Отчет по лабораторной работе 7: "Сервис тестирования корректности настройки SSL на сервере Qualys SSL Labs – SSL Server Test" по дисциплине "Методы и средства защиты информации"

Певцов Игорь, гр.53501/3

7 июня 2015 г.

Содержание

1 Цель работы

Изучить сервис тестирования корректности настройки SSL на сервере Qualys SSL Labs и его основные возможности.

2 Ход работы

2.1 Изучение

2.1.1 Лучшие практики по развертыванию SSL

- Использовать 2048-битные закрытые ключи. Использовать 2048-битный RSA или 256-битные ECDSA закрытые ключи для всех серверов. Ключи такой крепости безопасны и будут оставаться безопасными в течение значительного периода времени.
- Защитить закрытый ключ. Предоставить доступ к ключу как можно меньшей группе сотрудников.
- Обеспечить охват всех используемых доменных имен. Убедиться, что сертификаты охватывают все доменные имена, которые используются на сайте.
- Приобретать сертификаты у надежного CA.
- Использовать 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.
- Использовать безопасные протоколы. (TLS v1.0/v1.1/v1.2)
- Использовать безопасные алгоритмы шифрования. В данном случае подойдут симметричные алгоритмы с ключами более 128 бит.
- Контролировать выбор алгоритма шифрования. В SSL версии 3 и более поздних версиях протокола, клиенты отправляют список алгоритмов шифрования, которые они поддерживают, и сервер выбирает один из них для организации безопасного канала связи. Не все сервера могут делать это хорошо, так как некоторые выбирают первый поддерживаемый алгоритм из списка.
- Использование Forward Secrecy. Forward Secrecy — это особенность протокола, который обеспечивает безопасный обмен данными, он не зависит от закрытого ключа сервера. С алгоритмами шифрования, которые не поддерживают Forward Secrecy, возможно расшифровать ранее зашифрованные разговоры с помощью закрытого ключа сервера.
- Отключить проверку защищенности по инициативе клиента.

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

POODLE

Атака POODLE(Padding Oracle On Downgraded Legacy Encryption) работает по следующему сценарию: Взломщик отправляет свои данные на вервер по протоколу SSL3 от имени взламываемой структуры, что позволяет ему постепенно расшифровывать данные из запросов. Это возможно, так как в SSL3 нету привязки к MAC адресу.

Heartbleed

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. Информация об уязвимости была опубликована в апреле 2014 года, ошибка существовала с конца 2011 года.

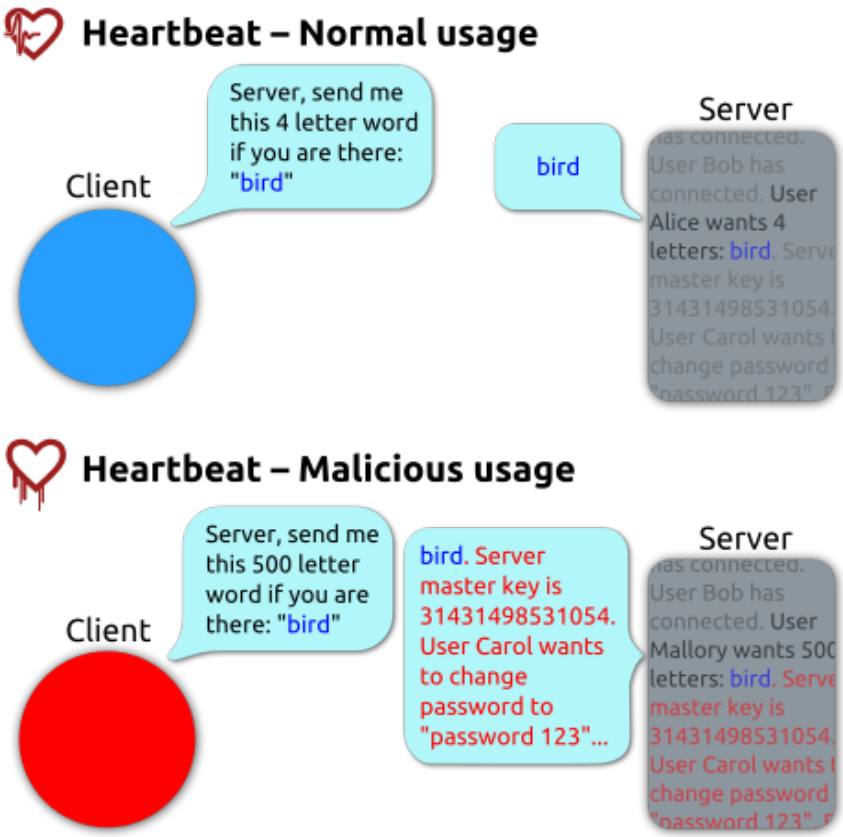


Рис. 1: Принцип работы heartbleed.

