Безопасность веб-приложений на Python

Криптография, TLS и устойчивость к атакам

Деннис Бирн

MANNING

ДМК

Оглавление

1 О защите в деталях ... 19

Часть I ОСНОВЫ КРИПТОГРАФИИ ... 32

2 Хеширование ... 33
3 Хеш-функции с ключом ... 48
4 Симметричное шифрование ... 60
5 Асимметричное шифрование ... 74
6 Transport Layer Security ... 87

Часть II ПРОВЕРКА ЛИЧНОСТИ И ПРЕДОСТАВЛЕНИЕ ПРАВ ... 110

7 Сеанс HTTP ... 111
8 Проверка личности ... 128
9 Пользовательские пароли ... 147
10 Авторизация ... 172
11 OAuth 2 ... 190

Часть III ПРОТИВОСТОЯНИЕ АТАКАМ ... 214

12 Работа с операционной системой ... 215
13 Никогда не доверяйте вводу ... 227
14 Атаки методом межсайтового скриптинга ... 247
15 Политики защиты содержимого ... 268
16 Подделка межсайтовых запросов ... 285
17 Совместное использование ресурсов между разными источниками ... 299
18 Кликджекинг ... 314

Содержание

Оглавление ... 5
Предисловие ... 12
Об авторе ... 17
Об иллюстрации на обложке ... 18

1 ***О защите в деталях*** ... 19
1.1 Пространство для атаки ... 20
1.2 Глубокая оборона ... 22
1.2.1 Стандарты обеспечения защиты ... 23
1.2.2 Проверенные приемы ... 24
1.2.3 Основные принципы безопасности ... 25
1.3 Инструменты ... 27
1.3.1 Меньше слов, больше дела ... 30
Итоги ... 31

Часть I ОСНОВЫ КРИПТОГРАФИИ ... 32

2 ***Хеширование*** ... 33
2.1 Что такое хеш-функция? ... 33
2.1.1 Свойства криптографических хеш-функций ... 36
2.2 Архетипичные персонажи ... 38
2.3 Целостность данных ... 39
2.4 Выбор криптографической хеш-функции ... 40
2.4.1 Безопасные хеш-функции ... 40
2.4.2 Небезопасные хеш-функции ... 41
2.5 Криптографическое хеширование в Python ... 43
2.6 Функции контрольного суммирования ... 45
Итоги ... 47

3 ***Хеш-функции с ключом*** ... 48
3.1 Подлинность данных ... 48
3.1.1 Генерация ключа ... 49
3.1.2 Хеширование с ключом ... 52
3.2 HMAC-функции ... 54
3.2.1 Проверка подлинности данных между системами ... 55

3.3 Атака по времени ... 57
Итоги ... 59

4 *Симметричное шифрование* ... 60
4.1 Что такое шифрование? ... 60
4.1.1 Управление пакетами ... 62
4.2 Пакет cryptography ... 63
4.2.1 «Взрывчатые вещества» ... 63
4.2.2 «Готовые рецепты» ... 64
4.2.3 Смена ключа ... 66
4.3 Симметричное шифрование ... 67
4.3.1 Блочные шифры ... 67
4.3.2 Потоковые шифры ... 69
4.3.3 Режимы шифрования ... 70
Итоги ... 73

5 *Асимметричное шифрование* ... 74
5.1 Загвоздка с передачей ключей ... 74
5.2 Асимметричное шифрование ... 75
5.2.1 RSA ... 76
5.3 Неопровержимость деяния ... 80
5.3.1 Цифровые подписи ... 80
5.3.2 Подписание данных криптосистемой RSA ... 82
5.3.3 Проверка подписи, созданной криптосистемой RSA ... 82
5.3.4 Подписание данных на базе эллиптических кривых ... 84
Итоги ... 86

6 *Transport Layer Security* ... 87
6.1 SSL? TLS? HTTPS? ... 88
6.2 Атака «человек посередине» ... 88
6.3 Процедура подтверждения связи ... 90
6.3.1 Переговоры о наборе шифров ... 90
6.3.2 Обмен ключами ... 91
6.3.3 Проверка подлинности сервера ... 94
6.4 Общаемся по HTTP с Django ... 98
6.4.1 Параметр DEBUG ... 99
6.5 Общаемся по HTTPS с Gunicorn ... 101
6.5.1 Самозаверенные сертификаты ... 102
6.5.2 Заголовок ответа Strict-Transport-Security ... 103
6.5.3 Переадресация на HTTPS ... 104
6.6 Пакет requests и TLS ... 105
6.7 Соединение с БД через TLS ... 106
6.8 Электронная почта через TLS ... 107
6.8.1 Режим «только TLS» ... 108
6.8.2 Проверка подлинности почтового клиента ... 108
6.8.3 Данные для доступа к SMTP-серверу ... 109
Итоги ... 109

Часть II ПРОВЕРКА ЛИЧНОСТИ И ПРЕДОСТАВЛЕНИЕ ПРАВ 110

7 *Сеанс HTTP* 111
7.1 Что такое сеанс HTTP? 111
7.2 HTTP cookie 113
7.2.1 Атрибут Secure 114
7.2.2 Атрибут Domain 114
7.2.3 Атрибут Max-Age 115
7.2.4 Сеанс, пока запущен браузер 116
7.2.5 Установка cookie в программном коде 116
7.3 Параметры сеанса 117
7.3.1 Упаковщик сеанса 117
7.3.2 Механизм на основе кеша 119
7.3.3 Механизм на основе кеша и базы данных 121
7.3.4 Механизм на основе базы данных 121
7.3.5 Механизм на основе файлов 122
7.3.6 Механизм на основе cookie 122
Итоги 127

