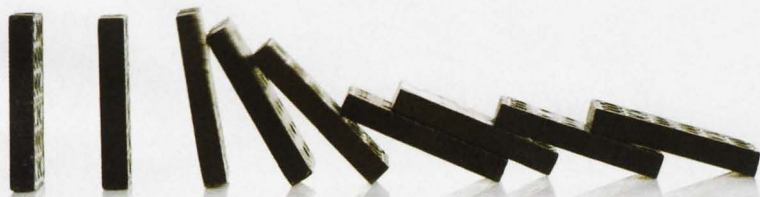




Пробивая Lotus, или история одного пентеста

ЭКСПЛУАТИРУЕМ ПРИВАТНУЮ ДЫРУ В LOTUS DOMINO CONTROLLER

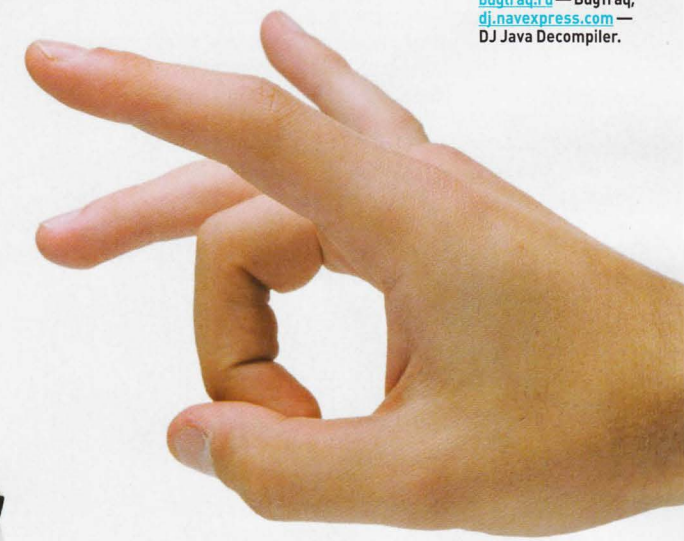
В этой статье я хотел бы рассказать об одном рабочем дне пентестера, которому, вопреки распространенному мнению, недостаточно просто запустить сканер и ждать отчета. Ему нередко приходится проявлять смекалку и прямо во время теста на проникновение писать спloitы.



ПРЕДЫСТОРИЯ

Однажды я проверял надежность защиты очередного объекта. На этот раз вся инфраструктура была поднята за счет оборудования и софта IBM, что совершенно точно влетело заказчику в копеечку. Основную часть инфраструктуры, как это обычно бывает, составляли сервера Lotus. В данном случае их было много. Очень много. На Lotus была построена вся кухня компании: почта, совещания, управление контентом и т. п. Кстати, здесь вполне уместно вспомнить старую статью Александра Полякова, в которой он героически описывал свой опыт покорения этого ПО. Однако время беспощадно, и те трюки, которые ещё пару лет назад работали на ура, сегодня уже не дают абсолютно никакого профита. Обновленный монструозный Lotus смотрел на меня как на обычного пользователя безо всяких прав. :) В такой ситуации любой начинающий взломщик полез бы на баг-трекеры и начал искать, к чему можно прицепиться, кроме устаревшего names.nsf в веб-сервисах.

На серверах, которые я тестировал, стоял почти самый свежий Lotus 8.5.2FP2. Ни Metasploit, ни exploit-db.com не порадовали меня ничем дельным. Однако я решил не полагаться на такие поповские источники эксплойтов и обратился за помощью в поиске багов без спloitов к ленте BugTraq, ZDI, сайту IBM с security-обновлениями и Гуглу. В результате я нашел кучу уязвимостей, связанных с переполнением буфера в различных сервисах, а также баг, позволяющий обойти аутентификацию и



выполнить произвольный код. Однако эксплойтов для всех этих уязвимостей не существовало, а описания ошибок были очень поверхностными и указывали лишь общее направление, в котором нужно двигаться. На первый взгляд, такие указания никак не могли помочь в разработке хоть сколько-нибудь эффективного эксплойта, но надо было двигаться дальше. :)

СКАЗ ПРО CVE-2011-1519

Бегло просмотрев различные уязвимости, я остановился на баге с обходом аутентификации, позволяющем выполнить произвольный код (а это как раз то, о чем мечтает каждый пентестер). Эта уязвимость, получившая на сайте ZDI код ZDI-11-110, на момент проведения пентеста числилась как Oday (сейчас уже имеется соответствующий патч). Приведу перевод описания указанной уязвимости с этого сайта:

«Эта уязвимость позволяет удаленному атакующему выполнить произвольный код на уязвимой установке Lotus Domino Server Controller. Для эксплуатации уязвимости не требуется аутентификация. Проблема существует в реализации функционала удаленной консоли, которая по умолчанию слушает TCP-порт 2050. При аутентификации пользователя сервер использует значение параметра COOKIEFILE, в котором пользователь передает путь для получения

INFO

IBM Lotus Domino Server — программное обеспечение компании IBM Lotus Software, серверная часть программного комплекса IBM Lotus Notes.

WWW

www.zerodayinitiative.com — ZDI;
www.ibm.com/software/ru/lotus/ — IBM Lotus Software;
bugtraq.ru — BugTraq;
dj.novexpress.com — DJ Java Decompiler.