International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

A Technical Review of SQL Injection Tools and Methods: A Case Study of SQL Map

[1]Mahmoud Baklizi, [2]Issa Atoum, [3]Nibras Abdullah, [4]Ola A. Al-Wesabi, [5]Ahmed Ali Otoom, [6]Mohammad Al-Sheikh Hasan

[1]Computer Science/Network Department, Faculty of Information Technology, Al-Isra University, Amman, Jordan, mbaklizi@iu.edu.jo
[2]Sofware Engineering Department, Faculty of Information Technology, The World Islamic Sciences and Education, Amman, Jordan, issa.atoum@wise.edu.jo
[3]School of Computer Sciences, Universiti Sains Malaysia ,11800 USM Penang, Malaysia; Faculty of Computer Science and Engineering, Hodeidah University, Hodeidah P.O. Box 3114, Yemen, neprasf@gmail.com
[4]Faculty of Computer Science and Engineering, Hodeidah University, Hodeidah P.O. Box 3114, Yemen, ola.wosabi@gmail.com
[5]Faculty of Science and Information Technology, Irbid National University, Irbid, Jordan, aotoom@inu.edu.jo
[6]Computer Science Department, University of Petra, Amman, Jordan, malsheikh@uop.edu.jo

Submitted: 22/07/2022 **Accepted:** 25/09/2022

Abstract: SQL injection is considered one of the most dangerous threats to websites and also databases, such vulnerability enabling the attacker to access the web and the databases. As it accesses databases it might change, steal the data, or destroy the database utterly. Currently, and with the implementation of sqlmap found in the literature being scarce and limited, SQL injection detection tools and methods are used without any detailed analysis of their strength and weakness. This paper demonstrated different types of SQL injection with an example, also we know how to detect the SQL injection, the paper shows the important tools that enable the detection of dangerous attacks to prevent the SQL injection and compares them according to the important performance parameter measures. Finally, with the implementation adopted on an ethical and legal website, the proposed paper implemented the most important tool which is called sqlmap. The implementation results reveal access to the database and extract the username and password.

Keywords: *SQL Injection, SQLMap, SQL Tools, Blind Injection,* Website Vulnerabilities

1. Introduction

The huge development in information technology last year led to a big acceleration in web applications on a wide scale in all organizations, whether they were government or private organizations. Dealing with web applications has become a fundamental task in all electronic transactions, such as, banking transactions, social media, student and teachers transactions, credit cards, and bank transfers [1]. Such development facilitates these transactions in a short time and minimize the effort required for storing important information in a database, which plays a main role in storing, retrieving and, processing these data [2].

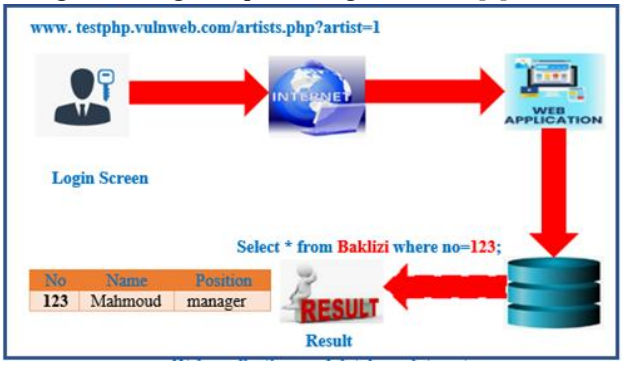

Fig 1: Web applications and databases interact

In a technical way, the website has been designed in a way that suits the users in one of the programming languages, such as PHP and HTML. These languages interact immediately with the database management system (DBMS) using the script that wrote by the programmer. Then the user can deal with the database by creating tables, adding data, and retrieving data [3]. See Fig. 1 which illustrates the interaction between the web and database.

This scenario where more organizations used as a standard in web applications facilitates the aforementioned electronic transaction that we mentioned before. However, the aforementioned approach may be a target for attacks by attackers that causes many problems that lead to access to sensitive data, changing the data stored in the database, which leads to grabbing credit cards, banking transfers from one account to another account, and annoyance of the users, with the main risk being to destroy the database utterly. These attacks from attackers called SQL injection take place by writing code that exploits a vulnerability in security in websites [4]. Many kinds of attacks that use SQL injection like SQLIA, which enables users to access the data through a query and destroy them. This causes financial loss and there is another threat by HTTP POST, which is one of the

most important methods used to pass the data to the server. Furthermore, HTTP POST is considered optimal for connecting with the server.

Current SQL injection detection tools and methods are used without any detailed analysis of their strength and weakness. Moreover, the implantations of SQLMAP found in the literature are scarce and limited. [5]. The researchers used many application programs to defend against SQL injection [6]. But it was enough to protect the database from an attacker; therefore, they presented many tools and methods. Here is presented SQL injection detection.

This paper studies various SQL injection tools, and methods and does extensive experiments on their implantation in practice. We used a new performance measure to compare tools to find the best tool for SQL injection, and then we applied the best tool in a practical scenario [7].

The remainder of this paper is organized as follows. Section two discusses the related work of this paper. Section three shows the SQL injection overview and detection approach. Section four discusses the SQL Injection Tools. Section five discusses the SQL injection Scenarios Study. Finally, Section six provides the conclusions and directions for future research.

2. Related work

The investigations on SQL injection tools are limited. For example, Shriya Vyamajala uses one SQL injection tool for people to understand SQL attacks simply. Moreover, the researcher does not focus on other SQL injection tools to show the weakness in SQL injection tools [8]. Areej Algaith uses and presents results of analyzing the performance of Static Analysis Tools, without showing the parameters performance measure for other SQL injection tools [9]. However, the list of performance measures is not enough to select the best tools for a specific SQL injection scenario [7]. A critical review of SQL injection was used in this paper. As a result, we have two themes of SQL injection types, Simple and blind. Figure 2 illustrates the type of SQL injection.

