В сети довольно много статей о взломе сайтов, о социальной инженерии, как о способе нападения. Довольно много сайтов, где можно скачать эксплоит на тот или иной скрипт. Однако статей, как от этого всего защититься, довольно мало. Я решил исправить этот недостаток и написал эту статью.

Сегодня мы научимся пользоваться социальной инженерией. А кто сказал, что её можно применять только при нападении? Сегодня мы будем при её помощи очень даже успешно защищаться! Говоря простым языком, социальная инженерия - развод лохов, т.е. фальсификация какой-либо информации и использование её в "нехороших" целях. Наверняка вам приходили сообщения типа: "Дайте нам ваш пароль от инета и будет вам счастье!". Это, конечно, немного утрированное сообщение - обычно такие сообщения очень тщательно пишутся и ложь всякими способами скрывается. Однако, большинство из нас с этим встречались и знают, что такое социальная инженерия. А почему бы нам не использовать что-то типа этого против тех, кто хочет нас взломать?

Для начала элементарные правила защиты. Над всем должен быть установлен жесточайший контроль, т.е. даже если есть какое-то маленькое незначительное поле ввода, которое почти ни на что не влияет, его обязательно нужно проверить, т.к. через такие мелкие дырки в основном и осуществляется взлом сайтов. Если вводится число - проверьте его границы (если оно должно не превышать что-то или, например, быть положительным). Если на вводе должны быть только целые числа - сразу берите число типа **int**, обрезая не числа. Если на вводе строка (не число) по возможности удаляйте **html** и **php** теги (**htmlspecialchars** и **strip_tags** вам в помощь). Где это возможно, старайтесь не отображать информацию в том виде, в каком её ввел пользователь. Т.е., например, вместо "*по запросу: < текст запроса > ничего найдено.*" лучше написать "*по Вашему запросу ничего не найдено.*", т.к. есть вероятность, что пользователь ввёл зловредный скрипт и он полностью выполнится и отобразится на странице. Даже если вы уверены, что всё обработали и просчитали, помните - бережёного бог бережёт, т.е. лишняя осторожность не помешает.

Чем меньше данных пользователь может залить к вам на сайт, тем меньше вероятность, что он зальёт вредоносный скрипт. Предположим, что у Вас есть форум, на который все пользователи могут заливать свои фотографии. Но если не проверять закачиваемые файлы, юзер с лёгкостью сможет залить на ваш сайт файл *hack.php*, который всё взломает. Запомните, возможность исполнения чужеродных скриптов на сайте равносильна полному контролю над сайтом! Т.е. как минимум нужно запретить закачивать файлы с расширением .php . А ещё лучше константно записать все разрешённые расширения файлов, до определённого уровня ограничить размер заливаемого файла и, в конце концов, везде вырезать теги.

Ну вот, теперь сайт уже немного защищён. А теперь прикинемся белыми, пушистыми, нихрена не знающими ламерами! На самом деле, взлом сайта довольно тяжёлая задача. Она требует прекрасных знаний языков, на которых написан данный сайт, логическое мышление и опыт. Далеко не все, кто считают себя хакерами, реально смогут взломать сайт. Теперь представим такую ситуацию: кто-то написал очень хороший, мощный движок сайта/форум. Очень много людей установило к себе на сайт эту прекрасную вещь. А какой-то хакер взломал этот движок/форум и написал универсальную программу для взлома данного типа программ (так называемый, експлоит [exploit]). Теперь любой ламер может скачать этот эксплоит и несколькими кликами мыши взломать огромное количество сайтов. Чаще всего такие "хакеры", которые только и умеют, что использовать чужие программы, и встречаются на просторах всемирной сети. Они видят надпись "Invision Power Board" (или подобную), достают эксплоит, выполняют его и вуаля - сайт хакнут! Кстати, так делают даже профессиональные хакеры - вовсе необязательно взламывать форум, если он уже взломан и нужно всего лишь почитать мануал (инструкцию) по взлому или скачать эксплоит.

