**SECURİTY AND PASSWORD**

Introduction

Security is the state of being free from danger or threat. There are 3 main types of security in computing:

**1. Physical Security:** Using physical barriers to prevent unauthorized access to data (like locking the door of the server room).  
**2. Software Security:** Fixing flaws in your application that could grant attackers unwanted levels of access to your systems.  
**3. Network Security:** Security of networked services (websites, [databases](https://lms.clarusway.com/mod/lesson/view.php?id=995" \o "Databases), etc).

The computer is like a castle with walls, inside and outside are very different. The bad guy cannot just access the bytes outside the computer but inside the computer at will. The bad guy needs to work at it.

A couple of bad guy strategies:

* obtain a password allowing access
* trick the computer into running bad guy code

| **metin içeren bir resim  Açıklama otomatik olarak oluşturuldu** |
| --- |
| *Bad guy will want to access your castle from open doors (network)* |

**Tanıtım**  
Güvenlik, tehlike veya tehditten uzak olma durumudur. Bilgi işlemde 3 ana güvenlik türü vardır:  
  
1. Fiziksel Güvenlik: Verilere yetkisiz erişimi engellemek için fiziksel engellerin kullanılması (sunucu odasının kapısının kilitlenmesi gibi).  
2. Yazılım Güvenliği: Saldırganların sistemlerinize istenmeyen düzeylerde erişmesine izin verebilecek uygulamanızdaki kusurları düzeltme.  
3. Ağ Güvenliği: Ağ bağlantılı hizmetlerin güvenliği (web siteleri, veritabanları vb.).  
  
Bilgisayar duvarları olan bir kale gibidir, içi ve dışı çok farklıdır. Kötü adam sadece bilgisayarın dışındaki baytlara değil, bilgisayarın içindeki baytlara istediği zaman erişebilir. Kötü adamın üzerinde çalışması gerekiyor.  
  
Birkaç kötü adam stratejisi:  
  
Erişime izin veren bir şifre alın  
Bilgisayarı kötü adam kodu çalıştırması için kandırmak

**Access Control**

Access Control is a framework for controlling who has access to what resources on a system. There are many ways to implement Access Control, but the three basic principles of Access Control are **Identification**, **Authentication**, and **Authorization**.

* **Identification:** Who is this person?
* **Authentication:** Is this the person who he claims to be?
* **Authorization:** Is this person allowed to perform this action?

**Giriş kontrolü**

Erişim Kontrolü, bir sistemde kimin hangi kaynaklara erişimi olduğunu kontrol etmek için bir çerçevedir. Erişim Denetimini uygulamanın birçok yolu vardır, ancak Erişim Denetiminin üç temel ilkesi Tanımlama, Kimlik Doğrulama ve Yetkilendirmedir.  
  
Kimlik: Bu kişi kim?  
Doğrulama: Olduğunu iddia ettiği kişi bu mu?  
Yetkilendirme: Bu kişinin bu eylemi gerçekleştirmesine izin veriliyor mu?

**Passwords**

Passwords are the de facto form of Authentication for computers, but they aren’t a perfect solution. Passwords are hard to remember and surprisingly easy for computers to guess.

There are some problems for passwords:

* People use same passwords for different accounts,
* People use simple passwords that are easy to guess,
* Passwords are hard to remember.

Solutions to these problems:

* Using a password manager,
* Changing passwords regularly,
* Using multi-step authentication.

**Şifreler**

Parolalar, bilgisayarlar için fiili Kimlik Doğrulama biçimidir, ancak mükemmel bir çözüm değildir. Parolaları hatırlamak zordur ve bilgisayarların tahmin etmesi şaşırtıcı derecede kolaydır.  
  
Şifreler için bazı sorunlar var:  
  
İnsanlar farklı hesaplar için aynı şifreleri kullanır,  
İnsanlar, tahmin edilmesi kolay basit şifreler kullanır,  
Şifreleri hatırlamak zordur.  
Bu sorunların çözümleri:  
  
Bir şifre yöneticisi kullanarak,  
Şifreleri düzenli olarak değiştirmek,  
Çok adımlı kimlik doğrulamayı kullanma.

**Phishing**

**Phishing** is the fraudulent attempt to obtain sensitive information such as usernames, passwords, and credit card details by disguising oneself as a trustworthy entity in an electronic communication. Typically carried out by email spoofing or instant messaging, it often directs users to enter personal information at a fake website that matches the look and feel of the legitimate site.

|  |
| --- |
| *Phishing web site acting like Paypal's official website* |

Phishing is an example of social engineering techniques being used to deceive users. Users are often lured by communications purporting to be from trusted parties such as social web sites, auction sites, banks, online payment processors or IT administrators. The above screenshot belongs to a phishing site, not the genuine PayPal site. If you type your username and password at this fake site, your credentials will be sent to the bad guy and then he will gain access to your account.