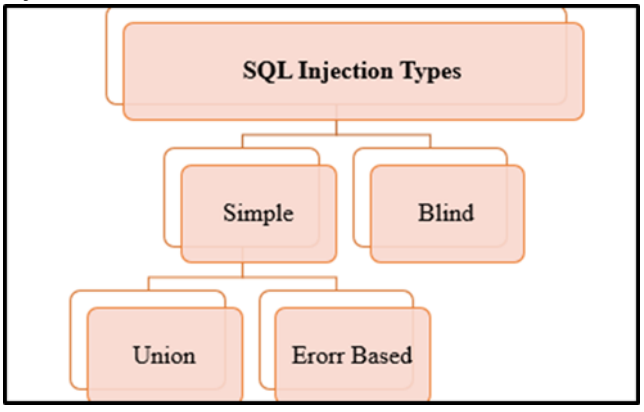

Fig 2: SQL injection types

In this part of the paper, the SQL injection types are thoroughly discusses. So, every type will be explained with its division and how the websites were attacked through weakness points. Moreover, it explains whether all SQL injection types run in synchronicity or if every type runs alone. Finally, it introduces examples for every type of SQL injection. See Fig. 2 illustrates the type of SQL injection.

SQL implementations. Small examples were given in the literature. To the best of our knowledge, this paper could be a contribution to those papers that carries out the full SQLMAP implementation. Further, the full source code is available to the public.

2.1. SQL Injection overview

SQL injection is a kind of web application vulnerability, which enables the attacker to modify and insert SQL statements and retrieve the data from the database. In case the user data is not protected enough, without varication and encoding the attacker can access the user sensitive data, such as credit card or some insensitive financial information [10].

In this paper, we illustrate the structure of Query Language (SQL), which is considered the real base in SQL injection. SQL is a language that depends on texts, to deal with database commands and queries which is resides always in the server-side, such as insert, update, create and delete [11]. To access the database obtained by the Query, which is executed by select command, which plays a main role in retrieving the data from the database in a table or more. Then the SQL query allowed the user to describe or insert the desired data, and after that leaves the DBMS, which is responsible for interacting immediately with the database and planning and understanding the processes.

To know the information, go through the query to the database, if it is not tested exactly, there is a chance SQL injection occurs. See the following example that illustrates the normal SQL query (Baklizi table of job information)..

```
select job from Baklizi where name
= “Mahmoud” and password= 123;
```

SQL injection depends completely on incorrect input and SQL commands through the web applications which goes through finally in databases. The attackers exploit this vulnerability to access the database and control, update, and destroy it. See the following example that shows the SQL injection statement using the SQL query.

```
Select * from Baklizi where name =’ “+ Mahmoud’ or 2=2 –
+ “’ AND password=’ “+ 123 + “’ “;
```

Finally, many recommendations help to degrade or prevent SQL injection for web applications. Consequently, SQL injection reduces the dangers of databases. One of the most important things that is considered dangerous on SQL statements is character spacing, which is not good to imply

to SQL statements but after the filtration process. And to be sure of its contents so as not to be caused by SQL injection. Also, we should be careful to avoid explaining the program and giving information because the hacker according to his experience can understand such information, he can access the weakness point that enables him to inject SQL injection. Also, the matter could be considered to avoid using the alert message, because it is a weak point which the hacker can use to access the web and database. Finally, it is advised to use guarantee tools to reveal weakness points, which could show you any weakness point you do not know or are not interested in and then you can avoid it before it comes to the hacker [12].

3. SQL injection detection approach

Test the web applications if they are connected to a database or not to access the database, test, and trial by injecting a query in the web application or URL to try to generate an error. This refers to the vulnerability existing in web application. Also, try to input the expected string value that the user always uses, using the UNION command, which is used in SQL detection that depends on connecting the main query select with the attacker query explained in detail in the next section. For that, the generating error message gives the attacker information whether to clearly be dependent on it with executing SQL query. Table 1 illustrates the character spacing used by the attacker.

Table 1. Character spacing used by the attacker

character	task
--	Line comment
“or”	String
/*---*/	Many lines comment
+ ,||	concatenate
?php1=abc&ad=mar	URL
’0:0:10’	Wait for the time delay

One of the most important and popular methods to detect SQL injection is an experience in writing the code by using high-safe language. Also, using the black box testing, which is considered one of the additional tools that are used to protect web applications, what makes it unique is that there is no information inside the code and no need to process any information about the network or the system. The person that he wants to test the weak points in the web application according to the attacker’s view. For that, using special characters, white space, SQL keywords, and oversized requests to define different terms for web applications [10]. Another way that detects SQL injection is fuzzy testing. This method is used to disclose errors in the code by inserting an amount of data to destroy the web application. In this method, the attacker executes different programs on the webserver to try to access the database. Therefore, fuzzy testing aims to direct access to the database and in this method, the identity of the attacker is unknown, at the same time the attacker takes advantage of exploiting security vulnerability and illegal access to the database [13].

The researchers have built many algorithms and tools that help in detecting the SQL injection and keep the web application secure [15 ,14]. Kanchana presents an algorithm to detect SQL injection to avoid breaches from attackers [16]. On the other hand, many automated tools depend on comparing normal queries and injection queries from the attacker .[17]

AMNESIA is designed to detect SQL injection attacks, it is a tool designed to detect if there is an injection or not. AMNESIA works by extracting from the code most of the queries that allow use and there is nothing that prevents it from using being not malicious. When the web runs the tool starts executing by comparing between the new query and allowed query and not malicious. Consequently, any query dos not suit stops directly. The advantages of this tool are short executing time which proves that it is fit as a tool to prevent the SQL injection [18].

