УДК 004

Учащ. З. С. Быковский
Науч. рук. преп. Е. Е. Новикова
(филиал БГТУ «Витебский государственный технологический колледж)

СПОСОБЫ ЗАЩИТЫ ОТ НЕПРАВОМЕРНОГО ДОСТУПА К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ В СЕТИ ИНТЕРНЕТ

Цель исследования — определить уровень защиты сайтов от неправомерного доступа в сети интернет и обозначить меры и способы защиты от разного рода взломов.

Результаты исследования.

Мы должны беспокоиться о безопасности информации и знать риски, связанные с предоставлением доступа к конфиденциальным, персональным данным. Электронные средства хранения более уязвимы, чем бумажные: размещаемые на них данные можно и уничтожить, и скопировать, и незаметно видоизменить.

С каждым годом растет число взломов и пострадавших от них владельцев сайтов. Чтобы грамотно защитить свой ресурс, владелец веб-ресурса должен понимать, какие есть варианты взлома, как действует злоумышленник, какие векторы атак наиболее критичны и как их закрыть.

Варианты взлома сайтов:

1. С использованием веб-приложений:

черезCMS;

через плагины;

через подрядчика.

2. С использованием сетевых технологий (беспроводные подключения).

Вариант взлома черезCMS (система управления контентом) заключается в следующем: разработчики допускают ошибки, недостаточно фильтруются входные параметры, не проверяются размещаемые в базе данные, информация выводится на странице «как есть», без безопасных преобразований.

Вариант взлома через плагины: чем больше плагинов, тем больше вероятность наличия уязвимостей. В идеале, использовать решение «из коробки», с примененными патчами и критическими обновлениями, которые закрывают все известные публичные уязвимости в ядре CMS. Но, поскольку, функциональности не всегда хватает, то перед установкой плагинов нужно обязательно проверять, насколько они защищены и безопасны.

Вариант взлома через подрядчика: бывает, что подрядчик устанавливает плагины, которые содержат уязвимости. Например, владелец сайта находит красивый плагин галереи для сайта и просит фрилансера купить и настроить этот модуль. Фрилансер находит такой же плагин на «левом» сайте, берет деньги с заказчика на покупку, но на самом деле скачивает бесплатно.

С использованием сетевых технологий: с помощью лишь одного телефона. (Да, именно поэтомуодногруппники больше не просят, чтобы я раздал им интернет). Более серьезные вещи делаются на компьютере и чаще всего на операционной системе Linux.

Sql-инъекции.

Очевидно, что если у сайта есть уязвимости, то его можно взломать с помощью веб-атак. Но даже если сайт защищен техническими средствами, работает на надежной CMS, его все равно могут скомпрометировать. Наиболее популярный взлом через Sql-инъекции.

Sql-инъекция – это атака на базу данных, которая позволит выполнить некоторое действие, которое не планировалось создателем скрипта.

Когда пользователь авторизуется на сайте и передает свой пароль и логин, затем эти данные посылаются в базу данных и сверяются с записями в базе данных, если данные совпадают, то база данных отвечает что пользователь верно ввел данные и сайт разрешает доступ пользователю, если же данные не верны, то база данных возвращает ответ «нет» и сайт не пускает пользователя дальше.

Чтобы было более понятно приведу, пример из жизни.

Отец, написал в записке маме, чтобы она дала Васе 100 рублей и положил ее на стол. Переработав это в шуточный SQL язык, мы получим:

ДОСТАНЬ ИЗ кошелька 100 РУБЛЕЙ И ДАЙ ИХ Васе.

Так как отец плохо написал записку (корявый почерк), и оставил ее на столе, ее увидел брат Васи − Петя. Петя, будучи хакером, дописал там «ИЛИ Пете» и получился такой запрос:

ДОСТАНЬ ИЗ кошелька 100 РУБЛЕЙ И ДАЙ ИХ Васе ИЛИ Пете.

Мама, прочитав записку, решила, что Васе она давала деньги вчера и дала 100 рублей Пете. Вот простой пример SQL инъекции из жизни. Не фильтруя данные (мама еле разобрала почерк), Петя добился успеха.

Как взламывают большинство сайтов: примеры нецелевого взлома.

Чтобы осуществить сам взлом 10 минут не достаточно. Но, буквально вчера был найден уязвимый сайт и принято решение привести его как пример для презентации доклада.