Q: Explain Phishing and how to prevent it.  
A: Phishing is a Cyberattack in which a hacker disguises as a trustworthy person or business and attempt to steal sensitive financial or personal information through fraudulent email or instant message.  
You can prevent Phishing attacks by using the following practices:

* Don’t enter sensitive information in the webpages that you don’t trust
* Verify the site’s security
* Use Firewalls
* Use AntiVirus Software that has Internet Security
* Use Anti-Phishing Toolbar

**E-dolandırıcılık**

Kimlik avı, elektronik bir iletişimde kendini güvenilir bir varlık kılığına sokarak kullanıcı adları, şifreler ve kredi kartı bilgileri gibi hassas bilgileri elde etmeye yönelik dolandırıcılık girişimidir. Tipik olarak e-posta sahtekarlığı veya anlık mesajlaşma yoluyla gerçekleştirilen bu işlem, kullanıcıları genellikle yasal sitenin görünümü ve hissi ile eşleşen sahte bir web sitesine kişisel bilgileri girmeye yönlendirir.  
  
  
Paypal'ın resmi web sitesi gibi davranan kimlik avı web sitesi  
Kimlik avı, kullanıcıları aldatmak için kullanılan sosyal mühendislik tekniklerine bir örnektir. Kullanıcılar genellikle sosyal web siteleri, açık artırma siteleri, bankalar, çevrimiçi ödeme işlemcileri veya BT yöneticileri gibi güvenilir taraflardan geldiği iddia edilen iletişimlerle cezbedilir. Yukarıdaki ekran görüntüsü, gerçek PayPal sitesine değil, bir kimlik avı sitesine aittir. Bu sahte siteye kullanıcı adınızı ve şifrenizi yazarsanız, kimlik bilgileriniz kötü adama gönderilecek ve ardından hesabınıza erişim kazanacaktır.  
  
S: Kimlik Avını ve nasıl önleneceğini açıklayın.  
C: Kimlik Avı, bir bilgisayar korsanının güvenilir bir kişi veya işletme kılığına girdiği ve dolandırıcılık amaçlı e-posta veya anlık ileti yoluyla hassas finansal veya kişisel bilgileri çalmaya çalıştığı bir Siber Saldırıdır.

Aşağıdaki uygulamaları kullanarak Phishing saldırılarını önleyebilirsiniz:  
Güvenmediğiniz web sayfalarına hassas bilgiler girmeyin  
Sitenin güvenliğini doğrulayın  
Güvenlik Duvarlarını Kullan  
İnternet Güvenliğine Sahip AntiVirüs Yazılımı Kullanın  
Kimlik Avı Önleme Araç Çubuğunu Kullan

**Malware**

The term **malware** is a contraction of **mal**icious soft**ware**. Put simply, malware is any piece of software that was written with the intent of damaging devices, stealing data, and generally causing a mess. Viruses, trojans, spyware, and ransomware are among the different kinds of malware.

A **computer virus** is a type of malicious code or program written to alter the way a computer operates and is designed to **spread** from one computer to another.

A Trojan horse or **Trojan** is a type of malware that is often disguised as legitimate software. Trojans can be employed by cyber-thieves and hackers trying to gain access to users' systems. Users are typically tricked by some form of social engineering into loading and executing Trojans on their systems.

**Spyware** is a type of malware that's hard to detect. It collects information about your surfing habits, browsing history, or personal information (such as credit card numbers), and often uses the Internet to pass this information along to third parties without you knowing.

**Ransomware Trojan** is a type of cyberware that is designed to extort money from a victim. Often, ransomware will demand a payment in order to undo changes that the Trojan virus has made to the victim’s computer.

|  |
| --- |
| *Bad guy* |

Q: Define Spyware.  
A: Spyware is a malware that aims to steal data about the organization or person. This malware can damage the organization's computer system.

**Kötü amaçlı yazılım**

Kötü amaçlı yazılım terimi, kötü amaçlı yazılımların kısaltılmış halidir. Basitçe söylemek gerekirse, kötü amaçlı yazılım, cihazlara zarar vermek, verileri çalmak ve genellikle bir karışıklığa neden olmak amacıyla yazılmış herhangi bir yazılım parçasıdır. Virüsler, truva atları, casus yazılımlar ve fidye yazılımları, farklı kötü amaçlı yazılım türleri arasındadır.  
  
Bilgisayar virüsü, bir bilgisayarın çalışma şeklini değiştirmek için yazılmış ve bir bilgisayardan diğerine yayılmak üzere tasarlanmış bir tür kötü amaçlı kod veya programdır.  
  