2.2 Выбрать со стартовой страницы SSL Server Test один домен из списка Recent Best и один домен из списка Recent Worst, интерпретировать результаты в разделе Summary

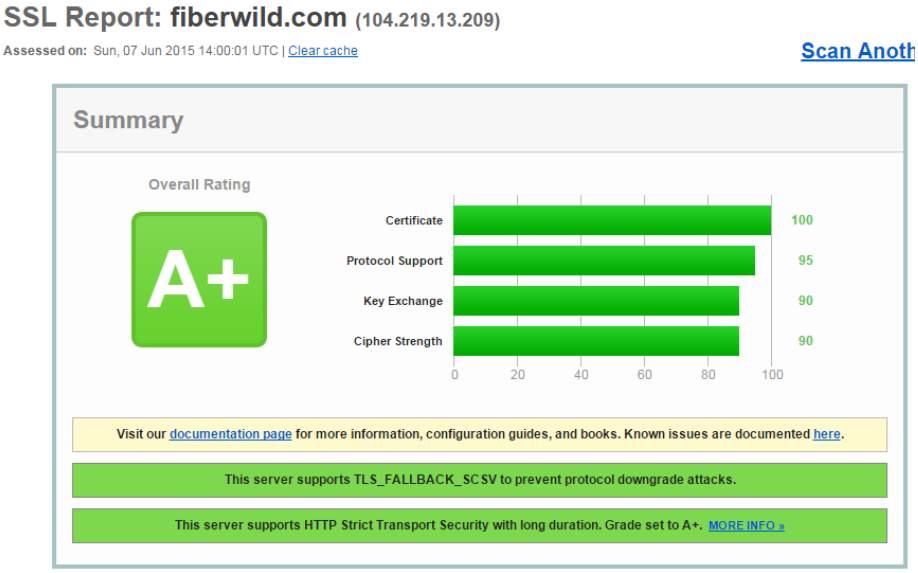


Рис. 2: Раздел Summary для Recent Best.

Recent Best

- Поддерживаются все версии протокола TLS.
- Поддерживается заголовок HTTP Strict Transport Security на протяжении длительного времени.
- Защита от downgrade-атак.

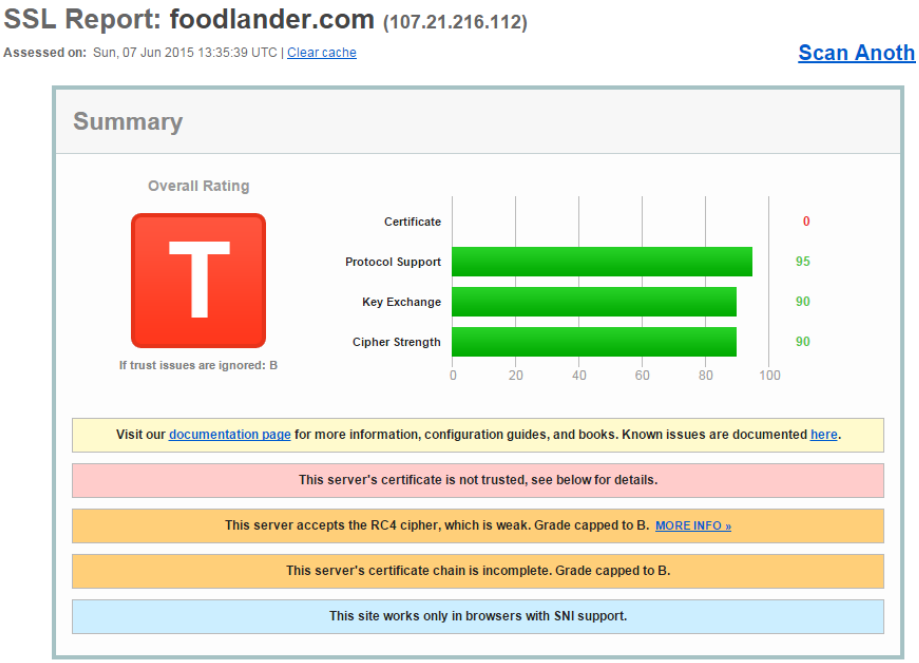


Рис. 3: Раздел Summary для Recent Worst.

