**Вам нужно знать о тестировании Web-Безопасности, если…**

* ПО вашей компании хранит любой вид персонально идентифицируемой информации (она определена законом, но обычно она может быть использована, чтобы найти вас или вашу семью)

Примеры: адреса, почты (обычно в комбинации с другой информацией), идентификации, выпущенные государством (номер социальной безопасности, номер водительского удостоверения, паспорт)

* ПО вашей компании использует или хранит любой тип платежной инфорации. Если вы храните информацию о кредитных картах, то в большинстве стран существуют очень жесткие правила про хранение и доступ к таким данным – и очень высокие штрафы за неспособность защитить эти данные. Если вы храните информацию о банковском счете, стандарты не столь строги, но вам все равно нужно глядеть в оба.
* Ваша компания должна придерживаться закона или процедур, касающихся безопасности данных. Некоторые известные мне примеры:

Медицинские компании в США должны следовать ряду федеральных законов.

Любая публично торгуемая компания в США должна следовать федеральным законам, касающимся стандартов. Если компания им не соответствует, она не может принимать платежи по кредитным картам и подлежит штрафам и другим наказаниям.

* У вашей компании есть требования по конфиденциальности данных, которые она хранит.

Если вы полагаете, что вам нужно больше узнать о тестировании web-безопасности, то, возможно, вам это действительно необходимо.

С чего начать

Начать изучать тестирование веб-безопасности довольно просто – есть отличные ссылки и инструменты, и вы потратите на них только свое время. Вы можете многое сделать, используя только браузер!

Осторожно! Впереди опасность!

Прежде чем вы начнете делать хоть что-то разрушительное, убедитесь, что вы абсолютно уверены, что у вас есть на это разрешение. Да, даже на тест-сервере – его могут использовать другие люди для других целей, ваша компания может отслеживать сеть на предмет подозрительного поведения – да и вообще, куча факторов играет тут роль, о которой вы можете не иметь ни малейшего понятия. Всегда, *всегда* убеждайтесь, что у вас есть разрешение поиграть в хакера.

Бесплатные инструменты

Все инструменты, которые я использую, сделаны под Windows, потому что я работаю в Windows-окружении. Некоторые из них кросс-платформенные, некоторые – нет. Все они довольно просты в использовании для новичка, пробующего воду безопасности в поисках багов.

* **Инструменты разработчика в браузере**. Если они не блокированы вашей компанией, то большинство современных браузеров позволяет исследовать код страницы, изучить JavaScript и просмотреть сетевой трафик между браузером и сервером. Вы также можете редактировать и запускать рандомные JavaScript в них, пробовать менять код, и повторять сетевые запросы.
* **Postman**. Несмотря на то, что это расширение для Chrome, Postman запускается и как отдельное приложение. Вы можете использовать его для отправки различных запросов и изучения ответов (тут есть фишка: почти все в тестировании безопасности можно сделать массой различных способов. Экспериментируйте, чтобы найти свои любимые).
* **Fiddler**. Telerik Fiddler – на данный момент мой любимый инструмент исследования веб-запросов и манипулирования ими. Он кросс-браузерный, работает на нескольких ОС, и с него легко начать тестировать безопасность.
* **IronWASP**. Один из меньшинства бесплатных сканеров безопасности, сделанный под Windows. С ним довольно просто работать, и он обычно дает неплохие результаты.
* **И еще**… Доступных инструментов очень много. Я только начала изучать безопасность, и всего лишь начала принюхиваться.

Я собираюсь сконцентрироваться на Fiddler в дальнейшем, потому что считаю его самым простым из бесплатных инструментов, и самым быстрым для того, чтобы перейти от тыкания интерфейса к действительно полезным результатам.

Использование Fiddler

Когда я наткнулась на эту огромную, и потенциально очень дорогую уязвимость, о которой я рассказывала выше, я как раз играла с Fiddler. Хорошо, что я нашла ее именно тогда: если бы она попала на прод, могли бы случиться большие неприятности.

Настройка

Я установила Fiddler с настройками по умолчанию. Под Windows вы еще получаете плагин для Internet Explorer, позволяющий запускаться напрямую через IE (и настроить его для мониторинга только IE-трафика намного легче, чем для других браузеров). В зависимости от того, что вы делаете, некоторые из этих плагинов могут быть очень полезными: вот мои любимые

* **Syntax View/Highlight.** Предоставляет подсвечивание синтаксиса для подготовки кастомизированных сценариев и просмотра HTML, Javascript, CSS и XML. Делает ковыряние в веб-коде куда менее болезненным, подсвечивая все тэги и ключевые слова. Я большой фанат штук, которые делают концентрацию на важном проще, и это – одна из них.
* **PDF –** **просмотр.**Очень важен, если ваше приложение строит PDF-файлы «на лету». Можно кликнуть по вкладке и увидеть рендер PDF. К примеру, если вы тестируете банковскую выписку в PDF-формате, чтобы убедиться, что открыть выписку другого пользователя невозможно, этот инструмент – ваш друг.