DOI: http://dx.doi.org/10.26483/ijarcs.v13i5.6903

Volume 13, No. 5, September-October 2022

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

AN ONLINE SQL VULNERABILITY ASSESSMENT TOOL AND IT'S IMPACT ON SMEs

Atdhe Buja
Faculty of Contemporary Sciences and Technologies
South East European University
Tetovo, North Macedonia

Zana Beqiri Luma
Mother Teresa University
Skopje, North Macedonia

Abstract: Information security has received everyone's attention, especially in the case of the global Covid-19 pandemic. SMEs are looking for solutions that offer greater security and a normal functioning of activities. Our research is aiming to measure the benefits from the usage of an online Vulnerability Assessment SQL tool (VA SQL). In the study, through an experiment of various tools used we can see different results in the findings. We present the best practice and a model of proactive approach to analyze database security using Microsoft technology. Currently, we need to have and use a lot of scripts or external tools to identify and fix the vulnerabilities. The findings, demonstration of the study should reveal and support our main hypothesis that there is direct link between the database security and the main factors that threat and risk the data. In this paper, we present VA SQL – a model for discovery, track and fix potential database security gaps of different information systems and web application databases.

Keywords: sql database, cybersecurity, assessment, vulnerability

I. INTRODUCTION

Management, administration of databases regardless of the technology or relational database management system (RDBMS) that is in place has been a challenge for SMEs in terms of data security. A database system which integrated the relational data model to a structured query languages or application programming interface known as RDBMS [1]. Most SMEs use third party tools or applications to maintain the level of security through scans, different assessments for databases. But with the development of technology, especially the Cloud, it has brought innovation and opportunity to the market, including the aspect of security for databases. Service providers have practically clearly understood the industry demand for the integration of some components of third-party tools in the existing RDBMS platforms. Risks, cyber threats are advancing every day more and more in methods and techniques, becoming impossible to identify and establishing protective measures through a different approach is necessary. Cyber-attacks are taking the form of a large scale, and are having a great impact on the operations of the industry, up to endangering human life.

The focus of this paper outline is to support identification of vulnerabilities and provide better presentation within integrated database environment. To identify and fix vulnerabilities, there are needed to be used a lot of external tools and accompanied scripts. In this paper, we present VA SQL– a new model for discovery, track and fix potential database security gaps of different information systems and web application databases. In general, data attacks are divided into passive and active attacks. The passive attack purpose is to gain information into a silent mode on the target but not changing any data on target, known as sniffing attack [2]. The mission of the active attacks have is to change the status of the target, to amend, or alter the data [2]. Active and passive attacks are classified as infection, exploiting and specific set of attacks, mainly they have a common purpose attempting to gain and maintain access to the target system [3].

Vulnerability assessment (VA) as a feature provided in Cloud technology by Azure gives an overview of your security and include a series of remediation actions to solve the issues and improve database integrity and availability. Moreover, VA as a cloud service within SQL server on premises and SQL Azure scans towards the database and try to identify possible flags and weak points of your database. The VA hands a base of knowledge of rules which identify and select or highlight security issues and not proper settings from that best which considers best countermeasures to protect the database. The knowledge base of rules has the trend to focus more in the security technical aspects which could pose a risk to the data.

The paper organization is on seven sections. In the first section, introduction of the actual trends and development of databases security. In the second section, a background and motivation described for the topic. The third section, describing the database vulnerabilities and potential cyber-attacks related to the operations of it. In the fourth section, concepts of types of security testing and comparative analysis between them. In the fifth and the rest sections, results and conclusions of the findings are presented including future works.

II. BACKGROUND AND MOTIVATION

Most of it professional like database administrators, web and information system administrators are faced with the issue of having a big picture of their infrastructure and resources used to work with them. Seeing the trends and globalization of information communication technology (ICT) industry, data security is considered as one of the main issues by security professionals. We have been studying the opportunities of RDBMS relational database management system vendors, which provide a quality, and effective protection of data in compliance with actual EU regulation GDPR. Complying with the general data protection

regulation (GDPR) [4] one needs to get familiar with the research in the articles [5, 6, 12-22, 25 and 32]. This will make the transitions to the GDPR less difficult. This task does not mean to be difficult and impossible, because there are a variety of tools and technologies which can be used and supported on implementing privacy by design in the data management system. According to the GDPR regulations anyone who have contact with data should be fully comply with the GDPRs definition of a "data processor" [5], which defines who is responsible. Data processors can be IT teams, developers, database administrators and others. Recently, the activity of cyber-attacks is increasing, especially for SMEs, this is a risk that they are facing. Because a cyber-attack can even bankrupt SMEs. According to [6] there is an increase of cyber-attacks on SMEs within 2022 by 89%. Another Eurobarometer survey for SMEs identify 29% of European SMEs have experiences at least one cybercrime within 2021 [7].