The smart matrix depends on an array that sores the legal process to work and creates a private query for injection. Then, it is compared with a legal query that is sored in the array. Finally, the tracing process starts to get the date and the IP address. Subsequently, this algorithm is considered good for SQL detection. See Table 2 which illustrated the SQL detection result in smart matric [19].

Table 2. SQL detection result in smart matric

The Address	SQL injection Type	Time and date
127.0.0.1	%	2013-11-14 22:8-56
127.0.0.1	=	2013-11-14 22:20-36
127.0.0.1	LIKE	2013-11-14 22:21:2
127.0.0.1	UPDATE	2013-11-14 22:21:52
127.0.0.1	INSERT	2013-11-14 22:22:41
127.0.0.1	1	2013-11-14 22:25:48
127.0.0.1	DELETE	2013-11-14 22:26:38
127.0.0.1	1	2013-11-14 22:27:37

The OWASP detects many breaches malicious because of SQL injection, which is a danger to web applications and databases. This study shows how to detect the SQL injection automatically not manually. and it is effective in Table 3 compared to detecting the weak points that allow the attacker to access the sensitive data between the automatic dedication query and normal detection query [20].

Table 3. Automatic and normal query comparison

Number	Details	Database results	Final Results
Q1	“Normal Query” AND “SQL injection”	S_D = 203 IEEE = 73	276-12(duplicate)=”264”
Q2	(“Machine learning”) AND (“SQL injection”)	S_D = 54 IEEE = 32	86-10(duplicate)=”76”

4. SQL injection tools

In the previous part, we learned about the types of SQL injection that attack the website and databases, and this was a major reason for the emergence of many tools that are used by the attacker to inject websites through them. These tools help the attacker to deal with many types of SQL injection and also these tools. It has a main role in facilitating the work of the attacker. In this part, we list a group of the most important tools that attackers use in their attacks against websites and databases, with a comparison of the most important elements that are important to have in these tools. In addition, this paper presents an actual application of the best tool among them on a legal and ethical site to access the database, tables, and data that belongs to the user, such as the username and the password.

Blind SQL Injection: This tool works automatically, as the hacker uses it to find any weak point to use to pounce on any database, this tool can deal with all types of databases, and it depends both on submitting questions to the server whose answer is true or false and in its work on machine learning. On the other hand, Blind SQL injection has a drawback which depends on test and trial, that it takes a lot of time for processing and maybe no right result occurs [21].

Marathon: This tool is designed to deal mainly with blind SQL injection types and relies on writing a complex query to understand and deal with blind SQL injection. One of the most important features that distinguish it is that it works to add values and variables inside cookies to control and access sensitive data. Marathon has many limitations, such as it cannot deal with system files that make it specific and dependent on writing a query to access the database [22].

Havij tools: This type is also executed automatically as it is interested in finding a weak point and exploits it on the web page and takes care and focuses on accessing system files and sabotaging the operating system, as it retrieves the required data from the system. The limitations of the Havij tool represent in cannot deal with all available databases and databases and depend on adding a variable in cookies that make the retrieve the data complex and maybe the data was retrieved is not important [23].

SQL brute: This tool is designed to deal with blind SQL injection types, and its main goal is to extract data from databases and deal with oracle databases. The tool works automatically based on machine learning. The limitation of SQL Brute tests more than one password to get to the correct password, and this requires a great deal of time. It is possible during experimentation for such a case that the target has noticed that one of the attackers is trying to reach it and takes action against this attack [24].

Sqlninja: This tool aims to find a weak point in the server, which in turn penetrates and controls it, and this is one of the most dangerous types of tools available. One of its advantages is that it uses VNC Server to get VNC Access to the server to be hacked. In the attack, such as the SQL server version, it is clear what permissions are granted to the server user, and we can ensure whether xp_cmdshell is enabled or not. It deals with all types of databases. It supports proxy servers, cookies array, and SSL. Many tools cannot deal with system files and this makes them specific .[25]

Absinthe: This tool deals with blind SQL injection types and is designed to speed up the data retrieval process. This tool is classified as working with a web page, where it asks questions that result in true or false. One of the well-known cases depends on the graphic interface, and the main goal of this tool is to speed up the process of recovering data from databases. The limitations of Absinthe are that it cannot deal with all available databases and it depends on trial and error [26].

Pangolin: It is considered one of the tools that work automatically, as it works like other tools to discover security vulnerabilities, as when accessing a direct vulnerability, it works automatically to choose between a set of stored options to control the database and retrieve the necessary tables and data. This tool is characterized by its ability to empty the database and its contents of tables and columns. Most types of databases are supported. This tool cannot deal with system files and this makes them specific and makes them deal just with file systems [27].

Sqlier: It is a tool dedicated to dealing with the URL and identifying the places of weakness in it, and then this tool extracts the important and necessary data to exploit the existing vulnerability. It does not need any intervention from the user, this is normal, but it may need intervention from the user if he cannot guess the names of the tables, for example. One of the most important features of this tool is its use of the union function in its work to extract the password. The drawbacks of Sqlier is that it cannot deal with all available databases and cannot deal with system files and this makes them specific. Finally, this tool is suitable in sites that are not well protected and usually not in the database that contains important and sensitive data [28].

SQLsus: It is also an open-source tool written in Perl. Through this tool, you can access the database and extract data from it by building a custom query for this purpose. You can also deal with web files, download them, copy the database completely, and have access to the MySQL console. The drawbacks of SQLsus tool are in dealing with the web directly, either through the URL or writing a query to access the database [29]

SQLMAP: It is considered one of the powerful tools in SQL injection for its great ability to detect vulnerabilities and exploit them in a great way to access databases, as well as quick access to tables in databases and execution of commands on operating systems. Among its features, it supports most types of databases currently available. This tool works with many types of SQL injection, the most important of which are blind SQL injection, error based, and union SQL injection [30].