Пускай у нас есть цель: сделать сайт с форумом. Причём, сайт мы кое-как уже

написали и некоторые странички динамически генерируются, а вот с форумом проблема. Выбор форума очень ответственен. В бесплатных каталогов скриптов их довольно много - выбирай на любой вкус. Нужно выбрать несколько, а потом попробовать поискать в сети информацию о взломе этих форумов (мануалы), эксплоиты на них. Выбираем тот форум, который душе ближе и в котором меньше всего дырок. Желательно, чтоб он не отличался какими-нибудь сверхъестественными способностями и не был уж очень большим. А теперь вся хитрость фокуса: попытаемся выдать наш форум за какой-нибудь другой! Приходит "хакер" к вам на сайт, видит знакомую модель форума, запускает сплоит, а тот посылает его куда подальше и говорит что форум не хакаем! Вот смеху-то будет!

Для того, чтобы выдать форум за другой, нужно хотя бы изменить его внешний вид. Чем реальнее Вы сможете сделать, тем лучше. Для этого я сохранил одну из страниц Invision Power Board (IPB) форума на винт и выдрал оттудова всю нужную мне информацию. Потом заменил старый внешний вид моего форума на вид IPB. Invision Power Board использует MySQL базу данных, в то время как форум, который выбрал я, все данные хранит в файлах. НИКАКОЙ эксплоит, рассчитанный на IPB мне не страшен. Также я полностью стёр информацию о том, какой форум на самом деле установлен, т.е. нельзя просто прийти на яндекс и спросить о взломе конкретной модели моего форума. Теперь если кто-то и захочет взломать форум, то ему придётся самостоятельно его изучать и искать дырки. Причём, если раньше он мог просто найти такую же модель форума, скачать её, и уже в исходниках искать дыры, то теперь этой возможности у взломщика нет...

Да, кстати, я надеюсь, вы не забыли профиксить баги своего форума, которые есть в сети?

Ну вот, форум защитили. Теперь приступим к защите сайта. Здесь также можно провернуть похожий финт - выдать один движок за другой. Однако, довольно часто движки сайтов отличаются не только внешним видом, так что сделать подмену инфы будет тяжелее. Обязательно удалите информацию о версии и типе движка. Даже там, где у вас статические страницы, сделайте вид, как будто они динамические, т.е. данные типа время генерации страницы и т.д., передавайте туда какие-нибудь параметры - пускай взломщик ломает статическую страницу, нам что, жалко что ли? Ведь её взломать невозможно!

Если ваш движок не использует БД можно выдавать строку типа: "Запросов к MySQL ..." и писать какое-нибудь число Пускай хакер ещё и MySQL дыры поищет - практиковаться полезно!

Ещё одним важным моментом является администраторская панель. Она - цель хакера. А что нам мешает положить на самое видное место файл **admin.php**, в котором будет находиться лже-админка? Внешне она должна быть максимально похожа на реальную, а при вводе данных говорить "*Введённые данные не верны*". Будет очень смешно, если кто-то решит перебором подобрать пароль к такой админке! .

Настоящая же админка должна находиться реально глубоко, например, в папке */downloads/games/* а сам файл админки должен называться, например, *tetris.php*, причём, при запуске админки без определённого параметра должен реально запускаться какой-нибудь JavaScript тетрис. Чтобы отвести подозрения, хорошо бы чтоб в данной папочке лежала ещё кучка JavaScript игр с расширением .php . Кто подумает, что там запрятана админка? Да никто... А вот вы в любую минуту сможете ввести http://your_site.com/downloads/games/tetris.php?a=not_hacker или что-то в этом роде. Не забывайте, авторизация пользователя всё равно обязательно должна присутствовать!

И на последок ещё одна частая ошибка веб-программиста. Вот пример запроса:

http://some_site.com/news.php?file=26.02.2006-news.txt

А вот как некоторые программисты обрабатывают данный запрос (приведён файл news.php):

PHP код:

```
<?php
  include($file);
?>
```

Во-первых, никакой проверки информации. Во-вторых файл не обязательно будет нужным, т.е. например:

http://some_site.com/news.php?file=forum/data/hack.php

Где hack.php - заранее залитый файл, либо файл с другого сервера. Т.е. по возможности никогда не подключайте файлы, переданные адресной строкой. Старайтесь это каким-нибудь образом обойти. Если обойти не получается - обязательно это контролируйте самым строжайшим образом!

Ну вот мы и научились некоторым приёмам защиты своего сайта. Некоторые из данных советов похожи на советы параноика: изменить внешний вид форума очень даже не просто. Однако, почти везде я старался объяснить зачем мы проводили те или иные действия. Рассмотрены далеко не все способы защиты - даже если вы и сделали всё, что в этой статье написано, это ещё не значит, что вас не хакнут. Настоящего хакера не остановит ни что...