In the US Defense Federal Acquisition Regulation Supplement (DFARS) [8] fourteen control requirements are involved such as security assessment, identification and authentication, incident response etc. [9].

III. DATABASE VULNERABILITIES

A. *SQL Injection*

SQL injection attacks can happen if the input from the client side is not filtered according to the standards, and as such if it is sent to the database, affects can be unimaginable. This can lead to risk bad results data leakage, manipulation of the SQL statements, with an aim of performing illegal operation on the database side. How they work is that these SQL injection vulnerabilities are authenticated or encoded before passing them to SQL queries which are executed on a database server [10]. While SQL injections are in progress of happening, an attacker looks for URLs that permit the submission of data to the database, areas such as login box, search box, and feedback pages within web application or website.

SQL injections attack include operation like update, insert, delete data through execution of commands on the server side which can make the malicious code such as viruses, sniffers, to steal data. In the following Queries, we are showing some of the SQL injection used in the User Input, which can be very harmful for our environment [11]:

- or '1' = '1
- "or "1" = "1
- 'or 1 = 1; --
- 1 or 1 = 1

As an SQL injection countermeasure, the input validation check must be carried out for every user input. To reduce the chances of happen an SQL injection attack, on development phases could be used a simple replace function to convert all single quotes to double quotes.

B. *Session Hijacking*

Session Hijacking it is about stealing a session ID. If the attacker finds it, he will have the real control of the client – server session. By having this communication, the attacker can steal the data, manipulate session, reroute it to the different place etc. Attacker will gain privileges for the session by sending the request to the server with real session ID and server cannot validate if this is malicious or not due to the same session ID and gives successful response [12].

C. *Privilege Escalation*

Privilege Escalation usually occurs when a malicious user designs a flaw or configuration error in an application or operating system (OS). Once the attacker has access to a remote system, he or she will try to increase access privileges by escalating process towards the Administrator [13], as presented in Fig. 1. The best countermeasure against this risk is to ensure that users have at least privileges to do the job.

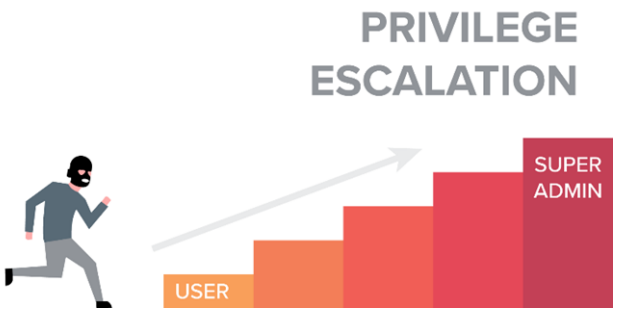

Figure 1. Privilege escalation overview

IV. TYPES OF PENETRATION TESTING

A. *Manual Penetration Testing*

Some of the vulnerabilities are difficult to identify by using automated tools. Those vulnerabilities can be identified by using manual testing utilizing the open source environments and tools. In addition, the manual penetration testing is done only by human resources using methods and techniques known by hackers to hack information systems [14]. Thus, through manual testing is very beneficial approach to detect and identify security gaps. Because, it helps the organization to expand and specify exactly the identification of a certain vulnerability in the infrastructure. Manual penetration testing is the right way to carry out such an activity. There are different methodologies that help in the implementation of the penetration testing process, including EC-Council, OWASP, etc. These methodologies are the best organizer of the Penetration testing work process, they standardize all the activity, techniques, and methods used. Each methodology emphasizes the way of realization and the possibility of identifying security weaknesses. Based on the scope of the penetration testing there are different types of it including internal or external, wireless, web or mobile application, phishing etc. SMEs can benefit from penetration testing in the simulation where they can mimic the cyber-attacks including hacking, malwares, DDoS etc. They also serve as a starting point for future treatment and response to cyber-attacks that may come. And these penetration testing can always be done in two ways, manual and automatic through different tools.

