

Общи проблеми със сигурността в уеб

1 Уеб сигурност

Интернет позволява публикуване на информация, обмен на данни и използване на различни услуги. Тези възможности са свързани и с рискове.

Уеб сигурността включва защита на информацията и услугите от неправомерно използване, разкриване, промяна и изтриване.

Успешната атака може да доведе до изтичане на информация, прекъсване на услуги, неправомерно използване на ресурси, унищожаване на данни, кражба на пароли, разпространение на злонамерени програми, измами и финансови загуби.

2 Основни видове заплахи

2.1 Загуба на целостта

Целостта означава информацията да бъде защитена от неразрешена промяна или изтриване.

Пример: Банковата сметка за плащане, посочена в уеб сайт, е променена без разрешение, така че парите да се превеждат по чужда сметка.

2.2 Загуба на конфиденциалност

Конфиденциалност означава информацията да бъде достъпна само за лица, които имат право да я използват.

Пример: Личните данни на регистрираните потребители стават достъпни за неупълномощени лица.

2.3 Загуба на услуги

Сайтът или услугата стават недостъпни за нормалните потребители. Причината може да бъде атака, претоварване или технически проблем.

Пример: Онлайн магазин спира да обслужва поръчки.

2.4 Загуба на контрол

Услугите се използват неправомерно от неоторизирани лица.

Пример: Чужд човек използва вашия профил без разрешение.

3 Атаки и злоупотреби в уеб

3.1 DoS и DDoS атаки

DoS (Denial of Service — отказ на услуга) е атака, която цели да направи сайт или друга услуга недостъпна. Един от начините е претоварване с огромен брой заявки.

Пример: Малък магазин има една каса. Ако много хора поискат обслужване едновременно, касата не може да обслужи всички. По подобен начин сървърът може да не успее да обработи прекомерния брой заявки.

DDoS (Distributed Denial of Service — разпределен отказ на услуга) се извършва едновременно от множество компютри или други устройства.

За такава атака може да се използва **ботнет** — мрежа от заразени устройства, управлявани дистанционно без знанието на собствениците им.

Защитата включва филтриране на злонамерения трафик и мерки за ограничаване на претоварването.

Важно: Голямото натоварване от действителни посетители не е непременно атака.

3.2 Sniffing

Sniffing е събиране и прихващане на данни, предавани по мрежата. Ако съдържанието не е криптирано, при прихващането му могат да бъдат прочетени пароли, съобщения и друга чувствителна информация.

Пример: Данни, изпратени чрез обикновена HTTP връзка в обществена Wi-Fi мрежа, могат да бъдат прочетени при прихващане на трафика.

Криптирането на комуникацията ограничава този риск.

3.3 IP Spoofing

IP Spoofing е подправяне на IP адреса на подателя в мрежови пакети. Създава се впечатление, че пакетите са изпратени от друго устройство.

Пример: Това прилича на изпращане на писмо с подправен адрес на подателя.

Техниката може да служи за прикриване на източника на трафика или като част от други атаки.

3.4 Ботове

Ботът е програма, която изпълнява автоматично задачи в интернет. Полезните ботове например обхождат страници за търсачките. Злонамерените могат да изпращат спам или да участват в атаки.

3.5 XSS

XSS (Cross-Site Scripting) е атака, при която чрез уязвим уеб сайт в браузъра на посетителя се изпълнява злонамерен скрипт. Това може да стане при небезопасна обработка и показване на въведено съдържание.

Пример: В коментар е добавен код, който уязвимият сайт позволява да се изпълни при отваряне на страницата.

Последиствията могат да включват промяна на съдържанието или злоупотреба с данни и действия на потребителя.

3.6 SQL Injection

SQL Injection е атака, при която чрез неправилно обработени входни данни се променя заявка към базата данни на сайта.

Пример: Текст, въведен във формуляр, се обработва от уязвимия сайт като част от команда към базата данни.

Това може да доведе до неоторизиран достъп, разкриване, промяна или изтриване на информация.

3.7 Отвличане на потребителска сесия

При **Session hijacking** се злоупотребява с активната сесия на потребител, така че друго лице да извършва действия от негово име.

Пример: Откраднат идентификатор на активна сесия се използва за достъп до профил без повторно въвеждане на паролата. Кражбата на сесийни бисквитки е един от начините за такава злоупотреба.

3.8 DNS отравяне

DNS свързва имената на сайтовете с техните IP адреси. При **DNS poisoning** се подменят DNS данни и потребителят може да бъде насочен към неправилен сървър.