See the following Table 4, which illustrated the comparison between SQL tools.

Table 4: Comparison between SQL tools

Tool_Name	Database Interacting	Support File System	executed automatically	Depending on machine learning	approach	Available source
Blind SQL Injection	Most of Database	No	Yes	yes	Ask question answers is true or false	“www.labs.portcullis.com.uk”
Marathon	SQL Server, Oracle, and MySQL	No	No	no	Insert variables and values in cookies	“www.marthontool.codeplex.com”
Havij tools	Interact with Web	Yes	Yes	yes	Retrieve the required data and information	“www.itsecteam.com”
SQL brute	Oracle	No	yes	yes	A large number of passwords to find the real password	“www.gdssecurity.com”
Sql_ninja	SQL Server	No	Yes	yes	Use VNC Server to get VNC Access for the target server	“www.sqlninja.sourceforge.net”
Absinthe	Interact with Web	Yes	Yes	yes	Ask question answers is true or false	“www.darknet.org.uk”
Pangolin	Most of Database	No	Yes	yes	Depend on choosing store commands to access the database	“www.nosec.org”
Sqlier	Interact with URL	No	No	no	Use union to retrieve the password	“www.bcable.net”
SQ_Lsus	MySQL	Yes	No	no	Create a query to access the database	“www.sqlsus.sourcefoge.net”
Sqlmap	All Database	Yes	Yes	yes	execute commands on the operating system to access tables of a database	“www.sqlmap.org”

In this paper, a comparison table was presented that shows the most important elements of interest to the hacker and through which he decides to use the tool that achieves his goals to reach his goal. We note from the table that the type of database that the tool deals with is very important. For example, some tools cannot deal with all available databases and some cannot deal with databases such as Havij, Sqlier, and Absinthe, and we note that some of them can deal with all databases such as SQLMAP and this is a strong motivation to use such types of tools and access important data, where it is known that important data is stored in a protected database. As well as concerning dealing with system files, many tools cannot deal with system files and this makes them specific, such as Pangolin and Sqlier.

And many of these tools are mentioned in the table, and also many of them can access and deal with system files such as Pangolin and SQLMAP, and this helps a lot in changing the files for the benefit of the user of the tool, which gives him an incursion and change to get to what he wants.

There is also an important element of the bases of comparison, whether the tool can work automatically or not. This feature depends on the method of building the tool, if it works automatically, you can access the database within multiple kittens built inside the tool without the

intervention of the person. And then the tool checks and tries to enter without the intervention of the same person, such as SQLMAP.

Also, does it depend on machine learning? This feature is also related to the one before. Machine learning enables the tool to work systematically and be based on the rules and experience of its programmer, so that it can deal with the responses that may be intended to protect data and sites; an example of this feature is SQLMAP.

Now concerning the method of work, the tools differ in the way they work according to the design of the tool and its programming, including what depends on trial and error, such as blind SQL and Absinthe. Some of them depend on adding a variable in cookies, such as Marathon and this includes him retrieving information that may be restricted to him to access something of interest, such as Havij. And some of them use the method of experimenting with more than one password to get to the correct password, and this requires a great deal of time. It is possible during experimentation for such a case that the target has noticed that one of the attackers is trying to reach it and takes action against this attack, for example, SQL brute.

Also, some tools store commands in the system to access the database, such as Pangolin. This method aims to sabotage more than to access data to steal it.

Many tools deal with the web directly, either through the URL or writing a query to access the database, but this method is suitable in sites that are not well protected and usually not in the database that contains important and sensitive data such as Sqlier and SQL plus.

Select * from Baklizi WHERE name =' ma' OR '1'= '1';

One of the best tools used is the one that can access the database and execute its commands to access all the data stored in databases such as SQLMAP.

Based on the foregoing, we note that the SQLMAP tool, compared to the aforementioned tools, is considered a powerful tool as it deals with all databases and works automatically through which we can access databases and deal with tables and data easily and flexibly.

5. SQL injection scenarios study

A. SQL injection types

In this part of the paper, the SQL injection types are introduced in detail. So, every type will be explained with its division and how the websites were attacked through weakness points. Also, this part of the paper shows if all types run in synchronicity or if every type runs alone. Finally, it introduces examples for every type. See Fig. 2 illustrates the type of SQL injection.

5.1. Simple SQL injection

This kind is executed through SQL query by inputting a group of strings inside the stamen, where one of the methods that are used in SQL injection is the comment, which is written in the last of the statement, and which is considered a part of SQL query that is written by the user. As shown in the following example.

Select * from Baklizi WHERE name = ' ma' AND Position IS NULL; - -';

Fig 3. Legal and ethical website

Also, maybe the attacker inserts a wrong query, to obtain useful information to access his goals, such as injecting table names. As one method of the all the methods used, the attacker can inject a statement where always its result is true to give him a result where, in all cases, even the WHERE condition is wrong. Also, the OR operator always obtains the right results, if one of the conditions is true. See the following example that uses an OR operator.

To make implementation of the previous methods, many legal and ethical websites can be used to implement acunetix. The proposed paper introduces real implementation to execute the previous commands, to show its effectiveness on the websites that contain a vulnerability that can inject and access sensitive data and information. See Fig. 3 which shows the legal and ethical website.