Recent Worst

- Сертификат не подписан.
- Сервер позволяет использовать слабый шифр RC4.
- Цепочка сертификации сервера неполная.
- Сайт работает только в браузерах, которые поддерживают SNI(Server Name Indication) - расширение к протоколу TLS

2.3 Выбор интернет-домена, защищенного SSL-шифрованием.

В качестве испытуемого был выбран домен fwallet.tk, над которым мы работали в курсе ТРПО. На домене развернут стандартный набор LAMP, а также используется бесплатный SSL сертификат от WoSign.

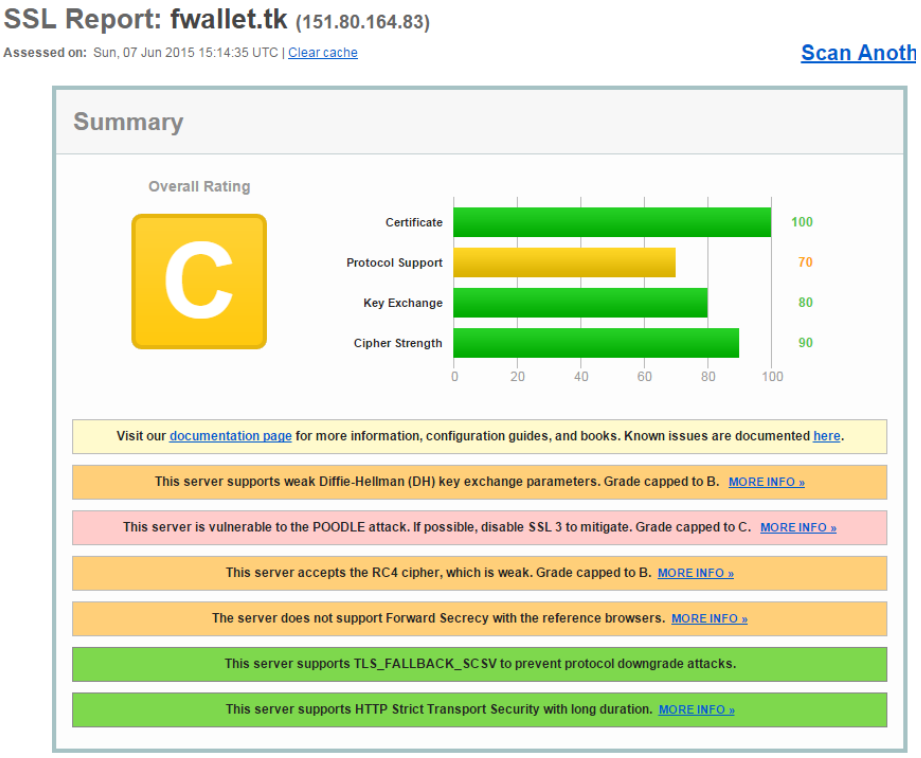


Рис. 4: Раздел Summary для Recent Worst.

Summary

- (-) Сервер подерживает слабую версию алгоритма Диффи-Хеллмана обмена ключами.
- (-) Сервер уязвим к атакам POODLE.
- (-) Сервер позволяет использовать слабый шифр RC4.
- (-) Сервер не поддерживает Forward Secrecy
- (+) Защита от downgrade-атак.
- (+) Поддерживается заголовок HTTP Strict Transport Security на протяжении длительного времени.

