Лабораторная работа №6.
SSL/TLC

Кенть Никита

23 мая 2016 г.

Оглавление

1 Цель работы

Изучить лучшие практики по развертыванию SSL/TLS. Изучить основные уязвимости и атаки на SSL последнего времени - POODLE, HeartBleed.

2 Изучение практик по развертыванию SSL/TLC

- Качество защиты, обеспечиваемой TLS полностью зависит от секретного ключа, закладывающего основу безопасности, и сертификата, который сообщает о подлинности сервера для его посетителей.
- Необходимо защищать закрытые ключи, предоставляя доступ к ним как можно меньшему числу сотрудников.
- Используйте 2048-битный RSA или 256-битные ECDSA закрытые ключи для всех ваших серверов. Ключи такой крепости безопасны и будут оставаться безопасными в течение значительного периода времени. Если у вас есть 1024-битные RSA ключи, то следует заменить их более сильными ключами как можно скорее.
- Защитите закрытый ключ
- Убедитесь, что ваши сертификаты охватывают все доменные имена, которые вы хотите использовать на сайте.
- Приобретайте сертификаты у надежного удостоверяющего центра
- Использование безопасных алгоритмов шифрования (подойдут симметричные алгоритмы с ключами более 128 бит).
- Используйте надежные алгоритмы подписи сертификата

  Безопасность сертификата зависит от длины закрытого ключа и прочности используемой функции хеширования. Сегодня большинство сертификатов используют алгоритм SHA1, который считается слабым.
- Отключение проверки безопасности по инициативе клиента.

3 Уязвимости POODLE и HeartBleed

- POODLE - тим атаки «человек по середине». Атака POODLE (Padding Oracle On Downgraded Legacy Encryption) позволяет восстановить содержимое отдельных секретных идентификаторов, передаваемых внутри зашифрованного SSLv3-соединения, и по своей сути напоминает такие ранее известные виды атак на HTTPS, как BREACH, CRIME и BEAST, но значительно проще для эксплуатации и не требует выполнения каких-то особых условий. Проблеме подвержен любой сайт, допускающий установку защищённых соединений с использованием протокола SSLv3, даже если в качестве более приоритетного протокола указаны актуальные версии TLS. Для отката на SSLv3 атакующие могут воспользоваться особенностью современных браузеров переходить на более низкую версию протокола, в случае сбоя установки соединения.
- Heartbleed (CVE-2014-0160) - ошибка (переполнение буфера) в криптографическом программном обеспечении OpenSSL, позволяющая несанкционированно читать память на сервере или на клиенте, в том числе для извлечения закрытого ключа сервера. Heartbleed осуществляется отправкой некорректно сформированного Heartbeat-запроса, в котором реальный размер строки очень мал, а число, символизирующее длину передаваемой строки, очень велико. Так можно получить в ответ от сервера больше всего скрытой информации. Таким образом, у жертвы возможно за один запрос узнать до 64 килобайт памяти, которая была ранее использована OpenSSL.

4 Изучение отчетов ресурса SSL Server Test

4.1 Домен из раздела Recent Best

В качестве домена из раздела Recent Best был выбран домен eu-survey.zoho.com. Отчет представлен на рисунке ??.

- Поддерживает все типы протоколов TLS;
- Поддерживает форсированное защищённое соединение через протокол HTTPS.

В качестве домена из раздела Recent Worst был выбран домен eu-static.zoho.com Отчет представлен на рисунке 2.