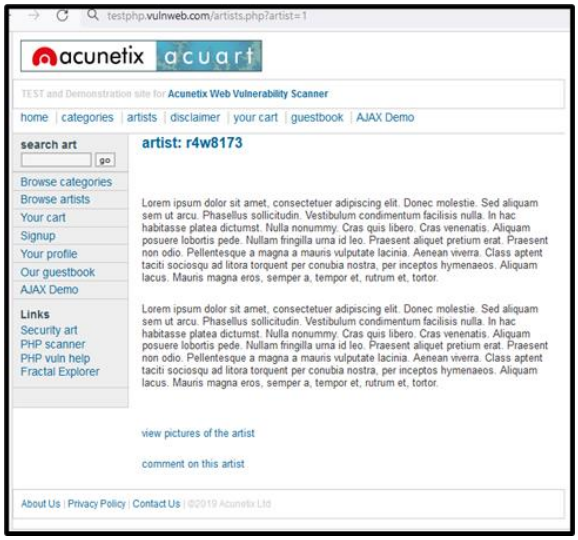

Fig 4. Failing to contents appear

From the previous figure, the website is executed without any error see the input URL that is related to the following legal and ethical website.

testphp.vulnweb.com/artists.php?artist=1

Also, the URL runs without a problem and all the contents appear as all websites that run normally without injection. The proposed paper put at the end of the URL the popular character space that was used to test the web if it has a weak point or not. Subsequently, the number 1 at the end of the URL changed to the value 4, see Fig. 4. The result reveals that contents of the website are failing to appear, which means, among other things, that the website has a weak point and gives the attacker a chance to inject SQL injection to access the database and sensitive data.

As we see, the web has a vulnerability point in the current website. So, we will inject an OR operator, and the contents of the website will appear content. The OR operator used by the attacker to obtain the result is always true, see the Fig. 5 that illustrates the result after injection.

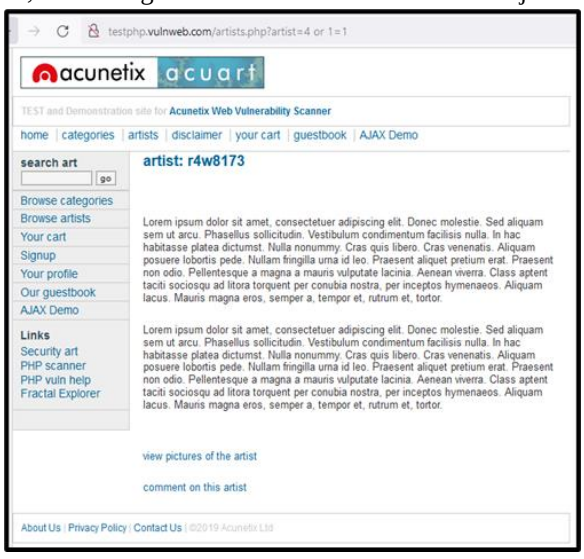

Fig 5. Result after injection

As we see, the first part of the query in the URL is wrong but the web page showed all its content because the OR operator result is right regardless of the first condition, this is how the hacker tries to reach the web.

As mentioned above the simple type is divided into union and error based, this part introduced the UNION type in detail.

5.1.1 Simple SQL injection

This type used depends mainly on the user's use of this operator, meaning if the user uses it, the hacker must take advantage of the weakness that exists as a result of using it and use it, and usually the Union precedes the order by, which is very important in this case to know the number of columns available in the database.

It is fortunate that the part before Union, this is for the user, does not concern the hacker, who has the hacker after Union, so I want to leave the sentence before Union always wrong so that the result that pertains to the hacker is not mixed with the result that pertains to the original user, so let the first queer have a value that gives an error result until Make sure that any result that will appear is the result of the hacker's sentence on which he will build an injection and what he will do as a result of the results that will appear to him. Look at the following examples that illustrate the work of the Union.

5.1.2 Error based SQL injection

It is one of the injection methods made by the hacker, where the aim is to target the database, mainly to collect information from it. This is where it is executed when the output is an error from the database, meaning that it depends on the error messages that results from the private server in the database.

The following example illustrates the database name through injection depends on error-based SQL injection.

URL>> or 1= convert (int, (Database name))- -

5.2 Blind SQL injection

This type of injection is like SQL injection, but there is a simple difference. Blind SQL injection depends on the error message, on the other hand, blind SQL injection did not depend on the error in the message. Therefore, Blind SQL injection is used mainly to access sensitive data or destroy the data in the database. In this method, the attacker steals the data using true or false questions through SQL query. Also in the Blind SQL injection, the attacker can extract the database name using the time-based blind injection method. The attacker guides the brute attack to the database name using the time before executing the query and sets a time after executing the query then the user benefits from the gain results [31].

B. SQLMAP Implementation

In this paper, the most important tools currently used by hackers, which are working to find a weak point in the database web application, were presented. SQL injection has multiple goals, some of which are concerned with accessing and controlling databases, with others focusing on data sabotage and access to sensitive information. Given the importance of these tools and because they are mainly used by hackers, this paper presents a scenario for using SQLMAP to hack the ethical and legal website "testphp.vulnweb.com/artists.php?artist=1."
The program was downloaded on the operating system WIN10, and the download of Python requires downloading it to work with the sqlmap tool.

The following steps show the steps to access the site and extract the user and password for the table that contains them
Run the program after and access the root and wrote the following command "Sqlmap.py," see Fig. 6 which shown the SQLMAP main screen.

