Сигурност при WWW

проф. д-р инж. Венета Алексиева,
проф. д-р инж. Христо Вълчанов

Основни моменти

- Защита на уебсайт
- HTTPS
- Защита на транзакциите:
  - SSL
  - TSL
- Електронен подпис

Компрометиране на сайт

Прави се с автоматизирани скриптове, с които:

- се крадат данни
- се обезобразява визията на уеб сайта с цел загуба на клиенти
- се опитва да използва сървъра като платформа за имейл спам
- се настройва сървъра, за да служи на файлове от незаконен характер

Защита на уебсайт - подходи

- Да се поддържа софтуера актуален
  - На ОС и приложенията
  - От хостинг компанията
  - От трети страни, осигуряващи услуги за сайта
- Да се защити от **SQL injection атаки** (използват се полетата на уеб форма или URL параметър, за да се получи достъп до базата данни) използването на стандартна Transact SQL не се препоръчва, т.к. допуска промяна в кода на заявката и манипулиране на таблиците. Да се ползват параметризирани заявки:

Например заявката:

```
"SELECT * FROM table WHERE column = '" + parameter
  + "';"
```

Може да бъде злонамерено променена на:

```
"SELECT * FROM table WHERE column = '' OR
  '1'='1';"
```

Тъй като 1=1 е винаги истина, това ще позволи на нападателя да добави допълнителна обработка в края на SQL заявката, която също ще бъде изпълнена.

Защита на уебсайт - подходи

- Да се формулират общо съобщенията за грешка:
  - “Сгрешено име или парола”, а не “Сгрешена парола” – атакуващият по метода на грубата сила ще разпредели сили върху 2 полета, т.к. не му е подсказано, че едното поле е вярно попълнено.
- Валидация и при клиента (браузера) и при сървъра
  - Малки пропуски във формата за въвеждане (празни полета, текст в поле за числа...) могат да доведат до “закачане” на злонамерен код

Защита на уебсайт - подходи

- Да се обмисли политиката за пароли за достъп
  - Силни пароли (>8 символа, ≠ тип символи...)
  - Честа смяна на пароли
  - Генератор на пароли
  - Съхраняват се криптирани с еднопосочен алгоритъм за хеширане SHA
  - .NETпредоставя вградени функции за сигурност - готови контроли за вход и за възстановяване на паролата.
- Да се ползва SSL протокол при обмен на чувствителна информация между браузера и уеб сървъра или базата данни.
- Да се ползва suPHP вместо PHP, за да се ползва сайта само от потребители, на които е разрешено това.

Защита на уебсайт - подходи

Качване (Upload) на файлове към сайта:

- Всеки файл може да съдържа скрипт, който да “хакне” сайта.
- Повечето формати за изображения позволяват съхраняване на коментар - част, която може да съдържа PHP код, който може да бъде изпълнен от сървъра.
- За форма за качване на изображения:
  - отваряне на файла и четене на заглавната част, за да се провери дали наистина е изображение;
  - да се провери файла да не е с двойно разширение (*opit.jpg.php*);
  - да се преименува файла при качването му, за да се гарантира, че няма да е с разширение на изпълним файл;

Защита на уебсайт - подходи

- Да се създаде файл .htaccess

```
deny from all
<Files ~ "^\w+\.(gif|jpe?g|png)$">
order deny,allow
allow from all
</Files>
```

- Да се предотврати директен достъп до всички качени файлове като се съхраняват в отделна папка, различна от *webroot*, например:

```
<img src="/imageDelivery.php?id=1234" />
 <?php
     // imageDelivery.php
     // Fetch image filename from database based on
  $_GET["id"]
     ...
     // Deliver image to browser
     Header('Content-Type: image/gif');
     readfile('images/'.$fileName);
   ?>
```

Защита на сървъра

- Ограничаване на физическия достъп до сървъра – само от оторизирани лица
- По възможност разполагане на сървъра в DMZ
- Вдигане на firewall и блокиране на неизползваните портове, разрешаване само на портове 80 и 443
- За отдалечен достъп и качване на файлове да се ползват само SSH или SFTP
- Ако е възможно, БД да бъде на отделна машина от тази на web сървъра, за да няма директен достъп до нея отвън.
- Ако се ползва хостинг – да се плати за VPS hosting, което гарантира отделянето на сайта от останалите и създаване на персонална защитна стена за него

