How Can Databases be Secured Against Various Threats?

A research project that investigates the process of securing a medical database using MYSQL

H Z

***Abstract*—**

"Database security refers to the range of tools, controls, and measures designed to establish and preserve database confidentiality, integrity, and availability." [4]

The aim of this research project is to investigate how databases can be compromised, what are the consequences of a data breach, and how can the medical database produced in the distinction task be secured against various attacks. This is necessary because a medical database contains confidential information about patients, this private information is expected to be protected from threat actors, all the while allowing users and doctors to retrieve their data when necessary. The investigation resulted in the development of a website and database that was secured against SQL Injections as well as an analysis of physical security and policies, and the creation of user accounts in MYSQL with limited access.

I. Introduction

A. Why Secure a Database?

Database breaches are extremely common and can have sever impacts if the data stolen is personal or critical to an individual or business. Threat actors can use confidential data to steal bank details, gain access to individuals accounts or to sell business secrets. It was reported that from the period between January 2020 and September 2020 36 billion records were breached from databases [3]. Security is required to protect the confidentiality, Integrity and Availability of data, ensuring data has not been stolen, is accurate and can be accessed by authorised people. There are multiple levels on which an attack can take place to steal or corrupt data, These Include: [4]

- The data in the database
- The database management system (DBMS)
- Any associated applications
- The physical database server and/or the virtual database server and the underlying hardware
- The computing and/or network infrastructure used to access the database

All these different levels of attack must be secured to ensure the CIA Triad of Database security, that is its Confidentiality, Integrity and Availability. GA Systems Outlines a series of important reasons as to why database security is important.

1) Prevents Data Breaches: Personal information is securely stored on a database, this information could be confidential, containing passwords, credit card information or confidential medical records. Database security prevents threat actors from accessing this information.

2) Avoid Fines and Protect Brand Reputation: For A business, a data breach can have an extremely damaging financial cost. If the database security was not implemented according to the current best standards, this could incur fines from the associated governments. Furthermore, Customers may distrust the companies' services [3] leading to reduced revenue and poor reputation.

3) Ensure the Continual Functioning of Business Operations: Many attacks on databases can be more about preventing access to data than stealing it, this could be in the form of damaging servers or over the network using a DOS attack, without proper database security the continued functioning of the business is put at risk.

B. What are the Legal Requirements for Storing Personal Data in Australia

The Legal requirements of collecting, using, storing, and disclosing personal information is outlined in the 1988 privacy act. [1] This legislation has undergone many revisions to accommodate the rapid developing digital technologies in the database management, social media, business, and government sectors. Further legislation at the state level also apply to the legal handling of personal data. A set of principles are outlined by the Office of the Victorian Information Commission. A summary of the principles from OVIC below:[7]

1) When Collecting data about an Individual, that individual should be aware of it and know how to contact the organisation. Only relevant information for the functioning of the business should be collected and only through that individual.
2) Regarding Use and Disclosure an organisation can only disclose information for the primary purpose as declared unless consent is given, or the secondary purpose is strongly related and would be reasonable to expect for its use. Information can also be used in anonymous research or if disclosing it could prevent serious harm.
3) The Data Quality of the information stored should be accurate complete and up to date.
4) For Data Security, an organisation should ensure reasonable practice in preventing unauthorised access and should destroy or de-identify information that Is no longer required.
5) An Organisation should have an openness about its use of the data and how it plans to manage it and should

disclose how an individuals data is handled and what information is stored if requested by that individual.

6) An Organisation must provide access to the information by the individual unless this would cause harm or violate other individual privacy.
7) Unique Identifiers should not be used to identify individuals unless not doing so would significantly impact the efficiency of the organisation.
8) Individuals should have the option of remaining anonymous if lawful.
9) Transfer of information to another organisation should only occur if lawful and necessary or consent is given.
10) Sensitive information should not be collected unless consent is given or required by law, or it would prevent serious harm.

C. What Sort Of Data Is Stored?

Fig. 1. Travel Data from Home to University

I requested my Data from applications such as Google, Discord and Steam to investigate what sort of data is stored for a user. Both Google and Discord returned with folders upon folders of csv files, JSON files and in googles cases other multimedia files. Steam gives access to user data through their desktop application. There were many pieces of information I expected such as Gameplay time in Steam, web history and email history in Google and Discord chat records. The information stored here dated back to when I first opened my accounts in these respective applications. And even included links to photos sent, various notes I had written in Google Notes. What was astonishing was complete records of all my travels including timestamps, location data and location names. Here is a record of travel going form my home to university in Hawthorn (Fig. 1). What piqued my interest was that despite having all the records I was given no information about how specifically my data was used, while Google has all my documents stored on Google Drive, I have no idea if they get analysed for YouTube recommendations, targeted Advertising, or any other possibility that my data could be used for. The broad range of personal data stored illustrates just how important data security is to ensure that individuals are not taken advantage of.

