

ГОЛОВОЛОМКИ

на

PHR

ДЛЯ

ХАКЕРА

Максим Кузнецов, Игорь Симдянов



PHR

+CD



Максим Кузнецов

Игорь Симдянов

ГОЛОВОЛОМКИ
на РНР
ДЛЯ
КАКЕРА

Санкт-Петербург

«БХВ-Петербург»

2006

УДК 681.3.06
ББК 32.973.26-018.1
К89

Кузнецов, М. В.

К89 Головоломки на PHP для хакера / М. В. Кузнецов, И. В. Симдянов. — СПб.: БХВ-Петербург, 2006. — 464 с.: ил.

ISBN 5-94157-837-7

Книга представляет собой задачник по Web-технологиям с уклоном в защиту Web-приложений от злоумышленников. Цель книги — помочь Web-разработчику научиться самостоятельно обнаруживать и устранять уязвимости в своем коде. На компакт-диске, поставляемом вместе с книгой, приведены скрипты, являющиеся ответами на предлагаемые задачи.

Для программистов и Web-разработчиков

УДК 681.3.06
ББК 32.973.26-018.1

Группа подготовки издания:

| | |
|---------------------------|-----------------------------|
| Главный редактор | <i>Екатерина Кондукова</i> |
| Зам. главного редактора | <i>Евгений Рыбаков</i> |
| Зав. редакцией | <i>Григорий Добин</i> |
| Редактор | <i>Ирина Иноземцева</i> |
| Компьютерная верстка | <i>Натальи Караваевой</i> |
| Корректор | <i>Виктория Пиотровская</i> |
| Дизайн серии | <i>Инны Тачиной</i> |
| Оформление обложки и фото | <i>Елены Беляевой</i> |
| Зав. производством | <i>Николай Тверских</i> |

Лицензия ИД № 02429 от 24.07.00. Подписано в печать 24.04.06.
Формат 70×100^{1/16}. Печать офсетная. Усл. печ. л. 37,41.
Тираж 3000 экз. Заказ №
"БХВ-Петербург", 194354, Санкт-Петербург, ул. Есенина, 5Б.

Отпечатано с готовых диапозитивов
в ГУП "Типография "Наука"
199034, Санкт-Петербург, 9 линия, 12

ISBN 5-94157-837-7

© Кузнецов М. В., Симдянов И. В. 2006
© Оформление, издательство "БХВ-Петербург", 2006

Оглавление

| | |
|--|-----------|
| Введение | 1 |
| Благодарности | 2 |
| Часть I. ЗАДАЧИ | 3 |
| Глава I.1. Строки | 5 |
| I.1.1. Количество и имена файлов в произвольном каталоге..... | 5 |
| I.1.2. Выравнивание по правому краю..... | 5 |
| I.1.3. Выравнивание по левому и правому краям..... | 7 |
| I.1.4. Вывод данных в три столбца..... | 7 |
| I.1.5. Передача массива между двумя страницами | 8 |
| I.1.6. Передача массива методом GET | 8 |
| I.1.7. Передача массива методом POST | 8 |
| I.1.8. Передача массива через сессии..... | 8 |
| I.1.9. Передача массива через cookies | 8 |
| I.1.10. Календарь | 9 |
| I.1.11. Вертикальный вывод строки | 9 |
| I.1.12. Число в денежном формате..... | 10 |
| I.1.13. Замена символов bbCode | 10 |
| Глава I.2. Регулярные выражения | 11 |
| I.2.1. Удаление всех тегов из HTML-страницы | 11 |
| I.2.2. Удаление изображений из HTML-страницы..... | 12 |
| I.2.3. Извлечение названия HTML-страницы..... | 12 |
| I.2.4. Конвертация даты из MySQL-формата в календарный формат..... | 12 |
| I.2.5. Проверка корректности ввода адреса электронной почты | 12 |
| I.2.6. Проверка корректности ввода URL..... | 13 |
| I.2.7. Подсветка URL..... | 13 |
| I.2.8. Проверка корректности ввода чисел | 13 |
| I.2.9. Изменение регистра | 13 |
| I.2.10. Разбивка длинной строки | 14 |
| I.2.11. Разбивка HTML-страницы на предложения | 14 |
| I.2.12. Количество слов в тексте..... | 14 |
| I.2.13. Интерпретация тегов bbCode..... | 14 |
| I.2.14. Подсветка PHP-кода | 15 |

| | |
|--|-----------|
| Глава I.3. Файлы | 16 |
| I.3.1. Загрузка файлов на сервер..... | 16 |
| I.3.2. Редактирование файлов на удаленном сервере..... | 17 |
| I.3.3. Уязвимость скрипта загрузки..... | 17 |
| I.3.4. Счетчик загрузок | 18 |
| I.3.5. Сохранение текстовых и графических файлов..... | 19 |
| I.3.6. Определение размера файла..... | 19 |
| I.3.7. Определение количества строк в файле..... | 19 |
| I.3.8. Изменение порядка следования строк в файле..... | 20 |
| I.3.9. Список файлов и подкаталогов в каталоге..... | 20 |
| I.3.10. Количество файлов в каталогах | 20 |
| I.3.11. Количество строк в файлах проекта..... | 21 |
| I.3.12. Замена строки во всех файлах вложенных подкаталогов..... | 21 |
| I.3.13. Загрузка файла на сервер по частям..... | 21 |
| I.3.14. Удаление каталога..... | 21 |
| I.3.15. Случайный вывод из файла..... | 22 |
| I.3.16. Редактирование файла | 22 |
| I.3.17. Сортировка содержимого текстового файла..... | 22 |
| I.3.18. Добавление записи в файл..... | 23 |
| I.3.19. Постраничная навигация..... | 23 |
| I.3.20. Система регистрации..... | 23 |
| I.3.21. Случайный вывод из файла..... | 24 |
| I.3.22. Определение даты создания изображения..... | 24 |
| I.3.23. Копирование содержимого одного каталога в другой..... | 24 |
| I.3.24. Взлом гостевой книги | 24 |
| Глава I.4. MySQL | 26 |
| I.4.1. Система регистрации | 26 |
| I.4.2. SQL-инъекция по числовому параметру..... | 28 |
| I.4.3. Определение версии сервера MySQL | 29 |
| I.4.4. Поиск пользователя — SQL-инъекция | 29 |
| I.4.5. Удаление пользователей при помощи SQL-инъекции | 31 |
| I.4.6. Постраничная навигация..... | 33 |
| I.4.7. Алфавитная навигация..... | 35 |
| I.4.8. Сортировка..... | 36 |
| I.4.9. Двойной выпадающий список..... | 37 |
| I.4.10. Удаление сразу нескольких позиций..... | 37 |
| I.4.11. Хранение MP3-файлов в базе данных..... | 38 |
| I.4.12. Хранение изображений в базе данных..... | 39 |
| I.4.13. Загрузка данных из дампа базы данных..... | 40 |
| Глава I.5. Сессии и cookies | 41 |
| I.5.1. Пользователи OnLine | 41 |
| I.5.2. Собственный механизм сессии..... | 42 |
| I.5.3. Защита HTML-формы при помощи сессии..... | 42 |
| I.5.4. Определение, включены ли cookie у посетителя | 43 |
| I.5.5. Подделка cookie | 43 |