- Не доверенный сертификат

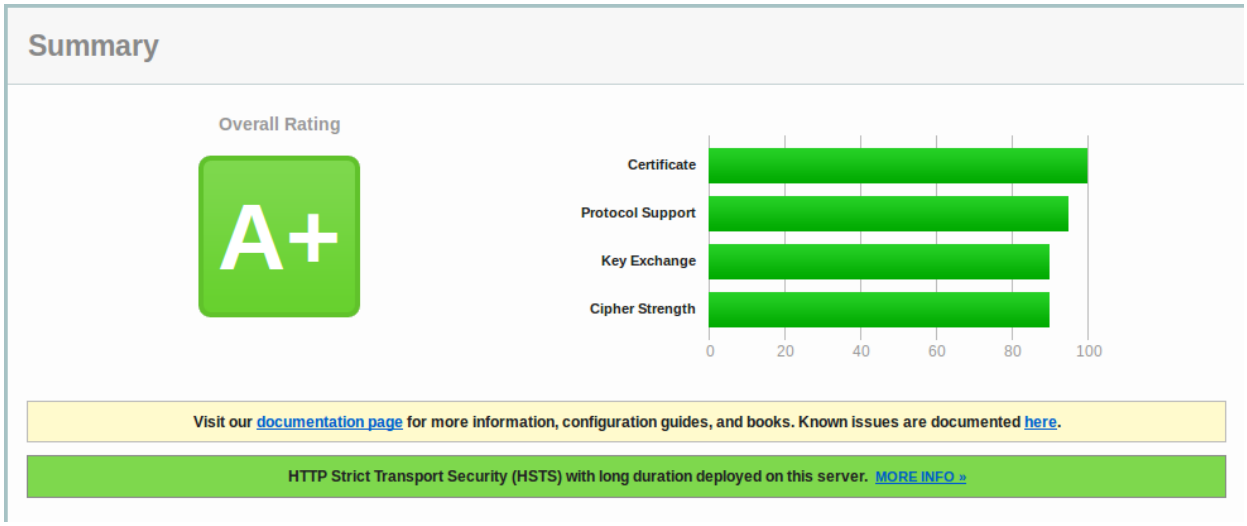

Рис. 1: Отчет для сайта eu-survey.zoho.com

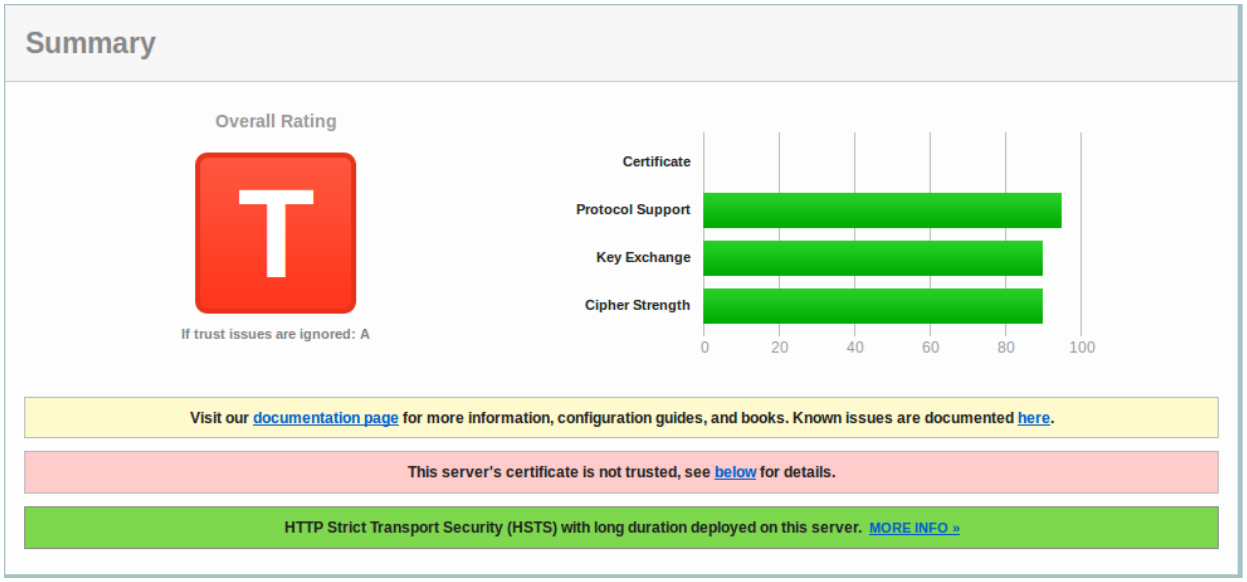

Рис. 2: Отчет для сайта eu-static.zoho.com

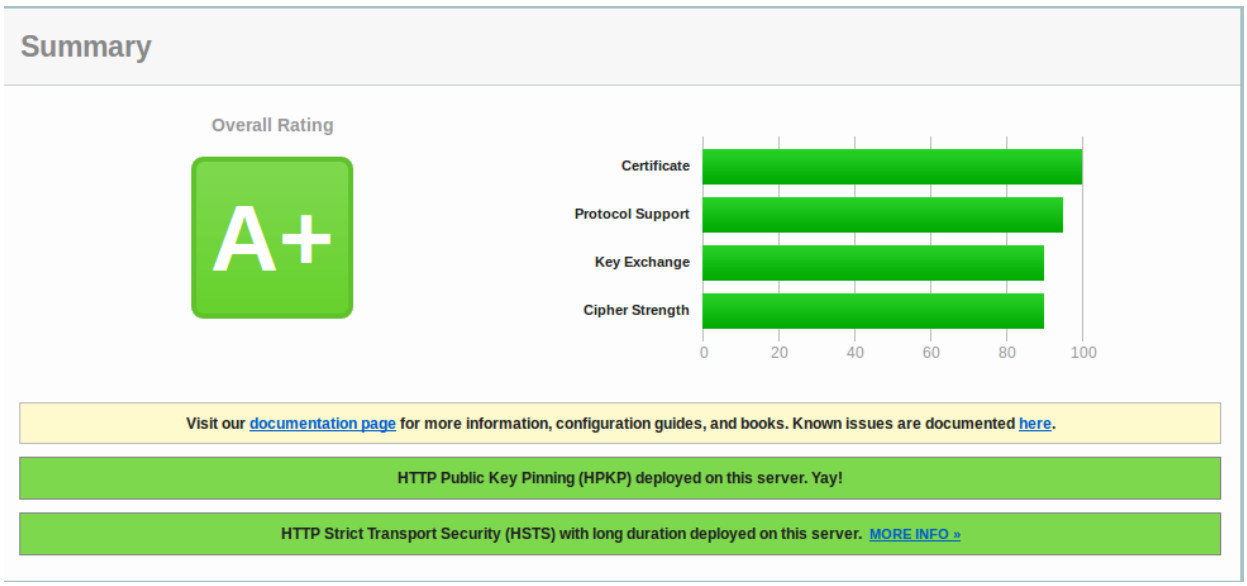

Рис. 3: Отчет для сайта github.com

- Поддерживает форсированное защищённое соединение через протокол HTTPS.

Для самостоятельного анализа был выбран сервер github.com. Результаты анализа приведены на рисунке 3

Как видно из рисунка 3, github.com поддерживает технологию HTTP Public Key Pinning, которая делает целевые атаки, связанные с Центрами Сертификации, намного более рискованными. Также поддерживает форсированное защищённое соединение через протокол

4.2 Расшифровка аббревиатур

Аббревиатуры представлены ниже:

```
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)   ECDH secp256r1 (eq. 3072 bits RSA)   FS
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)   ECDH secp256r1 (eq. 3072 bits RSA)   FS
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)   ECDH secp256r1 (eq. 3072 bits RSA)   FS
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)   ECDH secp256r1 (eq. 3072 bits RSA)   FS   128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)   ECDH secp256r1 (eq. 3072 bits RSA)   FS
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)   ECDH secp256r1 (eq. 3072 bits RSA)   FS   256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)  128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)  256
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)  128
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)     128
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)  256
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)
```

Расшифровка аббревиатур:

- TLS_ECDHE - алгоритм Диффи-Хэлмана на эллиптических кривых;
- RSA - алгоритм шифрования с открытым ключем;
- AES_128 - алгоритм шифрования с длиной ключа в 128 бит;
