Notes Oct 25 2018

OWASP

* OWASP Top 10 – 2017
  + The Ten Most Critical Web Application Security Risks

Table of Contents

* TOC – About OWASP….1
* FW – Forward…………….2
* I – Introduction………….3
* RN – Release Notes……4

Chapter 5

* Database and Data Center Security

Database Security

* Reasons database security has not kept pace with the increased reliance on databases are:
  + There is a dramatic imbalance between the complexity of modern database management systems (DBMS) and the security technique used to protect those critical systems.
  + Databases have a sophisticated interaction protocol, Structured Query Language (SQL), which is complex.
  + The increasing reliance on cloud technology to host part or all of the corporate database.
  + Most enterprise environments consist of a heterogeneous mixture of database platforms, enterprise platforms, and OS platforms, creating an additional complexity hurdle for security personnel
  + Effective database security requires a strategy based on a full understanding of the security vulnerabilities of SQL

Databases

* Structured collection of data stored for use by one or more applications.
* Contains the relationships between data items and groups of data items

Figure 5.1 DBMS Architecture

* Database utilities 🡪 DDL processor 🡪 Database description 🡪 DML and Query Language Processor 🡪 DBMS

Relational Databases

* Table of data consisting of rows and columns
  + Each column holds a particular type of data
  + Each row contains a specific value for each column
  + Ideally has one column where all values are unique, forming an identifier/key for that row.
* Enables the creation of multiple tables linked together by a unique

Figure 5.2 Example: Relational Database Model. A relational database uses multiple tables related to one another by

Relational Database Elements

* Relation
  + Table/file
* Tuple
  + Row/record
* Attribute
  + Column/field
* Primary Key
  + Uniquely identifies a row
  + Consists of one or more column names
* Foreign Key
  + Links one table to attributes in another
* View/virtual table
  + Result of a query that returns selected rows and columns from one or more tables
  + Views are often used for security purposes.

Table 5.1

Structured Query Language (SQL)

* Standardized language to define schema, manipulate, and query data in a relational database
* Several similar versions of ANSI/ISO standard
* All follow the same basic syntax and semantics
* SQL statements can be used to:
  + Create tables
  + Insert and delete data in tables
  + Create views
  + Retrieve data with query statements

SQL Injection Attacks (SQLi)

* One of the most prevalent and dangerous network-based security threats
* Designed to exploit the nature of Web application pages
* Sends malicious SQL commands to the database server
* Most common attack goal is bulk extraction of data
* Depending on the environment SQL injection can also be exploited to:

Figure 5.5 Typical SQL Injection Attack

* User 🡨🡪 Internet – Router – Firewall – Switch – Wireless access point
* Switch 🡨🡪 Web servers – Web application server – Database servers

Injection Technique

* The SQLi attack typically works by prematurely terminating a text string and appending a new command
  + Because the inserted command may have additional strings appended to it before it is executed the attacker terminates the injected string with a comment mark “--  
    “

SQLi Attack Avenues

* User input
  + Attackers inject SQL commands by providing suitable crafted user input.
* Server variables
  + Attackers can forge the values that are placed in HTTP and network headers and exploit this vulnerability by placing data directly into the headers
* A malicious user could rely on data already present in the system or database to trigger an SQL injection attack

Inband Attacks

* Uses the same communication channel for injecting SQL code and retrieving results
* The retrieved data are presented directly in application Web page
* Include:
* Tautology
  + The form of attack injects code in one or more conditional statements so that they always evaluate to true
* End of-line comment
  + After injecting code into a particular field, legitimate code that follows are nullified through usage of end of-line comments
* Piggybacked queries
  + The attacker adds additional queries beyond the intended query, piggy-backing the attack on top of a legitimate request

Inferential Attack

* There is no actual transfer of data, but the attacker is able to reconstruct the information by sending particular requests and observing the resulting behavior of the Website/database server
* Include:
  + Illegal/logically incorrect queries
    - This attack lets an attacker gather important information about the type and structure of the backend database of a Web application
    - The attack is considered a preliminary, information-gathering step for other attacks.
  + Blind SQL injection
    - Allows attackers to infer the data present in a database system even when the system is sufficiently secure to not display any erroneous information back to the attacker.

Out-of-Band Attack

* Data are retrieved using different channel
* This can be used when there are limitations on information retrieval, but outbound connectivity from the database server is lax.

SQLi: Countermeasures

* Three types:
  + Manual defensive coding practices
  + Parametrized query insertion
  + SQL DOM
    - Defensive coding
  + Detection
    - Signature based
    - Anomaly based
    - Code analysis
  + Check queries at runtime to see if they conform to a model of expected queries
    - Run-time prevention

Database Access Control

* Database access control system determines:
  + If the user has access to the entire database or just portions of it
  + What access rights the user has (create, insert, delete, update, read, write)
* Can support a range of administrative policies]
  + Centralized administration
    - Small number of privileged users may grand and revoke access rights
  + Ownership-based administration
    - The creator of a table may grant and revoke access rights to the table.

SQL Access Controls

* Two commands for managing access rights:
  + Grant
    - Used to grant one

Figure 5.6 Bob Revokes Privilege from David

* Ann
  + Bob
    - David
      * Frank
  + Chris

Role-Based Access Control (RBAC)

* Role-based access control eases ad

Table 5.2 Fixed Roles in Microsoft SQL Server

Figure 5.7 Indirect Information Access Via Inference Channel

* Non-sensitive data , Inference, Sensitive data

Figure 5.8 Inference Example

Database Encryption

* The database is typically the most valuable information resource for any organization
  + Protected by multiple layers of security
    - Firewalls, authentication, general access control systems, DB access control systems, database encryption.
    - Encryption becomes the last line of defense in database security
  + Can be applied to the entire database, of the record level, the attribute level, or level of the individual field
* Disadvantages to encryption:
  + Key management
    - Authorized users must have access to the decryption key for the data for which they have access
  + Inflexibility
    - When part or all of the database is encrypted it becomes more difficult to perform record searching.

Figure 5.9 A Database Encryption Scheme

* User

Data Center Security

* Data Center: An enterprise facility that houses a large number of servers, storage devices, and network switches and equipment

Figure 5.11 Key Data Center Elements

Figure 5.12 Data Center Security Model

* Data Security
  + Encryption, Password policy, secure IDs, Data Protection (ISO 27002), Data masking, Data retention, etc.
* Network Security
  + Firewalls, Anti-virus, Intrusion detection/prevention, authentication

TIA-492

* The Telecommunications Industry Association (TIA)

Figure 5.13 TIA-942 Compliant Data Center

Summary

* The need for database security
* Database management systems
* Relational databases
  + Elements of a relational database system
  + Structured Query Language
* SQL injection attacks
  + A typical SQLi attack
  + The injection technique
  + SQLi attack avenues and types
  + SQLi countermeasures
* Database access control
  + SQL-based access definition
  + Cascading authorizations
  + Role-based access control
* Interference