| | |
|---|-----------|
| I.5.6. Обход защищенной сессией HTML-формы..... | 44 |
| I.5.7. Межсайтовый скриптинг..... | 45 |
| I.5.8. Похищение cookie..... | 47 |
| Глава I.6. Пользовательские агенты и рефереры..... | 48 |
| I.6.1. Переходы с других сайтов..... | 48 |
| I.6.2. Защита HTML-формы при помощи реферера..... | 49 |
| I.6.3. Фальсификация реферера..... | 50 |
| I.6.4. Ключевые слова поисковых систем..... | 50 |
| I.6.5. Распознавание посещений сайта роботами поисковых систем..... | 50 |
| I.6.6. Защита от менеджеров загрузки..... | 50 |
| I.6.7. Фальсификация пользовательского агента..... | 51 |
| Глава I.7. Авторизация и аутентификация..... | 52 |
| I.7.1. Авторизация на файлах..... | 53 |
| I.7.2. Шифрование пароля..... | 54 |
| I.7.3. Подбор пароля..... | 55 |
| I.7.4. Подбор пароля по словарю..... | 55 |
| I.7.5. Генератор паролей..... | 56 |
| I.7.6. Защита текстовых файлов от просмотра в браузере..... | 56 |
| I.7.7. Авторизация при помощи cookie..... | 57 |
| I.7.8. Защита имени пользователя от подделки..... | 59 |
| I.7.9. Авторизация при помощи сессий..... | 60 |
| I.7.10. Шифрование пароля в базе данных..... | 62 |
| I.7.11. Базовая HTTP-авторизация..... | 62 |
| Глава I.8. Использование информации со сторонних сайтов..... | 63 |
| I.8.1. Загрузка страницы с удаленного хоста..... | 64 |
| I.8.2. Извлечение ссылок с Yandex..... | 64 |
| I.8.3. Извлечение ссылок с Google..... | 65 |
| I.8.4. Извлечение ссылок с Rambler..... | 66 |
| I.8.5. Извлечение ссылок с Aport..... | 67 |
| I.8.6. Определение курса валют из XML-файла..... | 68 |
| I.8.7. Определение динамики курса валют..... | 69 |
| Глава I.9. FTP-протокол..... | 72 |
| I.9.1. Определение типа операционной системы..... | 72 |
| I.9.2. Список файлов на FTP-сервере..... | 72 |
| I.9.3. Загрузка файлов..... | 73 |
| I.9.4. Изменение прав доступа..... | 73 |
| Глава I.10. Протокол HTTP..... | 74 |
| I.10.1. Загрузка страницы..... | 74 |
| I.10.2. Получение HTTP-заголовков с сервера..... | 75 |
| I.10.3. Определение размера файла на удаленном хосте..... | 75 |
| I.10.4. Отправка данных методом POST..... | 75 |

| | |
|--|-----------|
| Глава I.11. Электронная почта | 77 |
| I.11.1. Отправка почтового сообщения с сайта..... | 77 |
| I.11.2. Отправка письма с вложением | 77 |
| I.11.3. Массовая рассылка писем | 77 |
| I.11.4. Предотвращение массовой рассылки | 78 |
| I.11.5. Отправка почтового сообщения через SMTP-ретранслятор | 78 |
| I.11.6. Выяснение адресов почтовых ретрансляторов | 78 |
| Глава I.12. Whois-сервис | 79 |
| I.12.1. Определение принадлежности IP-адресов..... | 79 |
| I.12.2. Определение принадлежности европейских IP-адресов | 79 |
| I.12.3. Следование реферальному серверу | 80 |
| I.12.4. Определение IP-адреса по сетевому адресу | 81 |
| I.12.5. Определение сетевого адреса по IP-адресу..... | 81 |
| I.12.6. Выяснение, занят ли домен..... | 81 |
| Глава I.13. Операционная система UNIX | 82 |
| I.13.1. Использование утилиты ping | 82 |
| I.13.2. Работа с номером узла | 82 |
| I.13.3. Права доступа..... | 83 |
| I.13.4. Работа с архивами..... | 83 |
| Глава I.14. Шпионские скрипты | 84 |
| I.14.1. Слежение за ссылкой на удаленной странице | 84 |
| I.14.2. Проверка ссылочной целостности..... | 84 |
| I.14.3. Новые файлы на виртуальном хосте | 85 |
| I.14.4. Слишком большие файлы на виртуальном хосте | 85 |
| Глава I.15. Разное | 86 |
| I.15.1. Обмен значений переменных..... | 86 |
| I.15.2. Скрипт предзагрузки страницы | 86 |
| I.15.3. Эмуляция утилиты tar | 87 |
| I.15.4. Буферизация данных..... | 87 |
| Часть II. РЕШЕНИЯ | 89 |
| Глава II.1. Строки | 91 |
| II.1.1. Количество и имена файлов в произвольном каталоге | 91 |
| II.1.2. Выравнивание по правому краю | 95 |
| II.1.3. Выравнивание по левому и правому краям | 96 |
| II.1.4. Вывод данных в три столбца | 97 |
| II.1.5. Передача массива между двумя страницами..... | 99 |
| II.1.6. Передача массива методом GET | 100 |
| II.1.7. Передача массива методом POST..... | 102 |

| | |
|---|------------|
| П.1.8. Передача массива через сессии | 103 |
| П.1.9. Передача массива через cookies..... | 104 |
| П.1.10. Календарь..... | 106 |
| П.1.11. Вертикальный вывод строки..... | 109 |
| П.1.12. Число в денежном формате | 110 |
| П.1.13. Замена символов bbCode..... | 110 |
| Глава П.2. Регулярные выражения | 113 |
| П.2.1. Удаление всех тегов из HTML-страницы..... | 113 |
| П.2.2. Удаление изображений из HTML-страницы | 115 |
| П.2.3. Извлечение названия HTML-страницы | 116 |
| П.2.4. Конвертация даты из MySQL-формата в календарный..... | 117 |
| П.2.5. Проверка корректности ввода адреса электронной почты..... | 118 |
| П.2.6. Проверка корректности ввода URL..... | 120 |
| П.2.7. Подсветка URL | 121 |
| П.2.8. Проверка корректности ввода чисел..... | 121 |
| П.2.9. Изменение регистра..... | 122 |
| П.2.10. Разбивка длинной строки..... | 124 |
| П.2.11. Разбивка текста на предложения..... | 124 |
| П.2.12. Количество слов в тексте | 128 |
| П.2.13. Интерпретация тегов bbCode | 131 |
| П.2.14. Подсветка PHP-кода..... | 132 |
| Глава П.3. Файлы | 136 |
| П.3.1. Загрузка файлов на сервер | 136 |
| П.3.2. Редактирование файлов на удаленном сервере..... | 138 |
| П.3.3. Уязвимость скрипта загрузки..... | 140 |
| П.3.4. Счетчик загрузок..... | 144 |
| П.3.5. Сохранение текстовых и графических файлов | 147 |
| П.3.6. Определение размера файла..... | 148 |
| П.3.7. Определение количества строк в файле | 150 |
| П.3.8. Изменение порядка следования строк в файле | 150 |
| П.3.9. Список файлов и подкаталогов в каталоге | 151 |
| П.3.10. Количество файлов в каталогах..... | 152 |
| П.3.11. Количество строк в файлах проекта | 154 |
| П.3.12. Замена строки во всех файлах вложенных подкаталогов | 156 |
| П.3.13. Загрузка файла на сервер по частям | 157 |
| П.3.14. Удаление каталога | 159 |
| П.3.15. Случайный вывод из файла | 160 |
| П.3.16. Редактирование файла..... | 161 |
| П.3.17. Сортировка содержимого текстового файла | 162 |
| П.3.18. Добавление записи в файл | 167 |
| П.3.19. Постраничная навигация | 168 |
| П.3.20. Система регистрации | 170 |
| П.3.21. Случайный вывод из файла | 175 |
| П.3.22. Определение даты создания изображения | 175 |
| П.3.23. Копирование содержимого одного каталога в другой | 176 |
| П.3.24. Взлом гостевой книги..... | 177 |