B. *Automatic Penetration Testing*

A considerable number of Database vulnerability and Penetration testing tools are in the market, but not all of them established solution of proactive vulnerability assessment [11]. Tools like Sparta, Nikto is mostly running under the open source environments like Linux, Ubuntu. Their features cover different models of identifying vulnerabilities, such as (1) the manual penetration testing, (2) and advance or custom scanning. Those tools within web application security testing platform are an integral part of

ensuring compliance with international policies by identifying different vulnerability. Automatic penetration testing differs from manual in the way of conducting rather writing scripts or command, you can utilize a tool and give the target the rest will be for the tool to realize and give the report of findings. Usually for the best results and maybe something different on findings, is to combined those to methods manual and automatic penetration testing. Different penetration testing strategies are sometimes used for SMEs, and serve as a protective mechanism for these companies. For more, penetration test for SMEs has more to do with the computer systems, the network and the various applications that are used in these companies, whether on-premises or cloud. Parts of the penetration test strategy include planning, external or internal testing. Penetration testing should be an integral part of IT security in SMEs, because it prepares them to face cyber-attacks and various risks of the future.
The comparative analysis of different tools has been conducted as shown in Table 1.

V. RESULT

Despite there being a number of vulnerable databases prepared to allow an individual to validate their tool against some of the vulnerabilities, we select two databases. SQL VA provides a run scan for vulnerabilities in the target database within the RDBMS system this case SQL server, in the safe approach by not causing disruption of the database operation. The reason for conducting this experiment is to see the effectiveness, the state of the data of identifying security vulnerabilities from some of the tools used.

We have performed operation-automated and manual penetration testing on two databases.

1) OLTP database, and
2) Data Warehouse database.

A. *Run a scan*

1) VA FOR ON-PREMISES SQL SERVER

In the process of our penetration testing, we used open source and commercial penetration tools to test a number of vulnerabilities in databases. Further, to see the differences and their capability in the security aspects such experiments were needed to conduct and present the data following sections of the paper.
The following table shows automated tools we used for penetration testing, (Tab. II).

Table II. Automation scanner overview

Tools	Vendor
VA for on-premises SQL server	Microsoft
VA for Azure SQL Database	Microsoft
Sparta, Nikto	Secforce, Linux
Nessus	Tenable

The findings detected by using automated and manual penetration testing tools are as follows:

- X-XSS
- CGI Directories
- Clickjacking
- Permissions escalation
- Db owner not matching the real owner
- Missing TDE Transparent Data Encryption
- Auditing issues server level

In the following points, we will explain and present the results of experiment made from different tools including VA for on-premises SQL server, VA for Azure SQL Database, Sparta and Nikto, and Nessus

B. *The report*

The findings through using VA for on-premises SQL server in the experiment were various of them. We mention some of them including detection of the permissions escalation, database owner not matching the real owner, missing Transparent Data Encryption (TDE) etc.

How it works this tool and very valuable features is at the moment your scan has been completed, so the report with remediation steps automatically will be generated with an opportunity to export on different file type (i.e. csv). Therefore, report present the actual state of your database within the RDBMS system in regard to the security including issues by severity level, warnings based on knowledge of rules, existing snapshot, and some recommendations on remediation action steps.

The report as is shown in Figure 2 present an overview of the security state, about the issues and their severity. The result details include warning on deviations from the best security practices. The report will indicate and categorize total of failing or passing checks and gives an opportunity to include recommendations to those failed check by protecting the data.

The Figure 3 presents selected details from the overview report security state from Figure 2. For every finding a view is generated which includes information on the finding vulnerability, impact, and recommendation action steps in the way of remediation scripts.

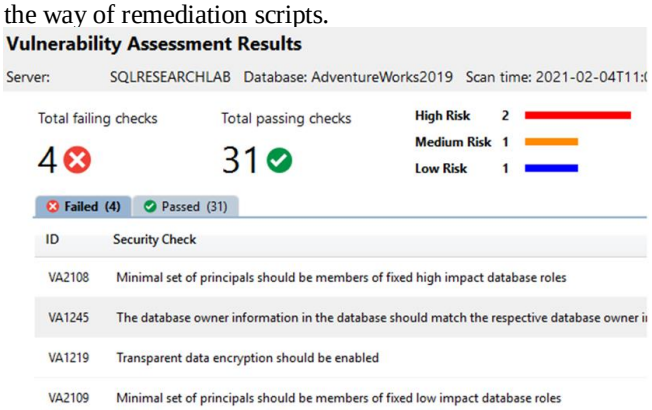

Figure 2. Report overview of the database security state, VA for on-premises SQL Server

