

Сервер тестирования корректности настройки SSL на сервере Qualys SSL Labs – SSL Server Test

Абрамов Антон

26 мая 2015 г.

Содержание

1	Цель работы	2
2	Ход работы	2
2.1	Recent Bes	2
2.1.1	Summary	2
2.1.2	Configuration	3
2.1.3	Protocol Details	5
2.1.4	Вывод по Recent Bes	5
2.2	Recent Worst	6
2.2.1	Вывод по Recent Worst	7
2.3	Что-то достаточно известное	8

1 Цель работы

2 Ход работы

Были изучены лучшие практики по развертыванию SSL/TLS, а также основные уязвимости и атаки на SSL последнего времени - POODLE, HeartBleed.

2.1 Recent Bes

Перейдем на сайт <https://www.ssllabs.com/ssltest/>.

Посмотрим недавно проверяемые сайты с хорошей защитой (Recent Bes). Один из таких сайтов **marketviewliquor.com (208.77.48.29)**.

2.1.1 Summary

Первое что мы увидим – это резюме, показывающее ранг безопасности сайта (от A до F). Кроме этого можно встретить ранг T и M. Также может использоваться знак коэффициента(+/-), уточняющий ранг безопасности.

В резюме отображается информация в процентном соотношении по следующим параметрам:

- Certificate (Сертификат);
- Protocol Support (Поддержка протокола);
- Key Exchange(Обмен ключами);
- Cipher Strength (Стойкость шифра).

Из этих параметров и выставляется окончательная оценка безопасности сайта. Ниже идет подробная оценка каждого пункта. Также, в резюме мы можем увидеть примечания к безопасности. В данном случае нам сообщают об использовании слабого промежуточного сертификата и поддержке TLS_FALLBACK_SCSV. (Рис. 1).

Из данного резюме можно сделать вывод, что сайт защищен достаточно хорошо, но не идеально. При этом он дотягивает до уровня A.

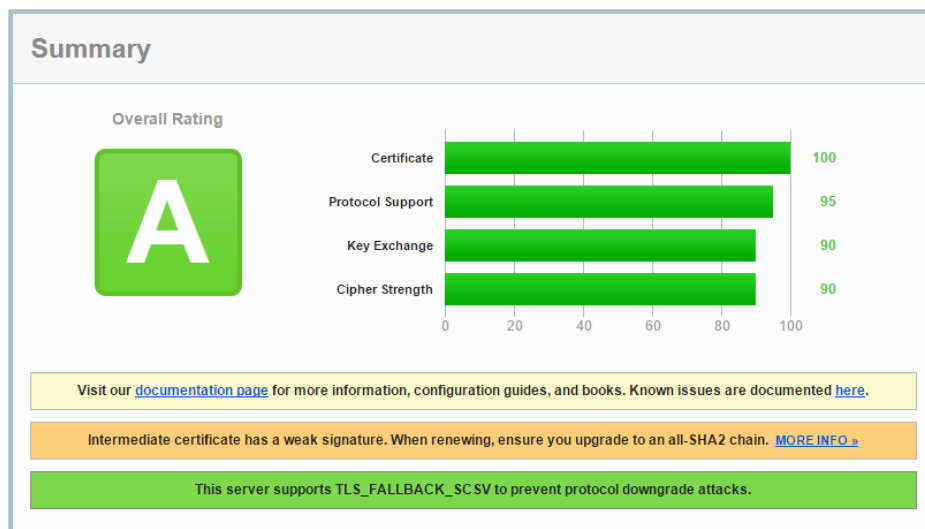


Рис. 1: Резюме Recent Bes

2.1.2 Configuration

Посмотрим, что находится ниже резюме. Первое что мы это пункт **Authentication** с идентификационными данными ресурса, за ним идет пункт **Configuration**. Рассмотрим его поподробней.

Используются следующие протоколы:

- TLS 1.2
- TLS 1.1
- TLS 1.0

При этом протоколы **SSL 3** и **SSL 2** не поддерживаются, что очень хорошо, так как эти протоколы являются устаревшими.