| | |
|---|------------|
| Глава II.4. MySQL и SQL-инъекции | 180 |
| II.4.1. Система регистрации | 180 |
| II.4.2. SQL-инъекция по числовому параметру | 183 |
| II.4.3. Определение версии сервера MySQL | 188 |
| II.4.4. Поиск пользователя — SQL-инъекция | 189 |
| II.4.5. Удаление пользователей при помощи SQL-инъекции | 195 |
| II.4.6. Постраничная навигация | 197 |
| II.4.7. Алфавитная навигация | 200 |
| II.4.8. Сортировка | 203 |
| II.4.9. Двойной выпадающий список | 205 |
| II.4.10. Удаление сразу нескольких позиций | 211 |
| II.4.11. Хранение MP3-файлов в базе данных | 213 |
| II.4.12. Хранение изображений в базе данных | 216 |
| II.4.13. Загрузка данных из дампа базы данных | 221 |
| Глава II.5. Сессии и cookies | 222 |
| II.5.1. Пользователи OnLine | 222 |
| II.5.2. Собственный механизм сессии | 225 |
| II.5.3. Защита HTML-формы при помощи сессии | 230 |
| II.5.4. Определение, включены ли cookie у посетителя | 232 |
| II.5.5. Подделка cookie | 233 |
| II.5.6. Обход защищенной сессией HTML-формы | 235 |
| II.5.7. Межсайтовый скриптинг | 238 |
| II.5.8. Похищение cookie | 240 |
| Глава II.6. Пользовательские агенты и рефереры | 241 |
| II.6.1. Переходы с других сайтов | 241 |
| II.6.2. Защита HTML-формы при помощи реферера | 243 |
| II.6.3. Фальсификация реферера | 244 |
| II.6.4. Ключевые слова поисковых систем | 246 |
| II.6.5. Распознавание посещений сайта роботами поисковых систем | 247 |
| II.6.6. Защита от менеджеров загрузки | 249 |
| II.6.7. Фальсификация пользовательского агента | 249 |
| Глава II.7. Авторизация и аутентификация | 251 |
| II.7.1. Авторизация на файлах | 251 |
| II.7.2. Шифрование пароля | 256 |
| II.7.3. Подбор пароля | 260 |
| II.7.4. Подбор пароля по словарю | 267 |
| II.7.5. Генератор паролей | 269 |
| II.7.6. Защита текстовых файлов от просмотра в браузере | 270 |
| II.7.7. Авторизация при помощи cookie | 271 |
| II.7.8. Защита имени пользователя от подделки | 278 |
| II.7.9. Авторизация при помощи сессий | 279 |
| II.7.10. Шифрование пароля в базе данных | 282 |
| II.7.11. Базовая HTTP-авторизация | 283 |

| | |
|--|------------|
| Глава II.8. Использование информации со сторонних сайтов..... | 286 |
| II.8.1. Загрузка страницы с удаленного хоста | 286 |
| II.8.2. Извлечение ссылок с Yandex | 287 |
| II.8.3. Извлечение ссылок с Google | 289 |
| II.8.4. Извлечение ссылок с Rambler | 295 |
| II.8.5. Извлечение ссылок с Aport..... | 297 |
| II.8.6. Определение курса валют из XML-файла | 298 |
| II.8.7. Определение динамики курса валют..... | 301 |
| Глава II.9. FTP-протокол..... | 305 |
| II.9.1. Определение типа операционной системы | 305 |
| II.9.2. Список файлов на FTP-сервере | 307 |
| II.9.3. Загрузка файлов..... | 310 |
| II.9.4. Изменение прав доступа | 312 |
| Глава II.10. Протокол HTTP | 314 |
| II.10.1. Загрузка страницы..... | 314 |
| II.10.2. Получение HTTP-заголовков с сервера..... | 318 |
| II.10.3. Определение размера файла на удаленном хосте | 320 |
| II.10.4. Отправка данных методом POST..... | 321 |
| Глава II.11. Электронная почта..... | 324 |
| II.11.1. Отправка почтового сообщения с сайта | 324 |
| II.11.2. Отправка письма с вложением | 326 |
| II.11.3. Массовая рассылка писем..... | 329 |
| II.11.4. Предотвращение массовой рассылки..... | 331 |
| II.11.5. Отправка почтового сообщения через SMTP-ретранслятор..... | 333 |
| II.11.6. Выяснение адресов почтовых ретрансляторов..... | 334 |
| Глава II.12. Whois-сервис | 336 |
| II.12.1. Определение принадлежности IP-адресов | 336 |
| II.12.2. Определение принадлежности европейских IP-адресов..... | 337 |
| II.12.3. Следование реферальному серверу..... | 338 |
| II.12.4. Определение IP-адреса по сетевому адресу..... | 341 |
| II.12.5. Определение сетевого адреса по IP-адресу | 342 |
| II.12.6. Выяснение, занят ли домен | 342 |
| Глава II.13. Операционная система UNIX..... | 350 |
| II.13.1. Использование утилиты ping | 350 |
| II.13.2. Работа с номером узла..... | 352 |
| II.13.3. Права доступа | 353 |
| II.13.4. Работа с архивами | 357 |
| Глава II.14. Шпионские скрипты | 359 |
| II.14.1. Слежение за ссылкой на удаленной странице | 359 |
| II.14.2. Проверка ссылочной целостности | 366 |

