éPeople's Democratic Republic of Algeria

Ministery of Higher Education and Scientific Research

Ferhat Abbas University of Setif 1



Faculty of Sciences

Computer Science Department

**THEME**

Detecting SQL injection using Deep Learning

Realized by: Supervised by:

ZITOUNI AHMED FAOUZI DR. BENZINE MEHDI

SEDJAL MOHAMED AYMEN DHIAEDDINE

**2024/2025**

**Table of contenets**

General introduction

Chapter 1 SQL injection

1.1 Introduction

1.2 Web application

1.2.1 Definition…………………………………………………………………………………………………………

1.3 SQL injection………………………………………………………………………………………………………….

1.3.1 Definition6

1.3.2 How SQL Injection Works……………………………………………………….7

1.3.3 Impact of SQL Injection Attacks…………………………………………………

1.4 Techniques of SQL Injection…………………………………………………………….

1.4.1 Tautology-Based SQL Injection…………………………………………………….

1.4.2 Error-Based SQL Injection………………………………………………………….

#### 1.4.3 Blind SQL Injection…………………………………………………………………

**Figures list**

Figure 1.1 SQL Injection attack…………………………………………….

Figure 1.2 Prepared Statements exemple using php………………………….

Figure 1.3 Stored Procedure example using java…………………………………….

Figure 1.4 Input Validation example using java………………………………..

**Chapter 1**

SQL Injections

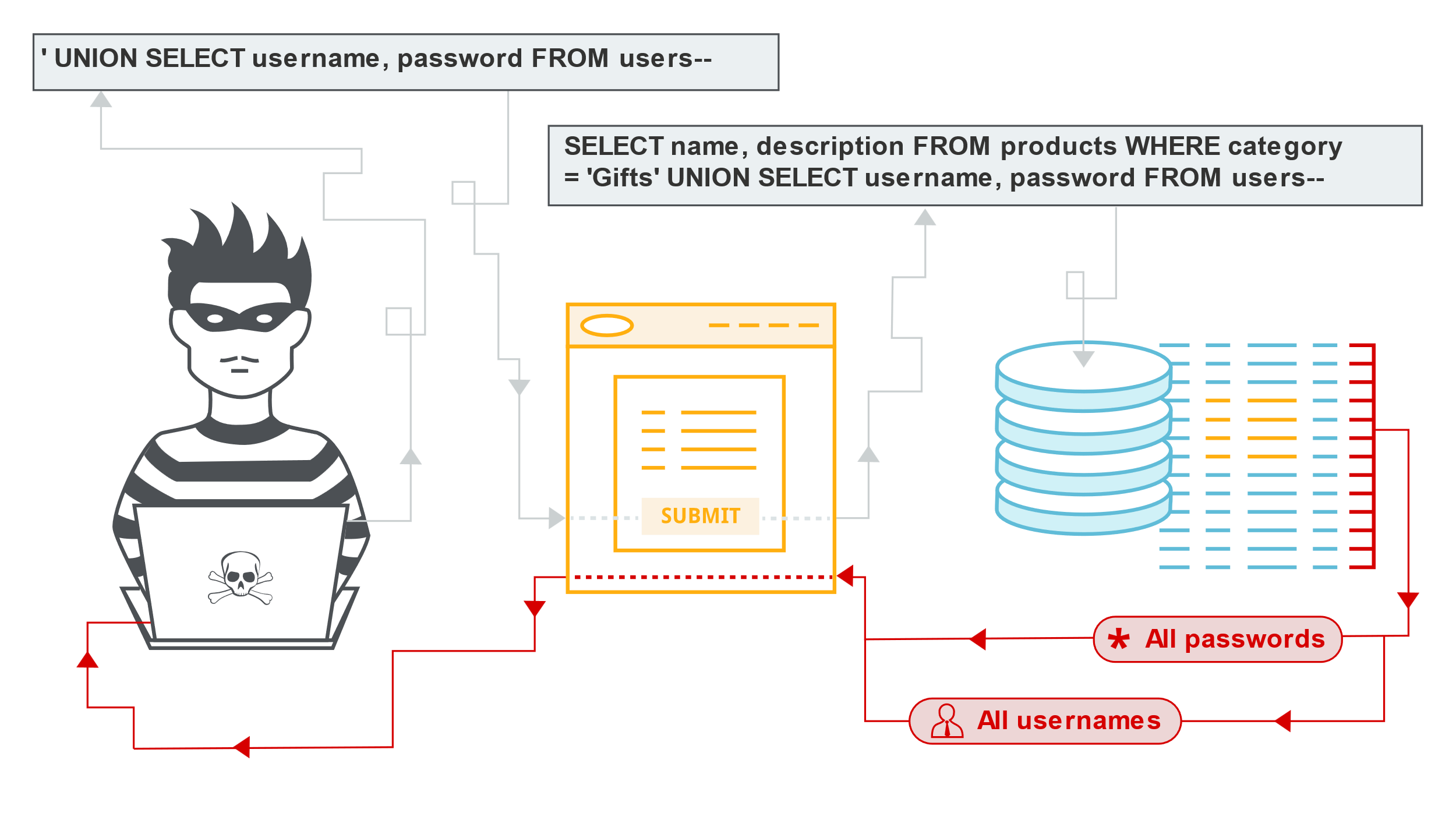
#### **1.1 Introduction**

With increasingly digital living, web applications are at the core of day to day life from managing finances and online purchasing to collaborating and communicating. This ease of the virtual world comes with inherent security challenges. Cyber attackers persistently evolve their methods to exploit weaknesses, thereby endangering unauthorized data access, downtime of services, and irreparable damage to reputation.

### **1.2 SQL injection**

#### **1.2.1 Definition**

A SQL injection attack consists of insertion or “injection” of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system. SQL injection attacks are a type of injection attack, in which SQL commands are injected into data-plane input in order to affect the execution of predefined SQL commands[[2].](#_[2]__)

**Figure 1.2** SQL Injection attack

**1.2.2 How SQL Injection Works**

It typically involves the following steps:

1. **Identification of vulnerable inputs:** Attackers first identify inputs within the web application that are vulnerable to SQL injection. These inputs could be text fields in a form, URL parameters, or any other input mechanisms.
2. **Crafting the malicious SQL query:** Once a vulnerable input is identified, attackers craft a SQL statement intended to be inserted into the query executed by the application. This statement is designed to modify the original SQL query to perform actions unintended by the application developers.
3. **Bypassing application security measures:** Attackers often have to bypass security measures like input validation or escaping special characters. They achieve this through techniques like string concatenation or utilizing SQL syntax to comment out parts of the original query.
4. **Executing the malicious query:** When the application executes the SQL query, it includes the attacker’s malicious input. This modified query can perform actions such as unauthorized viewing of data, deletion of data, or even database schema alterations.
5. **Extracting or manipulating data:** Depending on the attack, the outcome might be the extraction of sensitive information (like user credentials), altering existing data, adding new data, or even deleting significant portions of the database.
6. **Exploiting database server vulnerabilities:** Advanced SQL injections may exploit vulnerabilities in the database server, extending the attack beyond the database to the server level. This can include executing commands on the operating system or accessing other parts of the server’s file system.