Truva atı veya Truva atı, genellikle meşru yazılım olarak gizlenen bir tür kötü amaçlı yazılımdır. Truva atları, kullanıcıların sistemlerine erişmeye çalışan siber hırsızlar ve bilgisayar korsanları tarafından kullanılabilir. Kullanıcılar genellikle bir tür sosyal mühendislik tarafından sistemlerine Truva atları yüklemek ve yürütmek için kandırılır.  
  
Casus yazılım, tespit edilmesi zor bir tür kötü amaçlı yazılımdır. Gezinme alışkanlıklarınız, göz atma geçmişiniz veya kişisel bilgileriniz (kredi kartı numaraları gibi) hakkında bilgi toplar ve genellikle bu bilgileri sizin haberiniz olmadan üçüncü taraflara iletmek için İnternet'i kullanır.  
  
Fidye Yazılım Truva Atı, bir kurbandan zorla para almak için tasarlanmış bir tür siber yazılımdır. Genellikle fidye yazılımları, Truva atı virüsünün kurbanın bilgisayarında yaptığı değişiklikleri geri almak için bir ödeme talep eder.  
  
  
Kötü adam  
S: Casus Yazılımı tanımlayın.  
C: Casus yazılım, kuruluş veya kişi hakkındaki verileri çalmayı amaçlayan bir kötü amaçlı yazılımdır. Bu kötü amaçlı yazılım, kuruluşun bilgisayar sistemine zarar verebilir.

**SQL Injection-XSS-CSRF**

**SQL injection** is a code injection technique that might destroy your database. This type of attack usually occurs when you ask a user for input, like their user-name/user-id, and instead of a name/id, the user (bad guy) gives you an SQL statement that you will unknowingly run on your database.

**Cross-Site Scripting (XSS)** attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end-user.

**Cross-site Request Forgery (CSRF)** is a very common vulnerability. It's an attack that forces a user to execute unwanted actions on a web application in which the user is currently authenticated.

|  |
| --- |
| *Injecting SQL querry to web site form* |

Q: Explain SQL Injection and how to prevent it.  
A: SQL Injection (SQLi) is a code injection attack where an attacker manipulates the data being sent to the server to execute malicious SQL statements to control a web application’s database server, thereby accessing, modifying and deleting unauthorized data. This attack is mainly used to take over database [servers](https://lms.clarusway.com/mod/lesson/view.php?id=1015" \o "Servers).  
You can prevent SQL Injection attacks by using the following practices:

* Use prepared statements
* Use Stored Procedures
* Validate user input

**SQL Enjeksiyon-XSS-CSRF**

SQL enjeksiyonu, veritabanınızı yok edebilecek bir kod enjeksiyon tekniğidir. Bu tür bir saldırı genellikle bir kullanıcıdan kullanıcı adı/kullanıcı kimliği gibi bir girdi istediğinizde ve ad/kimlik yerine kullanıcı (kötü adam) size bilmeden çalıştıracağınız bir SQL ifadesi verdiğinde gerçekleşir. Veri tabanı.  
  
Siteler Arası Komut Dosyası Çalıştırma (XSS) saldırıları, kötü amaçlı komut dosyalarının normalde zararsız ve güvenilir web sitelerine enjekte edildiği bir tür enjeksiyondur. XSS saldırıları, bir saldırgan, genellikle tarayıcı tarafı komut dosyası biçiminde kötü amaçlı kodu farklı bir son kullanıcıya göndermek için bir web uygulaması kullandığında meydana gelir.  
  
Siteler Arası İstek Sahteciliği (CSRF) çok yaygın bir güvenlik açığıdır. Bir kullanıcıyı, şu anda kimliğinin doğrulandığı bir web uygulamasında istenmeyen eylemler yürütmeye zorlayan bir saldırıdır.  
  
  
SQL sorgusunu web sitesi formuna enjekte etme  
S: SQL Injection'ı ve nasıl önleneceğini açıklayın.  
C: SQL Enjeksiyonu (SQLi), bir saldırganın bir web uygulamasının veritabanı sunucusunu kontrol etmek için kötü niyetli SQL ifadeleri yürütmek için sunucuya gönderilen verileri manipüle ettiği ve böylece yetkisiz verilere eriştiği, değiştirdiği ve sildiği bir kod enjeksiyon saldırısıdır. Bu saldırı esas olarak veritabanı sunucularını ele geçirmek için kullanılır.  
Aşağıdaki uygulamaları kullanarak SQL Injection saldırılarını önleyebilirsiniz:  
Hazırlanmış ifadeleri kullanın  
Saklı Prosedürleri Kullanın  
Kullanıcı girişini doğrula

**Encryption**

**Encryption** is a way of scrambling data so that only authorized parties can understand the information. In technical terms, it is the process of converting **plaintext** (the original bytes (text, image, etc.)) to **ciphertext** (encrypted text). In simpler terms, encryption takes readable data and alters it so that it appears random. Encryption requires the use of an **encryption key** that is a set of mathematical values known only by the sender and the recipient of the encrypted message know.

