

# Отчет по лабораторной работе №5 SSL

Рикардо санчес

## 1 Цель работы

Научиться разворачивать SSL/TLS сервер.

## 2 Ход работы

### 2.1 Лучшие практики по разворачиванию SSL/TLS

1. Использовать 2048-битные ключи.
2. Закрывайте приватные ключи.
3. Позаботьтесь о достаточном покрытии доменных имен.
4. Получайте сертификаты у надежных СА.
5. Используйте криптостойкие алгоритмы для подписей.
6. Настраивайте сервер для работы с несколькими сертификатами.
7. Используйте безопасные протоколы.
8. Используйте криптостойкие алгоритмы шифрования. Ключ не менее 128 бит.
9. Используйте Forward Secrecy, позволяющую защищенный обмен, не зависящий от приватного ключа сервера.
10. Если нет необходимости, отключайте проверку защищенности соединения на стороне клиента.
11. Адаптируйте свою систему. Устанавливайте патчи к модулям защиты, когда они появляются.
12. Надо найти компромис между защищенностью системы и производительностью.
13. Шифруйте 100% вашего сайта.
14. Используйте защищенные куки.

## 2.2 Изучить основные уязвимости и атаки на SSL последнего времени – POODLE, HeartBleed

**HeartBleed** Уязвимости подвержены следующие версии OpenSSL 1.0.1 до 1.0.1f включительно.

Суть ошибки - неконтролируемое переполнение буфера, позволяющее 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.

**POODLE** Суть уязвимости: злоумышленник может заставить обе стороны перейти на ssl 3.0, в котором используется потоковое шифрование RC4, которое, при больших объемах трафика, позволяет получить информацию, помогающее дешифрованию.

## 2.3 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

### 2.3.1 SSL Report: bankorange.ru (84.52.66.47)

Рис. 1: SSL Report: bankorange.ru

Этот сервер уязвимым для POODLE attack, использует слабую подпись. Поддерживает только устаревшие протоколы. Сервер принимает уязвимое RC4 шифрование. Так же сервер не поддерживает Forward Secrecy.

### 2.3.2 SSL Report: luxexpress.eu (217.146.69.16)

Рис. 2: SSL Report: luxexpress.eu

У сервера нет доверенного сертификата. Сертификат имеет слабую подпись и истекает после 2016. Использует алгоритм Диффи-Хеллмана

для обмена ключами. Имеет неполную цепочку сертификатов. Но защищен от DownGrade атаки.

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH 256 bits (eq. 3072 bits)
FS 256	
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH 256 bits (eq. 3072 bits)
FS 128	
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH 256 bits (eq. 3072 bits)
FS 256	
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH 256 bits (eq. 3072 bits)
FS 128	
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH 256 bits (eq. 3072 bits)
FS 256	
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH 256 bits (eq. 3072 bits)
FS 128	

## 2.4 Прокомментировать большинство позиций в разделе Protocol Details

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: 0x35

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) No

Heartbleed (vulnerability) No (more info)

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

Forward Secrecy No WEAK (more info)

Next Protocol Negotiation (NPN) No

Session resumption (caching) Yes

Session resumption (tickets) No

OCSP stapling No

Strict Transport Security (HSTS) Disabled max-age=0

Public Key Pinning (HPKP) No

Long handshake intolerance No

TLS extension intolerance No

TLS version intolerance TLS 1.98 TLS 2.98

Incorrect SNI alerts -

Uses common DH prime No

SSL 2 handshake compatibility No

- Secure Renegotiation - Хранение доп параметров о TLS соединении.
- BEAST attack - защита от BEAST атаки.
- POODLE (SSLv3) - защита от пуделя по SSLv3.
- POODLE (TLS) - защита от пуделя по TLS.
- Downgrade attack prevention - защита от downgrade атаки.
- TLS compression - сжатие данных по tls.
- RC4 - использование алгоритма шифрования RC4
- Heartbleed - защита от уязвимости Heartbleed.
- OpenSSL CCS vuln. - SSL ChangeCipherSpec уязвимость.
- Forward Secrecy - защищенный обмен без приватного ключа сервера.
- Next Protocol Negotiation - расширение SSL, позволяющее договариваться о протоколе соединения.
- OCSP - Online Certificate Status Protocol проверка валидности сертификата.
- Strict Transport Security (HSTS) - механизм, активирующий форсированное защищённое соединение по HTTPS.
- Public Key Pinning (HPKP) - фиксирует привязку публичного ключа к данному узлу.
- Long handshake intolerance - поддержка длинных(больше 256 байт) handshake сообщений.
- TLS extension intolerance - поддержка TLS расширений.
- Incorrect SNI alerts - предупреждение при некорректном Server Name Indication.

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

На домене bankorange.ru (84.52.66.47) отсутствует защита от POODLE attack, имеется слабая электронная подпись, отсутствует поддержка Forward Secrecy.

### 3 Выводы

В ходе данной работы были изучены "best practice" использования SSL/TLS. Были рассмотрены основные возможности сервиса Qualys SSL Labs – SSL Server Test. Данный сервис позволяет провести анализ качества защищенности домена. В качестве резюме можно получить статус самых известных уязвимостей для данной сервера, а также информацию о поддерживаемых протоколах и режимах работы. Кроме того, сервис тут же предлагает дополнительную информацию по вопросам решения указанных проблем.