

САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ
ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
Кафедра Компьютерных Систем и Программных Технологий

ОТЧЕТ

по лабораторной работе №7

Тема: «Сервис тестирования корректности настройки SSL на сервере
Qualys SSL Labs — SSL Server Test»

Дисциплина: «Методы и средства защиты информации»

Выполнил: студент гр. 53501/2
Федоров Е.М.

Преподаватель
Вылегжанина К.Д.

Санкт-Петербург
2015

Содержание

1	Задание	2
2	Выполнение	3
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	Практическое задание	5
2.2.1	Выбрать со стартовой страницы SSL Server Test один домен из списка Recent Best и один домен из списка Recent Worst	5
2.3	Сделать итоговый вывод о реализации SSL на заданном домене (для анализа выбран первый)	9
3	Выводы	10

1 Задание

а) Изучение

- 1) Изучить лучшие практики по развертыванию SSL/TLS
- 2) Изучить основные уязвимости и атаки на SSL последнего времени — POODLE, HeartBleed

б) 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. Выбрать для анализа интернет-домен защищенный SSL-шифрованием, проделать следующие шаги:

- 1) Интерпретировать результаты в разделе Summary
- 2) Расшифровать все аббревиатуры шифров в разделе Configuration
- 3) Прокомментировать большинство позиций в разделе Protocol Details
- 4) Сделать итоговый вывод о реализации SSL на заданном домене

Инструмент выполнения: Qualys SSL Labs — SSL Server Test

2 Выполнение

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 СА.

— 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

2.1.2.1 POODLE

POODLE(Padding Oracle On Downgraded Legacy Encryption) — уязвимость, позволяющая злоумышленнику от имени жертвы отправлять данные на сервер и расшифровывать их если у него есть возможность прослушивать и подменять трафик жертвы. Об уязвимости стало известно после того, как Google опубликовал документ с названием «This POODLE Bites: Exploiting The SSL 3.0 Fallback».

Уязвимость позволяет злоумышленнику, используя атаку Man-in-the-middle, заставить браузер жертвы использовать SSL 3.0 (более старый протокол) вместо того, чтобы использовать современный TLS, и за счет этого эксплуатировать дыры в безопасности в SSL, чтобы украсть сессии браузера.

Если и браузер и сервер поддерживают протокол SSL 3.0, атакующий может принудить браузер использовать старый протокол. Другими словами, хоть и браузер будет пытаться использовать TLS, он будет принужден использовать SSL.

2.1.2.2 HeartBleed

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 Практическое задание

2.2.1 Выбрать со стартовой страницы SSL Server Test один домен из списка Recent Best и один домен из списка Recent Worst