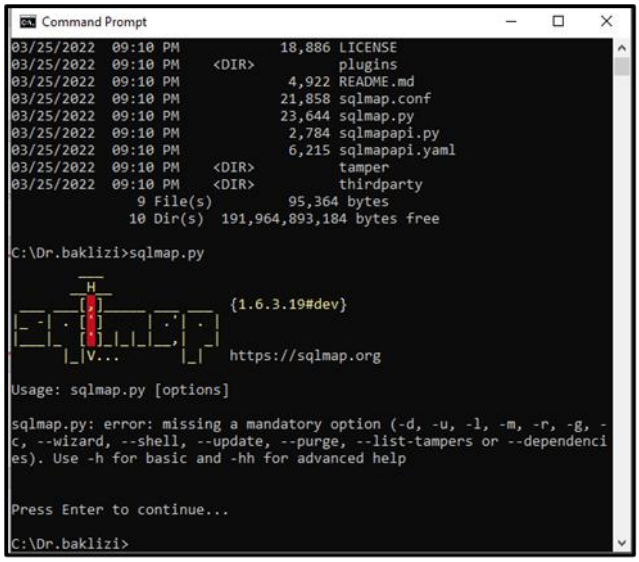

Fig 6. SQLMAP main screen

2- sqlmap.py -u http://testphp.vulnweb.com/artists.php?artist=1–DBS
This sentence is to extract the databases available on the site where the acuart database and information_schema were extracted
See Fig. 7 which shows the names of the databases available on the site

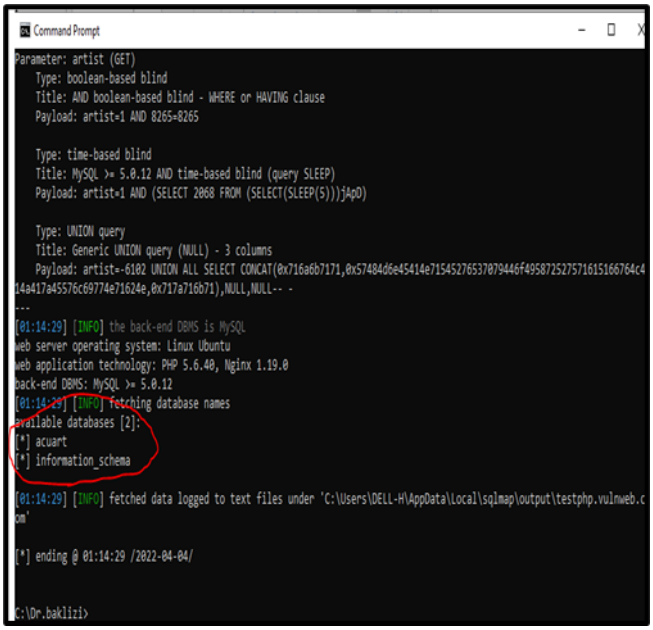

Fig 7. Extract database names

3- sqlmap.py -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart–tables
This syntax is used to extract the names of the tables available in the acuart database. Look at Fig. 8.

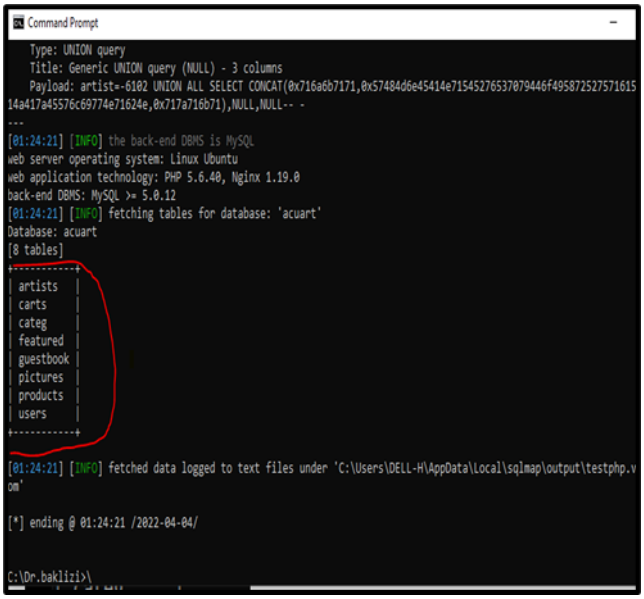

Fig 8. Extract table name

We also note that we extracted all the tables in the acuart database, and because of the available tables, the user's table is expected to contain the username and password of the user, so the attempt will start by injecting into the user table to reach the desired.
4- sqlmap.py -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users–columns
This command is used to show the columns available in the user's table. See Fig. 9.

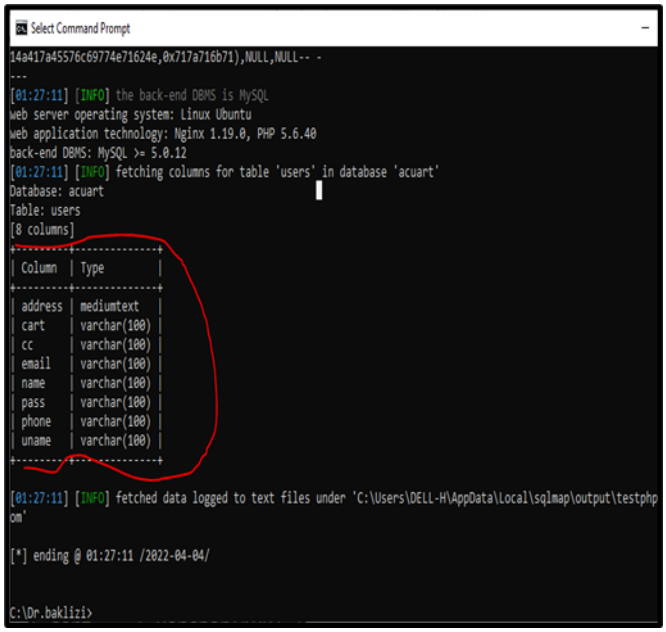

Fig 9. Column table

We note that the user's table contains uname and pass. We can now access the columns' values to gain full control over the site

5- sqlmap.py -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users -C unmae, pass–dump

This command is used to show the data for the unmae and pass columns. Look at Fig. 10.

