https://www.fuzzysecurity.com/tutorials/mr\_me/1.html

Что тут происходит, b33f?

Всем привет! Вы, наверное, думаете: Что мне дадут туториалы по эксплойтам кучи от b33f'а? Я надеюсь, это короткое введение ответит на все вопросы и станет еще одним поводом отправлять людей курить мануалы. Как вы наверняка знаете, я очень интересуюсь разработкой эксплойтов. Есть в этом определённый кайф (и расслабление), когда тебе наконец удаётся направить поток исполнения в ту точку, где ты разместил свой код.

Когда я начинал учиться этой чёрной магии, которой и является разработка эксплойтов, было всего несколько человек/групп, где можно было достать бесценные ресурсы. И дело было не только в том, что они были ниндзя, но и в том, что они были достаточно добры, чтобы поделиться своим опытом с окружающими их глупцами. Без таких людей как corelanc0d3r, mr\_me и многих других мы бы так и остались детьми.

Именно поэтому, когда я увидел этот твит от mr\_me, я понял, что я должен сделать что-то ради сохранения его таинственных туториалов по эксплойтам кучи Windows.

*I'm letting my old http://t.co/gvVS4gCKCG domain expire so if you are interested in heap overflowsI would suggest you pull the content now.*

*— mr\_me (@ae0n\_) June 25, 2015*

*Я решил, что не буду продлять мой старый домен http://t.co/gvVS4gCKCG, поэтому, если вы интересуетесь переполнением буфера, я рекомендую вам выскачивать содержимое прямо сейчас.*

*— mr\_me (@ae0n\_) Июнь 25, 2015*

Я написал письмо mr\_me. Он сказал, было бы круто, если бы я вместе с ним опубликовал его посты на FuzzySec. Все туториалы серии "Переполнение буфера для людей" были сохранены в оригинальном состоянии. Едиственное, что я добавил, это возможность интегрировать их в сайт. Это нужно чтобы они согласовались с общей темой FussySec. Список возможных побочных эффектов включает, но не ограничен: лёгкое подтекание лица, непроизвольное дергание и превращения в персонажа фильма Дэвида Линча. Наслаждайтесь на свой страх и риск!

Прогресс

Изначально я планировал выложить все туториалы скопом, однако процесс требует больше времени, чем я ожидал. Остальные части скоро будут доступны!

Прогресс импорта: 5 / 6