

Содержание

Введение	8
Глава 1. Интернет – "враждебная" среда	11
1.1. Динамика — прародительница всех дыр	11
1.2. Устойчивые системы	12
1.3. Фильтрация	15
1.4. Когда фильтрации недостаточно	17
1.5. Основные принципы безопасного программирования	20
Глава 2. Уязвимости в скриптах	23
2.1. Ошибки при различных методах передачи данных	23
2.1.1. HTTP <i>GET</i>	23
2.1.2. HTTP <i>POST</i>	25
2.1.3. <i>GET & POST</i>	27
2.1.4. HTTP cookie	30
2.1.5. Hidden-поля	33
2.1.6. Имитация HTTP-сеанса	34
2.1.7. Изменение посылаемых данных	36
2.2. Уязвимости в PHP-скриптах	36
2.2.1. Инъекция исходного кода PHP	37
2.2.2. Отсутствие инициализации переменных	64
2.2.3. Ошибки во включаемых файлах	71
2.2.4. Ошибки при загрузке файлов	77
2.3. Специфичные ошибки в Perl-скриптах	83
2.3.1. Ошибка Internal Server Error	83
2.3.2. Создание процесса в <i>open()</i>	87
2.3.3. Инъекция Perl-кода в функцию <i>require</i>	91
2.3.4. Выполнение и просмотр включаемых файлов	95
2.4. Ошибки, не связанные с конкретным языком программирования	97
2.4.1. Ошибки вывода произвольных файлов	97
2.4.2. Внедрение в функцию <i>system()</i>	106
2.4.3. Ошибки в загрузке файлов	112

2.4.4. Заголовок <i>REFERER</i> и <i>X-FORWARDED-FOR</i>	124
2.4.5. Раскрытие пути другой информации	129
Глава 3. SQL – инъекция, и с чем ее едят	131
3.1. Нахождение уязвимостей	131
3.1.1. Если вывод ошибок включен	132
3.1.2. Если ошибки не выводятся	133
3.2. Исследование запроса	142
3.2.1. Тип запроса	143
3.2.2. Кавычки в запросе	143
3.2.3. Пример	152
3.3. MySQL	160
3.3.1. Версии и особенности MySQL	161
3.3.2. Разграничение прав в MySQL	166
3.3.3. Определение MySQL	167
3.3.4. MySQL 4.x и похищение данных	176
3.3.5. MySQL 3.x и похищение данных	191
3.3.6. MySQL и файлы	199
3.3.7. Обход подводных камней	206
3.3.8. DOS в MySQL-инъекции	212
3.4. Другие типы серверов баз данных	214
3.4.1. PostgreSQL	214
3.4.2. MsSQL	221
3.4.3. Oracle	222
3.5. Заключение	223
Глава 4. Безопасная авторизация и аутентификация	225
4.1. Вход в систему	226
4.1.1. Длинный URL	226
4.1.2. Система аутентификации со стороны клиента	228
4.1.3. Одиночный пароль	231
4.1.4. Имя и пароль	232
4.2. Последующая аутентификация	232
4.2.1. HTTP <i>cookie</i>	233
4.2.2. Сессии	236
4.3. HTTP Basic-аутентификация	240
4.4. HTTPS	250
4.5. Приемы, улучшающие защиту	251
4.5.1. Ограничение по IP-адресу	251
4.5.2. Восстановление пароля	252
4.5.3. Достаточно хорошая защита	255
4.6. Заключение	259
Глава 5. XSS и похищенные cookie	261
5.1. Основы	261
5.2. Опасность уязвимости	268
5.2.1. Изменение вида страниц	270
5.2.2. Отправка данных методом JavaScript	280

5.2.3. Обход подводных камней	283
5.2.4. Получение cookies пользователей	285
5.3. Сбор статистики	289
5.4. Выполнение неявных действий администратором	292
5.5. Механизмы фиксации сессии	294
5.6. Уязвимость в обработке событий	298
5.7. Внедрение JavaScript в адресной строке	302
5.8. Как защититься от уязвимости	303
Глава 6. Миф о безопасной конфигурации	309
6.1. Безопасная настройка PHP	310
6.1.1. Директива конфигурации <i>allow_url_fopen</i>	310
6.1.2. Директива конфигурации <i>display_errors</i>	311
6.1.3. Магические кавычки	312
6.1.4. Глобальные переменные	313
6.1.5. Определение PHP	315
6.1.6. Некоторые другие директивы конфигурации	316
6.1.7. Защищенный режим PHP	317
6.2. Модуль Apache <i>mod_security</i>	323
6.2.1. Универсальный метод обхода <i>mod_security</i>	328
6.3. Методы пассивного анализа и обхода	336
6.3.1. Просмотр HTML	336
6.3.2. Hidden-поля и JavaScript	338
6.4. Ограничения в HTML	343
6.5. Log-файлы и определение атакующего	346
6.6. Заключение	349
Глава 7. Безопасность в условиях shared hosting	351
7.1. Доступ к файлам владельцев систем	351
7.2. Файлы и Web-сервер	353
7.3. Хостинг и базы данных	364
7.4. Проблема открытого кода	371
7.5. Точка зрения нападающего	380
7.5.1. Информация с сайта хостинга	380
7.5.2. Реверс-зона DNS	383
7.5.3. Информация из поисковых систем	383
7.5.4. Информация из базы данных <i>netcraft</i>	383
7.5.5. Кэш какого-либо DNS-сервера	384
7.6. Заключение	384
Глава 8. Концептуальный вирус	387
8.1. Идея создания	387
8.2. Анализ существующих вирусов	389
8.3. Поиск	391
8.4. Заражение	395
8.5. Заключение	397
Заключение	399

Приложение 1. Описание компакт-диска	401
Список файлов	401
Установка ПО с диска	406
Приложение 2. Задачи на проникновение в тестовые системы	407
Задача 1	407
Задача 2	408
Задача 3	408
Задача 4	409
Задача 5	409
Задача 6	410
Приложение 3. Решение задач	411
Задача 1	411
Задача 2	412
Задача 3	414
Задача 4	415
Задача 5	419
Задача 6	420
Предметный указатель	423