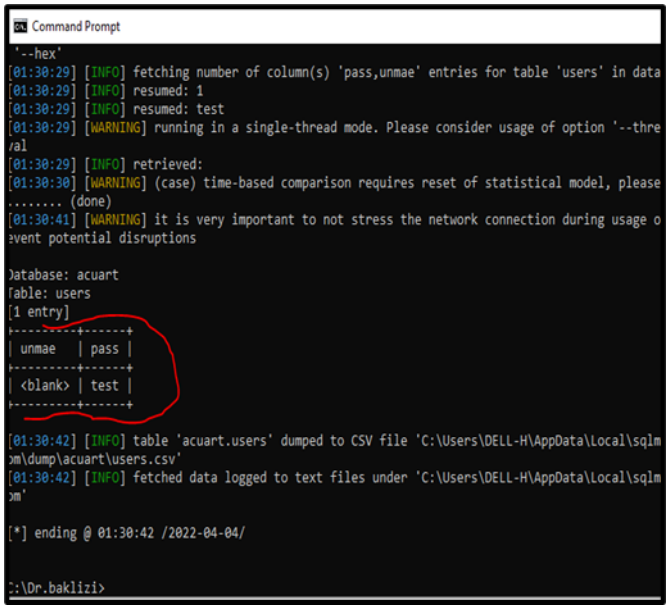

Fig 10. Extract username and password

If the value of the column uname is empty and also the password is tested, we have reached the control of the database. In the end, this tool was able to find a weak point in the tested site and through the commands inside it was able to reach the required database and then access the tables and columns and then access the information and data that enable it to fully control the database.

Based on the foregoing, the operating systems and protection programs must be improved, as well as writing the code securely and tightly that helps a lot in the spread of solutions to such dangerous attacks, but in return the rapid spread of websites increases weaknesses and allows a greater number of attacks and forces companies to develop continuously. For the protection systems, its network infrastructure and the operating systems available in the environment are of use.

6. Challenges of SQL injection

To protect it from SQL injection, which is considered a major threat as it makes many threats such as deceiving people that the website is the real one but it is not, changing prices, changing data in databases or even destroying them, reaching the highest validity of the admin, canceling access to Server, or access to important financial and confidential information, prevent important processes from running and modify existing records.

Several challenges exist and the security team should consider them before taking a decision:

1- SQL tools are scattered without complete real implementation in a practical case study. So, the proposed paper implements SQLMAP tool and generates the username and password for legal and ethical websites. Therefore, the selection of the best tool in regard to a specific problem, by make a comparison between the current tools.

2- Increase the experience of security manager depends on understanding the SQL injection types taxonomy. The paper provides a detailed analysis and experimental results of different scenarios

7. Conclusion

In this paper, the SQL injection is addressed as it is targeted for attack by hackers through the web to gain access to databases, thus accessing sensitive data, stealing important data, or completely sabotaging the data. We discussed in this paper the detection method used in detail. The result was that the sqlmap is one of the important tools that works automatically to achieve the goals of the hacker, the comparison being made with us touching on the types of SQL injection with the actual application of each type, and the most important tools used by hackers for use in accessing databases. Finally, the SQLmap tool was applied on a legal and ethical site to access the database of this site and then get the username and password and databases. The future goal is to protect the web and databases by building an algorithm that can deal with the input query and know its contents to filter it automatically using machine learning, in addition to knowing if the query contains an insert to deal with it independently because the insert is very important.

References

[1]. Tahir, F., A. Mitrovic, and V. Sotardi, Investigating the causal relationships between badges and learning outcomes in SQL-Tutor. Research and Practice in Technology Enhanced Learning, 2022. **17**(1): p. 7.

[2]. Falor, A., et al. A Deep Learning Approach for Detection of SQL Injection Attacks Using Convolutional Neural Networks. in Proceedings of Data Analytics and Management. 2022. Singapore: Springer Singapore.

[3]. Shah, A., et al., Blood Bank Management and Inventory Control Database Management System. Procedia Computer Science, 2022. **198**: p. 404-409.

[4]. Nouby M. Ghazaly, A. H. H. . (2022). A Review of Using Natural Gas in Internal Combustion Engines. International Journal on Recent Technologies in Mechanical and Electrical Engineering, 9(2), 07–12. https://doi.org/10.17762/ijrmee.v9i2.365

[5]. Baptista, K., E.M. Bernardino, and A.M. Bernardino. Detecting SQL Injection Vulnerabilities Using Artificial Bee Colony and Ant Colony Optimization. in Information Systems and Technologies. 2022. Cham: Springer International Publishing.

[6]. Ahmad, K. and M. Karim, A Method to Prevent SQL Injection Attack using an Improved Parameterized Stored Procedure. (IJACSA) International Journal of Advanced Computer Science and Applications, 2021. **12**(6).

[7]. Pawan Kumar Tiwari, Mukesh Kumar Yadav, R. K. G. A. . (2022). Design Simulation and Review of Solar PV Power Forecasting Using Computing Techniques. International Journal on Recent Technologies in Mechanical and Electrical Engineering, 9(5), 18–27. https://doi.org/10.17762/ijrmee.v9i5.370

[8]. Hu, H., Research on the technology of detecting the SQL injection attack and non-intrusive prevention in WEB system. Vol. 1839. 2017. 020205.

[9]. Azman, M.A., M.F. Marhusin, and R. Sulaiman, Machine Learning-Based Technique to Detect SQL Injection Attack. Journal of Computer Science, 2021. **17**(3).