| | |
|---|------------|
| П.14.3. Новые файлы на виртуальном хосте | 369 |
| П.14.4. Слишком большие файлы на виртуальном хосте | 371 |
| Глава П.15. Разное..... | 373 |
| П.15.1. Обмен значений переменных | 373 |
| П.15.2. Скрипт предзагрузки страницы | 374 |
| П.15.3. Эмуляция утилиты tar | 375 |
| П.15.4. Буферизация данных | 378 |
| ПРИЛОЖЕНИЯ..... | 381 |
| Приложение 1. Вопросы взлома и безопасности, напрямую не связанные с кодированием | 383 |
| Что такое прокси-сервер и зачем он нужен? | 383 |
| Классификация прокси-серверов..... | 383 |
| Анонимные прокси-серверы..... | 386 |
| Настройка браузера Internet Explorer для работы с прокси-сервером..... | 389 |
| Как построить цепочку из прокси-серверов? | 390 |
| Что такое port mapping?..... | 392 |
| Прокси-серверы и DNS-серверы | 392 |
| РАС-файлы | 393 |
| Где взять списки бесплатных прокси-серверов? | 394 |
| Зачем нужны постоянные обновления списков прокси-серверов?..... | 395 |
| Почему бесплатные прокси-серверы исчезают? | 395 |
| Проверка работоспособности прокси-серверов..... | 396 |
| Полезные ссылки | 398 |
| Приложение 2. Преступность в IT | 400 |
| Виды преступлений в IT-отрасли..... | 400 |
| Глава 28 УК РФ | 409 |
| Спрашивайте — отвечаем..... | 413 |
| Приложение 3. Введение в социальное программирование или кто такие социальные хакеры | 418 |
| Несколько примеров..... | 418 |
| Психология = программирование..... | 422 |
| Социальное программирование..... | 422 |
| Трансактный анализ | 423 |
| Введение в НЛП..... | 437 |
| Заключение или как стать социальным программистом | 448 |
| Приложение 4. Описание компакт-диска..... | 450 |
| Предметный указатель | 451 |

Введение

Предлагаемая книга является сборником задач по РНР с уклоном в защиту сайта и Web-приложений от злоумышленников.

Основная проблема создателей Web-приложений заключается в том, что они мыслят совсем другими категориями, нежели злоумышленники. Кроме того, Web-разработчики редко прибегают к тестированию своих разработок на предмет уязвимости, так как им подсознательно не хочется ломать свои собственные Web-приложения. Снять такой настрой поможет эта книга, где, наряду с задачами по защите Web-приложений, будет предложено большое количество задач по взлому сайта с применением самых различных технологий, от межсайтового скриптинга и SQL-инъекций до подбора паролей при помощи словаря. Это позволит читателю убедиться в том, как легко может быть нарушена работа Web-сайта и как дорого может обернуться беспечность при его разработке.

Наряду с "деструктивными" задачами будет предложено большое количество заданий, направленных на построение обороны сайта. Выполнив задания, вы получите в руки мощную систему защиты собственного сайта, которая будет отличаться от коммерческих и свободных аналогов тем, что вы будете знать в ней каждый винтик и сможете легко модернизировать ее, быстро устранять последствия взлома и находить уязвимости.

Книга разбита на две части: непосредственно задачник и ответы на задачи. Вы можете решать все задачи последовательно или, если вам необходимо срочно защитить свой сайт, можете воспользоваться готовыми кодами, находящимися на прилагаемом к книге компакт-диске. Коды примеров можно также загрузить с сайта IT-студии SoftTime по адресу <http://www.softtime.ru/security/>.

По всем вопросам, возникающим по мере чтения книги, вы можете обращаться на форум, расположенный на Web-сайте IT-студии SoftTime, сотрудниками которой являются авторы книги (<http://www.softtime.ru/forum/>).

Авторы присутствуют на форуме каждый день и с удовольствием ответят на ваши вопросы.

Благодарности

Авторы благодарят сотрудника отдела разработки программного обеспечения средств связи IT-студии SoftTime Ломалова В. П. за помощь в написании *Приложения 1*.

Авторы также выражают большую признательность следователю УФСБ РФ по Нижегородской области Зайченко Д. А. и старшему оперуполномоченному УФСБ РФ по Нижегородской области Новикову В. Б. за ценные консультации, которые они оказывали авторам при написании *Приложения 2*.

Авторы благодарны сотрудникам издательства "БХВ-Петербург", усилиями которых эта рукопись увидела свет, и посетителям форума <http://www.softtime.ru/forum/> за интересные вопросы и конструктивное обсуждение.

```
## Sample if1.cfg file
## Define preprocess
/DMY_PROJECT prepr
## Set extended leng
/4L132
## Set extended
##
## Set maximum float
/Opc80
##
## Additional direct
## files, before the
```

Часть I

ЗАДАЧИ

Глава I.1

```
## Sample if1.cfg file
## Define preprocess
/DMY_PROJECT prepr
## Set extended leng
/41132
## Set extended
## Set maximum float
/OpC80
##
## Additional direct
## files, before the
```

Строки

Работа со строками составляет основу любого программирования. Виртуозное манипулирование строками позволит программисту создавать более короткие и эффективные программы. Исследования показали, что плотность ошибок в программах не зависит от языка программирования, а зависит только от квалификации программиста. Чем короче будут программы, тем меньше ошибок и уязвимостей в них будет. Хорошее знание особенностей строк позволяет безошибочно определять возможные проблемные с точки зрения безопасности места в коде. Данная глава содержит задачи на знание строковых функций РНР и умение обращаться с ними.

Замечание

Все примеры из данной главы можно найти в каталоге scripts\1 компакт-диска, поставляемого вместе с книгой.

I.1.1. Количество и имена файлов в произвольном каталоге

Определите количество и имена файлов в каталоге, не прибегая к функциям работы с каталогами. Решение задачи основано на том факте, что в РНР существует несколько видов кавычек, каждый из которых обладает своими свойствами.

I.1.2. Выравнивание по правому краю

Пусть есть список файлов в массиве (листинг I.1.1). У имен файлов может быть различная длина, и необходимо выровнять их по правому краю так, как это изображено на рис. I.1.1. Для решения задачи не разрешается

прибегать к атрибуту `align` и CSS, можно использовать только теги `<pre>` и `</pre>`.

Листинг I.1.1. Массив `$filename` с именами файлов

```
<?php
    $filename = array("all.php", "auth.php",
                      "auth.txt", "base.txt",
                      "chat.html", "config.php",
                      "count.txt", "count_new.txt",
                      "counter.dat", "counter.php",
                      "create.php", "dat.db");
?>
```

Замечание

Файл с массивом можно найти на прилагаемом к книге компакт-диске (`scripts\1\1.2\1.php`).

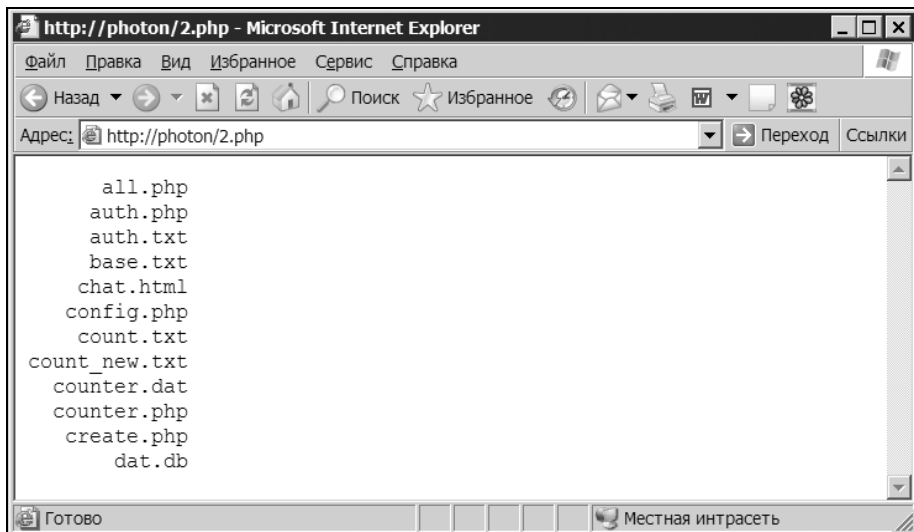


Рис. I.1.1. Выравнивание имен файлов по правому краю

1.1.3. Выравнивание по левому и правому краям

Необходимо разбить массив `$filename` (листинг 1.1.1) на две части и вывести в виде двух колонок так, как это представлено на рис. 1.1.2. Для решения задачи не разрешается прибегать к атрибуту `align` и CSS, можно использовать только теги `<pre>` и `</pre>`.