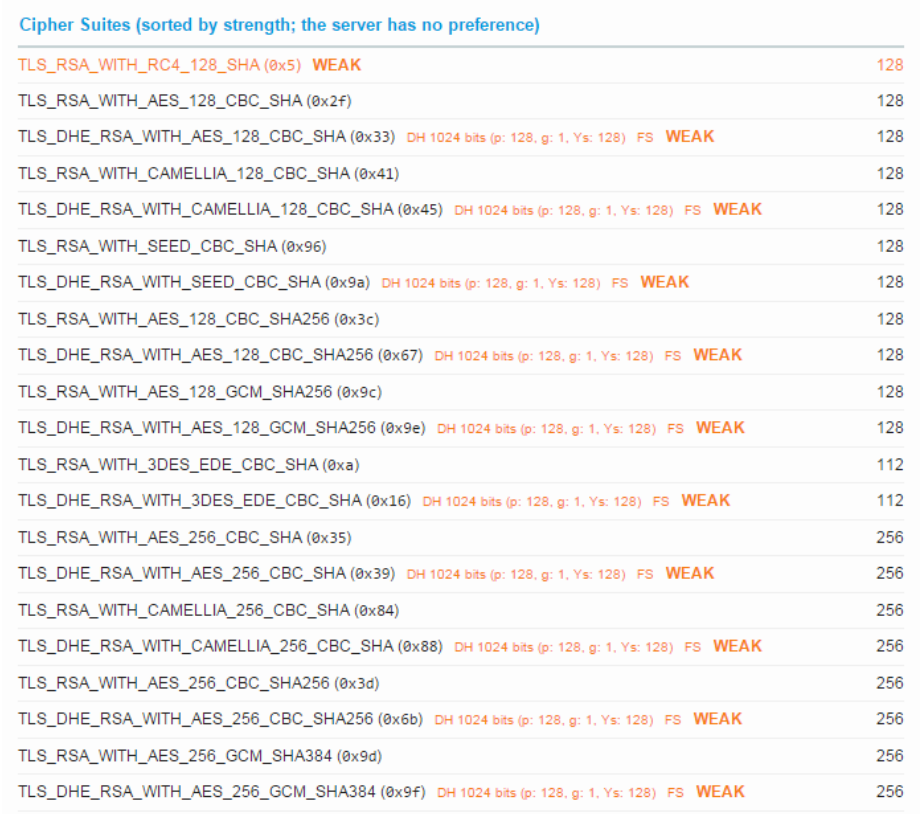
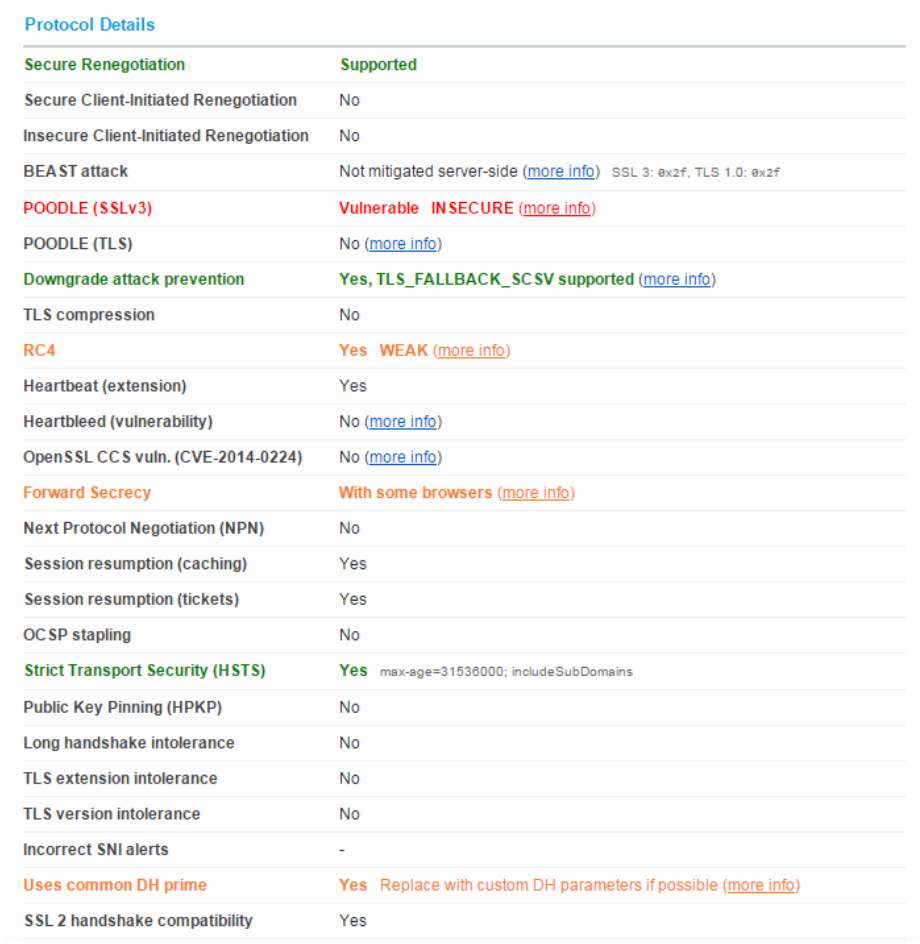