This process leverages the dynamic execution of SQL in applications where user inputs are directly included in SQL statements without proper validation or escaping. It exploits the way SQL queries are constructed, often in a way that the developers did not anticipate[[3].](#_[3]_Bright_security)

##### **Real-Life SQL Injection Attack Examples**

Over the past 20 years, many SQL injection attacks have targeted large websites, business and social media platforms. Some of these attacks led to serious data breaches. A few notable examples are listed below[.](SQL#_[3]_OWASP_)

###### **Breaches Enabled by SQL Injection**

* **GhostShell attack**—hackers from APT group Team GhostShell targeted 53 universities using SQL injection, stole and published 36,000 personal records belonging to students, faculty, and staff.
* **Turkish government**—another APT group, RedHack collective, used SQL injection to breach the Turkish government website and erase debt to government agencies.
* **7-Eleven breach**—a team of attackers used SQL injection to penetrate corporate systems at several companies, primarily the 7-Eleven retail chain, stealing 130 million credit card numbers.
* **HBGary breach**—hackers related to the Anonymous activist group used SQL Injection to take down the IT security company’s website. The attack was a response to HBGary CEO publicizing that he had names of Anonymous organization members.

### **1.3 Techniques of SQL Injection**

#### **1.3.1 Error-Based SQL Injection**

**Error-based**[**SQL injection**](https://beaglesecurity.com/blog/vulnerability/sql-injection-vulnerability.html) is a type of security vulnerability and attack that occurs when an attacker injects malicious SQL statements into a web application’s input fields, causing the application to generate SQL errors.

These errors can reveal sensitive information about the application’s database structure, data, or configuration[[4]](#_[4]_Beagle_Security).

**How It Works:**

**Injection point:** An attacker identifies a vulnerable input field, such as a search box or login form, where user input is directly incorporated into SQL queries.

**Injecting malicious code:** The attacker inputs carefully crafted SQL code as part of their input. This code is designed to cause SQL syntax errors when the application processes it[[4].](Blind#_[4]_OWASP,_)

**Example**[[5]](#_[5]_Dafydd_Stittard)**: Conditional Errors in Oracle/MS-SQL**

|  |
| --- |
| SELECT 1/0 FROM dual  WHERE (SELECT username FROM all\_users WHERE username = 'DBSNMP') = 'DBSNMP'; |

**Explanation**:

1. **Subquery**:
   * The subquery (SELECT username FROM all\_users WHERE username = 'DBSNMP') checks if a user named DBSNMP exists in the all\_users table.
2. **Condition**:
   * If the user DBSNMP exists, the condition (SELECT username FROM all\_users WHERE username = 'DBSNMP') = 'DBSNMP' evaluates to TRUE.
3. **Error Induction**:
   * When the condition is TRUE, the database evaluates the expression 1/0, which causes a **divide-by-zero error**.
   * If the condition is FALSE (i.e., the user does not exist), the expression 1/0 is **not evaluated**, and no error occurs.

**Detection**:

* If the application returns an **HTTP 500 error** or a database error message, the attacker can infer that the condition is TRUE (i.e., the user DBSNMP exists).
* If no error occurs, the condition is FALSE (i.e., the user does not exist).

**Advanced Use Case: Data Exfiltration**

**Scenario**:

* A web application allows users to sort search results using a sort parameter:

|  |
| --- |
| /search.jsp?department=30&sort=ename |

The backend SQL query:

|  |
| --- |
| SELECT ename, job, deptno, hiredate FROM emp  WHERE deptno = ?  ORDER BY [param\_sort] DESC; |

**Malicious Injection**:

The attacker injects a payload into the sort parameter to test a condition:

|  |
| --- |
| /search.jsp?department=20&sort=(SELECT 1/0 FROM dual  WHERE (SELECT SUBSTR(MAX(object\_name),1,1) FROM user\_objects)='Y'); |

**Explanation**:

1. **Subquery**:
   * The subquery (SELECT SUBSTR(MAX(object\_name),1,1) FROM user\_objects) extracts the **first character** of the largest object name in the user\_objects table.
2. **Condition**:
   * If the first character is 'Y', the condition evaluates to TRUE, and the database attempts to evaluate 1/0, causing a **divide-by-zero error**.
   * If the first character is not 'Y', no error occurs, and the query returns results normally.
3. **Inference**:
   * The attacker can use this technique to **brute-force** each character of the object name by testing different values (e.g., 'A', 'B', 'C', etc.).

**1.3.2 Blind SQL Injection**

Blind SQL (Structured Query Language) injection is a type of [SQL Injection](https://owasp.org/www-community/attacks/SQL_Injection) attack that asks the database true or false questions and determines the answer based on the applications response. This attack is often used when the web application is configured to show generic error messages, but has not mitigated the code that is vulnerable to SQL injection.

When an attacker exploits SQL injection, sometimes the web application displays error messages from the database complaining that the SQL Query’s syntax is incorrect. Blind SQL injection is nearly identical to normal [SQL Injection](https://owasp.org/www-community/attacks/SQL_Injection), the only difference being the way the data is retrieved from the database. When the database does not output data to the web page, an attacker is forced to steal data by asking the database a series of true or false questions. This makes exploiting the SQL Injection vulnerability more difficult, but not impossible [[6].](Blind#_[6]_OWASP,_)

##### **1.3.2.1 Content-Based Blind SQL Injection**

**How It Works:**  
 Unlike traditional SQL injection, where database error messages expose data directly, blind SQL injection does not return query results to the user. Attackers exploit this by providing conditional queries and observing the application's response to infer data from the database.

**Technical Explanation:**  
 Blind SQL injection relies on evaluating conditions based on the application's responses. Attackers inject SQL conditions and observe response differences (e.g., message change or page behavior) to deduce data.