D. Who is Liable When a Database is Breached

When a database gets hacked the Victorian state Privacy and Data Protection Act outlines methods for identifying responsibilities and compensation for Victorians. The Information Commissioner holds powers to hold public sector organisations to account for data breaches [6] Furthermore, OVIC outlines a complaints process to respond to data breaches. Once a compliant is processed VTAC is the authority that can order an organisation to provide compensation. In Australia as a whole, OAIC provides the Notifiable Data Breach Scheme (NDB) which ensures that any Organisation operating within Australia must notify individuals effected by a data breach as soon as Practicable [2]. However, only eligible data breaches fall under this scheme, if the data breach could cause harm, it is eligible, however if action was taken quickly and assessed to not be of risk then no notification is required [5]. In the case of a data breach that does cause severe harm or damage, OAIC can penalise an organisation up to $2.1 million or an individual up to $420,000 [2]

E. What are Common Ways a Database is Compromised

1) Deployment Failures: The first point of failure for a server is during deployment, while testing before adding a server to the network can reduce risk, there is always potential for misconfiguration or damaged parts.

2) Insider Threats: There three forms of Insider Threats, they include a disgruntled employee or former employee intending to do harm, a negligent or improperly trained employee that lacks sufficient skill to correctly configure a database securely or an outsider threat such as a visitor, customer, or business associate that aims to compromise the Datastore [4]

3) Human Error: Human error includes any misconfiguration, damage, or innocent mistake regarding the managing of a server and database. Human Error has the potential to create a security breach, or poorly effect availability of resources.

4) Excessive Privilege: Excessive privilege is when a user is given greater authority to devices in the system than they should be this can enable insider threats or if a user account is compromised, allow for more damage to occur by a cybercriminal. [3]

5) Injection Attacks: This occurs when threat actors input SQL statements into forms in web apps causing unintended queries or DDL code to be executed. [3]

6) DOS/DDOS: A denial-of-service attack aims to prevent the server from delivering its intended service such as overloading with many requests. So that legitimate requests cannot be processed.[4] Distributed DOS utilizes many compromised computers (zombies) to deliver requests.

7) Malware: Malware can be executed on servers causing corruption, encryption in the case of ransomware or to steal information and take control of systems. Malware can be delivered through phishing emails taking advantage of social engineering or installed directly in the case of insider threat.

II. Aim

The goal of this research project is to investigate how threats can be prevented to ensure that reasonable action has been taken to secure the Distinction Database against these threats and protect patients' data.

III. Method

1) Create the Medical Database as per the distinction task requirements.
2) Create a web form that allowed users to book an appointment and request their patient data. The SQL queries required for this are already determined in the distinction design report.
3) Analyse the risks present due to human error and the posibility of human error, record in results.
4) Create a floor plan for one of the medical clinics documenting procedures and physical security implmentations to guard against insider threats.
5) Create a second user account for a doctor in MYSQL so they only have access to needed data to ammend excessive privilege concerns
6) Perform an injection Attack using the website form and create the necessary restrictions to prevent it.
7) Secure Against A hypothetical DOS attack from teh doctor user by adding user restrictions

IV. Results

A. The Website

The HTML and PHP Code will be appended to the end of this document.

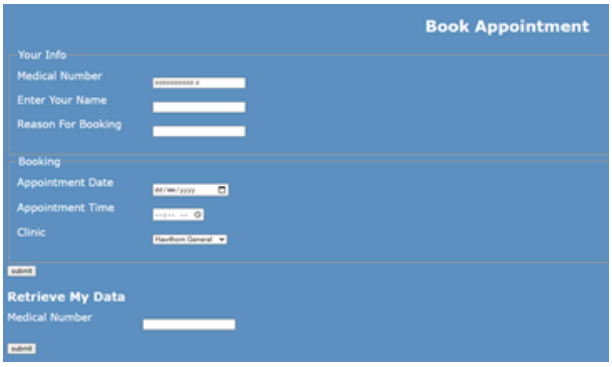

Fig. 2. Website Main Page

TABLE I
Sample Output From Requesting Patient Data

Name	MedicalNo	Date of Birth	Bloodtype	Sex	comments
James Leroy	1023786932.2	2002-05-31	AB+	M	

B. Human Error and Deployment Failures

XAMPP virtual server is hosting both the database server and a web server for the website. This allows users to request their data using the website which uses php to return data from the MYSQL Server. Best Practice dictates that the Web Server and Database Server should be separated but due to limited resources I am unable to do so. The Issue with this is that the server (my PC) becomes a single point of failure. Hence If the website is exploited or my PC is compromised a threat actor is given access to both the database and website.

