DOI: 10.53477/2668-2001-21-35

DATABASE – WEB INTERFACE VULNERABILITIES

Dorin Iordache[1]
"Ovidius" University

Abstract

The importance of information security in general, of managed information at the level of a database has increased with the expansion of the Internet. On the other hand, it has acquired new facets with the increase of the accessibility of the users to as many resources as possible. Large volume of private data in use and the limitation of unauthorized actions to information have brought new aspects to the issue of ensuring their protection. The scope of this field is wide and allows the operation in several directions: identification, description, creation, implementation and testing of mechanisms aimed at improving the working environment in which database management systems operates. Due to the importance of the information managed by a DBMS[2], it is necessary to define a framework safe and easy to use. The database fulfills not only the role of storage, but also of data provider to users. Thus, the information must be protected throughout the interaction process: generation, storage, processing, modification, deletion, etc. Therefore, the security of databases must not only be reduced to the protection of certain data considered sensitive, but also to the creation of a secure, authorized and controlled global environment through which information becomes available to users.

Keywords: database; cybersecurity; web-base vulnerabilities; network interface; user credentials.

INTRODUCTION

When we operate with the notions of incident or security breach, we analyze information security. The incident is a security event that compromises the integrity, confidentiality, or availability of a computer infrastructure (or even the date/information itself). (ISO.2005)

Database security mechanisms must not only be limited to the protection of certain sensitive information, but also to the creation of a secure, authorized and controlled global environment. The security objectives of information systems are defined as follows (Info sec.2002), (Gary Stoneburner. 2001): availability as a requirement to ensure the proper functioning of the system and services; the integrity of the data and the system, respectively the confidentiality, as the capacity to keep the "hidden" character of the information; journaling as a need to uniquely identify and store the action of an entity of the system pursued and last but not least, security as a confidence in the system whose adopted security, technical and operational measures function and perform exactly the designed actions.

Servers continue to be the leader in ever-increasing attack targets. This is mainly due to the shift of the industry to web applications (the most common variety of assets, Figure 1), with system interfaces delivered as Software as a Service (SaaS) (Verizon. 2020)

According to the 2020 Verizone report, cloud resources were involved in about 24% of security breaches, while local assets are still the target in 70% of all reported breaches. Cloud targets involving an e-mail server or web applications account for over 70%, confirming the trend for cybercriminals to find the fastest and easiest way to reach their victims. The report centralized elements of information technology (IT) compared to operational technology (OT), in the case of assets involved in incidents. It was found that 96% of cases of security breaches took place in the field of information technology and only 4% in the operational one.

[1] Corresponding author: dorin.iordache@365.univ-ovidius.ro
[2] DBMS – DataBase Management System

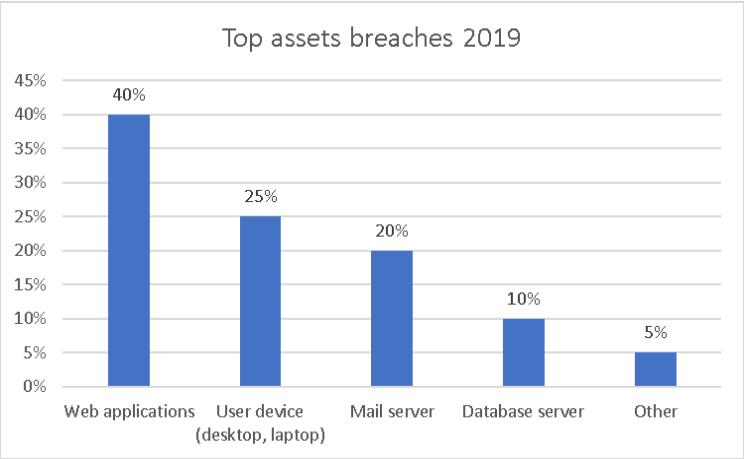

Figure 1. Top Asset varieties in breaches

Also, about 50% of reported security breaches are in the field of web applications correlated with database, because most of the time they interact.