**Example:**

vulnerable web application allows the attacker to inject SQL on a URL parameter that fetches data based on an id. The attacker confirms the vulnerability by injecting true/false statements in the id parameter to identify between valid and invalid SQL queries.

The attacker first sends a request like:

|  |
| --- |
| http://newspaper.com/items.php?id=2 |

This executes:

|  |
| --- |
| SELECT title, description, body FROM items WHERE ID = 2; |

Next, the attacker tests for SQL injection by adding a false condition:

|  |
| --- |
| http://newspaper.com/items.php?id=2 and 1=2 |

The query becomes:

|  |
| --- |
| SELECT title, description, body FROM items WHERE ID = 2 AND 1 = 2; |

Since 1=2 is false, the page returns no content, confirming the injection.

Then, the attacker tests a true condition:

|  |
| --- |
| http://newspaper.com/items.php?id=2 and 1=1 |

The query becomes:

|  |
| --- |
| SELECT title, description, body FROM items WHERE ID = 2 AND 1 = 1; |

This question retrieves the anticipated data, revealing the vulnerability.Contrasting the output of these two injections, the attacker can determine that the page is vulnerable to SQL injection and proceed to pull data from the database[[6]](Blind#_[5]_OWASP,_).

**Explanation:**

Here, the attacker uses a spurious condition (and 1=2) to decide whether the page is vulnerable to SQL injection. Since no information is returned, the attacker confirms the vulnerability. A real condition (and 1=1) provides expected information, ascertaining that the injection has been successful. The attacker now iterates data, e.g., table names or other confidential data, using similar true/false conditions based on the database schema.

##### **1.3.2.2 Time-Based Blind SQL Injection**

**How It Works:**  
 In time-based blind SQL injection, attackers use SQL functions like **SLEEP()** to introduce a delay in the server’s response. If the delay occurs, it indicates the injected SQL condition is true; if not, it is false. This helps attackers extract data even when no visible content is returned.

**Technical Explanation:**  
The attacker sends queries that include conditional delays, such as:  
xyz' AND IF(1=1, SLEEP(5), 0) – The server delays for 5 seconds, confirming the condition is true.  
xyz' AND IF(1=2, SLEEP(5), 0) – No delay occurs, confirming the condition is false.

**Example:**

Consider a web application that retrieves user information based on a user ID provided in the URL:

|  |
| --- |
| http://example.com/user.php?id=1 |

The corresponding SQL query might be:

|  |
| --- |
| SELECT \* FROM users WHERE id = 1; |

If the application is vulnerable to Time-Based Blind SQL Injection, an attacker can manipulate the id parameter to include a time delay function.

**Malicious Injection:**

|  |
| --- |
| http://example.com/user.php?id=1; IF(1=1, SLEEP(5), 0); |

In this example, the injected SQL statement includes a conditional function that causes the database to pause for 5 seconds if the condition 1=1 is true.

**Explanation:**

Here, the attacker is inserting a conditional SQL function that will intentionally delay the database's response time. The inserted SQL query is:

|  |
| --- |
| SELECT \* FROM users WHERE id = 1; IF(1=1, SLEEP(5), 0); |

The IF(1=1, SLEEP(5), 0) function will evaluate the condition 1=1, which is always fulfilled. So the SLEEP(5) function will be invoked, and the database will take 5 seconds to reply.

If the application responds in 5 seconds, the attacker confirms successful injection and exposure of the application to Time-Based Blind SQL Injection.

The attackers may use this technique to provide educated guesses on the structure and content of the database even when direct extraction is not possible.

### **1.3.3 Tautology-Based SQL Injection**

The term ‘tautology’ originates from the field of logic, where it is used to describe a statement that is always true, regardless of the truth values of its components. In other words, a tautological statement is one that is true by virtue of its logical form alone [[7]](SQL#_[7]_Moxso,_).

**How It Works:**

This attack exploits the use of tautological SQL statements always result in true and thus bypasses authentication and other security measures.

**Technical Explanation:**  
 A tautology is a logical statement that remains true under any combination of values. Malicious users insert such statements into SQL queries, compelling the database to execute and authenticate unauthorized requests.

|  |
| --- |
| SELECT \* FROM users WHERE username = ‘admin’OR ‘1’=’1’ – AND password =’anything’; |

**OR '1'='1'** in this example guarantees the condition will always be true, giving access.  
Real-World Scenario: An attacker hacks a login form on a web page, bypassing user authentication and accessing an administrator account**.**

### **1.3.4 Union-Based SQL Injection**

**How It Works:**

The UNION operator is used in SQL to combine the results of two or more SELECT statements into a single result set. When a web application contains a SQL injection vulnerability that occurs in a SELECT statement, attackers can utilize this operator to insert an additional query and merge its outcome with the outcome of the initial query[[5].](#_[5]_Dafydd_Stittard)

**Technical Explanation:**

Using this method, malicious users can retrieve unauthorized data from the database. UNION-based SQL injection is widely supported by all the major database management systems (DBMS) and is generally the best way to extract specific database contents when query results are directly presented on the application interface.

#### **Example 1**[[8]](#_[8]_Justin_Clarke,)**: Extracting the Current Database User**

**Scenario**

A web application shows product information based on a product ID passed in the URL. The application is susceptible to SQL injection since it puts user input directly into the SQL query without sanitizing. The attacker finds such vulnerability and chooses to exploit it in order to get the current database user, which can assist them in knowing the access level they have and strategize future attacks.  
  
The attacker knows that the application has a database backend (for example, Microsoft SQL Server, MySQL, or Oracle) and wishes to extract the username of the account which issued the queries..

***Malicious Injection:***

The attacker sends the following malicious URL to the application:

|  |
| --- |
| http://www.victim.com/products.asp?id=12+union+select+NULL,system\_user,NULL,NULL |

**Explanation:**

1. **Original Query:**  
   The application executes the following query to retrieve product details:

|  |
| --- |
| SELECT id, type, description, price FROM products WHERE id = 12 |

**This query returns the details of the product with ID 12.**

1. **Injected Query:**  
   The attacker appends a UNION SELECT statement to the original query to retrieve the current database user:

|  |
| --- |
| UNION SELECT NULL, system\_user, NULL, NULL |

* + The UNION operator combines the results of the original query with the results of the injected query.
  + The system\_user function (or equivalent, depending on the database) retrieves the username of the current database user.
  + The NULL values are used to match the number of columns in the original query (since the injected query only needs one column for the username, but the original query returns four columns).