Путем командной строки и программ была получена база данных, таблицы, затем поля из этих таблиц. И путем нехитрых действий просто выбраны поля, которые вызывают особый интерес, а именно пароли и e-mail пользователей. В данном докладе не демонстрируются способы взлома, основная цель – показать, что существует такая возможность.

Программист, владеющий методами технической защиты, несомненно, должен знать технологии взлома защит для того, чтобы, во-первых, не повторять ошибки существующих систем и, во-вторых, создавать более эффективные и надежные механизмы.

Пострадать в результате нецелевой атаки довольно просто: для этого достаточно не заметить или проигнорировать критическую уязвимость в CMS, шаблонах или плагинах своего сайта. Любая незакрытая брешь – отличный шанс очутиться среди «товарищей по несчастью» и прочно закрепиться в хакерской выборке кандидатов для взлома. А в случае «успешной» атаки приготовьтесь к тому, что ваш сайт начнут активно использовать для спам-рассылки, заражения пользователей, хостинга фишинговых страниц, атак на другие сайты или заработка на рекламе. Если на вашем сайте есть слабое звено и веб-проект уязвим к определенному виду атак, то рано или поздно вас взломают. Это нужно понимать каждому веб-мастеру и владельцу сайта.

Как же защититься от взлома?

Защитой сайта и его безопасностью должны заниматься две стороны – это владелец сайта и хостинг провайдер, на котором сайт находится.

Если хакеры взломают защиту хостинга, то они без труда могут получить доступ к файлам любого сайта, расположенного на нем и внедрить вирус или скрытую ссылку.

Не скачивайте плагины, различные шаблоны и модули с сомнительных ресурсов.

Не доверяйте создание и доработку сайта сомнительным людям. Это то, о чем говорилось в начале презентации «про подрядчиков». Отдали сайт человеку на доработку и он вставил туда какой-то новый плагин, это стало уязвимостью сайта.

Вовремя обновляйте ваши CMS, плагины и модули. Потому что зачастую разработчики в обновлениях закрывают дыры в обнаруженных уязвимых местах кода.

Способы защиты:

1. Установите антивирусную защиту.

2. Регулярно обновляйте операционную систему и программы.
3. Скачивайте файлы с надежных ресурсов.
4. Защитите Ваши персональные данные.
5. Используйте надежные пароли.

Конечно нельзя забывать про социальную инженерию. В наше время это популярно. У всех были ситуации, похожие на: «Зайди туда-то, нажми туда-то и получи 1000 $». Не доверяйте никому и даже самому себе.

Заключение.

Мотив большинства хакеров – это любопытство, вызов в жизни или ложное чувство силы, в то время как мотивом других являются только деньги. Однако, каким бы ни был мотив хакера, взлом вашего компьютера является незаконной деятельностью, а хакеры – это реальные люди, которые могут ворваться в ваш компьютер точно также, как воры могут проникнуть в ваш дом. Поэтому, вы должны знать, как остановить хакеров (воров) и как защитить компьютер от взломщиков, которые могут украсть ваши деньги или повредить вашей репутации.

ЛИТЕРАТУРА

1. SQL-injection в деталях [Электронный ресурс]. – Режим доступа : URL : http://xaknotdie.org/22h/12/10.html.

2. Методы и способы взломов сайта. Что такое SQL инъекции и что делать если сайт взломали? [Электронный ресурс]. – Режим доступа : URL : http://semantica.in/blog/vidy-vzlomov-sajtov-chto-delat-esli-sajt-vzlomali.html.

3. Атаки sql-injection (mysql) [Электронный ресурс]. – Режим доступа : URL : http://injection.rulezz.ru/sql-inj.html.

УДК 674.815

Учащ. В. В.Трутнёв, А. В. Гирдюк,
П. А. Корягин, В. В. Прудников
Науч.рук.преп. С.А. Остапчик, М.М. Шнитко
(филиал БГТУ «Витебский государственный технологический колледж)

ИССЛЕДОВАНИЕ СВОЙСТВ ПЛИТ МДФ

Введение. Тема исследовательской работы основана на том, что в последние два десятилетия плиты МДФ вытесняют из мебельного и столярно-строительного производства такие древесные материалы как древесно-стружечные плиты (ДСтП), ламинированные древесно-стружечные плиты (ЛДСтП)и фанеру.