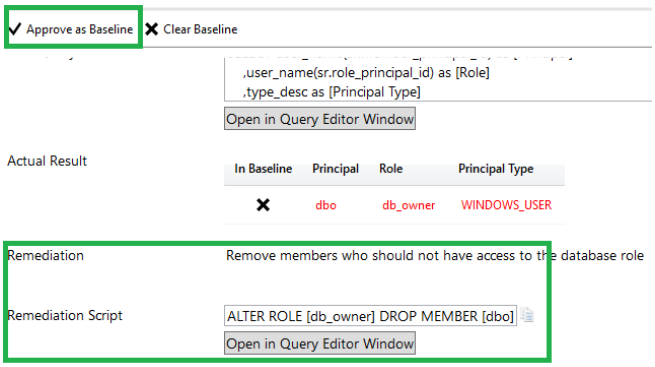

Figure 3. Selected findings from overview report

C. *Analysis of the results and findings*

The report helps to analyze the results and issues possibly coming with a remediations action steps. By using this

approach of VA for on-premises SQL server remediation action script steps provided by report, wouldn't take long time and effort to solve issues. Look over the results and decide the priority and importance of the particular findings if is a security issue within your database. Follow deep the issue by the result of report are the way where VA for on-premises SQL server provides for the SMEs IT departments. Report with remediation steps in csv you can find here: https://bit.ly/3oZgMia

D. Specify the baseline

As review your results you can see two metrics including total failing check, and total passing check. You can mark every finding as an acceptable level of security known as baseline at your database. Moreover, those result matching the baseline will considered as passing checks. Through this phase you save yourself the time and resources to deal with those findings that you have accepted their security level. Because VA for on-premises SQL server will report only the left issues which are not proper to the base knowledge rules, and you will deal those issues.

Scans can be repeated at any time, and VA for on-premises SQL server will report any findings that do not exceed the acceptance level threshold you have defined in base knowledge of rules.

2) VA FOR AZURE SQL DATABASE

VA for Azure SQL database is a service for scanning provided by Cloud Azure from Microsoft and operates same as VA for on-premises SQL server but its more flexible in terms of utilizing through the web. Following the process of configuring vulnerability assessment in the Azure portal for SQL database, running a scan, till to the report present the actual state of your database within the RDBMS system in regard to the security including issues by severity level, warnings based on knowledge of rules, existing snapshot, and some recommendations on remediation action steps.

The report as is shown in Figure 4 present an overview of the security state, about the issues and their severity. The result details include warning on deviations from the best security practices. The report will indicate and categorize total of failing or passing checks and gives an opportunity to include recommendations to those failed check by protecting the data.

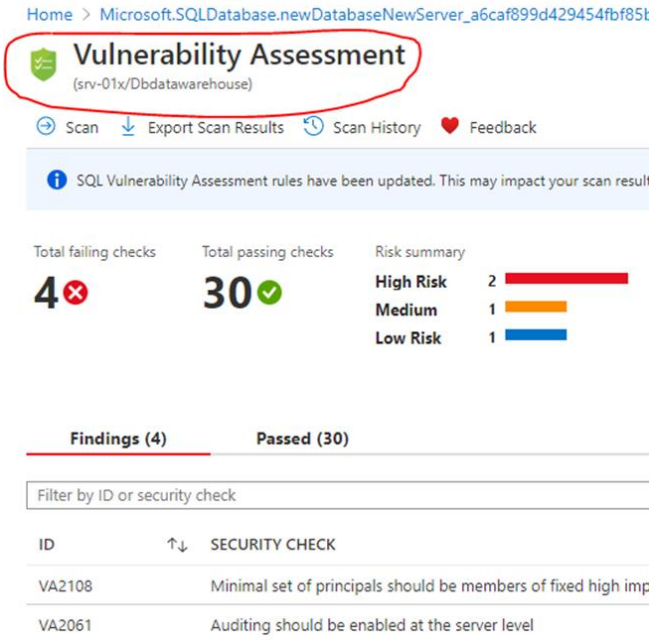

Figure 4. Report overview of the database security state, VA for Azure SQL database

Beside security center monitoring and assessment using VA for Azure SQL database there is option to conduct vulnerability assessments programmatically using PowerShell, and Azure CLI.

3) SPARTA AND NIKTO TOOLS

Sparta is a graphical application for penetration testing scanning and enumeration activities. Give you the capability to scan your target through a command and focusing on analyzing the results on the report. The tool works perfectly in the environment of Kali Linux operating system where you can utilize all the capabilities which has. Sparta tool save your time and resources to be engaged.