1. **Combined Query:**  
   The database executes the following combined query:

|  |
| --- |
| SELECT id, type, description, price FROM products WHERE id = 12  UNION  SELECT NULL, system\_user, NULL, NULL |

**Result:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Id** | **Type** | **Description** | **Price** |
| 12 | Book | SQL Injection Attacks | 50 |
| NULL | db\_user | NULL | NULL |

#### **Example 2: Extracting Multiple Rows from the customers Table**

**Scenario:**

A web application displays product details based on a product ID passed in the URL. The application is vulnerable to SQL injection because it directly incorporates user input into the SQL query without proper sanitization. The attacker discovers this vulnerability and decides to exploit it to extract sensitive customer data from the **customers** table in the database.

The attacker's goal is to retrieve the full list of customers (first and last names) from the database.

***Malicious Injection:***

The attacker sends the following malicious URL to the application:

|  |
| --- |
| http://www.victim.com/products.asp?id=12+union+select+userid,first\_name,second\_name,NULL+from+customers |

***Explanation:***

1. **Original Query:**  
   The application executes the following query to retrieve product details:

|  |
| --- |
| SELECT id, type, description, price FROM products WHERE id = 12 |

This query returns the details of the product with ID 12.

1. **Injected Query:**  
   The attacker appends a UNION SELECT statement to the original query to retrieve data from the customers table:

|  |
| --- |
| UNION SELECT userid, first\_name, second\_name, NULL FROM customers |

* + The UNION operator combines the results of the original query with the results of the injected query.
  + The NULL value is used to match the number of columns in the original query (since the customers table has only three columns, but the original query returns four columns).

1. **Combined Query:**  
   The database executes the following combined query:

|  |
| --- |
| SELECT id, type, description, price FROM products WHERE id = 12  UNION  SELECT userid, first\_name, second\_name, NULL FROM customers |

**Result:**

|  |  |  |  |
| --- | --- | --- | --- |
| id | **Type** | **Description** | **Price** |
| 12 | Book | SQL Injection Attacks | 50 |
| 1 | Charles | Smith | NULL |
| 2 | Lydia | Clayton | NULL |
| 3 | Bernard | Jones | NULL |

**4 Explanation of the Result:**

* The first row represents the product details from the original query.
* The subsequent rows represent the data extracted from **the customers** table, including **userid, first\_name**, and **second\_name**.
* The **NULL** value in the **Price** column is used to align the injected data with the original query's column structure.

### **1.4 Methods to prevent SQL Injection attacks.**

Attackers can use SQL injection on an application if it has dynamic database queries that use string concatenation and user supplied input. To avoid SQL injection flaws.

There are simple techniques for preventing SQL injection vulnerabilities and they can be used with practically any kind of programming language and any type of database [[9].](#_[7]_OWASP_Cheat)

#### **1.4.1 Prepared Statements (with Parameterized Queries)**

When developers are taught how to write database queries, they should be told to use prepared statements with variable binding (also known as parameterized queries). Prepared statements are simple to write and easier to understand than dynamic queries, and parameterized queries force the developer to define all SQL code first and pass in each parameter to the query later.

If database queries use this coding style, the database will always distinguish between code and data, regardless of what user input is supplied. Also, prepared statements ensure that an attacker cannot change the intent of a query, even if SQL commands are inserted by an attacker.

In PHP, PHP Data Objects (PDO) offer a more effective approach to database interactions. By providing methods that simplify parameterized queries, PDO ensures that user input is always treated as data rather than executable SQL code and enhances code readability and also ensures greater portability across multiple databases[.](#_[4]_OWASP_Cheat)

**Figure 1.3** Prepared Statements example using php[[10]](#_[4]_OWASP_Cheat)

< ?php

$dbh = new PDO('mysql:dbname=testdb;host=127.0.0.1', $user, $password);

$stmt = $dbh->prepare("INSERT INTO REGISTRY (name, value) VALUES (:name,:value)");

$stmt->bindParam(':name', $name);

$stmt->bindParam(':value', $value);

$stmt->execute();

#### **1.4.2 Stored Procedures**

Though stored procedures are not always safe from SQL injection, developers can use certain standard stored procedure programming constructs. This approach has the same effect as using parameterized queries, as long as the stored procedures are implemented safely (which is the norm for most stored procedure languages).

**Safe Approach to Stored Procedures :**

If stored procedures are needed, the safest approach to using them requires the developer to build SQL statements with parameters that are automatically parameterized, unless the developer does something largely out of the norm. The difference between prepared statements and stored procedures is that the SQL code for a stored procedure is defined and stored in the database itself, then called from the application.

Since prepared statements and safe stored procedures are equally effective in preventing SQL injection, your organization should choose the approach that makes the most sense for you.

The following code example uses Java’s implementation of the stored procedure interface (CallableStatement) to execute the same database query.

<?php  
$stmt = $dbh->prepare("CALL sp\_takes\_string\_returns\_string(?)");  
$value = 'hello';  
$stmt->bindParam(1, $value, PDO::PARAM\_STR|PDO::PARAM\_INPUT\_OUTPUT, 4000);   
  
// Call the stored procedure  
$stmt->execute();  
  
print "procedure returned: $value\n";  
?>

**Figure 1.4** Stored Procedure example using PHP[[11]](Prepared_statements#_[11]PHP_)

#### **1.4.3 Input Validation**

Input validation is performed to ensure only properly formed data is entering the workflow in an information system, preventing malformed data from persisting in the database and triggering malfunction of various downstream components.

Input validation should happen as early as possible in the data flow, preferably as soon as the data is received from the external party.

Data from all potentially untrusted sources should be subject to input validation, including not only Internet-facing web clients but also backend feeds over extranets, from [suppliers, partners, vendors or regulators](https://badcyber.com/several-polish-banks-hacked-information-stolen-by-unknown-attackers/), each of which may be compromised on their own and start sending malformed data.

Example validating the parameter "zip" using a regular expression :

<?php  
$email\_a = 'joe@example.com';  
$email\_b = 'bogus';  
  
if (filter\_var($email\_a, FILTER\_VALIDATE\_EMAIL)) {  
echo "Email address '$email\_a' is considered valid.\n";  
}  
if (filter\_var($email\_b, FILTER\_VALIDATE\_EMAIL)) {  
echo "Email address '$email\_b' is considered valid.\n";  
} else {  
echo "Email address '$email\_b' is considered invalid.\n";  
}  
?>

**Figure 1.5** Input validation example using PHP[[12]](Validation#_[12]PHP_,_)

#### **1.4.4 Escaping All User-Supplied Input**

In this approach, the developer will escape all user input before putting it in a query. It is very database specific in its implementation. This methodology is frail compared to other defenses, and we CANNOT guarantee that this option will prevent all SQL injections in all situations.