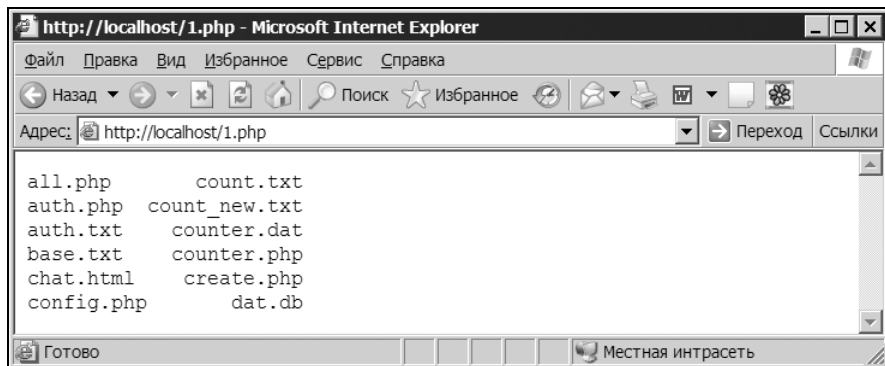


Рис. 1.1.2. Выравнивание имен файлов по левому и правому краям

1.1.4. Вывод данных в три столбца

Часто перед Web-разработчиками встает задача вывода таблицы, содержащей несколько столбцов. Выведите имена файлов из массива `$filename` (листинг 1.1.1) двумя способами, представленными на рис. 1.1.3 и 1.1.4 соответственно. При решении этой задачи необходимо динамически сформировать HTML-таблицу.



Рис. 1.1.3. Первый вариант вывода массива в три столбца



Рис. I.1.4. Второй вариант вывода массива в три столбца

I.1.5. Передача массива между двумя страницами

Пусть массив `$filename`, представленный в листинге I.1.1, определен на странице `first.php`. Отобразите его на странице `second.php`, используя инструкцию `include`.

I.1.6. Передача массива методом GET

Пусть массив `$filename`, представленный в листинге I.1.1, определен на странице `first.php`. Отобразите его на странице `second.php`, используя для передачи метод GET.

I.1.7. Передача массива методом POST

Пусть массив `$filename`, представленный в листинге I.1.1, определен на странице `first.php`. Отобразите его на странице `second.php`, используя для передачи метод POST.

I.1.8. Передача массива через сессии

Пусть массив `$filename`, представленный в листинге I.1.1, определен на странице `first.php`. Отобразите его на странице `second.php`, используя сессии.

I.1.9. Передача массива через cookies

Пусть массив `$filename`, представленный в листинге I.1.1, определен на странице `first.php`. Отобразите его на странице `second.php`, используя cookies.

1.1.10. Календарь

Создайте календарь на текущий месяц в двух форматах: американском (рис. 1.1.5) и российском (рис. 1.1.6).

Субботу и воскресенье необходимо подсветить красным цветом.

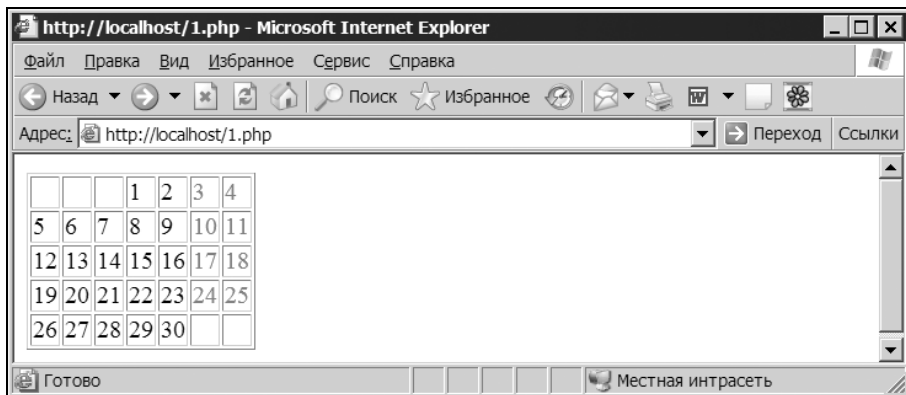


Рис. 1.1.5. Календарь на текущий месяц в американском формате

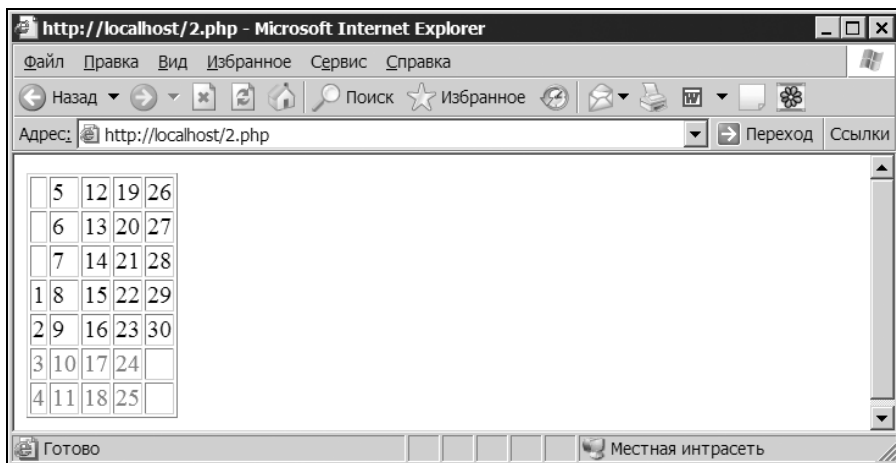


Рис. 1.1.6. Календарь на текущий месяц в российском формате

1.1.11. Вертикальный вывод строки

Выведите строку "Hello world!" вертикально, так, как это представлено на рис. 1.1.7.

