



НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
УНИВЕРСИТЕТ

Факультет компьютерных наук
Департамент программной инженерии

ОБЕСПЕЧЕНИЕ КАЧЕСТВА И ТЕСТИРОВАНИЕ

Семинар 10: Тестирование web-интерфейсов

Москва, 2020



WEB-ИНТЕРФЕЙС

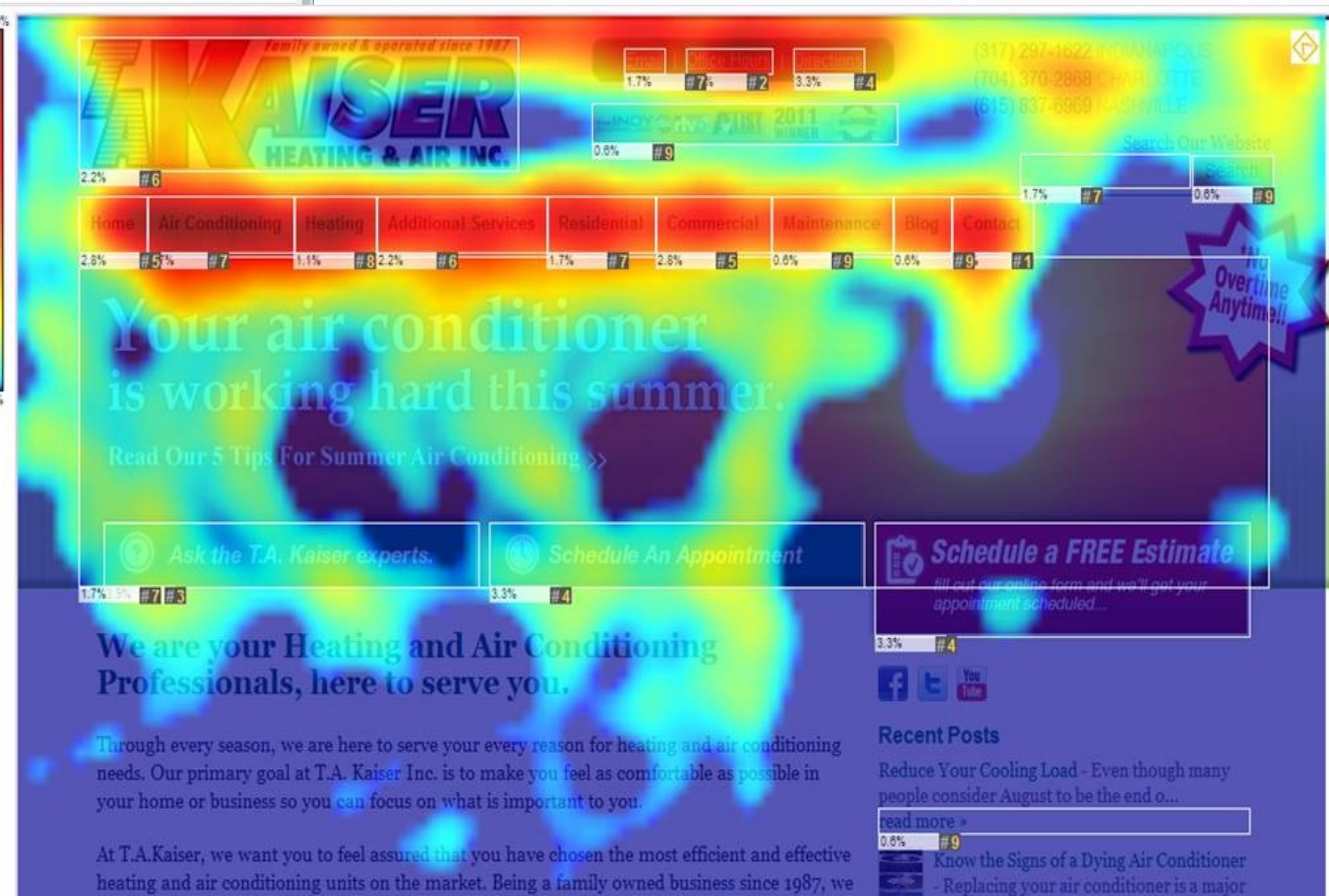
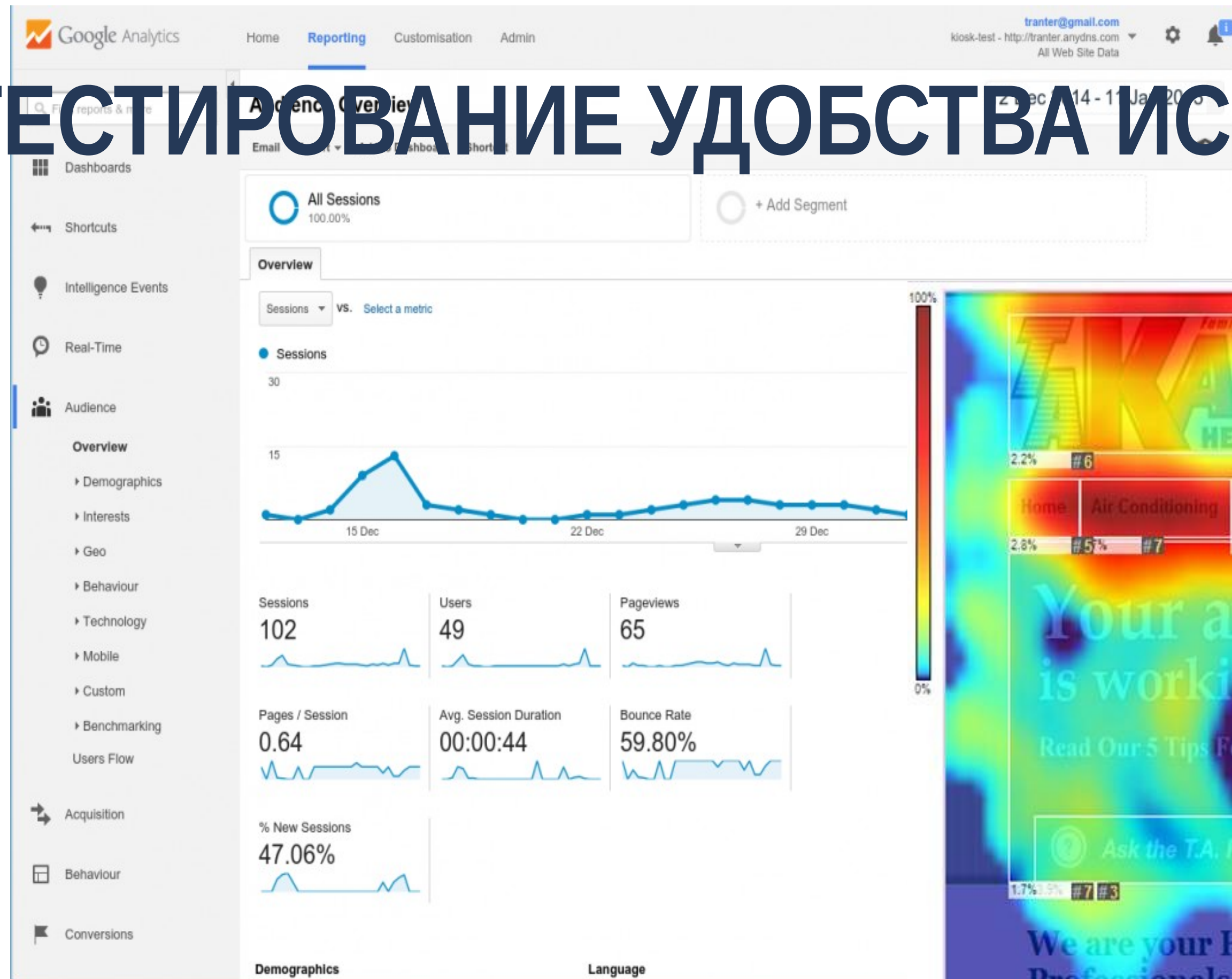
- **Web-интерфейс**— это совокупность средств, при помощи которых пользователь взаимодействует с веб-сайтом или любым другим приложением через браузер.