If an application is built from scratch or requires low risk tolerance, it should be built or re-written using parameterized queries, stored procedures, or some kind of Object Relational Mapper (ORM) that builds your queries for you.

**1.5 Conclusion**

SQL injection continues to pose a significant threat to web applications, even though effective countermeasures are available, such as input validation, use of prepared statements, and escaping the user input.

However, due to the large variety of SQL injection attacks, it tends to fail in protecting the sensitive data in the databases. For that reason, it is recommended to apply the techniques mentioned before.

**Chapter 2**

Deep Learning

#### **2.1 Introduction**

The field of **AI**, using the strongest tools available in computer science, works toward imitating intelligence in a human being .These systems can perform a variety of tasks typically attributed to human cognitive abilities, such as decision-making, pattern recognition, and problem-solving. Artificial intelligence has come a long way over the years, fueling innovations such as self-driving cars, intelligent virtual assistants, and highly advanced recommendation systems, revolutionizing industries and everyday life.

In this chapter, basic machine-learning (ML) methodologies are looked into, a major subfield of AI. We will describe the three paradigms of learning: supervised learning, unsupervised learning, and reinforcement learning. Standard algorithms in machine learning will also be addressed followed by a transition into deep learning (DL), which is an enhanced version of ML that exploits multi-layer neural networks. The immediate goal in this instance is to firmly establish some of the fundamental concepts of these methods and their frameworks, in preparation for their application to real-world problems, including cybersecurity and SQL injection detection.

**2.2 machine learning**

The field of machine learning is concerned with the question of how to construct computer programs that automatically improve with experience. In recent years many successful machine learning applications have been developed, ranging from data-mining programs that learn to detect fraudulent credit card transactions, to information-filtering systems that learn users' reading preferences, to autonomous vehicles that learn to drive on public highways. At the same time, there have been important advances in the theory and algorithms that form the foundations of this field.[[13]](#_[13]Mitchell,_T._M,)

**2.2.1 Machine Learning Types**

In machine learning, this kind of learning process is usually classed into three main parts which are supervised learning, unsupervised learning, and reinforcement learning. Each type serves a certain distinct purpose and is used with certain types of problems. Besides those three types, hybrid approaches such as commodity inclusion and special techniques have also emerged to maintain and solve more complex issues.

**2.2.1.1 Supervised Learning (SL):**

**Supervised learning (SL)** is a machine learning approach that leverages labelled data to educate a system in forecasting outcomes based on its training. It closely mimics the process of human learning under the guidance of an instructor, employing specific instances to deduce overarching principles. SL is typically divided into two main categories.

**Regression:** Regression is a term used in statistics, which is a type of statistical analysis that aims to understand the relationship between a dependent variable (response variable) and one or more independent variables (predictors) such as in market trends or weather forecasting. The most common type is linear regression.

**Classification:** Classification is a SL technique that involves categorizing data into distinct classes. It is a recursive process that recognizes and groups data objects into pre-defined categories or labels. This technique is used to predict the outcome of a given problem based on input features. It can be applied to structured or unstructured data, and the classes are commonly known as target, label, or categories. The aim of classification is to assign an unknown pattern to a known class. For example, classifying emails as "spam" or "not spam" is a common application of classification.

Both the Classification and Regression algorithms can be used for forecasting in machine learning and operate with the labelled datasets. But the distinction between classification vs regression is how they are used on particular machine learning problems. [[14]](#_[14]_Amer_F.A.H.)

**2.2.1.2 Unsupervised Learning:**

[Unsupervised learning](https://www.ibm.com/think/topics/unsupervised-learning), also known as unsupervised machine learning, uses machine learning algorithms to analyze and cluster unlabeled datasets (subsets called clusters). These algorithms discover hidden patterns or data groupings without the need for human intervention.

Unsupervised learning’s ability to discover similarities and differences in information make it ideal for exploratory data analysis, cross-selling strategies, customer segmentation, and image and pattern recognition. It’s also used to reduce the number of features in a model through the process of dimensionality reduction. [Principal component analysis (PCA)](https://www.ibm.com/think/topics/principal-component-analysis) and singular value decomposition (SVD) are two common approaches for this. Other algorithms used in unsupervised learning include neural networks, [k-means clustering](https://www.ibm.com/think/topics/k-means-clustering), and probabilistic clustering methods.[[15]](Machine#_[14]_IBM_,)

**2.2.1.3 Reinforcement Learning:**

Reinforcement learning problems involve learning how to map situations to actions to maximize a numerical reward signal. These problems are inherently closed-loop, as the system’s actions influence its future inputs. Unlike other forms of machine learning, the learner is not explicitly told which actions to take but must discover the best ones through trial and error. In more complex scenarios, actions impact not only immediate rewards but also future states and long-term rewards, making decision-making more challenging.[[16]](#_[15]_Reinforcement_Learning:)

**2.2.2 Machine learning algorithms**

**2.2.2.1 Logistic regression**

Logistic regression is a supervised machine learning algorithm used for classification tasks, predicting the probability that an instance belongs to a specific class. It is a statistical method that analyzes the relationship between independent variables and a categorical outcome.

Unlike linear regression, logistic regression applies the sigmoid function to map input values to a probability ranging between 0 and 1. Instead of fitting a regression line, it models an "S"-shaped curve to distinguish between classes.[[17]](_Logistic#_[17]GeeksforGeeks_,)

**Key Points:**

* Logistic regression predicts the output of a categorical dependent variable.
* The outcome is discrete (e.g., Yes/No, 0/1, True/False) but represented as a probability between 0 and 1

**2.2.2.2 SVM**

**A support vector machine (SVM) is a supervised learning algorithm used for many classification and regression problems, including signal processing, medical applications, natural language processing, and speech and image recognition.**

The objective of the SVM algorithm is to find a hyperplane that, to the best degree possible, separates data points of one class from those of another class. “Best” is defined as the hyperplane with the largest margin between the two classes, represented by plus versus minus in the figure below. Margin means the maximal width of the slab parallel to the hyperplane that has no interior data points. Only for linearly separable problems can the algorithm find such a hyperplane; for most practical problems, the algorithm maximizes the soft margin, allowing a small number of misclassifications.