8 *Проверка личности* 128
8.1 Регистрация пользователя 129
8.1.1 Шаблоны 133
8.1.2 Боб заводит учетную запись 135
8.2 Проверка личности 137
8.2.1 Встроенные представления 137
8.2.2 Создание приложения Django 139
8.2.3 Боб входит и выходит 141
8.3 Просим представиться загодя 143
8.4 Тестируем проверку личности и скрытое за ней 144
Итоги 145

9 *Пользовательские пароли* 147
9.1 Сценарий смены пароля 148
9.1.1 Собственное средство проверки пароля 150
9.2 Хранение паролей 153
9.2.1 Засолка 156
9.2.2 Функции формирования ключа 158
9.3 Настройка хеширования паролей 162
9.3.1 Встроенные средства хеширования паролей 163
9.3.2 Собственное средство хеширования 164
9.3.3 Хеширование паролей через Argon2 164
9.3.4 Смена средства хеширования 165
9.4 Сценарий восстановления пароля 169
Итоги 171

10 *Авторизация* 172
10.1 Авторизация на уровне приложения 173
10.1.1 Разрешения 174
10.1.2 Администрирование пользователей и групп 176
10.2 Принудительная авторизация 181
10.2.1 Сложный низкоуровневый путь 181
10.2.2 Простой способ высокого уровня 184
10.2.3 Отображение по условию 186
10.2.4 Тестирование авторизации 187
10.3 Антишаблоны и проверенные приемы 188
Итоги 189

11 *OAuth 2* 190
11.1 Типы авторизации 192
11.1.1 Процесс предоставления кода авторизации 192
11.2 Боб авторизует Чарли 196
11.2.1 Запрос авторизации 196
12.2.2 Предоставление авторизации 197
11.2.3 Обмен токенами 198
11.2.4 Доступ к защищенным ресурсам 198
11.3 Django OAuth Toolkit 200
11.3.1 Обязанности сервера авторизации 201
11.3.2 Обязанности сервера ресурсов 205
11.4 requests-oauthlib 209
11.4.1 Обязанности клиента OAuth 210
Итоги 213

Часть III ПРОТИВОСТОЯНИЕ АТАКАМ 214

12 *Работа с операционной системой* 215
12.1 Авторизация на уровне файловой системы 215
12.1.1 Определение разрешений 216
12.1.2 Работа с временными файлами 217
12.1.3 Работа с разрешениями файловой системы 218
12.2 Запуск внешних выполняемых файлов 221
12.2.1 Решение задач с помощью внутренних API 222
12.2.2 Использование модуля subprocess 224
Итоги 226

13 *Никогда не доверяйте вводу* 227
13.1 Управление пакетами с помощью Pipenv 228
13.2 Удаленное выполнение кода YAML 230
13.3 Расширение сущностей XML 233
13.3.1 Атака квадратичного взрыва 234
13.3.2 Атака «миллиард насмешек» 234

13.4 Отказ в обслуживании 236
13.5 Атаки с использованием заголовка Host 237
13.6 Атаки с непроверенной переадресацией 240
13.7 Внедрение SQL 243
13.7.1 Обычные SQL-запросы 244
13.7.2 Запросы на подключение к базе данных 245
Итоги 246

14 *Атаки методом межсайтового скриптинга* 247
14.1 Что такое XSS? 248
14.1.1 Хранимый XSS 248
14.1.2 Отраженный XSS 249
14.1.3 XSS на основе DOM 250
14.2 Проверка ввода 252
14.2.1 Проверка формы Django 255
14.3 Экранирование вывода 258
14.3.1 Встроенные утилиты отображения 260
14.3.2 Заключение атрибутов HTML в кавычки 262
14.4 Заголовки HTTP-ответа 263
14.4.1 Отключение доступа к cookie из JavaScript 263
14.4.2 Отключение анализа типа MIME 265
14.4.3 Заголовок X-XSS-Protection 267
Итоги 267

15 *Политики защиты содержимого* 268
15.1 Конструирование политик защиты содержимого 270
15.1.1 Директивы извлечения 271
15.1.2 Директивы навигации и документов 276
15.2 Развертывание политики с помощью django-csp 276
15.3 Использование индивидуальных политик 278
15.4 Отчеты о нарушениях CSP 281
15.5 CSP Level 3 283
Итоги 284

16 *Подделка межсайтовых запросов* 285
16.1 Что такое подделка запроса? 285
16.2 Управление идентификатором сеанса 287
16.3 Соглашения об управлении состоянием 290
16.3.1 Проверка метода HTTP 291
16.4 Проверка заголовка Referer 292
16.4.1 Заголовок ответа Referrer-Policy 294
16.5 Токены CSRF 295
16.5.1 POST-запросы 295
16.5.2 Другие небезопасные методы запроса 297
Итоги 298

17 *Совместное использование ресурсов между разными источниками* 299
17.1 Политика одного источника 300
17.2 Простые запросы CORS 301
17.2.1 Асинхронные запросы между источниками 302
17.3 Реализация CORS с django-cors-headers 303
17.3.1 Настройка Access-Control-Allow-Origin 304
17.4 Предварительные запросы CORS 305
17.4.1 Отправка предварительного запроса 306
17.4.2 Отправка ответа на предварительный запрос 309
17.5 Отправка cookie между источниками 311
17.6 Устойчивость к CORS и CSRF 312
Итоги 313

18 *Кликджекинг* 314
18.1 Заголовок X-Frame-Options 317
18.1.1 Индивидуализация ответов 317
18.2 Заголовок Content-Security-Policy 318
18.2.1 X-Frame-Options и CSP 319
18.3 Идите в ногу с Мэллори 320
Итоги 321

Предметный указатель 322