

Лабораторная работа №7  
Курс: Защита информации

Патраков Николай

24 сентября 2015 г.

## Содержание

<b>1</b>	<b>Цель работы</b>	<b>3</b>
<b>2</b>	<b>Ход работы</b>	<b>3</b>
2.1	Изучение . . . . .	3
2.2	Практическое задание . . . . .	5
<b>3</b>	<b>Вывод</b>	<b>10</b>

# 1 Цель работы

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

## 2 Ход работы

### 2.1 Изучение

**Изучить лучшие практики по развертыванию SSL/TLS**

- Использовать 2048-битные закрытые ключи.

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.

- 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 CA центра.
- 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.

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

**POODLE** Атака POODLE работает по следующему сценарию: Взломщик отправляет свои данные на сервер по протоколу SSL3 от имени вменяемой структуры, что позволяет ему постепенно расшифровывать данные из запросов. Это возможно, так как в SSL3 нету привязки к MAC адресу.

**HeartBleed** Эта атака использует уязвимость уязвимость криптографии OpenSSL, позволяя несанкционированно читать память на сервере и на клиенте, в том числе и для извлечения закрытого ключа сервера

## 2.2 Практическое задание

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

**Recent Best** SSL Report: customer-recruit.zoho.com (74.201.154.103)

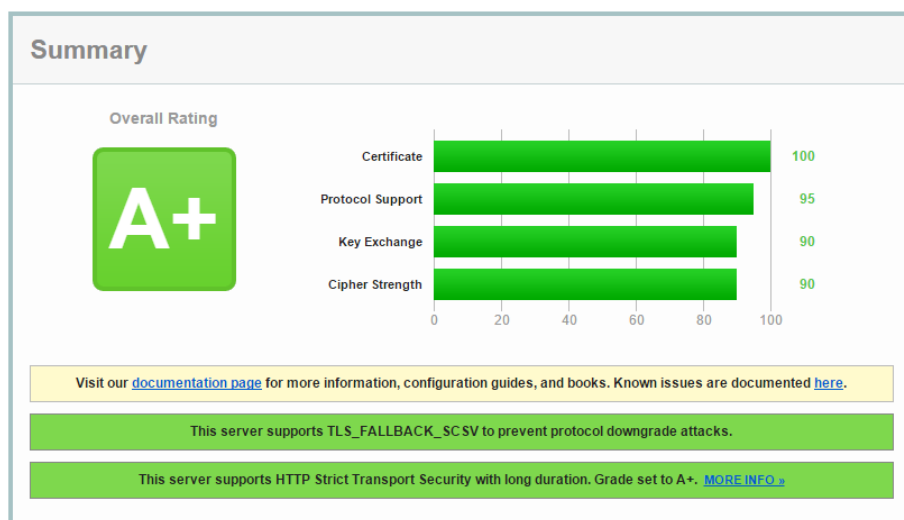


Рис. 1: Recently best.

- Поддерживает все типы протоколов TLS
- Поддерживает длительное форсированное защищенное соединение через HTTPS

**Recent Worst** SSL Report: mappiness.me (178.79.152.166)

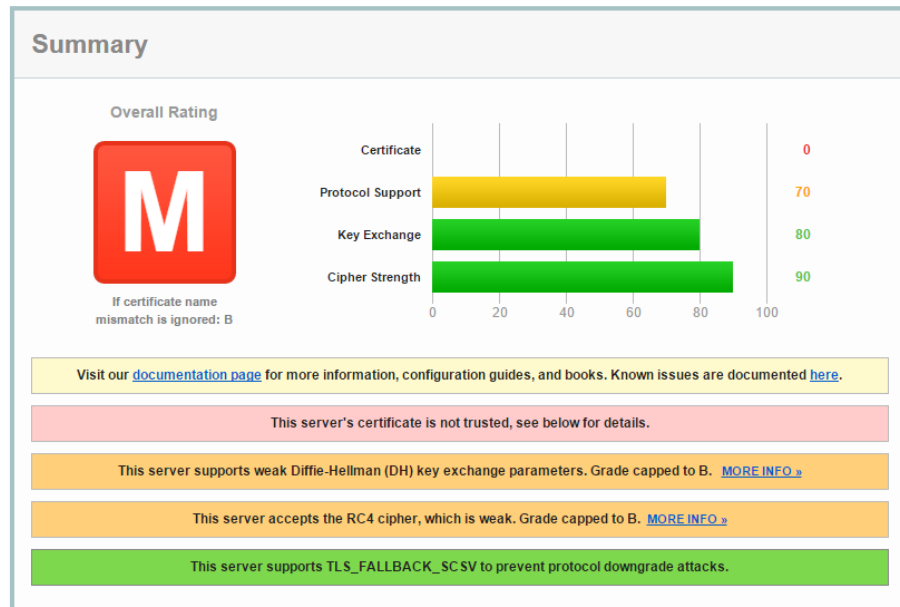


Рис. 2: Recently worst.

