

# Оглавление

00. Введение .....	10
О втором издании .....	10
Для кого эта книга .....	10
Об авторе .....	11
От издательства .....	12
<b>ЧАСТЬ I. ПРИСТУПАЯ К РАБОТЕ .....</b>	<b>13</b>
01. О хакинге и хакерах .....	14
Кто такие хакеры .....	14
Зачем хакеры взламывают веб-сайты .....	15
Собственная безопасность хакера .....	16
02. Подготовка .....	19
<b>ЧАСТЬ II. ОСНОВЫ ВЕБ-ХАКИНГА .....</b>	<b>29</b>
03. Первый взлом .....	30
04. PHP-инклюд .....	36
Локальный PHP-инклюд .....	36
Удаленный PHP-инклюд .....	41
Реальный пример PHP-инклюда — движок NaboPoll .....	46
Создание хакерского веб-шелла в логах Apache через локальный инклюд .....	47
Реальное местоположение логов .....	49
Защита от удаленного инклюда .....	50
Защита от локального инклюда .....	51
05. SQL-инъекция .....	53
Получение информации из базы данных .....	60
Создание веб-шелла .....	61
Защита от SQL-инъекции .....	62
Решение проблем с кодировкой .....	64
Вместо послесловия к главе 05 .....	65

06. Межсайтовый скриптинг . . . . .	66
Области применения XSS . . . . .	66
Пассивный межсайтовый скриптинг . . . . .	67
Активный межсайтовый скриптинг . . . . .	68
Пример мини-приложения, уязвимого для XSS . . . . .	69
Как хакеры обходят механизм фильтрации тега <script> . . . . .	74
07. Слепая SQL-инъекция . . . . .	77
Получение номера версии MySQL с помощью переменной @@version . . . . .	78
Проверка возможности доступа к таблице mysql.user . . . . .	79
Угадывание имен таблиц . . . . .	79
Угадывание имен столбцов в найденной таблице . . . . .	79
Извлечение данных из найденных таблиц/столбцов . . . . .	80
Слепая SQL-инъекция в движке NaboPoll . . . . .	82
Автоматизация механизма извлечения данных . . . . .	86
Поиск уязвимых сайтов . . . . .	87
Использование временных задержек . . . . .	88
08. Новые возможности PHP-инклюда . . . . .	91
Инъекция в файл /proc/self/environ . . . . .	91
Поиск логов сервера Apache . . . . .	92
Инклюд почтового сообщения . . . . .	92
«Повторение — мать учения» . . . . .	93
Немного о нестандартных ситуациях . . . . .	94
Выводы для веб-программистов . . . . .	97
09. CRLF-инклюд . . . . .	98
<b>ЧАСТЬ III. ЧТО ДАЛЬШЕ? . . . . .</b>	<b>99</b>
0A. Получение полноценного доступа к шеллу . . . . .	100
0B. Удаленный подбор паролей . . . . .	105
0C. Локальный взлом паролей . . . . .	113
Взлом хэшей паролей *nix-систем . . . . .	113
Особенности взлома LDAP-паролей . . . . .	116
Взлом MD5 и некоторых других хэшей . . . . .	117
Взлом хэшей паролей ОС Windows . . . . .	125
Локальный подбор паролей на компьютере жертвы . . . . .	128
0D. Повышение привилегий . . . . .	130
Как защититься от эксплойтов уровня ядра . . . . .	139
0E. Соккрытие следов присутствия . . . . .	143
0F. Исследование системы . . . . .	147
10. Алгоритмы получения контроля над сервером . . . . .	149
11. Удаленные эксплойты . . . . .	151

12. Противодействие хакерам .....	153
13. Реальные задачи IT-безопасности .....	157
Использование инсайдерской информации для взлома пароля .....	157
ICQ и работа для частного детектива .....	159
Работа для антихакера, или «привет из Бразилии» .....	161
Небезопасная программа VMware Player .....	163
Приложение 1. Основные *nix-команды .....	171
Приложение 2. SQL-инъекции в модуле show.php форума Cyphor .....	174
Приложение 3. Взлом паролей пользователей форума Cyphor .....	178
Приложение 4. Использование готового эксплойта для SQL-инъекции в форуме Cyphor .....	183
Приложение 5. Реализация SQL-инъекций в MS SQL Jet .....	186
Приложение 6. Усовершенствованный текст эксплойта naboroll.php .....	189
Приложение 7. Получение имен таблиц и данных через слепую SQL-инъекцию в MS Access .....	191
Приложение 8. Переустановка пароля администратора и угадывание его в instantCMS .....	192
Приложение 9. Быстрые методы слепой SQL-инъекции .....	195
Использование функции find_in_set(substr, strlist) .....	195
Использование конструкции find_in_set() + more1row .....	197
Приложение 10. Хакерский словарь .....	200