TLS (Transport Layer Security), как и его предшественник **SSL** (Secure Sockets Layer) — криптографические протоколы, обеспечивающие защищённую передачу данных между узлами в сети Интернет. **TLS** и **SSL** используют асимметричную криптографию для аутентификации, симметричное шифрование для конфиденциальности и коды аутентичности сообщений для сохранения целостности сообщений.

Данный протокол широко используется в приложениях, работающих с сетью Интернет, таких как веб-браузеры, работа с электронной почтой, обмен мгновенными сообщениями.

ECDHE (Elliptic Curve Diffie–Hellman Exchange) - расшифровывается как «эфемерный алгоритм Диффи-Хеллмана с использованием эл-

липтических кривых». После сеанса связи ключи уничтожаются, и даже владелец сервера не сможет расшифровать сессию, которую его сервер зашифровал прошлым ключом.

DHE (Diffie–Hellman Exchange) - Протокол Диффи-Хеллмана - криптографический протокол, позволяющий двум и более сторонам получить общий секретный ключ, используя незащищенный от прослушивания канал связи. Полученный ключ используется для шифрования дальнейшего обмена с помощью алгоритмов симметричного шифрования.

RAS (аббревиатура от фамилий Rivest, Shamir и Adleman) — криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших целых чисел.

AES (Advanced Encryption Standard) - симметричный алгоритм блочного шифрования (размер блока 128 бит, ключ 128/192/256 бит), принятый в качестве стандарта шифрования правительством США по результатам конкурса AES.

SHA (Secure Hash Algorithm) - безопасный алгоритм хеширования. Бывает версий 1, 2 и 3. SHA-2 - семейство криптографических алгоритмов — однонаправленных хеш-функций, включающее в себя алгоритмы SHA-224, SHA-256, SHA-384 и SHA-512.

3DES (Triple DES) — симметричный блочный шифр, созданный Уитфилдом Диффи, Мартином Хеллманом и Уолтом Тачманном в 1978 году на основе алгоритма DES, с целью устранения главного недостатка последнего — малой длины ключа (56 бит), который может быть взломан методом полного перебора ключа.

Camellia — алгоритм симметричного блочного шифрования (размер блока 128 бит, ключ 128, 192, 256 бит), один из финалистов европейского конкурса NESSIE (наряду с AES и Shacal-2), разработка японских компаний Nippon Telegraph and Telephone Corporation и Mitsubishi Electric Corporation

CBC (Cipher Block Chaining) - Режим сцепления блоков шифротекста — один из режимов шифрования для симметричного блочного шифра с использованием механизма обратной связи. Каждый блок открытого текста (кроме первого) побитово складывается по модулю 2 (операция XOR) с предыдущим результатом шифрования.

GCM (Galois/Counter Mode) - Режим обеспечивает аутентификацию и конфиденциальность передаваемых данных. Может быть распараллелен. Может работать только в режиме аутентификации данных: GMAC. В основе используется CTR режим с аутентификацией Галуа (перемножение полей Галуа может быть легко вычислено параллельно). GCM используется в MACsec, Fibre Channel Security Protocol (FC-SP), IPsec, SSH, TLS.

2.1.3 Protocol Details

В разделе **Configuration** находится подраздел **Protocol Details**. Рассмотрим несколько позиций в этом разделе.

Secure Renegotiation - Supported

Возобновление подключения TLS поддерживается.

POODLE (SSLv3) - No SSL 3 not supported

Атака POODLE через SSL3 невозможна, так как SSL не поддерживается

POODLE (TLS) - No

Атака POODLE через TSL невозможна.

RC 4 - No

Алгоритм RC4 не поддерживается. Это хорошо, т.к. алгоритм очень уязвим из-за использования не случайных или связанных ключей, а также один ключевой поток использует дважды.

Heartbeat (extension) - Yes

Внесено расширение, решающее проблему Heartbeat (переполнения буфера).

Heartbleed (vulnerability) - No

Уязвимости Heartbeat, связанной с проблемой переполнения буфера не зафиксировано.

OpenSSL CCS vuln. (CVE-2014-0224) - No

Баг с номером в CVE — CVE-2014-0224 отсутствует. Это значит, что нет возможности выполнить MITM атаку.

Session resumption (caching) - Yes

Session resumption (tickets) - Yes

Реализована возможность возобновления сеансов как с помощью кэширования, так и при помощи тикетов.