Пример: Въведено е правилното име на сайт, но подменен DNS запис насочва към фалшива страница.

3.9 Фишинг

Фишингът е измама, при която някой се представя за доверена организация или човек, за да получи пароли, лични данни или платежна информация.

Пример: Получавате съобщение „Профилът ви ще бъде закрит! Потвърдете данните си.“ Връзката отваря фалшива страница, която прилича на истинската.

За предпазване проверявайте адреса на сайта, не отваряйте подозрителни връзки и прикачени файлове и не изпращайте пароли чрез съобщения. При съмнение използвайте познатия адрес на услугата.

4 Бисквитки

Бисквитката (cookie) е малко количество данни, което браузърът съхранява за даден сайт и може да изпраща обратно при следващи заявки.

Бисквитките служат за запомняне на настройки, разпознаване на потребителска сесия, поддържане на количка за покупки и анализ на посещенията.

4.1 Видове според продължителността

Сесийни бисквитки — обикновено се премахват при приключване на браузърната сесия. При възстановяване на предишна сесия някои браузри могат да ги запазят.

Постоянни бисквитки — съхраняват се до определен срок или до изтриването им.

4.2 Видове според това кой ги задава

Бисквитки на първа страна — задават се от посещавания сайт.

Бисквитки на трета страна — задават се от друг сайт чрез вградено съдържание или услуги. Могат да се използват за реклама и проследяване.

Тези класификации не се изключват. Бисквитка на първа страна може да бъде сесийна или постоянна.

4.3 Рискове и управление

Кражба на бисквитки: Кражбата на валидна бисквитка, удостоверяваща активна сесия, може да позволи достъп до чужд профил. Не всяка бисквитка дава такъв достъп.

Отравяне на бисквитки (Cookie Poisoning): Променят се данни в бисквитка с цел да се повлияе на уязвим сайт.

Пример: Стойността „цена=100“ е променена на „цена=1“. Правилно разработеният сайт проверява цената на сървъра и не се доверява на променената бисквитка.

Потребителят може да изтрива или ограничава бисквитки чрез настройките на браузъра. Това може да повлияе на някои функции на сайта.

Проследяване чрез бисквитки: Бисквитките могат да съдържат идентификатор, чрез който се разпознава браузърът при следващи посещения. Когато една и съща външна услуга е вградена в различни сайтове, бисквитките на трета страна могат да подпомогнат свързването на посещенията и изграждането на профил на интересите на потребителя. Настройките за защита от проследяване в браузъра могат да ограничат това.

5 Уеб маяци

Уеб маякът (web beacon) е малко, често почти невидимо изображение, вградено в страница или имейл. Може да е с размер **1×1 пиксел**.

Използва се за статистика и проследяване на зареждането на съдържание.

При зареждането на маяка към външния сървър се изпраща заявка. Тя може да предостави информация като IP адрес, време на зареждане и данни за браузъра. В съчетание с бисквитки или други идентификатори тази информация може да се използва за проследяване на посещенията и интересите на потребителя.

Пример: При отваряне на имейл се зарежда изображение от външен сървър. Това може да подсказва, че съобщението е отворено, но не доказва, че е прочетено.

Уеб маякът сам по себе си не е вирус. Блокирането на външни изображения в имейли може да ограничи този вид проследяване.

6 Поверителност на потребителите

Сайтовете могат да събират лични данни чрез регистрации, поръчки и формуляри за контакт. Тези данни трябва да бъдат защитени от неразрешен достъп. Потребителите трябва да получават разбираема информация за използването на данните им и за бисквитките на сайта.

7 SSL и TLS

Криптирането преобразува информацията във вид, който може да бъде разчетен с подходящия ключ.

TLS е съвременният протокол за защита на връзката. **SSL** е негов предшественик, но названието „SSL сертификат“ все още се използва широко.

При **HTTPS** връзката между браузъра и сървъра е защитена чрез TLS.

7.1 Установяване на защитена връзка

Браузърът проверява сертификата на сайта. При успешно установена HTTPS връзка данните между браузъра и сървъра се предават в криптиран вид.

Адресът започва с **https://**. Браузърът предоставя информация за защитата на връзката, но иконата невинаги е катинар.

Важно: HTTPS защитава връзката, но не доказва, че сайтът е честен или съдържанието му е достоверно.