Средства за тестване сигурността на сайта

- Безплатните:
  - Netsparker - https://www.netsparker.com/web-vulnerability-scanner/
  - OpenVAS- http://www.openvas.org/
  - Fiddler - http://www.telerik.com/download/fiddler
  - Security Review for Drupal - https://www.drupal.org/project/security_review
  - Acunetix WP Security plugin for WordPress - https://wordpress.org/plugins/wp-security-scan/
- И платеният:
  - https://www.sitelock.com/

Сигурност на транзакциите - SSL

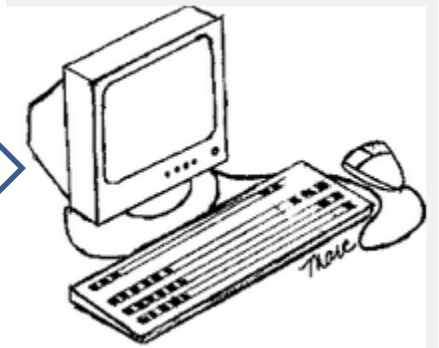
- SSL (Secure Socket Layer) протоколът осигурява криптирана връзка между сървъра (уеб сайта) и клиентския браузър, като по този начин защитава обменящата се информация от неоторизирано прихващане.
- Криптиране на връзката чрез SSL сертификат е препоръчително за всички онлайн платформи и електронни магазини, в които потребителите въвеждат лични данни и/или извършват онлайн разплащания.
- **SSL сертификатите печелят доверието и осигуряват на потребителите на сайта сигурност и спокойствие при въвеждането на конфеденциална информация.**

SSL- функциониране

Заявка за установяване на защитена SSL сесия

Изпращане на данни за валидност на сертификата и дали е с подпис от достоверен източник

Изпращане на ключ за криптиране на сесията, криптиран с публичния ключ на сървъра



Декриптиране на ключа с частния ключ и установяване на защитена SSL сесия

SSL сертификат

- Това е файл, инсталиран на уеб сървъра, на който се намира сайта.
- Той се състои от публичен ключ и допълнителна информация, закодирана в сертификата - името на домейна, името на фирмата, друга фирмена информация и т.н. в зависимост от типа на самия SSL сертификат.
- Публичният ключ се съдържа в сертификата и се изпраща на браузъра, след което браузърът проверява, дали сертификатът е валиден и верифицира, дали уеб сървърът е точно този, за който се представя.

Валиден сертификат

- Датата на изтичане на сертификата да е след текущата дата. Всички сертификати се издават с определен срок на валидност.
  - Ако сертификатът е изтекъл, то той се приема за невалиден и на посетителите на сайта се показва предупредително съобщение.
- Името на домейна (сайта) трябва да съвпада с това, което е зададено в сертификата.
  - В случай на несъвпадение, сертификатът се приема за невалиден и на потребителя се показва предупредително съобщение.

Видове SSL сертификати

- **Self Sign (безплатен)**
  - Това са сертификати, които не са издадени от "Certificate Authority" и при зареждането на сайта, браузърите показват съобщение, че сайтът може да съдържа потенциален риск за данните на клиента.
  - Този тип сертификати обикновено се използват по време на развоя и тестването на уеб приложението, но не са добър избор за реална работа на сайта.
- **Издадени от доверен оторизиращ орган (Certificate Authority)**
  - Сертификатът се издава от доверен оторизиращ орган “Certificate Authority” – GeoTrust, Symantec (VeriSign)...
  - При зареждането на сайта клиентът вижда, че сертификатът е валиден. Списъкът с всички доверени оторизиращи органи е достъпен във всеки един от съвременните уеб браузъри.

Например

GeoTrust

GeoTrust е вторият по големина издател на цифрови сертификати в света, с повече от 500 000 активни сертификата, инсталирани в над 170 страни. GeoTrust сертификатите печелят доверието на потребителите и осигуряват надеждни и защитени онлайн транзакции.

RapidSSL	1 година, 41.75 лв.	1	☐	41.75 лв.
QuickSSL Premium ⚠	1 година, 196.90 лв.	1	☐	196.90 лв.
True BusinessID	1 година, 284.90 лв.	1	☐	284.90 лв.
True BusinessID with EV	1 година, 625.90 лв.	1	☐	625.90 лв.
True BusinessID Wildcard	1 година, 1120.90 лв.	1	☐	1120.90 лв.

VeriSign

Symantec (VeriSign) е лидер сред издателите на SSL сертификати, ползващ се с най-голямо доверие при предлагането на онлайн решения за повишаване на сигурността. Сертификатите на Symantec (VeriSign) гарантират максимална сигурност при електронната търговия, комуникацията и обмяната на информация в Интернет.

