Федеральное государственное автономное образовательное учреждение Высшего профессионального образования

Санкт-Петербургский политехнический университет

Институт компьютерных наук и технологий

Кафедра компьютерных систем и программных технологий

Лабораторная работа №6

Сервис тестирования корректности настройки SSL на сервере Qualys SSL Labs - SSL Server Test

Выполнил студент
группы 53501/3
_____
П. П. Жук
«____» _____ 2016 г.

Проверил преподаватель
_____
К. Д. Вылегжанина
«____» _____ 2016 г.

Санкт-Петербург
2016 г.

Содержание

1 Задание

1. Изучить
   (a) Изучить лучшие практики по развертыванию SSL/TLS.
   (b) Изучить основные уязвимости и атаки на SSL последнего времени - POODLE, HeartBleed.
2. Практическое задание:
   (a) Выбрать со стартовой страницы SSL Server Test один домен Recent Best и один домен Recent Worst - изучить отчеты, интерпритировать результаты в разделе Summary.
   (b) Выбрать домен для анализа, проделать шаги:
      i. интерпритировать результаты в разделе Summary
      ii. Расшифровать все аббревиатуры шифров в разделе Configuration
      iii. Прокомментировать большинство позиций в разделе Protocol Details
      iv. Сделать итоговый вывод о реализации SSL на заданном домене

2 Ход работы

2.1 Изучить

2.1.1 Изучить лучшие практики по развертыванию SSL/TLS

1. Приватный ключ и сертификат
   (a) Используйте 2048-битные закрытые ключи
   (b) Защитите закрытый ключ
      - Генерируйте закрытые ключи и запросы на сертификат (CSRs) на доверенном компьютере.
      - Для предотвращения компромментации ключей используйте защиту паролем
      - После компрометации отзывайте старые сертификаты и генерируйте новые ключи.
      - Обновляйте сертификаты каждый год с новыми закрытыми ключами.
   (c) Необходимо убедиться в достаточном покрытии используемых доменных имен
   (d) Приобретайте сертификаты в надежных центрах сертификации
   (e) Используйте надежные алгоритмы подписи сертификата
2. Конфигурация
   (a) Настраивайте корректные цепочки сертификатов (коглда одного сертификата недостаточно)

(b) Используйте безопасные протоколы.Например, TLS v1.0, v1.1 и v1.2

(c) Используйте безопасные алгоритмы шифрования (Например симметричные с ключами не менее 128 бит)

(d) Контроль за выбором алгоритма шифрования

(e) Поддержка Forward Secrecy - особенности протокола, позволяющей обмениваться данными вне зависимости от приватного ключа сервера.

(f) Отключите возможности проверки безопасности со стороны клиента

3. Дизайн приложений

(a) Сайт должен быть защищенным на 100

(b) Используйте HSTS (HTTP Strict Transport Security) — механизм, активирующий форсированное защищённое соединение через протокол HTTPS. Данная политика безопасности позволяет сразу же устанавливать безопасное соединение, вместо использования HTTP-протокола.

(c) Отключите кеширование для важного с точки срежния безопасности контента.

(d) Используйте защищенные куки

2.1.2 Изучить основные уязвимости и атаки на SSL последнего времени - POODLE, HeartBleed

POODLE - это уязвимость в SSLv3. Злоумышленник отправляет на сервер свои данные на протоколу SSL3 от измени цели, что позволяет ему расшифровывать по 1 байту за 256 запросов. Происходит это из-за того, что в SSLv3 не учитывается MAC адрес.

Для реализации атаки POODLE необходимо:

- Иметь возможность прослушивать и подменять трафик атакуемого
- Иметь возможность совершать запросы от имени атакуемого с известным атакующему текстом

HeartBleed - это уязвимость в безопасности криптографической библиотеки OpenSSL (это открытая реализация протокола шифрования SSL/TLS), позволяющая несанкционированно читать память на сервере, в которой в этот момент могут содержаться раздичного рода приватные данные.
Уязвимость позволяет взломщику получить доступ к 64 килобайтам оперативной памяти сервера и осуществлять атаку вновь и вновь вплоть до полной потери данных. Heartbleed можно реализовать отправкой некорректно сформированного Heartbeat-запроса.