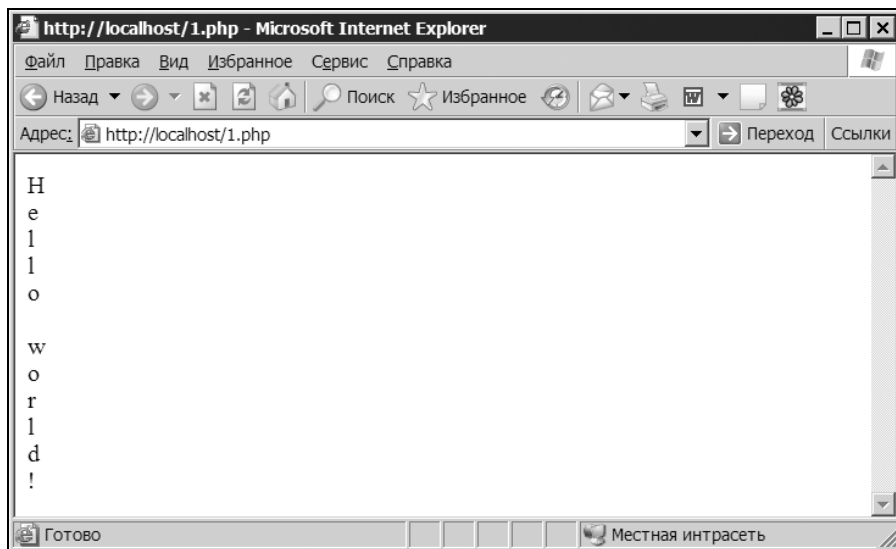


Рис. I.1.7. Вертикальный вывод строки

I.1.12. Число в денежном формате

Пусть имеется число 18439529234.5678, его необходимо представить в денежном формате, т. е. чтобы после запятой осталось только два знака, а триады были бы разделены пробелом — 18 439 529 234.57.

I.1.13. Замена символов bbCode

Замените в тексте "Очень [b]жирный[/b], жирный [b]текст" символы bbCode [b] и [/b] на их HTML-эквиваленты и , не прибегая к регулярным выражениям. То есть для решения задачи должны быть использованы только строковые функции.

Глава 1.2

```
## Sample if1.cfg file
## Define preprocess
/DMY_PROJECT prepr
## Set extended leng
/41132
## Set extended
## Set maximum float
/Opс80
##
## Additional direct
## files, before the
```

Регулярные выражения

Регулярные выражения являются мини-языком. Сложную задачу можно решить двумя способами: либо создав сложное решение, используя простые технологии, либо создав простое решение, используя сложную технологию. Точно так же и с регулярными выражениями — изучить их достаточно сложно, но, поняв их один раз, далее в одну строку можно решать задачи, для решения которых при помощи строковых функций может понадобиться сотня строк. В *главе 1* было сказано, что плотность ошибок тем меньше, чем короче программа — регулярные выражения позволяют создавать не просто короткие программы, а очень короткие. Данная глава содержит задачи на различные регулярные выражения.

Замечание

Все примеры из данной главы можно найти в каталоге `scripts\2` компакт-диска, поставляемого вместе с книгой.

1.2.1. Удаление всех тегов из HTML-страницы

На компакт-диске найдите HTML-страницу `scripts\2\index.htm`. Прочитайте содержимое страницы и удалите все HTML-теги, оставив только полезный текст. Текст необходимо вывести в окно браузера (рис. 1.2.1).

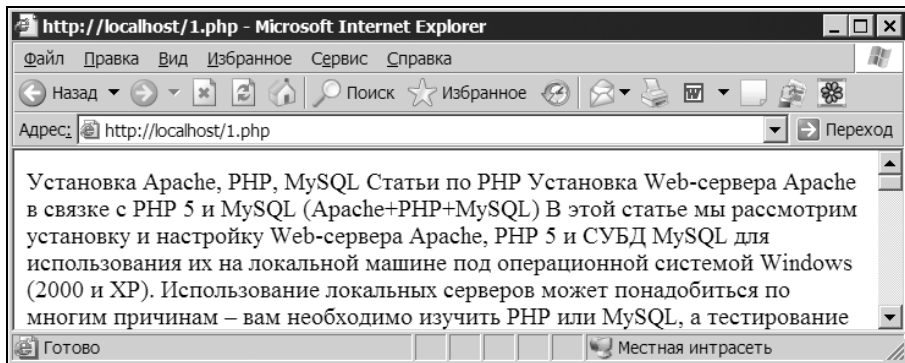


Рис. I.2.1. Чистый текст, извлеченный из HTML-страницы index.htm

I.2.2. Удаление изображений из HTML-страницы

На компакт-диске найдите HTML-страницу `scripts\2\index.htm`. Прочитайте содержимое страницы и удалите HTML-теги ``.

I.2.3. Извлечение названия HTML-страницы

На компакт-диске найдите HTML-страницу `scripts\2\index.htm`. Извлеките название страницы, которое помещается между тегами `<title>` и `</title>`.

I.2.4. Конвертация даты из MySQL-формата в календарный формат

Используя регулярные выражения, переконвертируйте дату из формата `2003-03-21` в формат `21.03.2003`.

I.2.5. Проверка корректности ввода адреса электронной почты

Разработайте HTML-форму, обработчик которой будет проверять корректность ввода адреса электронной почты (рис. I.2.2).

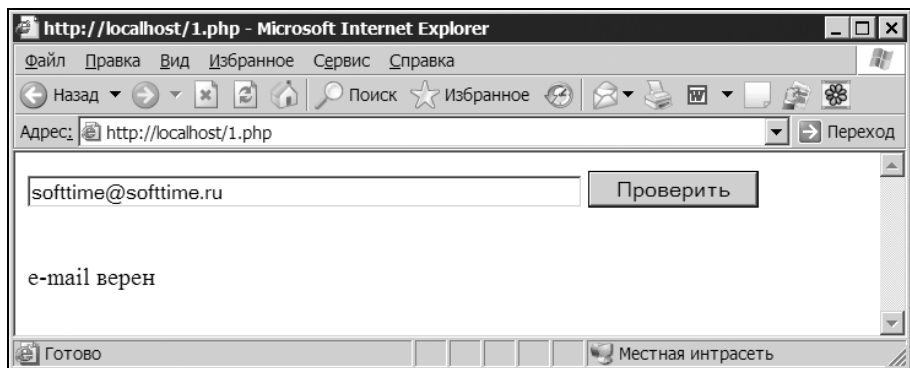


Рис. 1.2.2. HTML-форма проверки адреса электронной почты

1.2.6. Проверка корректности ввода URL

Разработайте HTML-форму, обработчик которой будет проверять корректность ввода адреса Web-сайта. Допускается ввод как с указанием протокола, например, <http://www.softtime.ru>, так и без него, например, www.softtime.ru. Следует учитывать, что адрес может содержать путь после доменного имени, а также параметры, например, http://www.softtime.ru/php5/index.php?id_article=43.

1.2.7. Подсветка URL

Часто возникает задача превращения текстовой ссылки в гиперссылку. На компакт-диске найдите текстовый файл `scripts\2\text.txt` и выведите его содержимое в окно браузера, преобразовав все URL в гиперссылки.

1.2.8. Проверка корректности ввода чисел

Создайте HTML-форму, состоящую из двух текстовых полей, в первом из которых вводится количество товарных позиций, а во втором их цена в формате `###.##`. Обработчик формы должен проверить, является ли введенная в первом поле информация целым числом, а во втором — удовлетворяющим денежному формату. Если все верно, необходимо вывести произведение этих двух чисел.

1.2.9. Изменение регистра

Пусть имеется фраза "ПРОГРАММИРОВАНИЕ — это ИСКУССТВО. Ему и ЖИЗНЬ посвятить не жалко". Создайте скрипт и регулярное выражение, которое заменит все слова в верхнем регистре на слова, начинающиеся с заглавной буквы: "Программирование — это Искусство. Ему и Жизнь посвятить не жалко".