WEB AND DATABASE VULNERABILITIES

Web applications include programs that perform certain actions mediated by a web browser, acting as a client interface (the program used to run the application). This architecture provides access to server services, including database management servers.

The need to take measures to ensure the confidentiality, integrity, and availability of resources within the systems used is growing due to the interaction with many insecure networks in an environment where it is not known who a potential attacker may be. Security attacks take countless forms such as: interceptions, disguises, forgeries, etc.

The advantages of the most important web applications refer to: flexibility, scalability, and increased redundancy. Because customers interact with a web browser, the type of computer or operating system does not affect accessibility.

Common web application vulnerabilities

OWASP Top 10 is a first step towards changing the software development culture within an organization, which refers to: Injection, Broken Authentication, Sensitive Data Exposure, XML External Entities (XXE), Broken Access Control, Security Misconfiguration, Cross-Site Scripting (XSS), Insecure Deserialization, Using Components with Known Vulnerabilities, Insufficient Logging & Monitoring (OWASP Project).

These vulnerabilities must be analyzed and prioritized according to:

- the degree of probability of vulnerability, in the sense that the easiest attack is when the resources involved are minimal (a simple web browser);
- detectability understood in the idea of detecting the threat as easily as possible. The most vulnerable information is the one produced in the URL, and the less in the lines of code;
- the impact or damage caused, if possible. If the computer system used is shut down, it is the biggest damage caused by the attack.

For the above reasons it is particularly important to know and assess, if possible, periodically, the state of the indicators as well as the listed vulnerabilities.

Database vulnerabilities

If there is an interaction of web services with a database management system, the issue of information security becomes even more important. Database security comprises a number of security features designed to protect the database management system (DBMS), which cover protecting the infrastructure of the database, securely configuring the DBMS and accessing the data itself. The security of database management systems must reflect the following: Deployment failure,

Excessive privileges, Privilege abuse, Platform vulnerabilities, Unmanaged sensitive data, Backup data exposure, Weak authentication, Database injection attacks[3].

By comparing the vulnerabilities of the two fields of study: web, and database, we observe common elements or means that facilitate the exploitation of information in the database.

EXAMPLES OF DATABASE EXPLOITS

In a simple investigation, using shodan, we can find out that there are still enough database management systems, incorrectly or insufficiently configured, in terms of their security.[4] In most relational database management systems, the default values are quite secure: connections are only accepted from the local interface, and the default authorization is inhibited or modified. However, there are situations when these minimum rules are not followed.

Such an example is shown in Figure 2, in which we see that a large amount of information is managed on a vulnerable MongoDB server from the perspective of default access settings, not being a singular case.