2.2 Практическое задание

2.2.1 Выбрать со стартовой страницы SSL Server Test один домен Recent Best и один домен Recent Worst - изучить отчеты, интерпритировать результаты в разделе Summary

Из Recent Best был выбран домен oldfashion.io. Сайт имеет оценку A. Отчет представлен на рисунке 1.

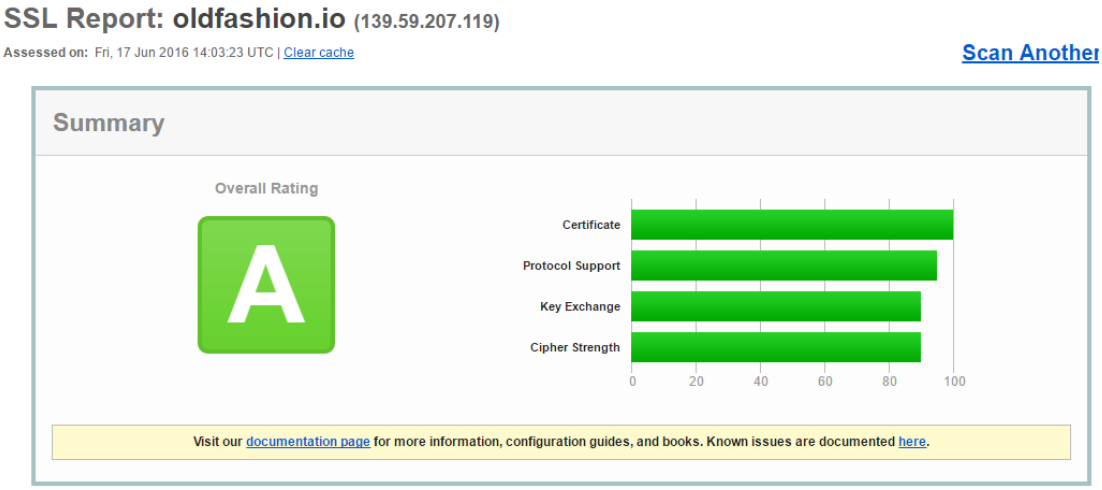

Рис. 1: Recent Best

Все характеристики не ниже 90. SSL/TLS настроен в соответсвии с лучшими практиками.

Из Recent Worst был выбран домен acs-inc.com. Сайт имеет оценку F. Отчет представлен на рисунке 2.

Дополнительно отмечается что сайт подвержен атаке типа DROWN. Это и является причиной присвоенного сайту рейтинга.

Атака DROWN - это атака, связанная с протоколом TLS, и осуществима в том случае, если осуществляется поддержка небезопасного протокола SSL2.

2.2.2 Выбрать домен для анализа. Проанализировать

Для самостоятельного анализа возьмем домен mail.ru.

Summary

Результаты анализа приведены на рисунке 3. Сайт имеет категорию A+ - максимально возможную оценку. Замечания отсутсвуют. Дополнительно отмечена поддержка HSTS.

Configuration

Расшифруем аббривиатуры из раздела Cobfiguration, представленные ниже.