ПОДХОДЫ К ТЕСТИРОВАНИЮ ВЕБ-ПРИЛОЖЕНИЙ

- тестирование удобства использования ;
- функциональное тестирование ;
- нагрузочное и стрессовое тестирование ;
- проверка ссылок и HTML-кода;
- тестирование безопасности.

ТЕСТИРОВАНИЕ УДОБСТВА ИСПОЛЬЗОВАНИЯ





ПОДХОДЫ К ФУНКЦИОНАЛЬ -НОМУ ТЕСТИРОВА -НИЮ ВЕБ -ПРИЛОЖЕНИЙ

Record & Play основан на возможности средств автоматизации тестирования автоматически генерировать код.

Functional Decomposition в основе лежит разбиение всех компонент фреймворка по функциональному признаку на бизнес-функции (реализуют/проверяют бизнес-функциональность приложения), user-defined функции (вспомогательные функции, которые еще имеют привязку к тестируемому приложению или к конкретному проекту), утилиты (функции общего назначения, не привязанные к конкретному приложению, технологии, проекту).

Data-driven основан на том, что к некоторому тесту или группе тестов привязывается источник данных, и этот тест или набор тестов циклически выполняется для каждой записи из этого источника данных. Вполне может применяться в комбинации с другими подходами.

Keyword-driven представляет собой фактически движок для обработки посылаемых ему команд, а сами инструкции выносятся во внешний источник данных.

Object-driven основан на том, что основные ходовые части фреймворка реализованы в виде объектов, что позволяет собирать тесты по кирпичикам.

Model-based основан на том, что тестируемое приложение (или его части) описывается в виде некоторой поведенческой модели.



НАГРУЗОЧНОЕ И СТРЕССОВОЕ ТЕСТИРОВАНИЕ

- **Тест на устойчивость к большим нагрузкам** – Load-testing, stress-test или performance test. Такой тест имитирует одновременную работу нескольких сотен или тысяч посетителей (каждый из которых может "ходить" по сайту в соответствии со своим сценарием), проверяя, будет ли устойчивой работа сайта под большой нагрузкой.



ЦЕЛИ НАГРУЗОЧНОГО ТЕСТИРОВАНИЯ

- оценка производительности и работоспособности приложения на этапе разработки и передачи в эксплуатацию;
- оценка производительности и работоспособности приложения на этапе выпуска новых релизов, патч-сетов;
- оптимизация производительности приложения, включая настройки серверов и оптимизацию кода;
- подбор соответствующей для данного приложения аппаратной (программной платформы) и конфигурации сервера.



ТЕСТЫ НАГРУЗО -ЧНОГО ТЕСТИРОВА -НИЯ 4.1

Тестирование производительности и (Performance)	Определение масштабируемости приложения под нагрузкой.
Стрессовое тестирование (Stress Testing)	Насколько приложение и система в целом работоспособны в условиях стресса и также оценить способность системы к регенерации, т.е. к возвращению к нормальному состоянию после
Объемное тестирование (Volume Testing)	оценки производительности при увеличении объемов данных в базе данных приложения
Тестирование стабильности или надежности (Stability / Reliability Testing)	проверка работоспособности приложения при длительном (многочасовом) тестировании со средним уровнем нагрузки



ТЕСТЫ НАГРУЗО -ЧНОГО ТЕСТИРОВА -НИЯ 4.12

Моделирование Транзакций (Transaction Simulation, TS)	Позволяет измерять производительность работы приложения "с точки зрения пользователя" и, при этом, не требует доступа к коду пользовательского
Метод "Анализ данных на стороне клиента" (Client Capture, CC)	Метод основан на извлечении данных о работе приложения из операционной системы компьютера, где установлено пользовательское приложение
Метод "Анализ Сетевого Трафика" (Network Sniffing, NS)	Основан на извлечении информации о производительности приложений из сетевого трафика



ПРОВЕРКА HTML-КОДА

- Утилиты
- Валидаторы встроенные в web-редактор
- Валидаторы встроенные в браузеры

Часто включает в себя и тестирование ссылок.

ТЕСТИРОВАНИЕ УЯЗВИМОСТЕЙ

- **Тестирование на проникновение** — метод оценки безопасности компьютерных систем или сетей средствами моделирования атаки злоумышленника. Процесс включает в себя активный анализ системы на наличие потенциальных уязвимостей, которые могут спровоцировать некорректную работу целевой системы, либо полный отказ в обслуживании.



ТОП УЯЗВИМОСТЕЙ OWASP

OWASP Top 10 – 2013 (Previous)	OWASP Top 10 – 2017 (New)
A1 – Injection	A1 – Injection
A2 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References - Merged with A7	A4 – Broken Access Control (Original category in 2003/2004)
A5 – Security Misconfiguration	A5 – Security Misconfiguration
A6 – Sensitive Data Exposure	A6 – Sensitive Data Exposure
A7 – Missing Function Level Access Control - Merged with A4	A7 – Insufficient Attack Protection (NEW)
A8 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
A9 – Using Components with Known Vulnerabilities	A9 – Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards - Dropped	A10 – Underprotected APIs (NEW)



XSS-ИНЪЕКЦИИ

Межсайтовый скриптинг (XSS) – это уязвимость, которая заключается во внедрении кода, исполняемого на стороне клиента (JavaScript) в веб-страницу, которую просматривают другие пользователи.

Выделяют:

- Хранимые
- Отраженные



XSS-ИНЪЕКЦИИ

Например в безобидный комментарий

Привет! Нравится твой сайт.

Встраиваем код

Привет! Нравится твой сайт.<script>alert("XSS")</script>

XSS AUDITOR

- В Google Chrome (а также в Opera) используется XSS аудитор, который будет пытаться предотвратить XSS.
- При тестировании веб-сайтов с помощью браузера стоит помнить, что может оказаться, что веб-приложение уязвимо, но вы не видите всплывающего подтверждения только по той причине, что его блокирует браузер.