**Support vectors** are a subset of the training observations that define the position of the separating hyperplane. These are the data points closest to the hyperplane and are crucial for determining the optimal margin. While SVMs are originally designed for binary classification, they can be extended to multiclass problems by combining multiple binary classifiers.

To handle non-linearly separable data, SVMs use **kernel methods**. Kernel functions transform the data into a higher-dimensional space, where classes may become linearly separable. This transformation is implicit and computationally efficient, thanks to the **kernel trick**. Common kernel types include:

* **Linear**: Suitable for linearly separable data.
* **Polynomial**: Captures polynomial relationships between features.
* **Radial Basis Function (RBF)**: Effective for complex, non-linear boundaries.
* **Sigmoid**: A Mercer kernel under specific conditions.

Training an SVM involves solving a quadratic optimization problem to find the hyperplane that minimizes the soft margin. The number of transformed features depends on the number of support vectors, making the model compact and efficient once trained.

**Key advantages of SVMs** include their ability to handle high-dimensional data, robustness to outliers, and effectiveness in solving non-linear problems using kernels. Once trained, only the support vectors are needed to define the decision boundary, making SVMs suitable for automated code generation and real-world applications.[[18]](Support#_[17]_GeeksforGeeks_,)

**2.2.3 Real-world machine learning use cases**

Here are just a few examples of machine learning you might encounter every day:

**Speech recognition :** It is also known as automatic speech recognition (ASR), computer speech recognition, or speech-to-text, and it is a capability which uses natural language processing (NLP) to translate human speech into a written format. Many mobile devices incorporate speech recognition into their systems to conduct voice search—e.g. Siri—or improve accessibility for texting.

**Customer service :** [Online chatbots](https://www.ibm.com/products/watsonx-orchestrate/customer-service) are replacing human agents along the customer journey, changing the way we think about customer engagement across websites and social media platforms. Chatbots answer frequently asked questions (FAQs) about topics such as shipping, or provide personalized advice, cross-selling products or suggesting sizes for users. Examples include [virtual agents](https://www.ibm.com/products/watsonx-assistant" \t "_self) on e-commerce sites, messaging bots, using Slack and Facebook Messenger; and tasks usually done by virtual assistants and voice assistants.

**Computer vision** : This [AI](https://www.ibm.com/consulting/artificial-intelligence) technology enables computers to derive meaningful information from digital images, videos, and other visual inputs, and then take the appropriate action. Powered by convolutional neural networks, computer vision has applications in photo tagging on social media, radiology imaging in healthcare, and self-driving cars in the automotive industry.

**Recommendation engines :** Using past consumption behavior data, AI algorithms can help to discover data trends that can be used to develop more effective cross-selling strategies. Recommendation engines are used by online retailers to make relevant product recommendations to customers during the checkout process.  
  
**Robotic process automation (RPA) :** Also known as software robotics, RPA uses intelligent automation technologies to perform repetitive manual tasks.

**Automated stock trading** : Designed to optimize stock portfolios, AI-driven high-frequency trading platforms make thousands or even millions of trades per day without human intervention.

**Fraud detection:** Banks and other financial institutions can use machine learning to spot suspicious transactions. Supervised learning can train a model using information about known fraudulent transactions. Anomaly detection can identify transactions that look atypical and deserve further investigation.[[19]](Machine#_[18]_IBM_,)

**2.3 Deep Learnig**

Deep learning is a subfield of machine learning that employs deep neural networks for analyzing and interpreting complex data. Such networks are modeled after the human brain and allow the computer to identify patterns and relationships without human intervention in large amounts of unstructured information. The deep learning model is continuously improving its accuracy by tuning internal parameters with training**.**

Deep learning models can be trained to perform classification tasks and recognize patterns in images, text, audio, and other types of data. This technology also enables automation of tasks that typically require human intelligence, such as image description and audio transcription. Where human brains have millions of interconnected neurons that work together to learn information, deep learning features neural networks constructed from multiple layers of software nodes that work together.

This technique has achieved astonishing outcomes in image recognition, understanding natural language, and processing speech, making it the foundation of contemporary artificial intelligence systems.[[20]](What#_[19]_TeckTarget,_)

**2.3.1 Artificial Neural Networks (ANNs)**

Artificial Neural Networks (ANN) are inspired by the way biological neural system works, such as the brain process information. The information processing system is composed of a large number of highly interconnected processing elements (neurons) working together to solve specific problems. ANNs, just like people, learn by example. Similar to learning in biological systems, ANN learning involves adjustments to the synaptic connections that exist between the neurons.



Here [X1, X2, X3] are the input features to the neural networks represented as X. Whereas the superscript [1] is used to denote the layer. The weights are denoted by [W1, W2, W3] associated with each connection to the neuron from the input of that particular layer. The bias is represented by b associated with the neuron. “z” is the weighted sum of inputs added with the bias which is linear in nature. “a” is the activation function that is applied to z to add non-linearity as complex models can't be represented as a line.

The activation function is applied to the weighted sum of inputs to the neuron, including the bias term, and the resulting value becomes the neuron's output, which is then passed to the next layer. Its primary role is to introduce non-linearity into the model, allowing the network to learn complex patterns and approximate any arbitrary function. In this one-layer neural network architecture, the output of the activation function in layer [1] serves as the final output, denoted as y’. This output is used to compute the loss function, L (a, y), which measures the deviation between the predicted and actual output. This deviation is crucial for backpropagation and optimization, which will be discussed in later sections[.[21]](#_[21]_Medium_\“Basic)



An artificial neural network is primarily composed of three layers: the input layer, one or more hidden layers, and the output layer. These layers collectively work to process the information and yield meaningful predictions.

**Input layers** serve as the entry point for data into the neural network. Each neuron in this layer corresponds to either a specific feature of the input dataset or an input vector. For instance, in an image classification problem, all input neurons may specify the intensity of each individual pixel. This layer exists purely for the purpose of passing on the raw input values to the next layer without change.

**Hidden layers** serve to process and transform information passed to them from the input layer. They are called hidden since nothing about their inner workings can be observed directly. In a typical hidden layer, a neuron takes in inputs from the preceding layer, applies a weighted summation, adds a bias, and applies an activation function on the result. Depending on the complexity of the task, a network can have varying numbers of hidden layers with varying numbers of neurons in each layer. DNNs having multiple hidden layers are quite popular in applications such as image recognition, speech processing, and natural language understanding since they can efficiently extract many complex patterns from the data.