Secure Site	1 година, 1142.90 лв.	1	☐	1142.90 лв.
Secure Site Pro	1 година, 2748.90 лв.	1	☐	2748.90 лв.
Secure Site With EV	1 година, 2858.90 лв.	1	☐	2858.90 лв.
Secure Site Pro With EV	1 година, 4178.90 лв.	1	☐	4178.90 лв.

SECTIGO

Sectigo е една от известните и доверени марки в сферата на IT сигурността. SSL сертификатите Sectigo са максимално гъвкави и достъпни и отговарят на широк спектър от потребности за защита.

Sectigo Essential	1 година, 44.83 лв.	1	☐	44.83 лв.
Sectigo Essential Wildcard	1 година, 251.90 лв.	1	☐	251.90 лв.
Sectigo Premium Wildcard	1 година, 548.90 лв.	1	☐	548.90 лв.
Sectigo EV	1 година, 649.00 лв.	1	☐	649.00 лв.

Ниво на валидация на SSL сертификатите

- Валидация по домейн
- Валидация по организация
- Разширена валидация (Extended Validation)

Издаване на SSL сертификат

- Да се избере точното име на **домейн**, с който ще се използва сертификата.
  - За SSL сертификатите superhosting.bg е различен от www.superhosting.bg (технически това са различни домейни, тъй като "www." е поддомейн и един сертификат не би могъл да обслужва и двата адреса).
  - Няма проблем сертификатът да се издаде за един от двата адреса и след това, за страниците, за които ще се криптира връзката, в кода на сайта линковете да са към съответния адрес, позволяващ криптирането на връзката и ползването на сертификата.
- Да има създаден валиден имейл към домейна
  - Например ssladmin@yourdomain.com
- Да се въведат данните, които ще се използват за сертификата
  - име на **фирма**, адрес, имейл, телефон.
- Да се генерира и изпрати Certificate signing request (CSR).
- За издаването на **сертификат с разширена валидация (Extended Validation)** има някои особености:
- Следващата стъпка е верификация на компанията, за която е заявен сертификата- проверка, дали фирмата е регистрирана в съответната държава, компанията да посочи адрес на офис и фирмен телефон. За всяка компания може да бъдат извършени проверки на различни нива, като това зависи от преценката на издателя на сертификата.

Инсталиране на SSL сертификат

- SSL сертификат задължително се инсталира на реален статичен IP адрес.
- Инсталацията и конфигурацията на IP адреса и сертификата се извършват напълно безплатно, изцяло от отдела по техническа поддръжка на хостинг компанията.

Transport Layer Security (TLS)

- Разработен от Netscape Communications.
- Описан е в RFC 5246 и се основава на SSL.
- Криптографски протокол, който осигурява сигурност на комуникацията по Интернет.
- Предназначен за предотвратяване на подслушване и подправяне на комуникацията клиент-сървър.
- Работи на Transport Layer, използвайки асиметрична криптография за личния message authentication code за надеждността на съобщението.

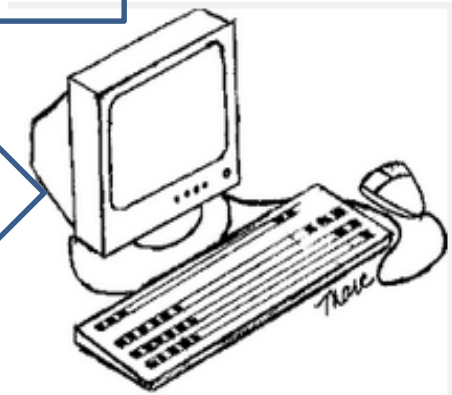
TLS- функциониране

TLS клиентът и сървърът договарят динамична връзка чрез handshaking процедура.

Заявка за установяване на защитена TLS сесия, придружена със списък на ciphers и hash functions

Сървърът избира най-силния шифър и хеш функция и уведомява клиента за решението. Сървърът изпраща обратно идентификацията си под формата на цифров сертификат. Сертификатът обикновено съдържа името на сървъра, издалият го certificate authority (CA) и публичен ключ за криптиране на сървъра.