HTML-ИНЪЕКЦИИ

- **HTML-инъекции** - тип атаки, которая благодаря отсутствию надлежащей обработки пользовательского ввода позволяет злоумышленнику встроить на сайт собственный HTML-код.

SQL-ИНЪЕКЦИИ

- **SQL-инъекция** – это уязвимость, которая возникает из-за недостаточной фильтрации вводимых пользователем данных, что позволяет модифицировать запросы к базам данных. Результатом эксплуатации SQL-инъекции является получение доступа к данным, к которым в обычных условиях у пользователя не было бы доступа.

ПРИЗНАК НАЛИЧИЯ SQL-ИНЪЕКЦИИ

- Главными признаками наличия SQL-инъекции является вывод ошибки или отсутствие вывода при вводе одинарной или двойной кавычки. Эти символы могут вызвать ошибку и в самом приложении, поэтому чтобы быть уверенным, что вы имеете дело именно с SQL-инъекцией, а не с другой ошибкой, нужно изучить выводимое сообщение.

SQL-ИНЪЕКЦИИ

```
SELECT `name`, `status`, `books` FROM `members` WHERE  
name = 'Demo' AND password = '111'
```

Если вместо Demo пользователь вводит Demo' --

```
SELECT `name`, `status`, `books` FROM `members` WHERE  
name = 'Demo' -- ' AND password = '111'
```

Следовательно выполняться будет запрос

```
SELECT `name`, `status`, `books` FROM `members` WHERE  
name = 'Demo'
```

SQL-ИНЪЕКЦИИ

Важно помнить, что запрос может быть написан по-разному, например, все следующие формы возвращают одинаковый результат:

```
SELECT * FROM table_name WHERE id='1'
```

```
SELECT * FROM table_name WHERE id="1"
```

```
SELECT * FROM table_name WHERE id=('1')
```

```
SELECT * FROM table_name WHERE id=("1")
```

Как выполнить селекты для всех id?

SQL-ИНЪЕКЦИИ



SQL-ИНЪЕКЦИИ





SQL-ИНЪЕКЦИИ

Продолжаем менять логику запроса, и в качестве имени пользователя используем Demo' OR 1 -- Получаем запрос

```
SELECT `name`, `status`, `books` FROM `members` WHERE name = 'Demo' OR 1 -- ' AND password ='111'
```

Будет выполнен запрос


```
SELECT `name`, `status`, `books` FROM `members` WHERE name = 'Demo' OR 1
```



BWAPP

http://localhost/bWAPP/login.php

bWAPP - Login

bWAPP 
an extremely buggy web application!

[Login](#) [New User](#) [Info](#) [Blog](#) [ITSEC Training](#)





/ Login /

Enter your credentials (*bee/bug*).

Login:

Password:

Set the security level:
low



СКАНЕРЫ УЯЗВИМОСТИ

Сетевые сканеры	задача — раскрыть доступные сетевые сервисы, установить их версии, определить ОС и т. д.	<ul style="list-style-type: none">• Nmap• IP-Tools
Сканеры брешей в веб-скриптах	пытаются найти популярные уязвимости (SQL inj, XSS, LFI/RFI и т.д.) или ошибки (не удаленные временные файлы, индексация директорий и т.п.)	<ul style="list-style-type: none">• Nikto/Wikto• Acunetix Web Vulnerability Scanner
Эксплойтинг	продукты, которые избавляют от ручного поиска эксплоитов, и применяют их автоматически.	<ul style="list-style-type: none">• Metasploit Framework• Armitage• Tenable Nessus®
Автоматизация инъекций	утилиты, которые конкретно занимаются поиском и эксплуатацией инъекций.	<ul style="list-style-type: none">• sqlmap• bsqlbf-v2
Дебаггеры (снифферы, локальные прокси и т.п.)	Эти инструменты в основном используют разработчики, при проблемах с результатами выполнения своего кода.	<ul style="list-style-type: none">• Fiddler• Burp Suite



ЛИТЕРАТУРА

1. OWASP TOP-10 2017 https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf
2. Сервисы для проверки навыков пентестера - <https://habrahabr.ru/company/pentestit/blog/261569/>
3. Книга “Основы веб-хакинга. Более 30 примеров уязвимостей” - <https://drive.google.com/open?id=0BxSD8FAEX1XfaVVxUy1pWDFXakk>
4. Основы SQLi
(пример работы с bWAPP) - <https://hackware.ru/?p=3362>



HOMEWORK ?...?

- Just kidding

СПАСИБО! ВОПРОСЫ?



НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
УНИВЕРСИТЕТ