**The output layer is** the final layer of the network that provides the prediction made by the model. The structure of this layer is based on the solved problem. In the case of classification networks, each output neuron corresponds to one class; in regression problems, usually only one output neuron provides a continuous value: an activation function is then used in the output layer according to the type of task, e.g., softmax for multi-class classification and any linear function for regression.

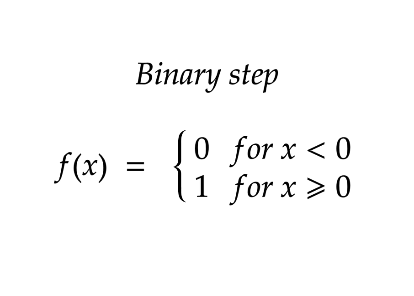
These layers are interconnected by **weighted links** that determine the importance of each input. The weights are adjusted during training through a system called **backpropagation** whereby errors are carried backward from the output to the hidden layers enabling the network to learn and enhance its performance with time. Persistent adjustments of these weights equate to an increasing ability of the neural network to predict correctly.

**2.3.2 Activation functions**

Activation functions play a fundamental role in neural networks by determining how neurons process input data and transfer information to subsequent layers. The choice of activation function significantly influences the network's performance and learning capability

**2.3.2.1 Binary Step Function**

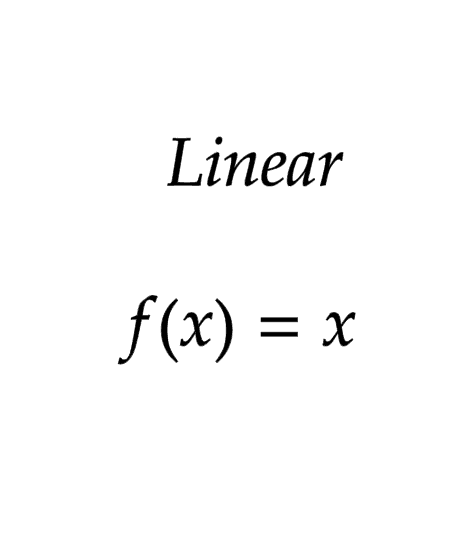
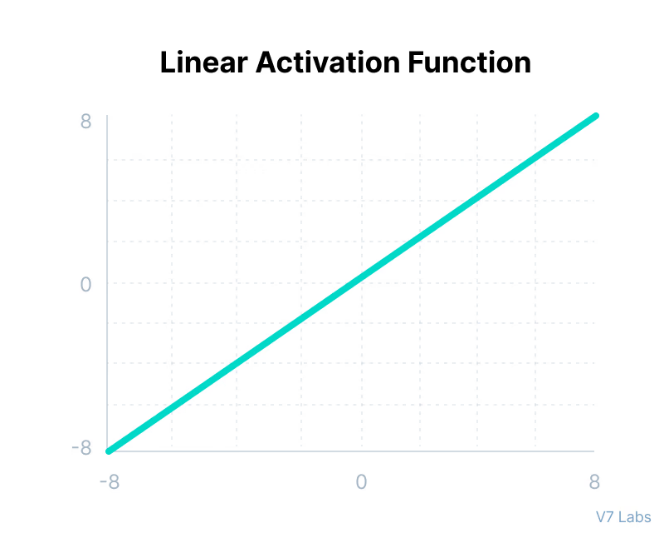
The Binary Step Function is a threshold-based activation function that decides whether a neuron is activated or remains inactive. If the input surpasses a predetermined threshold, the neuron is activated; otherwise, it stays dormant, meaning it does not contribute to the next layer.



This function is simple and computationally efficient but is unsuitable for tasks requiring multi-class classification due to its binary output. Additionally, its derivative is zero, preventing the backpropagation process and hindering learning.

**2.3.2.2 Linear Activation Function**

The Linear Activation Function, also known as the identity function, outputs the input valuewithout modification, allowing direct propagation of signals through the network.

****

Backpropagation is ineffective with this function since its derivative is constant and does not depend on input values. Additionally, using a linear activation function across multiple layers results in a network that is functionally equivalent to a single-layer model, limiting its ability to learn cmplex patterns.

### **2.3.2.3. Non-Linear Activation Functions**

A network using only a linear activation function is essentially equivalent to a simple linear regression model, limiting its ability to capture complex patterns in data. Non-linear activation functions enable deep networks to model intricate relationships between inputs and outputs.

They allow backpropagation by ensuring derivatives depend on input values, facilitating effective weight adjustments. They also enable the creation of deep networks, where transformed outputs from one layer pass non-linearly to the next, improving the model's ability to learn complex representations.

**1. Sigmoid (Logistic) Activation Function**

This function takes any real value as input and outputs values in the range of 0 to 1 making it useful for probabilistic models and binary classification tasks.

 The larger the input (more positive), the closer the output value will be to 1.0, whereas the smaller the input (more negative), the closer the output will be to 0.0, as shown below.

****

It is ideal for probability-based applications due to its constrained output range and is differentiable, ensuring smooth gradient updates during optimization. However, it suffers from the vanishing gradient problem, as extreme values lead to near-zero derivatives, hindering learning. Additionally, it is not zero-centered, which can slow down the training process.

**2.Tanh (Hyperbolic Tangent) Function**

The Tanh function is similar to the sigmoid function but maps input values to a range between -1 and 1, providing stronger non-linearity.

****

Its outputs are zero-centered, which improves convergence speed in deep networks, and it is often used in recurrent neural networks (RNNs) and convolutional neural networks (CNNs). However, it still suffers from the vanishing gradient problem, albeit less than the sigmoid function.

**3. ReLU (Rectified Linear Unit) Function**

ReLU is one of the most commonly used activation functions in deep learning. It introduces non-linearity by outputting zero for negative inputs while retaining positive values unchanged.



It is computationally efficient, as only a subset of neurons activates at a time, and helps accelerate gradient descent convergence due to its non-saturating nature. However, it suffers from the Dying ReLU problem, where neurons can become permanently inactive for negative inputs, preventing further updates.[[22]](#_[22]_V7_Labs,)

**2.3.3 Deep learning architectures**

Deep learning has enjoyed tremendous advancement in the last few years, serving as the major pillar for innovation in many different fields. Each architecture is designed for particular problems, with the performance in each case optimized for the specific needs of the task at hand.