C. Insider Threat

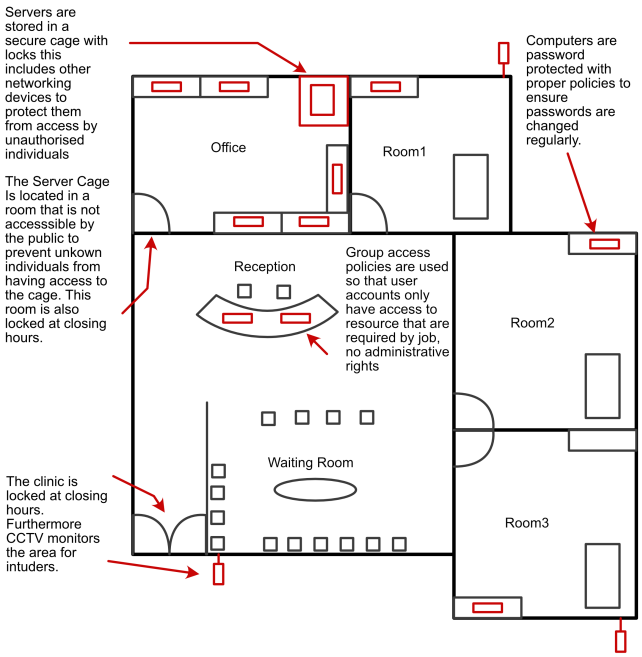

Fig. 3. Clinic Floor Plan

D. Excessive Privilege

The employees would currently access the database using the root user, which is of concern, as a disgruntled employee could cause severe damage to the systems. In Fig 3 I have documented the process of creating a doctor user that can only access the records needed for their job.

E. SQL Injection

In php the query works in a predictable manner to retrieve data. It would be easy for a threat actor to presume that the medical no is stored in a variable ($mno) and then inserted into a query like so. "select * from patientData where medicalno = '$mno';"; Hence an attack can occur quite simply by inserting sql code to retrieve data the user shouldn't have access to. (Fig. 5)

Inserting this into the box creates the query: "select * from patientData where medicalno = '1034897235.4' or ''=";" as ''=" is always true all tuples will be returned (Fig. 6)

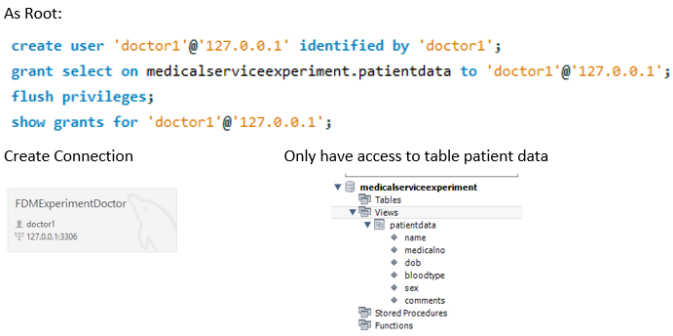

Fig. 4. User Creation

Fig. 5. SQLInjection

In order to protect against this kind of attack the input needs to be sanitised: The function (Fig.7) removes most HTML syntax and whitespace. This combined with a check against a regex expression prevent the SQL injection from functioning.

F. DOS From Compromised User

In order to protect from DDos Attack that could use the medical service computers if they were compromised the following commands can be made to alter the permissions of the users. (Fig. 8)

By entering the commands in Fig. 8 the number of queries, reconnections and simultaneous connection allowed can be altered, this could prevent a dos attack where a threat actor either uses this user to overload the database system with many queries or tries to establish thousands of connections util no more can be made. If the doctor1 user tries to create a second connection to the database a n error occurs preventing them from doing so.