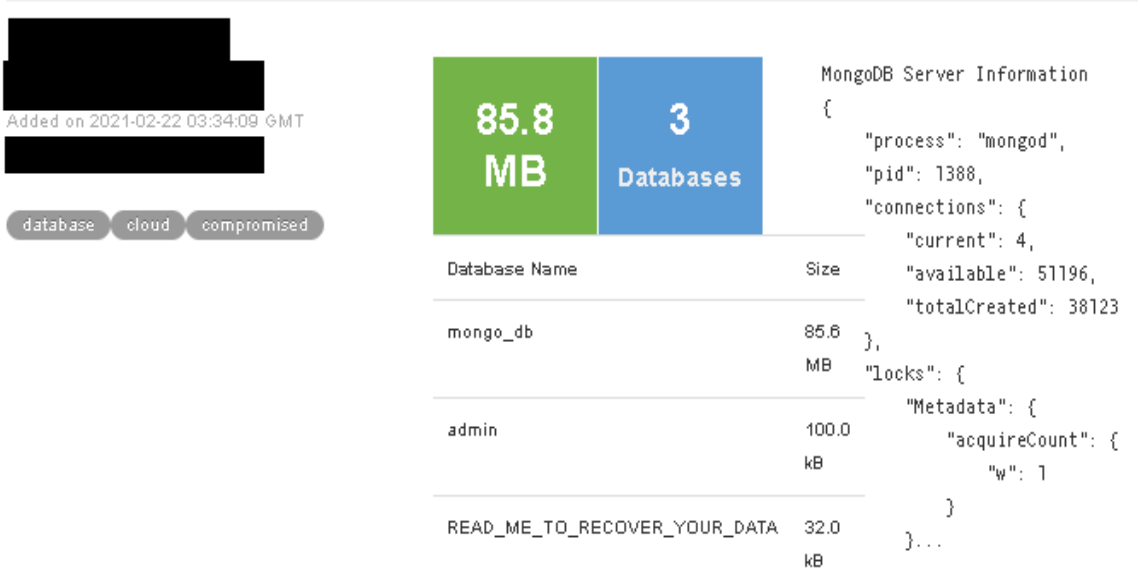

Figure 2. Vulnerability example at the administration level

Many of these instances, not being updated to the latest version, have the effect of introducing new vulnerabilities and security risks to the managed data.

Most MongoDB public implementation operates in the cloud: Amazon, Alibaba Advertising CO, Digital Ocean, OVH complete the most popular destinations for hosting MongoDB without authorization enabled. In fact, I have noticed this trend everywhere: cloud services tend to be more vulnerable than traditional data center hosting.

Not only for the reasons stated above, keeping the data itself secure is important also. In addition, the security mechanisms put in place must provide protection against countless security threats. All this to ensure protection for: Deployment failure, Excessive privileges, Privilege abuse, Platform vulnerabilities, Unmanaged sensitive data, Backup data exposure, Weak authentication, Database injection attacks.

For the study, we chose to detail the vulnerability of *Poor Encryption and Data Breaches*, which is a side often overlooked. Most of the time certain information stored in the database needs to be encrypted. In this way they can once again protect themselves against attacks and information/data leaks.

[3] https://looker.com/definitions/database-security
[4] Over 70000 instances, according shodan.io MongoDB search.

Data breaches are known among specialists in which important amounts of information have been accessed unauthorized, regarding: including social security numbers, birth dates, addresses, and in some cases drivers' license numbers (approximately 147.9 million consumers) (Josh Fruhlinger. 2020), 617 million online account details stolen from 16 hacked websites (email addresses, usernames, PBKDF2 password hashes, and other personal data)[5], and perhaps the largest data leak, was Yahoo compromised the real names, email addresses, dates of birth and telephone numbers of 3 billion users account. Yahoo claimed that most of the compromised passwords were hashed[6].

"*Yahoo on Tuesday said "recently obtained new intelligence" showed all user accounts had been affected. The company said the investigation indicated that the stolen information did not include passwords in clear text, payment card data, or bank account information. But the information was protected with outdated, easy-to-crack encryption, according to academic experts. It also included security questions and backup email addresses, which could make it easier to break into other accounts held by the users*."(Jonathan Stempel, Jim Finkle. 2017)

The conclusion we reach by analyzing the events listed above materializes in the threat is real, present, constantly evolving and companies do not always take the best security measures to protect our personal data. In this regard, we have an example. In September 2019, the Zynga database was accessed unauthorized and more than 218 million user accounts were stolen. Zynga confirmed email addresses, salted SHA-1 hashed passwords, phone numbers, and user IDs for Facebook and Zynga accounts were stolen (Player security.2019)

POOR ENCRYPTION AND DATA BREACHES

Data breach might include:

- loss or theft of hard copy notes, USB drives, computers, or mobile devices;
- an unauthorized person gaining access to computers, account, or network;
- personal data email sending to the wrong person;
- sending emails using 'to' or 'cc', instead of 'bcc' (blind carbon-copy);
- employee copying a list of contacts for its personal use, etc.

The above incidents may occur due to the negligence of users with intent or not, due to breaches of security rules or their lack. But at the same time they can happen as a result of cybercrime, hacking.

Although it seems obvious, in some situations not all the data in the database are in encrypted form. It is practically impossible to encrypt everything. There are network interfaces in the databases that can be easily tracked by hackers if your data is not encrypted.