OCSP stapling - No

OCSP stapling – это расширение TLS/SSL, целью которого является повышение производительности SSL-переговоров при сохранении конфиденциальности посетителя. И данное расширение тут не настроено.

2.1.4 Вывод по Recent Bes

Как и следовало ожидать, на данном домене SSL реализована на высоком уровне. Существует защита от множества уязвимостей. Используются безопасные протоколы. Однако используется слабый промежуточный сертификат.

2.2 Recent Worst

Посмотрим недавно проверяемые сайты с плохой защитой (Recent Worst). Один из таких сайтов mail.vscnet.com (98.173.8.124). В этом случае резюме, показывающее ранг безопасности сайта F (Рис. 2). Поддержка протоколов равен 0. Разберёмся, почему это произошло.

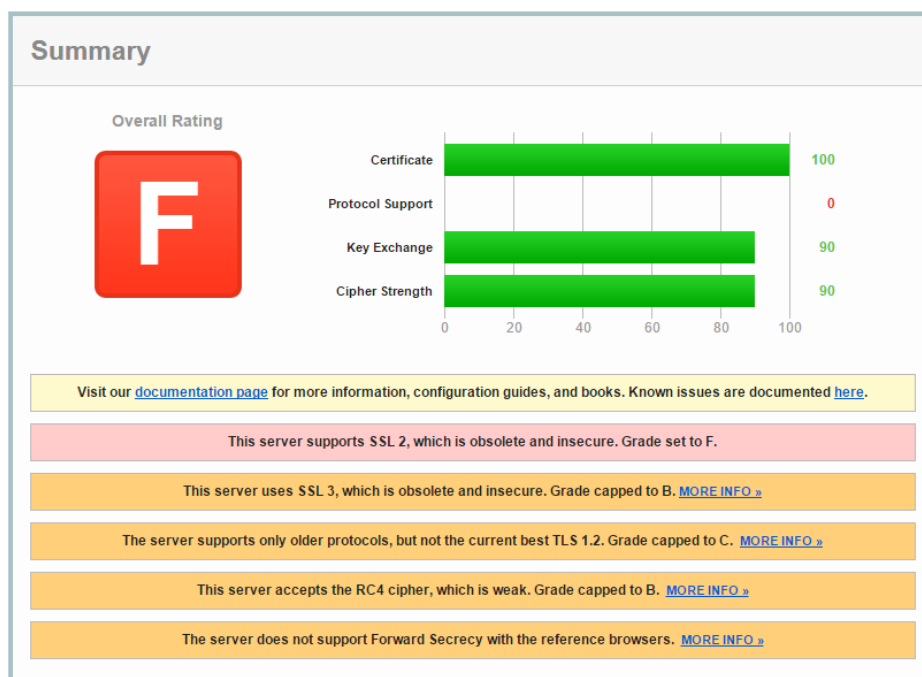


Рис. 2: Резюме Recent Worst

Первое сообщение которое расположено в резюме: **This server supports SSL 2, which is obsolete and insecure. Grade set to F.** Говорит о поддержке протокола SSL2, что и стало причиной понижения рейтинга до F. Далее идет сообщение **This server uses SSL 3, which is obsolete and insecure. Grade capped to B.** Оно говорит о поддержке протокола SSL3, что послужило причиной понижения рейтинга до статуса B. Третье сообщение **The server supports only older protocols, but not the current best TLS 1.2. Grade capped to C.** Оно говорит о том, что сервер не поддерживает лучший на данный момент протокол TLS1.2, а поддерживает только старые протоколы. Оценка снижена до C. Если заглянуть в **Configuration**, то можно увидеть, что используются устаревшие протоколы SSL2 и SSL3, а протокол TLS 1.2 не поддерживается (Рис. 3).

Еще одной причиной снижения рейтинга сервера является то, что




Protocols	
TLS 1.2	No
TLS 1.1	No
TLS 1.0	Yes
SSL 3 INSECURE	Yes
SSL 2 INSECURE	Yes

Рис. 3: Список поддерживаемых сертификатов

сервер принимает шифр RC4, который является слабым. О RC4 написано выше.