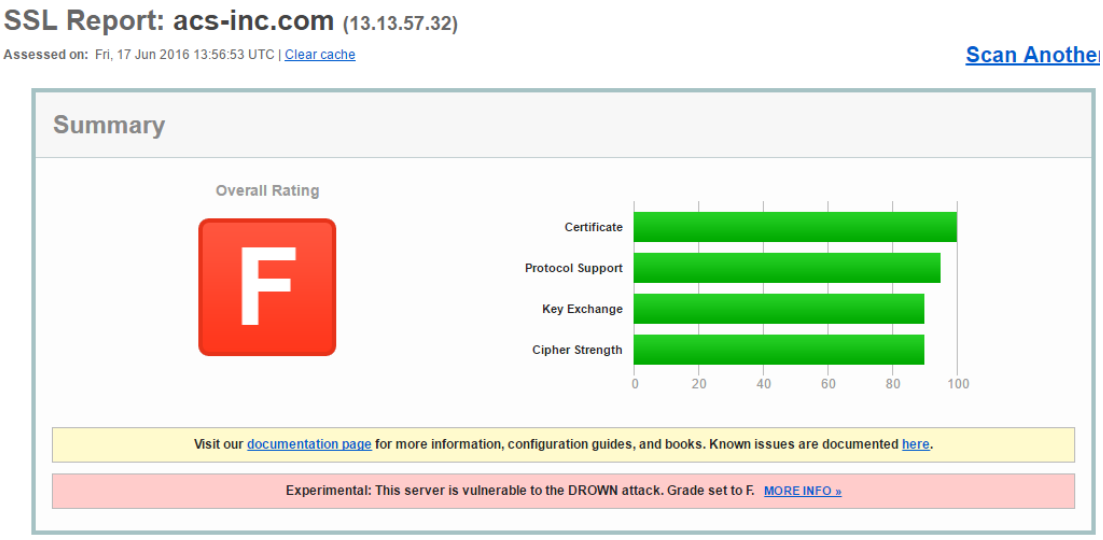

Рис. 2: Recent Worst

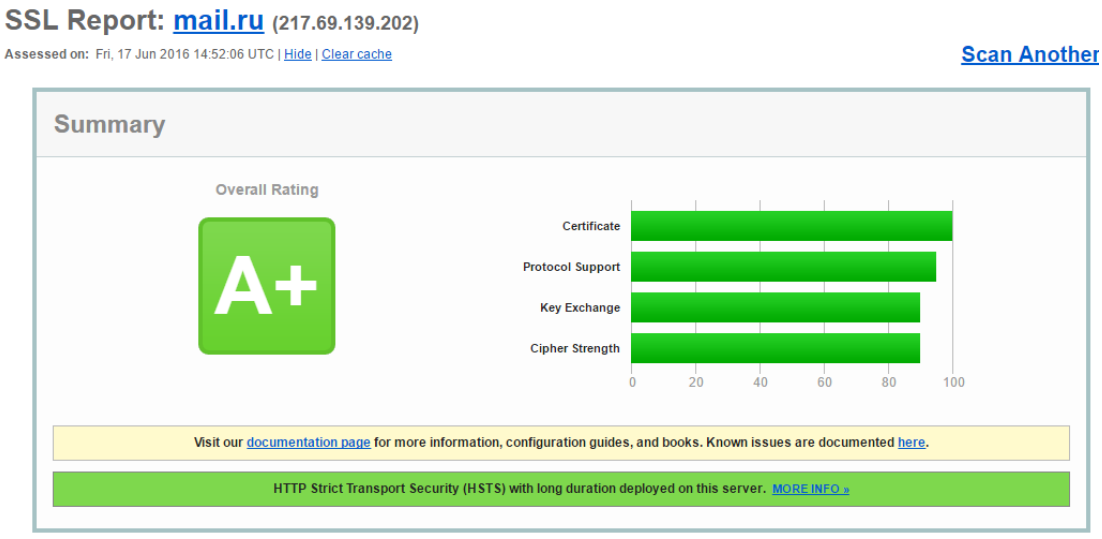

Рис. 3: Анализ mail.ru

```
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)   ECDH secp256r1 (eq. 3072 bits RSA)   FS
256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)   ECDH secp256r1 (eq. 3072 bits RSA)   FS
128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)   ECDH secp256r1 (eq. 3072 bits RSA)   FS
256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)   ECDH secp256r1 (eq. 3072 bits RSA)   FS
128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)   ECDH secp256r1 (eq. 3072 bits RSA)   FS
256
```

```
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)   ECDH secp256r1 (eq. 3072 bits RSA)   FS
128
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012)   ECDH secp256r1 (eq. 3072 bits RSA)   FS
112
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f)   DH 2048 bits   FS 256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b)   DH 2048 bits   FS 256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39)   DH 2048 bits   FS 256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88)   DH 2048 bits   FS 256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e)   DH 2048 bits   FS 128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67)   DH 2048 bits   FS 128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33)   DH 2048 bits   FS 128
TLS_DHE_RSA_WITH_SEED_CBC_SHA (0x9a)   DH 2048 bits   FS 128
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45)   DH 2048 bits   FS 128
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16)   DH 2048 bits   FS 112
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) 256
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) 256
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) 256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84) 256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) 128
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) 128
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) 128
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41) 128
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) 112
TLS_RSA_WITH_SEED_CBC_SHA (0x96) 128
```

Расшифровки:

- TLS - протокол защищенной передачи данных;
- ECDHE / ECDH / DH - алгоритм Диффи-Хэлмана на эллиптических кривых;
- RSA - алгоритм шифрования с открытым ключем;
- AES_128 - алгоритм шифрования с длиной ключа в 128 бит;
- GCM - режим блочного шифрования;
- SHA256 - хэш-функция с длиной ключа 256 бит;