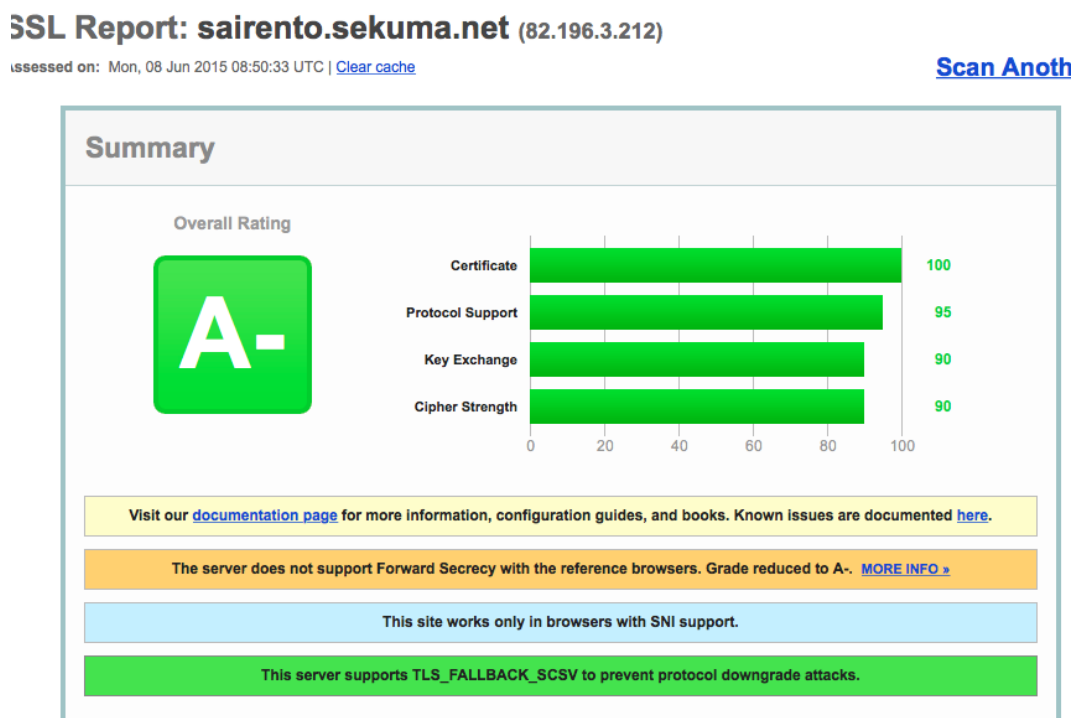


Рисунок 1 — Recent best

- а) Сервер не поддерживает поддержку защиты наперед с некоторыми браузерами.
- б) Этот сайт работает только с браузерами с поддержкой SNI(Server Name Indication)
- в) Этот сервер поддерживает TLS_FALLBACK_SCSV, чтобы избежать нисходящие атаки

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


Рисунок 2 — Configuration

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 крипто-

графию 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.

Конфигурация поддерживает основные виды TLS, в то же время не поддерживает SSL 3 и SSL 2, что очень хорошо, так как эти протоколы являются устаревшими.




Cipher Suites (sorted by strength; the server has no preference)

TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) DH 2048 bits (p: 256, g: 1, Ys: 255) FS	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH 256 bits (eq. 3072 bits RSA) FS	128
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67) DH 2048 bits (p: 256, g: 1, Ys: 256) FS	128
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)	128
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) DH 2048 bits (p: 256, g: 1, Ys: 256) FS	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH 256 bits (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH 256 bits (eq. 3072 bits RSA) FS	128
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)	112

Рисунок 3 — Cipher Suites

- RSA — Rivest, Shamir, Adleman — криптографический алгоритм
- RC4 — Rivest Cipher 4 — потоковый шифр 4-й версии
- SHA/SHA256/384 — Secure Hash Algorithm — алгоритм хэширования (цифра соответствует длине ключа)
- AES — Advanced Encryption Standard — симметричный алгоритм блочного шифрования
- GCM и CBC — 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) TLS 1.0: 0x2f
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
Downgrade attack prevention	Yes, TLS_FALLBACK_SCSV supported (more info)
TLS compression	No
RC4	No
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)	No
Public Key Pinning (HPKP)	No
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	No

Рисунок 4 — Protocol Details

- Поддерживает возобновление подключения TLS
- Нету поддержки возобновления подключения TLS с инициализированным клиентом. Есть некоторые случаи, в которых возобновление должно быть инициализировано сервером, но нет никакой известной необходимости для клиентов, чтобы это сделать.
- BEAST атака смягчена со стороны сервера
- Нет POODLE, Heartbleed и RC4 уязвимостей.
- OCSP (или Online Certificate Status Protocol) — протокол, проверяющий, был ли отозван SSL-сертификат. Используя OCSP, браузер посылает запрос к OCSP URL и получает ответ, содержащий состояние достоверности сертификата. Не поддерживается.