Также стоит сказать о том, что сервер не поддерживает Forward Secrecy с браузеров (Рис. 4).



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: 0x5, TLS 1.0: 0x2f
POODLE (SSLv3)	No, mitigated (more info) SSL 3: 0x5
POODLE (TLS)	No (more info)
Downgrade attack prevention	No, TLS_FALLBACK_SCSV not supported (more info)
TLS compression	No
RC4	Yes WEAK (more info)
Heartbeat (extension)	No
Heartbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
Forward Secrecy	No WEAK (more info)

Рис. 4: Protocol Details

Все это послужило снижением рейтинга сервера до F, а показателя поддержки протоколов до 0.

2.2.1 Вывод по Recent Worst

Есть предположение, что данный сервер специально выключил поддержку последних протоколов и подвергся тестированию в экспериментальных целях. Если же это не так и данное состояние сервера является рабочим, то работа с таким сервером крайне небезопасна, а обмен данными с сервером уязвим.

2.3 Что-то достаточно известное

Из достаточно известных сайтов было решено выбрать один из серверов mail.ru, а именно **mail.ru (217.69.139.200)**. Стоит сразу сказать, что все сервера **mail.ru** имеют статус В, выбранный сервер не исключение. Посмотрим на резюме (Рис. 5).

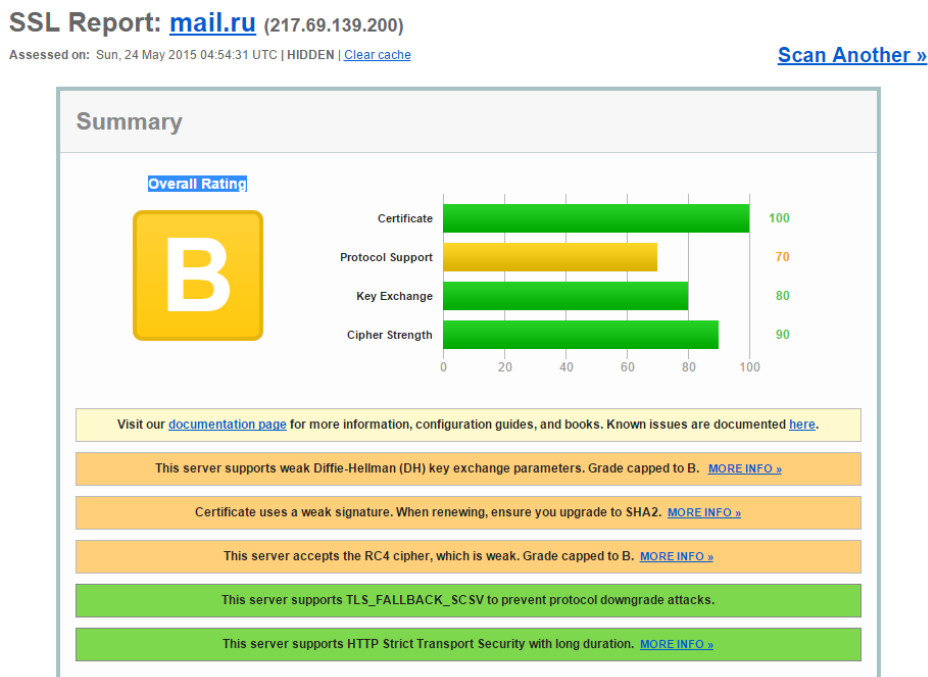


Рис. 5: Резюме mail.ru

Сразу стоит сказать, что немного страдает поддержка протоколов 70%, а также обмен ключами 80%.

Причин, по которой ранг сервера был снижен до В несколько. Одной из них является использование слабого алгоритма DH. Другой, тот факт, что сервер принимает шифр RC4, который является слабым.

Еще одним недостаток является использование слабых подписей.

Но есть и положительные стороны, отмеченные в резюме. Во-первых, этот сервер поддерживает TLS_FALLBACK_SCSV. Во-вторых, есть поддержка HTTP Strict Transport Security.

2.3.1 Вывод по mail.ru

В целом серверах mail.ru реализация SSL достаточно хорошая. Есть некоторые слабые места, но скорей всего они существуют для совместимости

и поддержке каких-либо технологий, необходимых для работы сервиса.