- FS - forward secrecy;
- CBC - режим блочного шифрования;
- CAMELLIA - симметричный блочный шифр;
- 3DES - симметричный блочный шифр;
- SEED - симметричный блочный шифр;

Protocol Details

Прокомментируем данный раздел подробнее.

```
DROWN (experimental) No, server keys and hostname not seen elsewhere with SSLv2
BEAST attack Not mitigated server-side (more info)   TLS 1.0: 0xc014
POODLE (SSLv3) No, SSL 3 not supported (more info)
POODLE (TLS) No (more info)
Downgrade attack prevention Yes, TLS_FALLBACK_SCSV supported (more info)
```

Сайт не подвержен атакам DROWN, BEAST, POODLE (SSLv3), POODLE (TLS), Downgrade (понижение версии протоколов).

```
Secure Renegotiation Supported
```

Поддерживается защищенное переподключение.

```
Secure Client-Initiated Renegotiation No
Insecure Client-Initiated Renegotiation No
```

Любые виды переподключения по инициативе клиента запрещены.

```
SSL/TLS compression No
RC4 No
```

Потоковый шифр и сжатие отключены.

```
Heartbeat (extension) Yes
Heartbleed (vulnerability) No (more info)
```

Сайт защищен от heartbleed.

```
OpenSSL CCS vuln. (CVE-2014-0224) No (more info)
OpenSSL Padding Oracle vuln.
(CVE-2016-2107) No (more info)
```

Отсутсвуют данные уязвимости.

```
Forward Secrecy Yes (with most browsers)   ROBUST (more info)
```

Имеется поддержка Forward Secrecy для большинства собверменных браузеров.

```
ALPN Yes
NPN Yes   http/1.1
```

Поддерживается протокол ALPN (Application-Layer Protocol Negotiation) и его более ранняя версия NPN.

```
Strict Transport Security (HSTS) Yes
max-age=16070400
HSTS Preloading Not in: Chrome  Edge  Firefox  IE  Tor
```

Имеетмя поддержка HSTS.

```
Public Key Pinning (HPKP) No
Public Key Pinning Report-Only No
```

Технология привязки ключей не поддерживается.

Вывод
Домен mail.ru имеет наивысшую оценку (A+) по реализации SSL. Сайт защищен от всех тестируемых видов атак. Также поддерживаются: Forward Security для современных браузеров, ALPN, возможность возобновления сессии при помощи механизма кеширования и другое. Можно сделать вывод о хорошей защищенности данного сайта.

3 Вывод

В ходе данной лабораторной работы были изучены возможности сервиса SSL Labs, анализирующего качество защиты домена.

Были рассмотрены отчеты для сервисов с высокой и низкой оценками. Также был проанализирован домен mail.ru. Был просмотрен отчет по данному домену, и изучены детали: используемые способы шифрования, защита от уязвимстей и другое. В результате был сделан вывод, что сайт mail.ru является хорошо защищенным.