[10]. Vyamajala, S., T.K. Mohd, and A. Javaid. A Real-World Implementation of SQL Injection Attack Using Open Source Tools for Enhanced Cybersecurity Learning. in 2018 IEEE International Conference on Electro/Information Technology (EIT). 2018.

[11]. Algaith, A., et al. Finding SQL Injection and Cross Site Scripting Vulnerabilities with Diverse Static Analysis Tools. in 2018 14th European Dependable Computing Conference (EDCC). 2018.

[12]. Chen, D., et al., SQL Injection Attack Detection and Prevention Techniques Using Deep Learning. Journal of Physics: Conference Series, 2021. **1757**(1): p. 012055.

[13]. Schwanz, L.E., et al., Best practices for building and curating databases for comparative analyses. Journal of Experimental Biology, 2022. **225**(Suppl_1): p. jeb243295.

[14]. Ping-Chen, X., SQL injection attack and guard technical research. Procedia Engineering, 2011. **15**: p. 4131-4135.

[15]. Saidu Aliero, M., et al., Classification of Sql Injection Detection And Prevention Measure. IOSR Journal of Engineering, 2016. **Volume 6**: p. 06-17.

[16]. Hlaing, Z.C.S.S. and M. Khaing. A Detection and Prevention Technique on SQL Injection Attacks. in 2020 IEEE Conference on Computer Applications(ICCA). 2020.

[17]. Tang, P., et al., Detection of SQL injection based on artificial neural network. Knowledge-Based Systems, 2020. **190**: p. 105528.

[18]. Natarajan, K. and S. Subramani, Generation of Sql-injection Free Secure Algorithm to Detect and Prevent Sql-Injection Attacks. Procedia Technology, 2012. **4**: p. 790-796.

[19]. Jang, Y.-S. and J.-Y. Choi, Detecting SQL injection attacks using query result size. Computers & Security, 2014. **44**: p. 104-118.

[20]. Halfond, W.G.J. and A. Orso. Detection and Prevention of SQL Injection Attacks. in Malware Detection. 2007. Boston, MA: Springer US.

[21]. Ramasamy, P. and S. Abburu, SQL INJECTION ATTACK DETECTION AND PREVENTION. International Journal of Engineering Science and Technology, 2012. **4**.

[22]. Ananthakrishnan, B., V. . Padmaja, S. . Nayagi, and V. . M. "Deep Neural Network Based Anomaly Detection for Real Time Video Surveillance". International Journal on Recent and Innovation Trends in Computing and Communication, vol. 10, no. 4, Apr. 2022, pp. 54-64, doi:10.17762/ijritcc.v10i4.5534.

[23]. Al-Maliki, M.H.A. and M.N. Jasim, Review of SQL injection attacks: Detection, to enhance the security of the website from client-side attacks. International Journal of Nonlinear Analysis and Applications, 2022. **13**(1): p. 3773-3782.

[24]. Ventura, R., Blind SQL Injection Attacks Optimization. 2020. 99-109.

[25]. SOOD, M. and S. SINGH. Study on sql injection-threats, attacks, types, prevention techniques and tools. in Proceedings of International Conference on Recent Innovations in Engineering and Technology. 2017.

[26]. Widiastuti, W. and A. Susanto, SQL Injection dengan Tools Havij dan Sqlmap. 2017.

[27]. Kushwaha, J. and D. Soni, A Survey on Malware & Session Hijack Attack over WebEnvironments. IOSR Journal of Computer Engineering (IOSR-JCE), 2018. **20**(2): p. 30-35.

[28]. Boyapati, B. ., and J. . Kumar. "Parasitic Element Based Frequency Reconfigurable Antenna With Dual Wideband Characteristics for Wireless Applications". International Journal on Recent and Innovation Trends in Computing and Communication, vol. 10, no. 6, June 2022, pp. 10-23, doi:10.17762/ijritcc.v10i6.5619.

[29]. Pundlik, S., SQLIJHS: SQL Injection Attack Handling System. International Journal of Engineering Research & Technology (IJERT), 2013. **2**.

[30]. Liban, A. and S.M. Hilles, Enhancing Mysql Injector vulnerability checker tool (Mysql Injector) using inference binary search algorithm for blind timing-based attack. 2014. 47-52.

[31]. Wheeler, R. BlindCanSeeQL: Improved Blind SQL Injection For DB Schema Discovery Using A Predictive Dictionary From Web Scraped Word Based Lists. 2015.

[32]. Gupta, D. J. . (2022). A Study on Various Cloud Computing Technologies, Implementation Process, Categories and Application Use in Organisation. International Journal on Future Revolution in Computer Science &Amp; Communication Engineering, 8(1), 09–12. https://doi.org/10.17762/ijfrcsce.v8i1.2064

[33]. Muhammad, K., SQL injection detection and exploitation framework for penetration testing. 2019, London Metropolitan University.

[34]. Jose, A., et al., A Novel Approach for Password Cracking by Integrating Sqlsus and John the Ripper, in International Conference on Emerging Computer Applications. 2020. p. 111-123.

[35]. Kumar, S., Gornale, S. S., Siddalingappa, R., & Mane, A. (2022). Gender Classification Based on Online Signature Features using Machine Learning Techniques. International Journal of Intelligent Systems and Applications in Engineering, 10(2), 260–268. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2020

[36]. Azman, M., M.F. Marhusin, and R. Sulaiman, Machine Learning-Based Technique to Detect SQL Injection Attack. Journal of Computer Science, 2021. **17**: p. 296-303.

[37]. Foong Yew, J. and S. Vinesha. A Study of SQL Injection Hacking Techniques. in Proceedings of the 3rd International Conference on Integrated Intelligent Computing Communication & Security (ICIIC 2021). 2021. Atlantis Press.