Nikto is a command line tools for penetration testing scanning and enumeration activities. Mostly the tool is used for web server scanner or web applications. It is built in Perl language within the open source. The toll in its feature of vulnerability scanner provides all the security gaps identified in the target including fingerprint, outdated versions, misconfigurations, ports and services etc.

In the experiment a scenario was to use Sparta and Nikto tool for penetration testing and they have detected various vulnerabilities the Figure 5 shows including X-XSS, cgi directories, clickjacking.

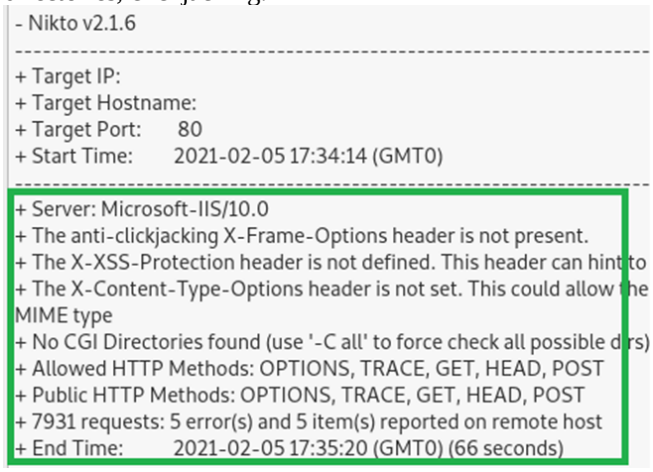

Figure 5. Vulnerability Assessment by Nikto

4) NESSUS TEENABLE TOOL

The Nessus tool provided by Tenable is a penetration testing tool for active scanning, and vulnerability assessment. Using this tool in the experiment provides report results for vulnerabilities where Figure 6 gives us an overview. This tool can scan different targets for various vulnerabilities and exposures of security flaws. Can be run in any operating system because it's a web application running in your or cloud environment. The Figure 6 presents the findings vulnerabilities by using the Nessus tool includes the severity, cvss factor, plugin, and a name for each finding. Moreover, a detailed vulnerability report in pdf format can found here in the link https://bit.ly/3oZgMia

Vulnerabilities Total: 43

SEVERITY	CVSS	PLUGIN	NAME
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	6.1	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.0	57608	SMB Signing not required
MEDIUM	5.0	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
INFO	N/A	46180	Additional DNS Hostnames

Figure 6. Vulnerability Assessment by Nessus

Therefore, using different other tools including Sparta, Nikto to perform penetration testing for experiment gives us different results on the findings. While penetration testing conducted with Nessus on vulnerability assessment process has identified a quite number of vulnerabilities related to server. Those vulnerabilities identified impact very highly the databases and its data. However, those findings were not included in the results because their relation is more with server level rather so much little with databases.

The Figure 7 shows the graph data of experiment conducted by different tools but the same target database. The data presents the analysis of type of penetration testing including automated, and manual penetration testing. Looking at Figure 7 shows us that there is a difference between manual and automatic penetration testing through different tools. For more, the findings are presented according to the type and method by which they are identified, i.e. manual and automatic penetration testing. The identification of security vulnerabilities depends a lot on the manual or automatic method we use. From the multiple tests and the combined methods used, they give us a clearer result to truly see the security weaknesses in our infrastructure, in this case the database. With the advancement of hacking methods, at the same time, security weaknesses have become difficult to identify, this is because the development of technology is making it difficult to deal with all security flaws.

Figure 7. Summary vulnerability detection manual or automatic penetration testing

VI. FUTURE WORK

Within latest years, societies, people become more dependent on Internet. Innovative concepts and solutions are making use of many web applications. Those solutions technological ones are having the vulnerabilities to a number of threats, attacks. Many companies within industry are seeing as advance model to those issues to build secure solutions by using Machine Learning and Artificial Intelligence. The testing of vulnerabilities is done with intention to see where the security gaps are and possible ways to gain access of the system.

Intelligence and security are being enviable by many companies Microsoft have built into it with SQL Server edition 2019. As Microsoft SQL Intelligent Database System, approach has become available with Microsoft products like SQL Server, Azure SQL. Moreover, Gartner Magic Quadrant for Cloud Database Management Systems identify Microsoft on the leader quadrant. Microsoft is a Leader in this Magic Quadrant. It provides a broad range of cloud DBMS services [15]. This will remain a continuation of the research work to address other problems of SMEs in relation to information security.