SSL Report: vpn.kingold.com (183.59.158.221)

Assessed on: Mon, 08 Jun 2015 08:47:03 UTC | [Clear cache](#)

[Scan Another](#)

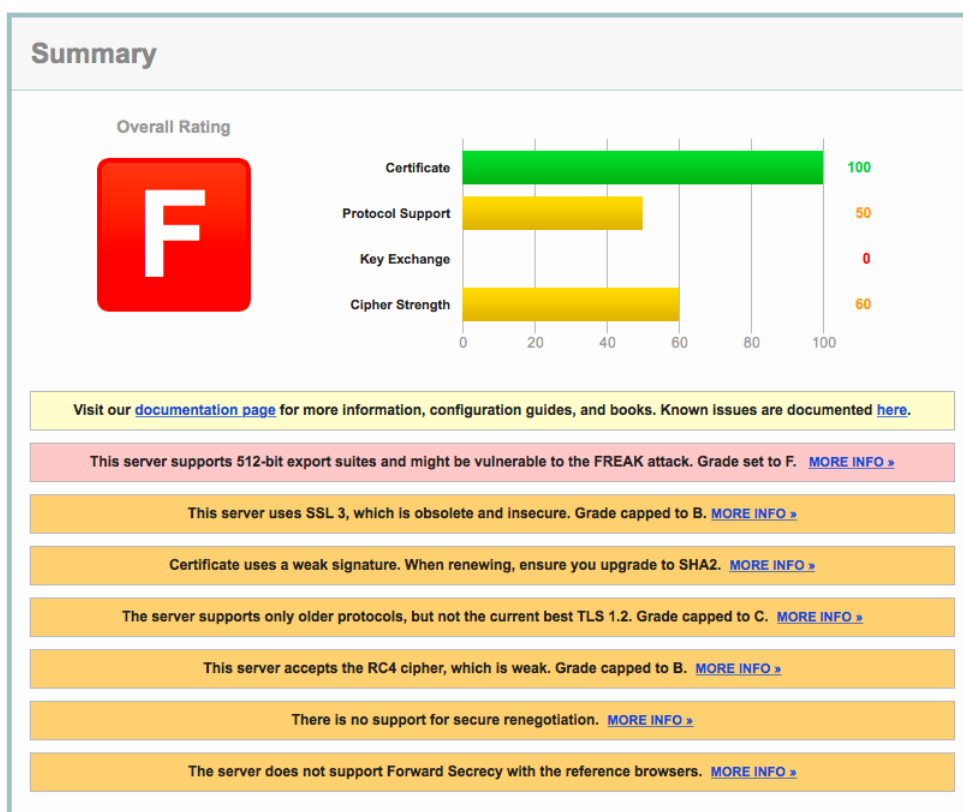


Рисунок 5 — Recent worst

- а) Сервер поддерживает пакеты для экспорта в 512-бит и могут быть уязвимы к FREAK атакам
- б) Сервер использует устаревший и небезопасный SSL 3
- в) Сертификат имеет слабую подпись. Использует старый алгоритм шифрования SHA-2
- г) Сервер поддерживает старые протоколы
- д) Использует потоковый шифр RC4, считающийся слабым
- е) Нет поддержки безопасного пересмотра
- ж) Сервер не поддерживает поддержку защиты наперед с некоторыми браузерами.

Для более детального описания какой либо информации об уязвимости, на сайте можно нажать вкладку «MORE INFO» в соответствующей вкладке.

2.3 Сделать итоговый вывод о реализации SSL на заданном домене (для анализа выбран первый)

В целом, после сервис дает очень развернутую информацию о любом домене, поскольку выбранный для анализа домен был из категории «А-», то и критичных уязвимостей у него не было обнаружено.

3 Выводы

В результате выполнения лабораторной работы были изучены возможности веб-сервиса Qalys SSL LABS, который позволяет получить развернутую статистику по уровню защищенности сокетов (SSL) для запрашиваемого домена.

Анализируя данные таким способом, можно избавиться от дыр в безопасности сервера, закрыв критические уязвимости.