Рис. 5: Раздел Summary для Recent Worst.

Configuration

- Все шифры, испльзующие DHE(Diffie-Hellman Exchange) помечены как WEAK(слабые).
- RSA - Rivest, Shamir, Adleman - криптографический алгоритм
- RC4 - Rivest Cipher 4 - потоковый шифр 4-й версии
- SHA/SHA256/384 - Secure Hash Algorithm - Алгоритм хэширования. Цифра - длина ключа
- AES - Advanced Encryption Standard - симметричный алгоритм блочного шифрования
- GCM и CBC это два режима блочного шифрования
- TLS - Transport Layer Security - криптографический протокол
- 3DES - Digital Encryption Standard - алгоритм блочного шифрования
- EDE - Encrypt, Decrypt, Encrypt - режим работы алгоритма 3DES
- Camellia - симметричный алгоритм блочного шифрования



Protocol Details

Secure Renegotiation	Supported
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side (more info) SSL 3: 0x2f, TLS 1.0: 0x2f
POODLE (SSLv3)	Vulnerable INSECURE (more info)
POODLE (TLS)	No (more info)
Downgrade attack prevention	Yes, TLS_FALLBACK_SCSV supported (more info)
TLS compression	No
RC4	Yes WEAK (more info)
Heartbeat (extension)	Yes
Heartbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
Forward Secrecy	With some browsers (more info)
Next Protocol Negotiation (NPN)	No
Session resumption (caching)	Yes
Session resumption (tickets)	Yes
OCSP stapling	No
Strict Transport Security (HSTS)	Yes max-age=31536000; includeSubDomains
Public Key Pinning (HPKP)	No
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	No
Incorrect SNI alerts	-
Uses common DH prime	Yes Replace with custom DH parameters if possible (more info)
SSL 2 handshake compatibility	Yes

Рис. 6: Раздел Summary для Recent Worst.

Protocol details

- Строки 1-3 - перепроверка сертификата и защищенность этого процесса, все в порядке.
- Строки 4-7 - Проверка уязвимости к атакам BEAST, POODLE, downgrade. Система уязвима к POODLE SSLv3
- Строки 8 - сжатие TLS не используется
- Строка 9 - Используется слабый шифр RC4
- Строки 10-12 - уязвимости OpenSSL Heartbleed, etc.
- Строка 13 - совместимость Forward Secrecy с новыми браузерами.
- Строки 15-16 - Поддерживает возобновление сессии с помощью частичного хэндшейка

- Строка 18 - Поддерживает заголовки HSTS
- Строка 19 - Не поддерживает заголовок HPKP - ассоциацию сервера с ключом
- Строка 24 - Используются стандартные параметры для алгоритма Диффи-Хеллмана.
- Строка 25 - Совместим с SSL 2 handshake

2.4 Сделать итоговый вывод о реализации SSL на заданном домене

Подводя итог, можно сказать, что сервер защищен достаточно слабо, поскольку имеется критическая уязвимость к POODLE, а также используется слабый шифр RC4, что может привести к расшифровке трафика. С сертификатом проблем не обнаружено, значит в подлинности сервера сомневаться не приходится. Сервер поддерживает восстановление TLS-сессии при помощи неполного хэндшейка, что существенно сокращает потребление процессорного времени и ускоряет работу. Forward Secrecy поддерживается только для новых браузеров, что впринципе не является проблемой.

3 Выводы

В результате выполнения данной лабораторной работы были изучены возможности веб-сервиса Qualys SSL LABS. Сервис позволяет получить развернутую статистику по SSL для запрашиваемого домена. Анализируя данные, полученные таким способом, можно значительно улучшить стабильность и безопасность сервера, закрыв все явные уязвимости.