1.2.10. Разбивка длинной строки

При построении различных Web-приложений, главным образом гостевых книг, форумов и чатов часто возникает необходимость защиты дизайна страниц от длинных последовательностей символов, которые могут исказить дизайн. Создайте функцию, разбивающую на части все слова, длина которых превышает 25 символов.

1.2.11. Разбивка HTML-страницы на предложения

На компакт-диске найдите HTML-страницу `scripts\2\index.htm`. Прочитайте содержимое страницы и поместите каждое предложение текста в элементы массива `$text` так, чтобы первое предложение оказалось в элементе с индексом 0 — `$text[0]`, второе в элементе с индексом 1 — `$text[1]` и т. д. После чего в цикле преобразуйте массив `$text` в двумерный массив таким образом, чтобы в элементе `$text[0][0]` хранилось первое слово первого предложения, в элементе `$text[0][1]` хранилось второе слово первого предложения и т. д. Проконтролируйте результаты работы, отправив дамп массива в окно браузера при помощи функции `print_r()`.

1.2.12. Количество слов в тексте

На компакт-диске найдите HTML-страницу `scripts\2\index.htm`. Прочитайте содержимое страницы и сосчитайте, сколько в нем содержится одно-, двух-, ..., десятибуквенных слов.

1.2.13. Интерпретация тегов bbCode

В Интернете большое распространение получили теги в квадратных скобках, именуемые так же, как теги в стиле phpBB (известного и широко распространенного форума). Удобство использования таких тегов заключается в том, что все теги HTML можно запретить, преобразуя их при помощи функции `htmlspecialchars()` в безопасную форму, и в то же время разрешить посетителям использовать их эквиваленты. Например, `[i]` вместо `<i>` и `[code]` вместо `<code>`. Теги в квадратных скобках можно заменить на теги в угловых скобках уже после преобразования текста при помощи функции `htmlspecialchars()`. Чаще всего прибегают к тегам `[url]`, которые имеют следующий синтаксис:

```
[url = ссылка] имя ссылки [/url]
```

При выводе на страницу этот шаблон следует преобразовать в

```
<a href=ссылка>имя ссылки</a>
```

Если используется форма тега

```
[url]ссылка[/url]
```

то на страницу выводится гиперссылка вида:

```
<a href=ссылка>ссылка</a>
```

На компакт-диске найдите HTML-страницу `scripts\2\bb.txt`, содержимое этой страницы представлено на рис. 1.2.3.

Необходимо преобразовать все имеющиеся на странице теги в их HTML-эквиваленты (рис. 1.2.4).

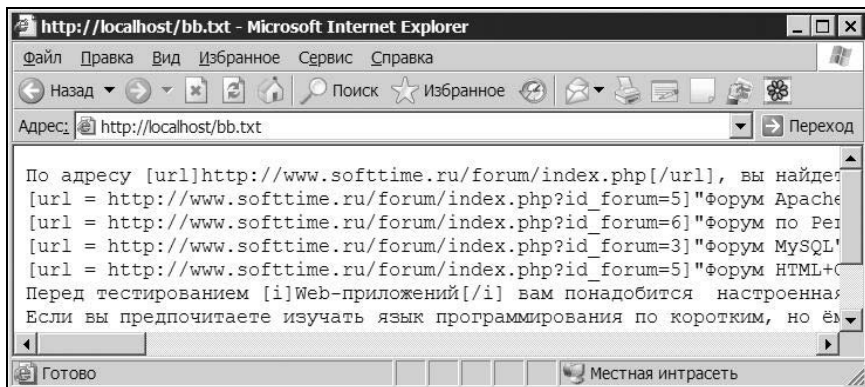


Рис. 1.2.3. Содержимое файла bb.txt

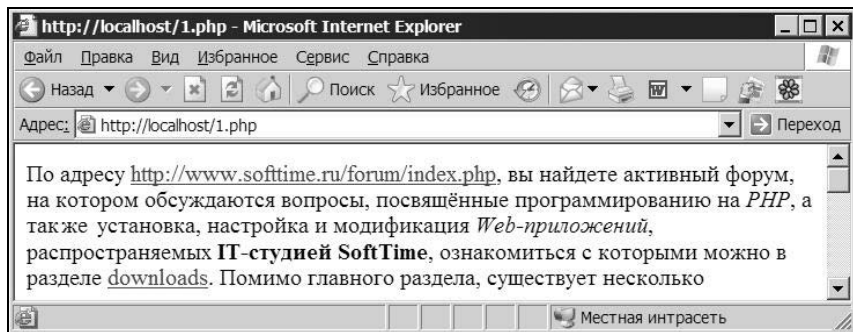


Рис. 1.2.4. Преобразованное содержимое файла bb.txt

1.2.14. Подсветка PHP-кода

В PHP есть две стандартные функции для подсветки кода: `highlight_string()` и `highlight_file()`. Данные функции имеют два серьезных недостатка: поддерживается только подсветка PHP-кода и только кода, размещенного между тегами `<?php` и `?>` (а также `<?>` и `?>`). Создайте собственную функцию подсветки синтаксиса, лишенную этого недостатка.

Глава 1.3

```
## Sample if1.cfg file
## Define preprocess
/DMY_PROJECT prepr
## Set extended leng
/41132
## Set extended
## Set maximum float
/0cc80
##
## Additional direct
## files, before the
```

Файлы

Работа с файлами является неотъемлемой частью Web-приложений — в них хранится как информация, так и код самих Web-приложений. Поэтому от эффективности использования файлов зависит и производительность Web-приложений, и их безопасность.

Замечание

Все примеры из данной главы можно найти в каталоге scripts\3 компакт-диска, поставляемого вместе с книгой.

1.3.1. Загрузка файлов на сервер

Создайте Web-приложение, позволяющее загружать на сервер произвольное количество файлов (рис. 1.3.1).

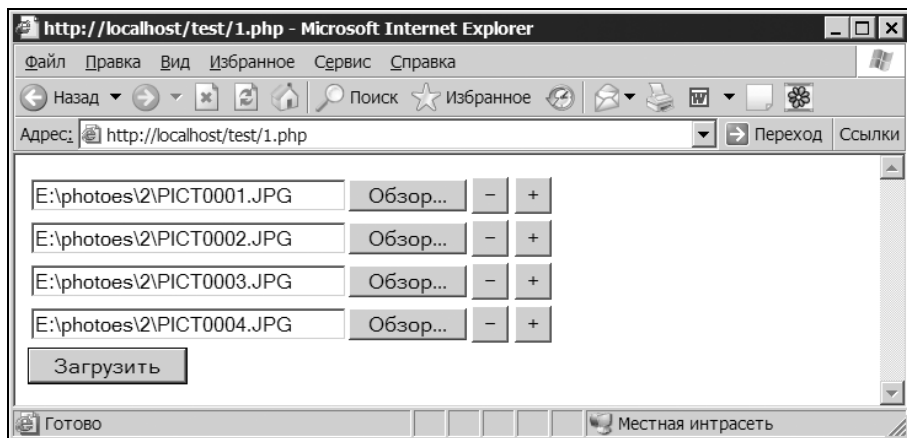


Рис. 1.3.1. HTML-форма для загрузки произвольного числа файлов на сервер

1.3.2. Редактирование файлов на удаленном сервере

Создайте Web-приложение, позволяющее открывать указанный файл на сервере. Содержимое файла должно передаваться в текстовую область. После редактирования файла должна быть возможность сохранить изменения (рис. 1.3.2).

