Manual QA course

Lecture 23. Полезные инструменты для тестировщика

Шабалин Евгений

hillel
компьютерная школа

Mozilla Firefox

Bugmagnet - позволяет вводить проблемные данные и граничные значения в поля ввода (удобно для исследовательского тестирования) (так же для хрома)

Host Spy - показывает какие еще сайты имеются на этом же сервере.

ShowIP - показывает в строке состояния ip адрес текущего сайта. Также можно получить дополнительную информацию (страна, компания и т.д.) просто щелкнув по IP в строке состояния

Wappalyzer - позволит получить информацию о технологиях, используемых на сайте. Он попытается определить CMS (CMF), используемые фреймворки, используемый веб сервер и ОС

Mozilla Firefox

Header Spy - выводит в строке состояния HTTP заголовки сервера

User-Agent Switcher - позволяет быстро изменять свой User-Agent

Modify Headers - позволяет редактировать не только заголовок User-Agent, но и все остальные, в том числе, добавлять собственные

Tamper Data - позволяет анализировать все HTTP-запросы, которые выполняются между клиентом и сервером. Огромный плюс в том, что можно редактировать любой посланный заголовок. Отличие от Modify Headers: он устанавливается глобально для всех сайтов, а Tamper Data может работать с конкретной страницей или скриптом.

Mozilla Firefox

Cookie Monster - позволяет просматривать, изменять и добавлять новые cookie

Live HTTP Headers - позволяет оперировать с HTTP заголовками: удалять, добавлять и изменять. Можно установить любой метод запроса, помимо GET и POST.

Groundspeed - позволит изменять формы на сайте: удалять ограничения на длину символов, редактировать JS события, изменять скрытые поля

HTTPFox – позволяет отслеживать и анализировать весь входящий и исходящий трафик между клиентом и сервером. Предоставляет следующую информацию о запросе: заголовки запроса и ответа, отправленные и полученные cookie, GET/POST параметры, тело ответа сервера

Mozilla Firefox

HTTP Requester – позволяет выполнять PUT/POST/DELETE запросы. Выполненные запросы хранятся в архиве, что позволяет вернуться к ним позже для анализа или повтора

SQL Inject Me - поможет проверить сайт на наличие sql инъекций, проанализировать все GET параметры и формы на текущей странице.

XSS Me - аналогичен предыдущему, но ищет XSS уязвимости

Hackbar - предназначен для облегчения проведения ручных инъекций в адресной строке. Он может удобно разбить адресную строку по параметрам, позволит быстро вставлять различные векторы для проверки уязвимостей, имеет несколько полезных инструментов, например, для кодирования URL, строк и символов (сможет перевести строку в CHAR(N,N,N,N), что крайне удобно, когда экранируются кавычки)

Google Chrome

Для тестирования XSS, прежде всего, стоит отметить, что с 7ой версии этого браузера он имеет XSS Auditor, который не дает возможность провести проверку наличия XSS. Но есть способы обхода XSS Auditor:

- можно запустить браузер с ключом --disable-xss-auditor;
- если есть возможность оставить один тег незакрытым, то бразуер сам попытается его закрыть. Причем сначала отработает XSS Auditor, а затем браузер попытается закрыть теги;
- отправить специальный HTTP-заголовок, который отключает XSS Auditor: header("X-XSS-Protection: 0");

Google Chrome

Form Filler - позволяет заполнить все доступные для ввода поля случайными данными

Wappalyzer - аналогичен расширению Firefox

Chrome Sniffer - во многом повторяет функционал Wappalyzer. Всего в базе сейчас находятся слепки 100 популярных инструментов. В случае удачного распознавания их иконки отображаются прямо в адресной строке

IP Address information - аналогичен расширению ShowIp Firefox

Web Server Notifier - в адресной строке показывает информацию о веб сервере, который использует ресурс

Google Chrome

Web Technology Notifier - в адресной строке показывает информацию о технологии, которая использована для разработки приложения

HTTP Headers - позволяет быстро просмотреть заголовки в ответах сервера

Request Maker - практически аналог Tamper Data Firefox, но в силу ограничений архитектуры расширений Google Chrome полностью реализовать аналогичный функционал пока невозможно

HTTP Response Browser - предназначено для составления самых разных HTTP-запросов (правда с помощью XMLHttpRequest, что накладывает ограничения).

Google Chrome

Advanced REST client Application - Chrome-приложение (программа, работающая внутри браузера). В отличие от HTTP Response Browser, Advanced REST client предлагает более обширный функционал, в том числе продвинутый просмотр ответов в форматах JSON и XML с подсветкой синтаксиса, удобный составитель HTTP-заголовков (подсказки + система автодополнения) и многое другое

Edit This Cookie - позволяет через всплывающую панель удалить произвольные cookie на текущем сайте, редактировать их значения или создать новые

Swap My Cookies - позволяет использовать несколько аккаунтов на одном и том же ресурсе. Это менеджер сессий, для любого сайта можно создать несколько профилей, каждый со своим набором cookie, и быстро переключаться между ними. Так же можно сделать это с помощью горячих клавиш

Google Chrome

Web Securify - выполняет анализ сайта на наличие таких уязвимостей, как SQL Injection, Cross-site Scripting, Cross-site Request Forgery, Local/Remote File Include и т.д. Все работает в автоматическом режиме

XSS Rays - включает в себя XSS-сканер и инспектор объектов. Поможет быстро реализовать инъекцию во всех возможных местах ввода данных (расширение само их определит и предложит на выбор). Инспектор объектов позволяет в реальном времени изменять содержимое функций и быстро разобраться в логике работы веб-приложения

OWASP Mantra

Mantra - это надстройка к браузеру, специально разработана для тестирования безопасности WEB-приложений. Имеет все возможные расширения других браузеров. Инструмент является портативным, гибким и легким в использовании, в то же время имеет очень мощную платформу для тестирования безопасности за счет наличия всех возможных расширений для этой отрасли.

Веб-приложения

Generate Data - имеет варианты генерации тестовых данных для разных стран + несколько поддерживаемых форматов для импорта

Mockaroo - очень большой список типов тестовых данных + несколько поддерживаемых форматов для импорта

Fakenamegenerator - генерирует полный профиль человека + дополнительные генераторы

Fakefilegenerator - генерирует нерабочий файл + можно выбрать тип, задать имя и размер (same)

Lorempixel - генерирует картинки разных типов, размеров, категорий + можно задать текст поверх картинки (same and same)