- Сертификат не заверен
- Используется слабый алгоритм Диффи-Хэлмана
- Использует слабый алгоритм шифрования RC4 с современными браузерами
- Защищен от downgrade атак

## Самостоятельный анализ SSL Report: zohoplatform.com (74.201.154.174)

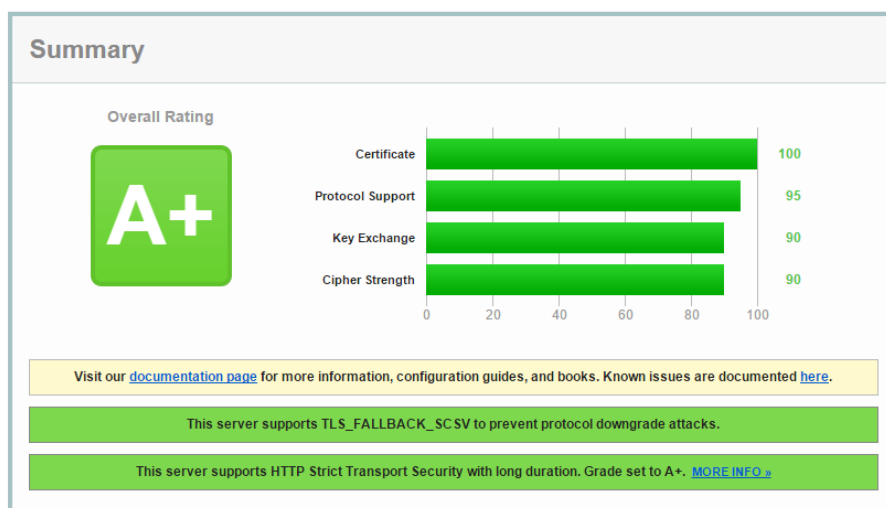


Рис. 3: Zoho сервер.

### Интерпретировать результат в разделе summary

- Защищен от downgrade атак
- Поддерживает длительное форсированное защищенное соединение через HTTPS

**Расшифровать все аббревиатуры шифров в разделе Configuration**  
Вот список используемых алгоритмов.



**Cipher Suites (SSL 3+ suites in server-preferred order; deprecated and SSL 2 suites at the end)**


TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH 256 bits (eq. 3072 bits RSA)	FS	128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH 256 bits (eq. 3072 bits RSA)	FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH 256 bits (eq. 3072 bits RSA)	FS	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH 256 bits (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_256_CBC_SHA256 (0x3d)			256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH 256 bits (eq. 3072 bits RSA)	FS	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH 256 bits (eq. 3072 bits RSA)	FS	256
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)			256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)			128
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012)	ECDH 256 bits (eq. 3072 bits RSA)	FS	112
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)			112

Рис. 4: Список алоритмов.

Расшифруем некоторые аббревиатуры.

- TLS ECDHE означает Алгоритм Диффи-Хэлмана на эллиптических кривых
- RSA это алгоритм шифрования с открытым ключом.
- AES 128 так же алгоритм шифрования с длиной ключа в 128 бит
- GCM и CBC это два режима блочного шифрования
- SHA256 -это хэш функция с длиной ключа в 256 бит





Protocol Details	
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: 0xcc013
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	No
Heartbeat (extension)	Yes
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> )
Next Protocol Negotiation (NPN)	Yes http/1.1
Session resumption (caching)	Yes
Session resumption (tickets)	Yes
OCSP stapling	No
Strict Transport Security (HSTS)	Yes max-age=15768000
Public Key Pinning (HPKP)	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

Рис. 5: Protocol details.

### Прокомментировать большинство позиций в разделе Protocol Details

- Строки 1-3 Перепроверка сертификата и защищенность этого процесса
- Строки 4-7 Уязвимости к атакам Poodle, Beast, downgrade
- Строка 9 Не используется слабый алгоритм RC4
- Строка 10 -11 уязвимость HeartBleed
- Строка 13 Совместимость Forward Secrecy с браузерами
- Строка 14 Наличие NPN  
в настоящее время используется для согласования использования SPDY

в качестве протокола прикладного уровня на порт 443, а также для выполнения SPDY согласования версии.

Основной задачей SPDY является снижение времени загрузки веб-страниц и их элементов. Это достигается за счёт расстановки приоритетов и мультиплексирования передачи нескольких файлов таким образом, чтобы требовалось только одно соединение для каждого клиента.

- Строка 15-16 Параметры сессии
- Строка 18 Реализация HSTS  
HSTS — механизм, активирующий форсированное защищённое соединение через протокол HTTPS. Данная политика безопасности позволяет сразу же устанавливать безопасное соединение, вместо использования HTTP-протокола. Механизм использует особый заголовок HTTP Strict-Transport-Security, для переключения пользователя, зашедшего по HTTP, на HTTPS-сервер.
- Строка 19 Реализация HPKP  
Позволяет указать, какой сертификат выдан доверительным центром, а какой нет, это позволяет отклонить TLS соединения с сайтов, CA которых заведомо неправильный. Это мешает использовать такие атаки как "человек посередине".  
Функция связывает набор хэшей открытых ключей для доменного имени, например: при подключении к сайту, используя TLS браузера, гарантирует, что есть пересечение открытых ключей в компьютерной цепочке доверия и множества отпечатков, связанных с этим доменом. Эта проверка выполняется во время верификации сертификата фазы связи, до того, как данные посылаются или обрабатываются браузером.
- Строка 25 Совместимость с SSL2 handshake

**Сделать итоговый вывод о реализации SSL на заданном домене**  
Конфигурация сервера отличная. Сервер использует доверенный сертификат и защищен от некоторых типов атак. Forward Secrecy реализовано не для всех браузеров, однако реализации отсутствуют только для самых старых, так что это можно не относить к первичным проблемам. В целом, сервер имеет необходимый набор защиты.

### 3 Вывод

В ходе данной работы были изучены возможности сервиса Qualys SSL LABS. Данный сервис анализирует качество реализации защиты домена, предоставляет отчет об используемых технологиях и об известных уязвимостях

сервера. Также можно посмотреть используемые протоколы. Стоит отметить, что использование такого рода сервисов важно в коммерческом плане, но только для первичного анализа.