HTML или других языков разметки) от описания внешнего вида этой веб-страницы (которое теперь производится с помощью формального языка CSS). Такое разделение может увеличить доступность документа, предоставить большую гибкость и возможность управления его представлением, а также уменьшить сложность и повторяемость в структурном содержимом.

CSS

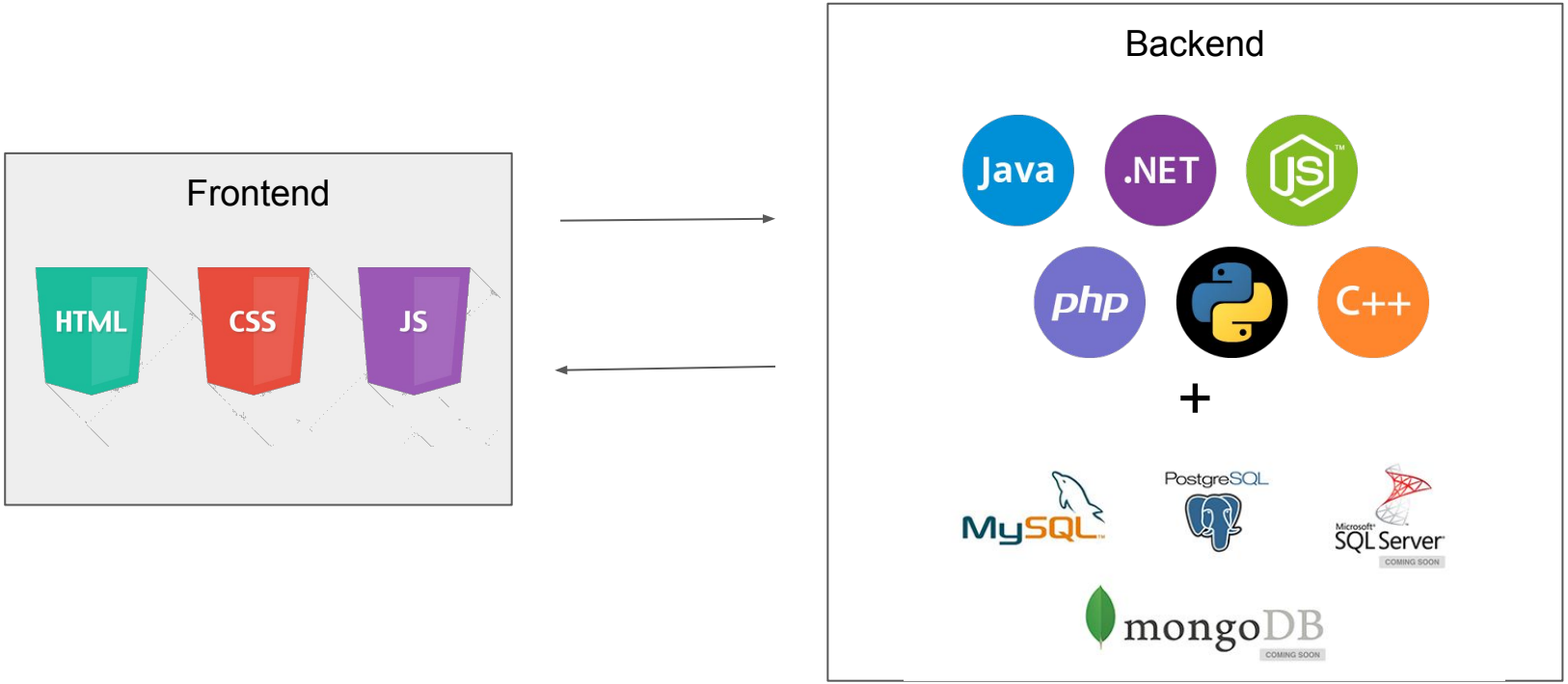
```
body {
  font-family: Arial, Verdana,  sans-serif; /* Семейство шрифтов */
  font-size: 11pt; /* Размер основного шрифта в пунктах  */
  background-color: #f0f0f0; /* Цвет фона веб-страницы */
  color: #333; /* Цвет основного текста */
}
.gost {
  color: green; /* Цвет текста */
  font-weight: bold; /* Жирное начертание */
}
#help {
  position: absolute; /* Абсолютное позиционирование */
  left: 160px; /* Положение элемента от левого края */
  top: 50px; /* Положение от верхнего края */
  width: 225px; /* Ширина блока */
  padding: 5px; /* Поля вокруг текста */
  background: #f0f0f0; /* Цвет фона */
}
```

Полный список на http://htmlbook.ru/css

JavaScript

Изначально создавался для того, чтобы сделать web-странички «живыми». Программы на этом языке называются *скриптами*. В браузере они подключаются напрямую к HTML и, как только загружается страничка – тут же выполняются.

Из чего состоит сайт?



Системы управления базами данных (СУБД)

- Реляционные
- Документо-ориентированная (нереляционная)

Реляционные СУБД

База данных состоит из таблиц, таблицы содержат колонки и строки, а строки состоят из значений колонок. Все строки одной таблицы имеют единую структуру.

- MySQL
- PostgreSQL
- SQL server
- …..

Нереляционная СУБД

Для доменов можно провести аналогию с таблицами, однако в отличие от таблиц для доменов не определяется структура данных. Домен – это такая коробка, в которую вы можете складывать все что угодно. Записи внутри одного домена могут иметь разную структуру.

На этом, кажется, все

Вопросы?

Всем спасибо за внимание

Следующая тема лекции - XSS уязвимости.

Необходимо принести ноутбуки.