Переходим к следущему тому, что обещал в заголовке.

Проходя мимо сайта оплаты МТС, случайно обнаружил протесты баннерорезки. К счастью, скриптов не очень много. Но популярная гуглоаналитика там есть. Прямо вот на страничке, где вы вводите номера карточек и CVV.

Небольшое поясняющее видео:

Опишу происходящее на видео, если кто-то не может его посмотреть. Обманув DNS, я перенацелил скрипты аналитики на свой веб-сервер, где их благополучно подменил на свои. Это не взлом и целью выставить обнаруженное уязвимостью нет, хотя некоторая вероятность такого тоже существует. Своими скриптами я благополучно собрал вводимые самим собой тестовые произвольные номера кредиток и отправил себе на сервер. Для демонстрации возможностей скрипта я еще и сумму оплаты поменял.

Извините, повторюсь, есть некоторая компания (перечисленные выше, как и многие другие, не суть название). Они пишут сайт, в который закладывают секретности и какой-то функционал, где (я верю в это) личные данные никто править не должен и они наружу никуда не утекают. Для того, чтобы собирать статистику по своим пользователям, они ленятся и пользуются чужими скриптами. Т.е. браузерам пользователей они в своем сайте дают команду — зайдите на другой сервер и возьмите там скрипт для статистики. Какой этот скрипт в данный момент времени знают только владельцы другого сервера. Что он делает, владельцы сайта не могут знать. Более того, браузерам пользователя в некоторых случаях можно сказать, чтобы скрипты брались откуда-то еще и тогда количество тех, кто может их поменять, резко возрастает. Владельцы же серверов статистики и прочих вставок вообще без проблем могут собирать все, до чего дотянутся. Куда им захочется дотянуться, тоже уверен, владельцы основных сайтов вообще не представляют.

Это сообщение отредактировал **Goldfray** - 28.09.2017 - 17:19

Read Full Article