- GCM и CBC - режимы блочного шифрования;
- SHA256 - хэш-функция с длиной ключа 256 бит.

4.3 Protocol Details

Содержимое раздела Protocol Details представлено ниже:

- Проверка сертификата:

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

- Уязвимость к атакам Poodle, Bcast, Downgrade

```
BEAST attack:    Not mitigated server-side (more info)   TLS 1.0: 0xc013
POODLE (SSLv3): No, SSL 3 not supported (more info)
POODLE (TLS)     :       No (more info)
Downgrade attack prevention      Yes, TLS_FALLBACK_SCSV supported (more info)
```

- Слабый алгоритм RC4 не используется

```
RC4      No
```

- Сервер защищен от атак HeartBleed

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

- Совместимость Forward Security с браузерами

```
Forward Secrecy          With modern browsers
```

- Наличие NPN (отсутствует).

```
NPN                  No
```

- Параметры сессии.

```
Session resumption (caching)     Yes
Session resumption (tickets)     No
```

- Реализация HSTS.

```
Strict Transport Security (HSTS)          Yes
max-age=31536000;
HSTS Preloading          Chrome  Edge  Firefox  IE  Tor
```

- Реализация HPKP (отсутствует).

```
Public Key Pinning (HPKP)          Yes
```

- Совместимость с SSL2 (совместим).

```
SSL 2 handshake compatibility    Yes
```

4.4 Вывод о реализации SSL на выбранном домене

Сервис github.com имеет хорошую конфигурацию: сервер использует доверенный сертификат и защищен от основных типов атак.

Сервис имеет поддержку Forward Security для большинства браузеров. Исходя из этого, можно сделать вывод о том, что сервис хорошо защищен.

5 Выводы

В данной работе мы изучили возможности, которые предоставляет сервис «SSLLabs», анализирующий качество защиты домена. Изучили отчеты, предоставляемые сервисом, а так же проанализировали защиту сервиса github.com. Сервис позволяет увидеть защищенность домена от различных атак, список используемых протоколов, совместимость с различными браузерами и др.