I. CONCLUSIONS

As attacks evolve more advance in methods and techniques, it is important that organizations, companies to have training, learning program for themselves on cyber security threats. The database structure developers have to be aware of different threats, attacks in order to follow proper coding practices. Which includes validation of user input to prevent injection attacks can solve most of database and web application vulnerabilities. The proposed new model, which proactively monitor the databases deployed in premises or cloud and will run a vulnerability, data classification checks by using VA SQL or Azure version of it. To use this process by organizations within them plans for manual and automated penetration testing models will increase accuracy on identifying vulnerabilities and proactively monitoring for security of the data. VA provides with more than penetration testing including remediation steps and code, data classification, set a baseline etc.

Table I. Comparison beetwen tools

Features↓	**Tools→**	VA for on-premises SQL Server	VA for Azure SQL Database	Nessus	Sparta, Nikto

Vulnerability Assessment	√	√	√	√
Penetration Testing		√	√	√
GDPR meet compliance	√	√	√	√
Meet data privacy standards	√	√	√	√
Vulnerability Impact (Drill-down)	√	√		
Remediation Actions (script generation)	√	√		
Database settings		√		
Data Discovery & Classification	√	√		
Ease of use	√		√	
Availability	Free/Paid	Free/Paid	Free/Paid	Free/Paid

Sample of a Table footnote. (Table footnote)

II. REFERENCES

[1] Gartner, "RDBMS (Relational Database Management System)," [Online]. Available: https://www.gartner.com/en/information-technology/glossary/rdbms-relational-database-management-system#:~:text=A%20database%20management%20system%20(DBMS,(SQL)%20application%20programming%20interface..

[2] EC-Council, "EC-Council Blog," 07 23 2020. [Online]. Available: https://blog.eccouncil.org/how-to-identify-network-security-threats-and-vulnerabilities/.

[3] A. Mohiuddin Ahmed, "A survey of network anomaly detection techniques," Elsevier, Journal of Network and Computer Applications, pp. 19-31, 2016.

[4] EU, "General Data Protection Regulation," 04 05 2016. [Online]. Available: https://gdpr-info.eu/.

[5] EU, "Art. 4 GDPR," 04 05 2016. [Online]. Available: https://gdpr-info.eu/art-4-gdpr/.

[6] A. Adepetun, "Cyber attack on Nigerian SMEs up by 89 per cent in 2022," 2022. [Online]. Available: https://guardian.ng/business-services/cyber-attack-on-nigerian-smes-up-by-89-per-cent-in-2022/.

[7] E. C. E. Commission, "Eurobarometer," 2022. [Online]. Available: https://europa.eu/eurobarometer/surveys/detail/2280.

[8] U. Government, "DFARS," 30 11 2020. [Online]. Available: https://www.acquisition.gov/dfars.

[9] CyberSaint, "The Definitive Guide to DFARS Compliance and NIST SP 800-171," CyberSaint.

[10] M. A. A. Ossama B. AlKhurafi, "Survey of Web Application Vulnerability Attacks," Application Vulnerability Attacks Advanced Computer Science Applications and Technologies, no. IEEE, 2016.

[11] Port Swigger, "SQLi," [Online]. Available: https://portswigger.net/web-security/sql-injection. [Accessed 01 02 2021].

[12] OWASP, "Session hijacking attack," [Online]. Available: https://owasp.org/www-community/attacks/Session_hijacking_attack.

[13] MITRE, "Privilege Escalation," [Online]. Available: https://attack.mitre.org/tactics/TA0004/.

[14] I. A. J. A. D. F. u. R. M. R. Insha Altaf, "Vulnerability Assessment and Patching Management," ICSCTI), no. IEEE, 2015.

[15] Gartner, "Magic Quadrant for Cloud Database Management Systems," Gartner, 2020.

[16] [Microsoft Croporation, "Track and remediate potential database vulnerabilities with SQL Vulnerability Assessment," 2017.

[17] EC-Council, "EC-Council Blog," 04 06 2020. [Online]. Available: https://blog.eccouncil.org/what-are-sniffing-attacks-and-their-types/.

[18] PortSwigger, "The web vulnerability scanner that does more," PortSwigger, [Online]. Available: https://portswigger.net/burp/vulnerability-scanner. [Accessed 01 02 2021].

[19] Burp Suite Professional, "Features," Burp Suite Professional, [Online]. Available: https://portswigger.net/burp/pro/features. [Accessed 01 02 2021].