Over the years, many deep learning models have been developed, often extending some fundamental designs. Among these, convolutional neural networks (CNNs), recurrent neural networks (RNNs), and long short-term memory networks (LSTMs) are the most commonly known. In their respective areas, these architectures have been very efficient, thereby enabling progress in image recognition, sequence modeling, and time series analysis.

**2.3.3.1 Recurrent Neural Networks**

Recurrent Neural Networks (RNNs) are neural networks designed to recognize patterns in sequences of data. They’re used for identifying patterns such as text, genomes, handwriting, or numerical time series data from stock markets, sensors, and more.

Unlike traditional [feedforward neural networks](https://www.analyticsvidhya.com/blog/2022/03/basic-introduction-to-feed-forward-network-in-deep-learning/), where inputs are processed only once in a forward direction, RNNs possess a unique feature: They have loops in them, allowing information to persist.

This looping mechanism enables RNNs to remember previous information and use it to influence the processing of current inputs. This is like having a memory that captures information about what has been calculated so far, making RNNs particularly suited for tasks where the context or the sequence is crucial for making predictions or decisions[.[23]](#_[23]_Shelf_“Why)



RNNs are made of neurons: data-processing nodes that work together to perform complex tasks. The neurons are organized as input, output, and hidden layers. The input layer receives the information to process, and the output layer provides the result. Data processing, analysis, and prediction take place in the hidden layer.

### **Hidden layer**

RNNs work by passing the sequential data that they receive to the hidden layers one step at a time. However, they also have a self-looping or recurrent workflow: the hidden layer can remember and use previous inputs for future predictions in a short-term memory component. It uses the current input and the stored memory to predict the next sequence.

For example, consider the sequence: Apple is red. You want the RNN to predict red when it receives the input sequence Apple is. When the hidden layer processes the word Apple, it stores a copy in its memory. Next, when it sees the word is, it recalls Apple from its memory and understands the full sequence: Apple is for context. It can then predict red for improved accuracy. This makes RNNs useful in speech recognition, machine translation, and other language modeling tasks.

### **Training**

Machine learning (ML) engineers train deep neural networks like RNNs by feeding the model with training data and refining its performance. In ML, the neuron's weights are signals to determine how influential the information learned during training is when predicting the output. Each layer in an RNN shares the same weight.

ML engineers adjust weights to improve prediction accuracy. They use a technique called backpropagation through time (BPTT) to calculate model error and adjust its weight accordingly. BPTT rolls back the output to the previous time step and recalculates the error rate. This way, it can identify which hidden state in the sequence is causing a significant error and readjust the weight to reduce the error margin.

## **types of recurrent neural networks:**

RNNs are often characterized by one-to-one architecture: one input sequence is associated with one output. However, you can flexibly adjust them into various configurations for specific purposes. The following are several common RNN types.

### **One-to-many**

This RNN type channels one input to several outputs. It enables linguistic applications like image captioning by generating a sentence from a single keyword.

### **Many-to-many**

The model uses multiple inputs to predict multiple outputs. For example, you can create a language translator with an RNN, which analyzes a sentence and correctly structures the words in a different language.

### **Many-to-one**

Several inputs are mapped to an output. This is helpful in applications like sentiment analysis, where the model predicts customers’ sentiments like positive, negative, and neutral from input testimonials[.[24]](#_[24]_Amazone_Web)

#### **References**

#### [1]

#### [2] OWASP “SQL Injection (SQLI)”:

<https://owasp.org/www-community/attacks/SQL_Injection>

#### [3] Bright security “SQL Injection Attack”:

<https://brightsec.com/blog/sql-injection-attack/>

#### [4] Beagle Security “Error based SQL Injection”

<https://beaglesecurity.com/blog/vulnerability/error-based-sqli.html>

#### [5] Dafydd Stittard and Marcos Pinto,The web Application Hacker’s Handbook: Finding and Exploiting Security Flaws, 2nd Edition, Wiley Publishing Inc, 2011.

#### [6] OWASP, “Blind SQL injection”:

<https://owasp.org/www-community/attacks/Blind_SQL_Injection>

#### [7] Moxso, “SQL Tautology” :

<https://moxso.com/blog/glossary/tautology>

#### [8] Justin Clarke, SQL Injection Attackes and Deffense

#### [9] OWASP Cheat Sheet Series, “SQL Injection Prevention”:

<https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html>

#### [10] OWASP Cheat Sheet Series, “Query Parameterization”:

<https://cheatsheetseries.owasp.org/cheatsheets/Query_Parameterization_Cheat_Sheet.html>

#### [11] PHP “Prepared statements and stored procedures”:

[https://www.php.net/manual/en/pdo.prepared-statements.php](https://www.php.net/manual/en/pdo.prepared-statements.php )

#### [12] PHP , “Validation”:

<https://www.php.net/manual/fr/filter.examples.validation.php>

#### [13] Mitchell, T. M, Machine Learning. McGraw-Hill, 1997.

#### [14] Amer F.A.H. ALNUAIMI and Tasnim H.K. ALBALDAWI, An overview of machine learning classification techniques.

#### [15] IBM ,“Machine Learning”

<https://www.ibm.com/think/topics/machine-learning>

#### [16] Reinforcement Learning: An Introduction Second edition, in progress Richard S. Sutton and Andrew G. Barto c 2014, 2015

#### [17]GeeksforGeeks ,“ Logistic Regression in Machine Learning”

<https://www.geeksforgeeks.org/understanding-logistic-regression/>

#### [18] MathsWorks, “Support Vector Machine”

<https://www.mathworks.com/discovery/support-vector-machine.html>

#### [19] IBM ,“Machine Learning”

<https://www.ibm.com/think/topics/machine-learning>

#### [20] TeckTarget, “What is deep learning and how does it work?”

<https://www.techtarget.com/searchenterpriseai/definition/deep-learning-deep-neural-network>

#### [21] Medium “Basic Notations and Representation: Neural Networks”

<https://medium.com/@anushruthikae/basic-notations-and-representation-neural-networks-d46a1be97471>

#### [22] V7 Labs, “Activation Functions in Neural Networks [12 Types & Use Cases]”

<https://www.v7labs.com/blog/neural-networks-activation-functions#3-types-of-neural-networks-activation-functions>

#### [23] Shelf, “Why Recurrent Neural Networks (RNNs) Dominate Sequential Data Analysis”

<https://shelf.io/blog/recurrent-neural-networks/>

#### [24] Amazone Web Services, “What is RNN (Recurrent Neural Network)?”

<https://aws.amazon.com/what-is/recurrent-neural-network/?nc1=h_ls>