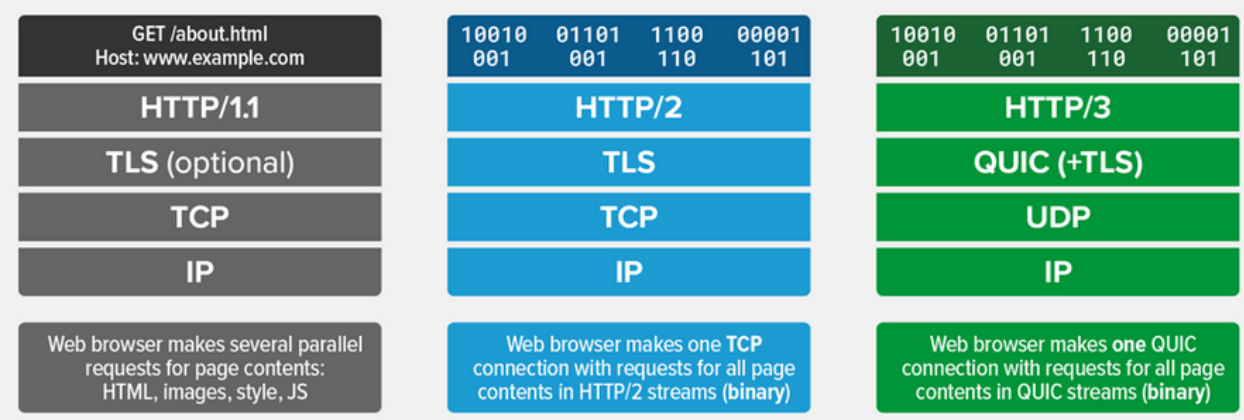
Клиентът може да потвърди валидността на сертификата. клиентът криптира случайно число с публичния ключ на сървъра и му изпраща резултата



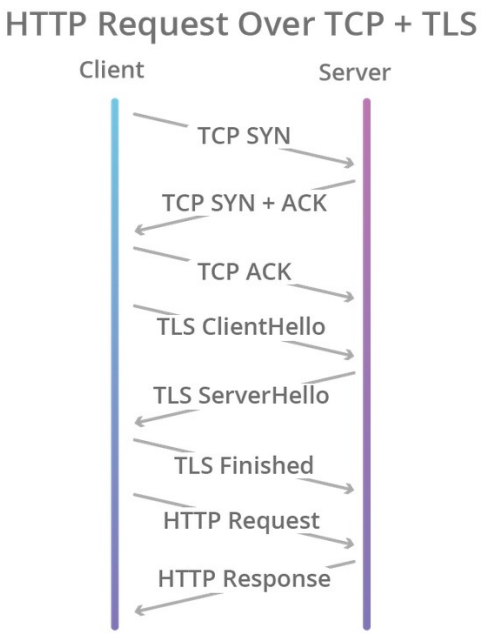
Декриптиране на ключа с частния ключ и установяване на защитена TLS сесия

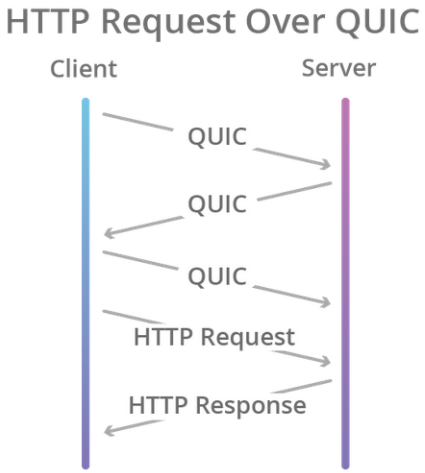
Сигурност при HTTP2.0 / HTTP3.0

HTTP2.0	HTTP3.0
Използва TLS	Не ползва TLS като отделен слой
Компресира хедърите	
Приоритизира заявките	
Изпраща корелативни (свързани) HTTP ресурси, за да минимизира заявките към тях в една TCP конекция	
Пренася се от TCP	Пренася се от Quick UDP Internet Connections (QUIC), разработен от Google: • вградено мултиплексиране, • per-stream flow control, • установява конекция с low-latency • включва TLS 1.3, а не го ползва като отделен слой.



Договаряне на версията на HTTP





- При HTTP2.0 се използва TLS handshake, за да се открие дали клиентът и сървърът са способни да комуникират през HTTP2.0 преди връзката да бъде установена.
- Клиентът установява TCP връзка за първоначалната HTTP заявка.
- Отговорът от сървър, който поддържа HTTP3.0, включва в хедъра Alt-Svc, за да посочи UDP порта, на който слуша за HTTP3.0 трафик.
- Браузърът помни кои сайтове поддържат QUIC, за да елиминират времето за размяна на служебни съобщения за договаряне на връзката.

