

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

Виктор БОРИСОВ

May 30, 2016

## Contents

<b>1</b>	<b>Цель работы</b>	<b>3</b>
<b>2</b>	<b>Ход работы</b>	<b>3</b>
2.1	Изучение . . . . .	3
2.1.1	Лучшие практики по развертыванию SSL . . . . .	3
2.1.2	Основные уязвимости и атаки на SSL последнего времени - POODLE, HeartBleed . . . . .	4
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 . . . . .	4
2.3	Выбор интернет-домена, защищенного SSL-шифрованием. . .	7
2.4	Сделать итоговый вывод о реализации SSL на заданном домене	9
<b>3</b>	<b>Выводы</b>	<b>10</b>

# 1 Цель работы

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

## 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. Относитесь к закрытым ключам как к важным активам, предоставляя доступ к как можно меньшей группе сотрудников.
- Обеспечить охват всех используемых доменных имен. Убедитесь, что ваши сертификаты охватывают все доменные имена, которые вы хотите использовать на сайте.
- Приобретать сертификаты у надежного удостоверяющего центра (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 сервер 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.

### 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

SSL Report: [www.instantmacsupport.nl](http://www.instantmacsupport.nl) (171.33.130.146)

Assessed on: Sun, 29 May 2016 18:53:47 UTC | [Clear cache](#)

[Scan Another »](#)

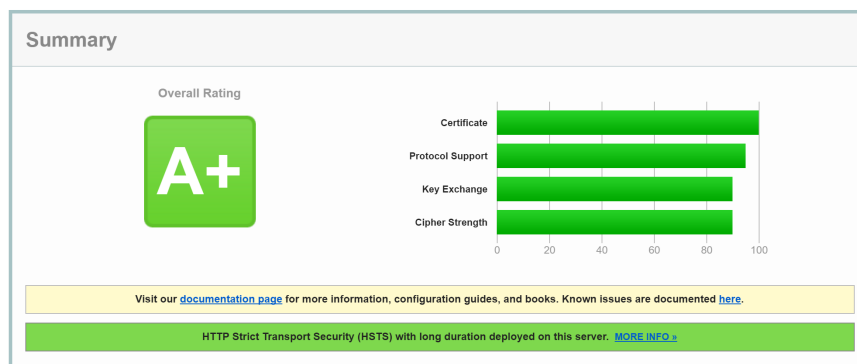


Figure 1: Summary для Recent Best.

#### Recent Best

- Поддержка всех версии протокола TLS.
- Поддержка заголовков HTTP Strict Transport Security на протяжении длительного времени.
- Поддержка forward secrecy. Свойство некоторых протоколов согласования ключа (Key-agreement), которое гарантирует, что сессионные ключи, полученные при помощи набора ключей долговременного пользования,

не будут скомпрометированы при компрометации одного из долговременных ключей

- Защита от downgrade-атак.

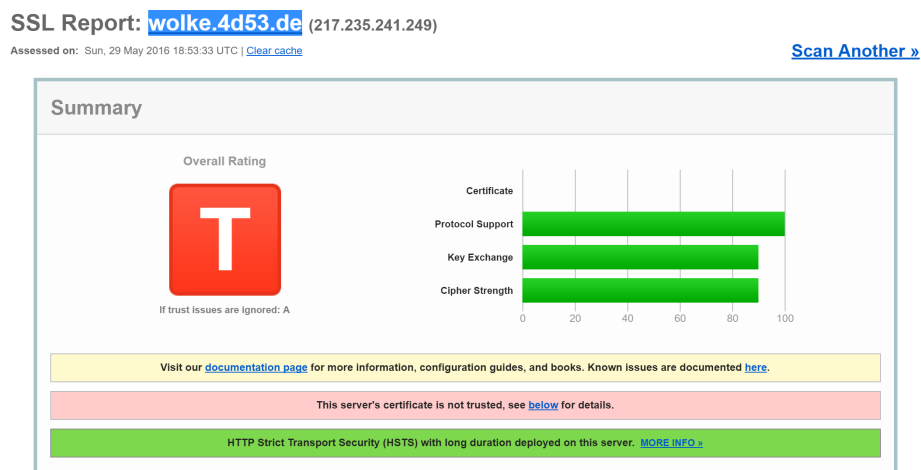


Figure 2: Summary для Recent Worst.

### Recent Worst

- Срок действия сертификата истек.
- Поддержка заголовков HTTP Strict Transport Security на протяжении длительного времени.
- Поддержка TLS только версии 1.2
- Поддержка forward secrecy.

Видимо низкая оценка данному хосту потсавлена лишь из-за просроченного сертификата.

## 2.3 Выбор интернет-домена, защищенного SSL-шифрованием.

Для анализа защищенности SSL шифрованием был выбран домен [instagram.com](https://instagram.com).

SSL Report: [instagram.com](https://instagram.com) (52.4.41.248)

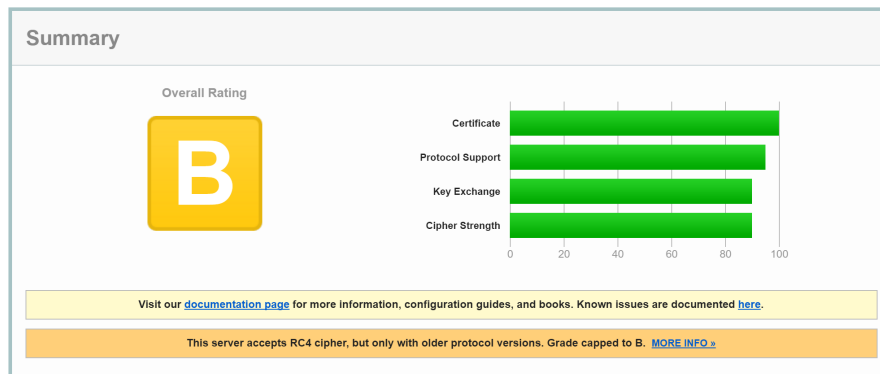


Figure 3: Summary для [instagram.com](https://instagram.com).