**Şifreleme**

Şifreleme, yalnızca yetkili tarafların bilgileri anlayabilmesi için verileri karıştırmanın bir yoludur. Teknik anlamda düz metinlerin (orijinal baytların (metin, resim vb.)) şifreli metne (şifreli metin) dönüştürülmesi işlemidir. Daha basit bir ifadeyle, şifreleme, okunabilir verileri alır ve rastgele görünecek şekilde değiştirir. Şifreleme, yalnızca şifreli mesajın göndericisi ve alıcısı tarafından bilinen bir dizi matematiksel değerden oluşan bir şifreleme anahtarının kullanılmasını gerektirir.

**Decryption**

**Decryption** is a process of converting encoded/encrypted data (ciphertext) in a form that is readable and understood by a human or a computer. This method is performed by un-encrypting the text manually or by using keys that were used to encrypt the original data.

|  |
| --- |

**Şifre çözme**  
Şifre çözme, kodlanmış/şifrelenmiş verilerin (şifreli metin) bir insan veya bilgisayar tarafından okunabilir ve anlaşılabilir bir biçimde dönüştürülmesi işlemidir. Bu yöntem, metnin şifresini manuel olarak çözerek veya orijinal verileri şifrelemek için kullanılan anahtarları kullanarak gerçekleştirilir.

**Hashing**

Hashing is the process of converting a given key to another value. A **hash function** is used to generate the new value according to a mathematical algorithm. The result of a hash function is known as a **hash value** or simply, a **hash**.

Hashing is also used in data encryption (we will learn in the following lessons). Passwords can be stored in the form of their hashes so that even if a database is breached, plaintext passwords are not accessible. **MD5**, **SHA-1** and **SHA-2** are popular cryptographic hashes.

|  |
| --- |

Q: What is the hashing function?  
A: The hashing function is a one-way mathematical function. This means that it can be used to encode data, but it cannot decode data. Its primary purpose is not to encrypt the ciphertext; rather, its primary purpose is to prove that the message in the ciphertext has not changed in any way, shape or form. This is also referred to as “message integrity.” If the mathematical function has changed in any way, the message has then changed.

**Hashing**

Hashing, verilen bir anahtarı başka bir değere dönüştürme işlemidir. Matematiksel bir algoritmaya göre yeni değeri üretmek için bir hash fonksiyonu kullanılır. Bir hash fonksiyonunun sonucu, bir hash değeri veya basitçe bir hash olarak bilinir.  
  
Hashing, veri şifrelemede de kullanılır (ilerideki derslerde öğreneceğiz). Parolalar, bir veri tabanı ihlal edilse bile düz metin parolalara erişilemeyecek şekilde hashleri ​​şeklinde saklanabilir. MD5, SHA-1 ve SHA-2, popüler şifreleme karmalarıdır.

S: Karma işlevi nedir?  
C: Karma işlevi, tek yönlü bir matematiksel işlevdir. Bu, verileri kodlamak için kullanılabileceği, ancak verilerin kodunu çözemeyeceği anlamına gelir. Birincil amacı, şifreli metni şifrelemek değildir; Asıl amacı, şifreli metindeki mesajın hiçbir şekilde, şekil ve biçimde değişmediğini kanıtlamaktır. Buna “mesaj bütünlüğü” de denir. Matematiksel fonksiyon herhangi bir şekilde değiştiyse, mesaj da değişmiştir.

**Cryptocurrency**

**Cryptocurrency** is an internet-based medium of exchange which uses cryptographical functions to conduct financial transactions. Cryptocurrencies leverage blockchain technology to gain decentralization, transparency, and immutability.

**Blockchain** is the technology that enables the existence of cryptocurrency. **Bitcoin** is the name of the best-known cryptocurrency, the one for which blockchain technology was invented. A cryptocurrency is a medium of exchange, such as the US dollar, but it is digital and uses encryption techniques to control the creation of monetary units and to verify the transfer of funds.

**Kripto para**  
Kripto para birimi, finansal işlemleri yürütmek için kriptografik işlevleri kullanan internet tabanlı bir değişim aracıdır. Kripto para birimleri, ademi merkeziyetçilik, şeffaflık ve değişmezlik elde etmek için blok zinciri teknolojisinden yararlanır.  
  
Blockchain, kripto para biriminin varlığını sağlayan teknolojidir. Bitcoin, blockchain teknolojisinin icat edildiği en iyi bilinen kripto para biriminin adıdır. Bir kripto para birimi, ABD doları gibi bir değişim aracıdır, ancak dijitaldir ve para birimlerinin oluşturulmasını kontrol etmek ve fon transferini doğrulamak için şifreleme teknikleri kullanır.