Електронен подпис

- Електронен подпис – комбинация от букви и цифри, чрез която се идентифицира притежателят на подписа.
- Служи за :
  - Неопровержимост на сделката чрез издаване на документи, свързани с е-подпис
  - Конфиденциалност на сделката
  - Валидност по време
- Има сертифициращ орган, който издава сертификати, удостоверяващи идентичността на физическото/юридическото лице, които съдържат:
  - Име на потребителя
  - Дата на издаване
  - Срок на валидност
  - Публичен ключ
  - Частен ключ (е-подписа)

Видове е-подпис

- Обикновен - достатъчно сигурен и разкрива кой е автора, удостоверява съгласието му в сделката и защитава съдържанието на документа от последващи промени
- Усъвършенстван - “преобразувано електронно изявление, включено, добавено или логически свързано със същото изявление преди преобразуването”, т.е. Добавя се допълнителен текст, една част от който е явен ключ, а останалата е конфиденциална и се преобразува при електронно изявление
- Универсален - удостоверението за него е издадено от доставчик на удостоверителни услуги

Доставчици, които имат разрешение да издават електронен подпис в България

https://nssi.bg/kontakti/vryzki/dostavchici-koito-imat-razreshenie-da-izdavat-elektronen-podpis-bg/

- „Борика-Банксервиз” АД
- „Информационно обслужване” АД
- „Инфонотари” ЕАД
- „Евротръст Технолъджис“ АД
- „СЕП България” АД

Стандарти за цифров подпис....

Reference	Feature
PDF Reference 1.7 (ISO 32000-1) . See also PDF for Archive (PDF/A) and PDF for Exchange (PDF/X).	Representing signatures in the PDF language.
RFC 3280, Internet X.509v3 Public Key Infrastructure, Certificate and Certificate Revocation List (CRL) Profile.	CRL revocation checking, chain building, path validation, cross certificates, multiple chains.
RFC 2560, X.509 Internet PKI Online Certificate Status Protocol-OCSP.	OCSP revocation checking.
RFC 3161, Internet X.509 Public Key Infrastructure Time-Stamp Protocol	Timestamping: signing and signature validation.
RFC 3281, Attribute Certificate Profile, S. Farrell, R. Housley April 2002.	Attribute certificates.
RFC 2437, PKCS #1: RSA Cryptography Specifications Version 2.0 (1024, 2048, 4096).	A format used for creating a digital signature object which is embedded in a document.
RFC 2898, PKCS #5: Password-Based Cryptography Specification Ver. 2.0.	Password security.
RFC 2315, PKCS #7: Cryptographic Message Syntax, Version 1.5.	A format used for creating a digital signature object which is embedded in a document.
PKCS #11: URI Scheme	Cryptographic token interface (smart cards, tokens, etc.)
RFC 1321, The MD5 Message-Digest Algorithm	Creating a document hash during signing.
RFC 3174, US Secure Hash Algorithm 1 (SHA1)	Creating a document hash during signing. Deprecated with 11.0.
RFC 6234 US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)	Creating a document hash during signing.
FIPS PUB 186-2, Digital Signature Standard. Describes DSA signatures.	Digital signatures. Deprecated with 11.0.
FIPS PUB 186-3, Digital Signature Standard. Supported by 11.x products.	Digital signatures. 11.0 introduces support for 3 ECDSA named curves.
FIPS PUB 186-4, Digital Signature Standard. Supported by 11.x products.	Digital signatures.
FIPS PUB 197, Advanced Encryption Standard (AES 128, 256).	Certificate security.
ISIS-MTT Specification v.1.1 March 2004.	Attribute certificates.
NIST PKITS "Public Key Interoperability Test Suite Certification Path Validation"	Chain building and path validation, including cross certificates and multiple chains.
OIDS. ASN.1	Object identifiers (OIDs)
RFC 2396, Uniform Resource Identifiers (URI): Generic Syntax.	All.
RFC 2595, Using TLS with IMAP, POP3 and ACAP.	The PLAIN authentication mechanism used by the roaming ID feature.
RFC 3778, The application/pdf Media Type. Adobe Systems Incorporated.	Describes PDF media type, digital signatures, and encryption.
ETSI 102 778 PDF Advanced Electronic Signatures (PAdES), Parts 1,2,3 and 4.	Digital signature; especially LTV.
ETSI/ESI Technical Standard (TS) 102 778	Digital signatures.
JITC: Joint Interoperability Test Command PKI compliance test suite	DoD-mandated PKI test suite. Compliant since 7.x. See http://blogs.adobe.com /security/tag/jitc.

10:20 AM

Въпроси ?

Благодаря за вниманието !