Aside to Injection flaws: SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

If we add to all this the elements of GDPR[7], we realize that it is very important to protect our personal data. GDPR calls for appropriate technical measures that include, but are not limited to, encryption in certain forms will be a requirement. (NICVA)

Penetration tests database

Given the previous examples where sensitive user information was stolen or leak, we can say that entities should not clearly store sensitive data in a database. At the same time, all external connections to the database should always use encryption mechanisms. In other words, sensitive data must be encrypted both at rest and moving.

Although new security standards and procedures have emerged, there are still organizations, as we saw earlier, that use weak algorithms for storing passwords, such as SHA-1. (Marc Stevens,

[5] https://www.theregister.com/2019/02/11/620_million_hacked_accounts_dark_web/

[6] https://www.reuters.com/article/us-yahoo-cyber/yahoo-says-all-three-billion-accounts-hacked-in-2013-data-theft-idUSKCN1C8 2O1

[7] GDPR – General Data Protection Regulation.

2017) On the other hand, there are many users who use common words for passwords used or of low complexity. These aspects can be very easily exploited by interested people.

We performed some tests on the resistance to attacks on users' access passwords stored in a database. Passwords were protected with different hash functions: MD5, and SHA with different levels of complexity. Following the experiments, using common tools: sqlmap and hashcat, in which we also used dictionaries to attack this information, the results can be summarized as follows: the low complexity of the password generated success in identifying it, almost regardless of the standard used. On the other hand, a more complex password determined the failure to determine it, within a reasonable time.

In order to verify the resistance of these credentials, we executed an attack, on a vulnerable database, as in figure 3.

```
sqlmap -u http://192.168.43.78/pai_c/modificare_clienti.php?idclient=14 -D bd_pai_c
            |-T members -C username,password,email,admin --dump

[11:25:32] [INFO] using default dictionary do you want to use common password suffixes? (slow!) [y/N]
[11:25:33] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[11:25:33] [WARNING] multiprocessing hash cracking is currently not supported on this platform
[11:25:34] [INFO] cracked password '12345' for user 'test5'
[11:25:39] [INFO] cracked password 'abcd' for user 'test_user'
[11:25:39] [INFO] cracked password 'abcde' for user 'test7'

Database: bd_pai_c
Table: members
[13 entries]
+-----------+-----------------------------------------------------------------------------------------
| username  | password
+-----------+-----------------------------------------------------------------------------------------
| test_user | e2fc714c4727ee9395f324cd2e7f331f (abcd)
| user      | 430780c5b24102335aa77032a615fa70709bd5c44a0a1cf6c310b7287f3518dc7412038ff96986b2f24dc77c
| admin     | 430780c5b24102335aa77032a615fa70709bd5c44a0a1cf6c310b7287f3518dc7412038ff96986b2f24dc77c
| test      | $2y$10$HhLDYUIktcSosskj862Edu8uG73O0HUZfV0NxlkpwHytjwUDGdQ5m
| test2     | $2y$10$IlLLwhp3x1FnOXfv73lF5OrP0ukQWZ5x/.pj6ayoFIp5H3TREPW1.
| test3     | 7bcba40edfdb12fae3001d3b271304109b225462015a3eccb0097d4f1d2d9a9baa0f947f7f8e1947e80c9b12
| test4     | D8022F2060AD6EFD297AB73DCC5355C9B214054B0D1776A136A669D26A7D3B14F73AA0D0EBFF19EE333368F0
| test5     | 827ccb0eea8a706c4c34a16891f84e7b (12345)
| test7     | ab56b4d92b40713acc5af89985d4b786 (abcde)
```

Figure 3. Sample result of the password atack on vulnerable database

Following the execution of this simulated attack, I obtained the clear password for some input data, for others obviously not.