V. Discussion

The Research Conducted showed how the threats to databases operate on many levels. Of Concern is the physical security of the server hosting the database, insider threats and the policies that dictate access to resources. Furthermore, by providing the public with access to data through a website, a variety of threats are introduced including SQL Injections, Data Manipulation, and Denial of Service. The Practical research conducted illustrated how to protect against a subset of possible attacks, the security implementations successfully prevent SQL injections and insider threats. A variety of attacks were able to be prevented such as an SQL Injection from the Retrieve My Data Query, and the possibility of a compromised user overloading the number of connections to the MySQL

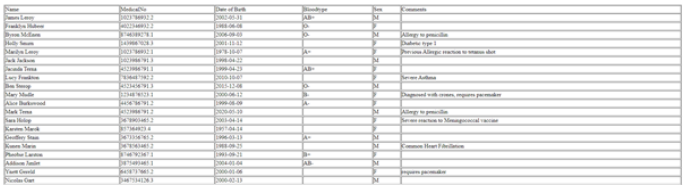

Fig. 6. All Tuples

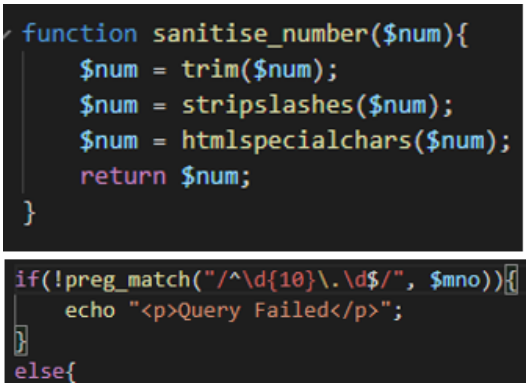

Fig. 7. Data Sanitisation

server. However, there are still many attacks that could occur, dos attacks on the web server can still occur, as well as Buffer Overflow attacks and backup attacks. There are still many much more sophisticated attacks that this database is vulnerable to and in further studies an exploration of how to over come them could be conducted.

VI. Conclusion

In Conclusion following best practice security for databases can protect a database from many attacks. However due to the type s of valuable information stored in databases there will always be threats to this data, with many new zero-day attacks and vulnerabilities security is a constant arms race of patches and configuration to protect private data.

References

[1] Attorney-General Department. (n.d.). Privacy. Retrieved from Privacy—Attorney-GenralDepartment: https://www.ag.gov.au/rights-and-protections/privacy

[2] Bogle, A. (2018, Feburary 22). Data breaches: If a company has lost your personal info, they now have to tell you. Retrieved from ABC NEWS: https://www.abc.net.au/news/science/2018-02-22/-companies-must-inform-consumers-of-data-breaches/9462170

[3] GA Systems. (2021, Semptember 1). Why Good Database Security is Important in 2021. Retrieved from GA Systems: https://www.gasystems.com.au/blog/database-security/

[4] IBM Cloud Education. (2019, August 27). Database Security. Retrieved from Database Security: An Essential Guide: https://www.ibm.com/au-en/cloud/learn/database-security

[5] OAIC. (2019, July 13). Part 4: Notifiable Data Breach (NDB) Scheme. Retrieved from OAIC Website: https://www.oaic.gov.au/privacy/guidance-and-advice/data-breach-preparation-and-response/part-4-notifiable-data-breach-ndb-scheme/

[6] OVIC. (n.d.). IDENTIFYING REALISTIC OUTCOMES IN PRIVACY COMPLAINTS. Retrieved from OVIC Website: https://ovic.vic.gov.au/privacy/identifying-realistic-outcomes-in-privacy-complaints/

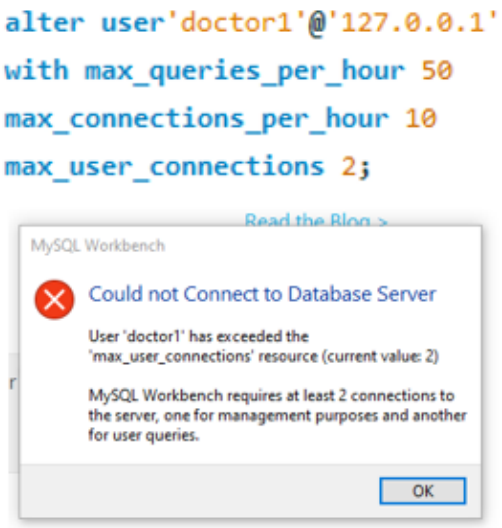

Fig. 8. Restricting A User

[7] OVIC. (n.d.). INFORMATION PRIVACY PRINCIPLES – FULL TEXT. Retrieved from OVIC Website: https://ovic.vic.gov.au/privacy/information-privacy-principles-full-text/

[8] Rubens, P. (2021, March 5). Database Security Best Practices. Retrieved from eSecurityPlanet: https://www.esecurityplanet.com/networks/database-security-best-practices/

[9] Sinha K. (2020, June, 16). Create An HTML Form And Insert Data Into The Database Using PHP Retrieved from C#Cornor: https://www.c-sharpcorner.com/UploadFile/52bd60/create-an-html-form-and-insert-data-into-database162/