Securing Applications and Data

AP Cybersecurity · Vocabulary in context

Word	Example
Applications /ˌæplɪˈkeɪʃnz/	**Applications** like word processors help you get work done.
administrative /ədˈmɪnɪstrətɪv/	**Administrative** rights let you install software.
injection attack /ɪnˈdʒekʃn əˈtæk/	An **injection attack** sneaks commands into a form.
Data validation /ˈdeɪtə ˌvælɪˈdeɪʃn/	**Data validation** checks that input follows the rules.
Cross-site scripting (XSS) /krɒs saɪt ˈskrɪptɪŋ/	**Cross-site scripting (XSS)** runs an attacker's script in your browser.
parameterised queries /ˌpærəˈmetəraɪzd ˈkwɪərɪz/	**Parameterised queries** stop SQL injection.
Buffer overflow /ˈbʌfə ˌəʊvəˈfləʊ/	A **buffer overflow** writes past the end of the memory space.
buffer /ˈbʌfə/	A **buffer** holds data until the printer is ready.
Directory traversal /daɪˈrektəri træˈvɜːsl/	**Directory traversal** uses ../ to reach hidden files. ../
at rest /æt rest/	Data **at rest** is stored on a disk.
in transit /ɪn ˈtrænsɪt/	Data **in transit** is moving across a network.
in use /ɪn juːs/	Data **in use** is being worked on by a program.
regulated /ˈregjʊleɪtɪd/	Banks are **regulated** by strict laws.

exercises.lol exercises.com.cn

Word	Example
compliance /kəmˈplaɪəns/	**Compliance** means following the rules.
personally identifiable information (PII) /ˈpɜːsənəli aɪˈdentɪfaɪəbl ˌɪnfəˈmeɪʃn/	Your phone number is **personally identifiable information (PII)**.
protected health information (PHI) /prəˈtektɪd helθ ˌɪnfəˈmeɪʃn/	Medical records are **protected health information (PHI)**.
payment card information (PCI) /ˈpeɪmənt kɑːd ˌɪnfəˈmeɪʃn/	Card numbers are **payment card information (PCI)**.
Role-based (RBAC) /rəʊl beɪst/	In **role-based (RBAC)** access, teachers and students get different rights.
Rule-based (RuBAC) /ruːl beɪst/	In **rule-based (RuBAC)** access, rules such as "only 9 to 5" decide access. "only 9 to 5"
Discretionary (DAC) /dɪˈskreʃənəri/	In **discretionary (DAC)** access, the owner of a file decides who can open it.
Mandatory (MAC) /ˈmændətəri/	In **mandatory (MAC)** access, labels like "top secret" decide access. "top secret"
principle of least privilege /ˈprɪnsɪpl ɒv liːst ˈprɪvɪlɪdʒ/	The **principle of least privilege** gives each user only the rights they need.
Cryptography /krɪpˈtɒgrəfi/	**Cryptography** keeps messages secret.
plaintext /ˈpleɪntekst/	The message before encryption is **plaintext**.
key /kiː/	You need the **key** to decrypt the message.

Word	Example
ciphertext /'saɪfətekst/	The encrypted message is **ciphertext**.
keyspace /'ki:speɪs/	A larger **keyspace** makes a key harder to guess.
Symmetric encryption /sɪ'metrɪk en'krɪpʃn/	**Symmetric encryption** uses the same key to lock and unlock.
AES /ˌeɪ i: 'es/	**AES** is a common way to encrypt data with a shared key.
block cipher /blɒk 'saɪfə/	A **block cipher** encrypts data in fixed-size pieces.
Asymmetric encryption /ˌeɪsɪ'metrɪk en'krɪpʃn/	**Asymmetric encryption** uses a public key and a private key.
key pair /ki: peə/	A **key pair** has one public key and one private key.
public key /'pʌblɪk ki:/	Anyone can use your **public key**.
private key /'praɪvət ki:/	Keep your **private key** secret.
elliptic curve cryptography (ECC) /ɪ'lɪptɪk kɜ:v krɪp'tɒgrəfi/	**Elliptic curve cryptography (ECC)** gives strong security with short keys.
Secure by design /sɪ'kjʊə baɪ dɪ'zaɪn/	**Secure by design** means planning security from the start.
Secure by default /sɪ'kjʊə baɪ dɪ'fɒlt/	**Secure by default** means the safe settings are already on.
input sanitization /'ɪnpʊt ˌsænɪtaɪ'zeɪʃn/	**Input sanitization** removes dangerous characters from user input.

exercises.lol exercises.com.cn

Word	Example
* **special characters** /'speʃl 'kærɪktəz/	**Special characters** like ' and ; can break SQL commands. ' ; SQL
accounting /ə'kaʊntɪŋ/	**Accounting** records who did what and when.
honeypot /'hʌnɪpɒt/	A **honeypot** is a fake system that attracts attackers.
data loss prevention (DLP) /'deɪtə lɒs prɪ'venʃn/	**Data loss prevention (DLP)** stops secret files from leaving the company.
SQL injection /ˌes kju: 'el ɪn'dʒekʃn/	**SQL injection** runs an attacker's code in the database.