The following table lists some of the relevant tests:

Table 1. Hash atack results[8]

Information	Method	Result	Success
e2fc714c4727ee9395f324cd2e7f331f	MD5	abcd	Yes
827ccb0eea8a706c4c34a16891f84e7b	MD5	12345	Yes
ab56b4d92b40713acc5af89985d4b786	MD5	abcde	Yes
3627909a29c31381a071ec27f7c9ca97 726182aed29a7ddd2e54353322cfb30 abb9e3a6df2ac2c20fe23436311d6785 64d0c8d305930575f60e2d3d048184d79	SHA512	12345	Yes
878ae65a92e86cac011a570d4c30a7eae c442b85ce8eca0c2952b5e3cc0628c2e7 9d889ad4d5c7c626986d452dd86374b6 ffaa7cd8b67665bef2289a5c70b0a1	SHA512	abcde	Yes
27664cd89fdb076072835d7e69a5c2cdc8 e264e486917457c1bf36e4a7c5d0998696f ca8fbc9892295ed818ded8ee45778feb700 ed33d1d191032cc22bcfd72f	SHA512	p3U/3ZGMEf7v\	No

[8] sqlmap and hashcat tools.

If more companies used SHA-512 the situation would be better, because, at least for now, the algorithm is still relatively safe from brout-force attacks, if we take into account the statistics provided by the blockchain in the mining stage.

One such example is the mining process used in bitcoin. Bitcoin mining process is performing now at more than 153000 TeraHashes per second[9] (where SHA-256d(x)=SHA-256(SHA-256(x)), that is two SHA-256) and also it is time and energy consumming process without a certain positive result.

Administrative actions

From the elements stated above, we note that it is imperative personal data be protected. Certain actions must be implemented by the service provider, but also the regular user must apply certain own actions.

These actions are simple. The most important of which is the management of data access. All this depends on the level of training and knowledge of users in the field of cyber security.

In order to assess the level of knowledge of regular users, we initiated an ad-hoc survey, through which we followed the way of managing the passwords of the access accounts. We focused on the objectives for identifying how to manage users' access data in email accounts, the interaction with the online payment environment, as well as the level of preparation and studies.

Following the survey, we found the following:

- Over 70% of respondents do not consider that they have a training in the field of cyber security;
- Although 25% have secondary education and 75% higher education, 95% use Internet services frequently;
- At least 30% have a personal email account, and 64% more than two email accounts, both organizational and personal;
- 16% use the same password for all email accounts, which is risky;
- Mobile technology is widely used, 70%, both for interaction with the Internet, e-mail, banking, etc.,
- Over 60% use password complexity, lowercase, uppercase and special characters, longer than 8 characters;
- 80% use electronic payment services, using the computer or mobile terminal.

From the survey we found the following risk factors regarding access data management and use of electronic services, figures 4 and 5:60% never change the access password or only at the request of the service provider:

- 30% use the same access password for different accounts and services;
- 80% do not use or do not know what a password manager is;
- 15% had security incidents in the last year, and 3% with total loss of data or account.