7.2 Видове сертификати

Самоподписан сертификат: Подписан е от самия издател. Използва се например за тестове. Браузърът обикновено предупреждава, ако сертификатът не е добавен като доверен.

Сертификат от сертифициращ орган (CA): Издава се след съответните проверки. Може да бъде безплатен или платен. Приема се без предупреждение, когато е валиден за домейна и веригата му води до доверен орган.

8 CAPTCHA

CAPTCHA е тест или механизъм за разграничаване на хора от автоматизирани програми.

Примери са въвеждане на изкривени символи и избор на изображения по условие. CAPTCHA се използва за ограничаване на спам и автоматизирани злоупотреби с регистрации, коментари и формуляри.

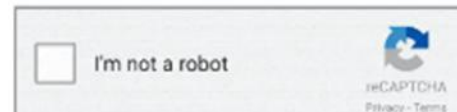
Примери за CAPTCHA с изкривени символи



При визуални тестове е важно да има достъпна алтернатива, **например** звукова проверка. **reCAPTCHA** е услуга на Google, която може да бъде интегрирана в сайт чрез подходяща приставка или код.

Терминологично уточнение: В учебната програма CAPTCHA е обозначена като „**публичен ключ за сигурност**“.

CAPTCHA е механизъм за разграничаване на хора от автоматизирани програми, а не криптографски публичен ключ. Тя не осигурява абсолютна защита срещу ботове.



9 Средства за повишаване на сигурността

Защитата е комплексен процес и не може да бъде осигурена само с един инструмент.

9.1 Обновяване на софтуера

Редовно се обновяват CMS, темите, приставките и сървърният софтуер.

9.2 Редовно архивиране

Създават се резервни копия на файловете и базата данни. Те позволяват възстановяване при повреда, изтриване или пробив.

9.3 Проверка за уязвимости

Специализирани инструменти проверяват за слабости и неправилни настройки на сайта и сървъра.

9.4 SSL и TLS сертификат

HTTPS защитава информацията при предаването ѝ между браузъра и сървъра.

9.5 Управление на достъпа

За защита се използват силни пароли, ограничени административни права и двуфакторна автентикация.

Двуфакторната автентикация (2FA) изисква два различни фактора за потвърждаване на самоличността.

- Нещо, което потребителят **знае** — например парола.
- Нещо, което **притежава** — например телефон с приложение за генериране на кодове.

Пример: При вписване потребителят въвежда паролата си, а след това еднократен код от приложение на телефона. Така само откраднатата парола обикновено не е достатъчна за достъп.

Важно: Парола и таен въпрос не са два различни фактора — и двете са нещо, което потребителят знае.

9.6 Проверка на входните данни

Данните от формуляри трябва да се обработват безопасно, за да не позволяват изпълнение на злонамерени команди или скриптове.

9.7 Защитни приставки

Приставката (plug-in) е допълнителен модул, който разширява възможностите на CMS. Защитните приставки могат да ограничават спам, да проверяват за злонамерено съдържание и да добавят CAPTCHA.

9.8 Наблюдение на сайта

Следи се за необичайна активност и признаци като невъзможност за достъп до административната част, неочаквана промяна на съдържанието, пренасочване към непознат сайт, предупреждения от браузъра и сигнали от хостинг доставчика или потребителите.

Тези признаци изискват проверка, но не доказват сами по себе си атака.

10 Правила за безопасна работа

- Използвайте доверени сайтове, особено при предоставяне на лична или платежна информация.
- Проверявайте внимателно адреса на сайта и предупрежденията на браузъра.
- Не отваряйте подозрителни връзки и прикачени файлове.
- Изтегляйте програми от проверени източници.
- Поддържайте софтуера актуален.
- Използвайте дълги и сложни пароли.

Практическа задача: Проверка на сигурността и поверителността

1. Отворете своя учебен сайт. Проверете дали адресът започва с https:// и дали браузърът показва предупреждение за връзката.
2. Чрез информацията за сайта в браузъра отворете данните за сертификата. Намерете за кой домейн е издаден, кой го е издал и какъв е срокът му на валидност.
3. Отворете настройките на браузъра за бисквитки и данни на сайтовете. Намерете записаните данни за своя учебен сайт.
4. Изтрийте данните само за този сайт и го заредете отново. Проверете дали трябва да влезете отново в профила си или дали са променени запомнени настройки.
5. Намерете настройката за ограничаване на бисквитки на трета страна или защита от проследяване. Приложете я и проверете дали използваният сайт продължава да работи нормално.