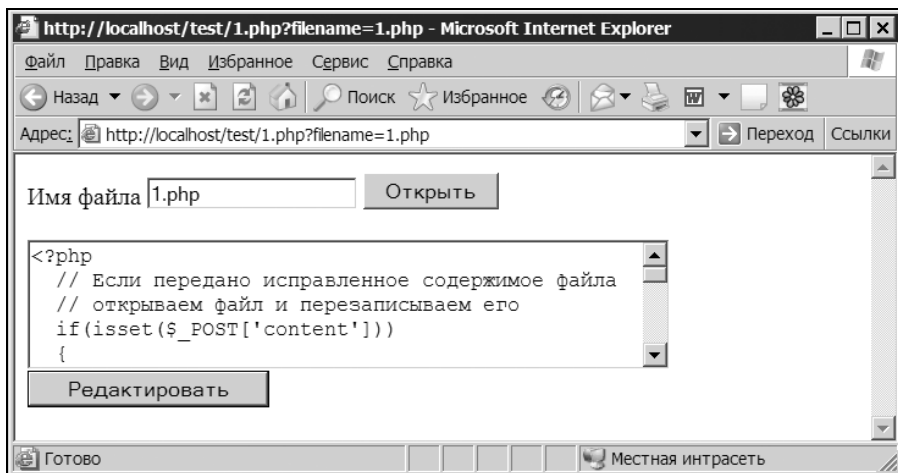


Рис. 1.3.2. Редактирование файлов на удаленном сервере

1.3.3. Уязвимость скрипта загрузки

В листинге 1.3.1 представлен скрипт загрузки (upload.php) — он содержит уязвимость. Используя эту уязвимость, уничтожьте файл upload.php. Разработайте скрипт загрузки файла на сервер, защищенный от этого вида уязвимости.

Замечание

Скрипт из листинга 1.3.1 можно найти на компакт-диске, поставляемом вместе с книгой (scripts\3\upload.php).

Листинг 1.3.1. Скрипт загрузки файла на сервер

```
<form enctype='multipart/form-data' method=post>
  <input type="file" size="32" name="filename"><br>
  <input class=button type=submit value='Загрузить'>
</form>
```

```
<?php
// Обработчик формы
if(!empty($_FILES['filename']['tmp_name']))
{
    // Сохраняем файл в текущем каталоге
    if(copy($_FILES['filename']['tmp_name'],
        $_FILES['filename']['name']))
    {
        echo "Файл успешно загружен - <a href=" .
            $_FILES['filename']['name'] . ">" .
            $_FILES['filename']['name'] . "</a>";
    }
}
?>
```

I.3.4. Счетчик загрузок

На сервере для свободной загрузки располагаются три файла `archive1.zip`, `archive2.zip` и `archive3.zip`. Необходимо создать скрипт, подсчитывающий количество загрузок файлов с сервера (рис. I.3.3).

Замечание

Файлы `archive1.zip`, `archive2.zip` и `archive3.zip` можно найти на компакт-диске, поставляемом вместе с книгой (scripts\3).

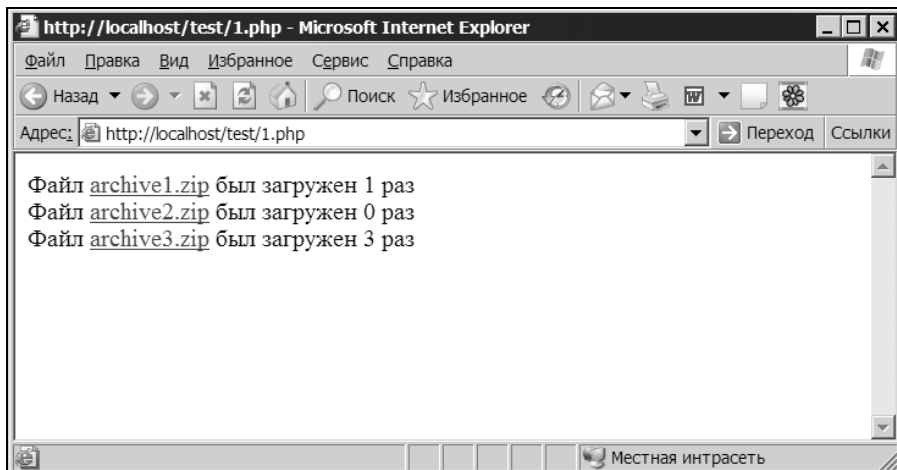


Рис. I.3.3. Счетчик загрузок файлов

1.3.5. Сохранение текстовых и графических файлов

Скрипт подсчета загрузок файлов решает еще одну проблему, связанную с безопасностью системы, — он скрывает от посетителя истинный путь к файлам. Их можно спрятать глубоко в системе, при этом посетитель будет всегда видеть только адрес страницы загрузки.

Тем не менее, если в качестве файла для загрузки указать текстовый файл, браузер не предоставит окна загрузки, а загрузит его, не только обнаружив путь к файлу, но и вынудив пользователя самостоятельно сохранять файл при помощи меню **Сохранить как**. Та же участь ожидает графические файлы и вообще любые файлы, которые браузер может отобразить. Создайте скрипт, позволяющий сохранять текстовые и графические файлы, предоставляя соответствующее окно для сохранения файлов (рис. 1.3.4).

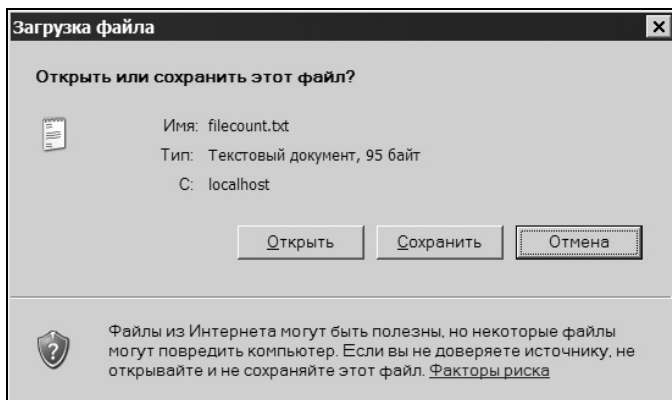


Рис. 1.3.4. Диалоговое окно для загрузки файла

1.3.6. Определение размера файла

Разработайте функцию, которая принимает в качестве единственного аргумента имя файла и возвращает его размер в байтах, килобайтах или мегабайтах. Если размер файла меньше 1024 байт — функция возвращает размер в байтах, если размер меньше 1024 Кбайт — объем файла оценивается в Кбайтах, если превышен порог в 1024 Кбайт — оценка идет в Мбайтах.

1.3.7. Определение количества строк в файле

Разработайте функцию, которая принимает в качестве единственного аргумента имя файла и возвращает количество строк в нем.