### Summary

- (-) Сервер позволяет использовать слабый шифр RC4.
- (+/-) Сервер поддерживает Forward Secrecy только с современными браузерами
- (+) Защита от downgrade-атак.
- (+) Поддерживается заголовок HTTP Strict Transport Security на протяжении длительного времени.

### Configuration

- Шифры, использующие RC4 отмечены как INSECURE.
- ECDH - Elliptic curve Diffie-Hellman - Протокол Диффи-Хеллмана на эллиптических кривых
- RSA - Rivest, Shamir, Adleman - криптографический алгоритм
- RC4 - Rivest Cipher 4 - потоковый шифр 4-й версии
- SHA/SHA256/384 - Secure Hash Algorithm - Алгоритм хеширования.  
Цифра - длина ключа
- AES - Advanced Encryption Standard - симметричный алгоритм блочного шифрования



Configuration			
 <b>Protocols</b>			
TLS 1.2			Yes
TLS 1.1			Yes
TLS 1.0			Yes
SSL 3			No
SSL 2			No
 <b>Cipher Suites (SSL 3+ suites in server-preferred order; deprecated and SSL 2 suites at the end)</b>			
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	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_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_SHA (0x2f)			128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)			256
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	112
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)			112
TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011)	ECDH secp256r1 (eq. 3072 bits RSA)	FS <b>INSECURE</b>	128
TLS_RSA_WITH_RC4_128_SHA (0x5)		<b>INSECURE</b>	128
TLS_RSA_WITH_RC4_128_MD5 (0x4)		<b>INSECURE</b>	128

Figure 4: Configuration для instagram.com.

- 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

#### Protocol details

- Secure Renegotiation - Возобновление подключения TLS
- Secure Client-Initiated Renegotiation, Insecure Client-Initiated Renegotiation - подверженность процесса проверки сертификата атаке.
- BEAST attack, POODLE (SSLv3), POODLE (TLS) - проверка уязвимости к данным атакам.
- Downgrade attack prevention - атака, при которой клиента принудительно заставляют использовать предыдущие (менее надежные) версии протоколов
- SSL/TLS compression - сжатие SSL/TLS не используется
- RC4 - Используется слабый шифр RC4
- Heartbeat (extension), Heartbleed (vulnerability), OpenSSL CCS vuln. (CVE-2014-0224) - уязвимости OpenSSL Heartbleed и тд.
- Forward Secrecy - совместимость Forward Secrecy с новыми браузерами.

Protocol Details	
DROWN (experimental)	No, server keys and hostname not seen elsewhere with SSLv2 (1) For a better understanding of this test, please read <a href="#">this longer explanation</a> (2) Key usage data kindly provided by the <a href="#">Censys</a> network search engine; original DROWN test <a href="#">here</a> (3) Censys data is only indicative of possible key and certificate reuse; possibly out-of-date and not complete
Secure Renegotiation	Supported
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side ( <a href="#">more info</a> ) TLS 1.0: 0xc013
POODLE (SSLv3)	No, SSL 3 not supported ( <a href="#">more info</a> )
POODLE (TLS)	No ( <a href="#">more info</a> )
Downgrade attack prevention	Yes, TLS_FALLBACK_SCSV supported ( <a href="#">more info</a> )
SSL/TLS compression	No
RC4	Yes INSECURE ( <a href="#">more info</a> )
Heartbeat (extension)	No
Heartbleed (vulnerability)	No ( <a href="#">more info</a> )
OpenSSL CCS vuln. (CVE-2014-0224)	No ( <a href="#">more info</a> )
Forward Secrecy	With modern browsers ( <a href="#">more info</a> )
ALPN	Yes
NPN	Yes h2 h2-fb http/1.1
Session resumption (caching)	No (IDs assigned but not accepted)
Session resumption (tickets)	Yes
OCSP stapling	No
Strict Transport Security (HSTS)	No
HSTS Preloading	Not in: Chrome Edge Firefox IE Tor
Public Key Pinning (HPKP)	No
Public Key Pinning Report-Only	No
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	No
Incorrect SNI alerts	No
Uses common DH primes	No, DHE suites not supported
DH public server param (Ys) reuse	No, DHE suites not supported
SSL 2 handshake compatibility	Yes

Figure 5: Protocol details для instagram.com.

- Strict Transport Security (HSTS) - форсированное переключение на HTTPS
- SSL 2 handshake compatibility - Совместимость с SSL 2 handshake

## 2.4 Сделать итоговый вывод о реализации SSL на заданном домене

Общую защищенность сервера можно оценить как удовлетворительную. Это только из-за поддержки устаревшего алгоритма шифрования RC4. Все остальные характеристики удовлетворяют лучшим практикам развертывания SSL.



### 3 Выводы

В результате выполнения работы были изучены лучшие практики по развертыванию SSL серверов, а так же средство для проверки SSL серверов Qualys SSL Server Test, которое позволяет подробно изучить любой домен. Полученные данные помогут получить действительную картину защищенности сервера и понять какие действия необходимо предпринять для улучшения стабильности и безопасности сервера.