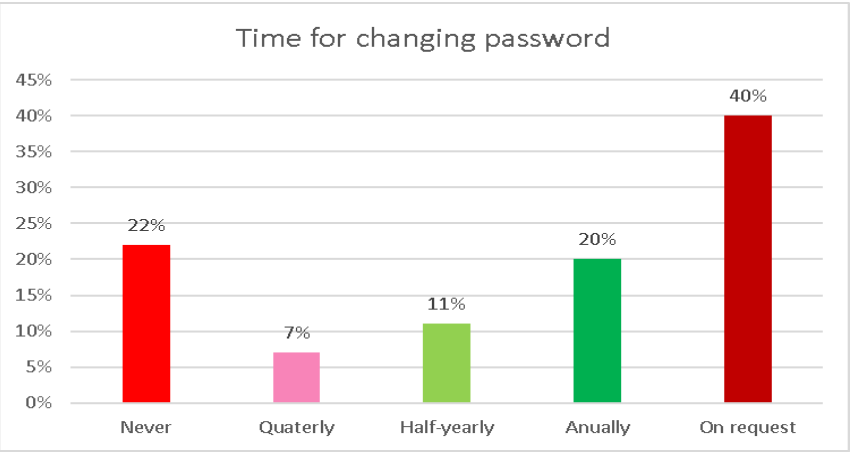

Figure 4. Password change frequency

[9] https://www.blockchain.com/charts/hash-rate

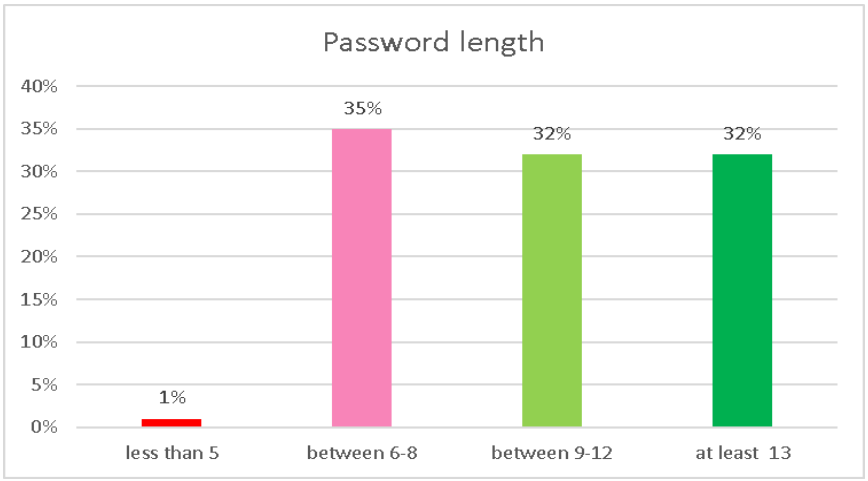

Figura 5. Length of the password

CONCLUSIONS

As a result of security tests on vulnerable databases, we have found that the information stored is not always secure. This finding is also confirmed by the multitude of events of theft of personal information, especially access data in various accounts. Although there is an improvement in the security environment, through the actions taken by major service providers, it is necessary for regular users to adopt appropriate behavior.

A large part of users widely uses electronic services at least email. But, through e-mail we exchange sensitive information: account access passwords, bank information, electronic payments, invoices, etc.

Following the survey, even if it has no sociological representation, we deduced that to a large extent they either misuse access data or do not know the implications of misuse.

A small number of users have been the subject of a cyber attack with or without data loss/email account. We can deduce that certain cyber attack situations may not have been reported by them, because often the unauthorized access to the email account is hidden for a long time. Attackers investigate the information circulated, analyze the behavior of users acting only in situations presumed to be advantageous to them, most often for illegal purposes.

That is why it is important to choose our electronic service providers that ensure a certain level of increased security. At the same time, it is necessary to respect and use the security mechanisms implemented by them. We must add the widespread training of users to raise the level of knowledge and skills in the field of cybersecurity, aside the technical measures mentioned above.

REFERENCES

Fruhlinger, Josh. 2020, “Equifax data breach FAQ: What happened, who was affected, what was the impact?”, https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html

Info sec. 2002. “Information Security Management Best Practice”, https://www.pitt.edu/~dtipper/2825/ISO_Article.pdf, accessed January 10, 2021.

ISO. 2015. “ISO-Security techniques – code of practice for information security management”, accessed 2005.

NICVA. “GDPR and Encryption”, https://www.nicva.org/data-protection-toolkit/templates/gdpr-and-encryption, accessed February 11, 2021.

OWASP Project. “Top 10 Web Application Security Risks”, https://owasp.org/www-project-top-ten/

Player security. 2019. “Player Security Announcement”, September 2019, https://investor.zynga.com/news-releases/news-release-details/player-security-announcement

Stempel, Jonathan, Jim Finkle. 2017. “Yahoo says all three billion accounts hacked in 2013 data theft”, October 3, 2017, https://www.reuters.com/article/us-yahoo-cyber/yahoo-says-all-three-billion-accounts-hacked-in-2013-data-theft-idUSKCN1C82O1, Last accessed February 11, 2021.

Stevens, Marc. 2017. “The first collision for full SHA-1”, https://shattered.io/static/shattered.pdf

Stoneburner, Gary. 2001. “Computer security. National Institute of Standards and technology”, (NIST 800-33), 2001, https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=151250, accessed January 10, 2021.

Verizon. 2020. “Data Breach Investigations Report”, https://enterprise. verizon.com/resources/reports/dbir/, accessed December 03, 2020.