SUDAN UNIVERSITY OF SCIENCE & TECHNOLOGY
FACULTY OF COMPUTER SCIENCE & INFORMATION TECHNOLOGY

SQLI SCANNING TOOL FOR WEB APPLICATIONS

أداة فحص **SQLI** لتطبيقات الإنترنت

OCTOBER 2015

THESIS SUMITTED AS A PARTIAL REQUIREMENTS 0F B.Sc. (HONOR) DEGREE IN COMPUTER SCIENCE

بسم الله الرحمن الرحيم

SUDAN UNIVERSITY OF SCIENCE & TECHNOLOGY
FACULTY OF COMPUTER SCIENCE & INFORMATION TECHNOLOGY

SQLI SCANNING TOOL FOR WEB APPLICATIONS

أداة فحص **SQLIA** لتطبيقات الإنترنت

OCTOBER 2015

PREPARED BY

STUDENT: FATIMA MOHAMED ALI
STUDENT: MARAM MAKKAWI MUBARAK
STUDENT: OMNIA MOHAMED ADAM

THESIS SUMITTED AS A PARTIAL REQUIREMENTS 0F B.Sc. (HONOR) DEGREE IN COMPUTER SCIENCE

SIGNATURE OF SUPERVISOR **DATE**
…….OCTOBER 2015

T. Dalia Mahmoud Elsir

آية

قال تباركوتعالى:

}يَرْفَعِ اللَّهُ الَّذِينَ آمَنُوا مِنكُمْ وَالَّذِينَ أُوتُوا الْعِلْمَ دَرَجَاتٍ {

[المجادلة: 11]

بسم الله الرحمن الرحيم

الحمد لله حمدا كثيرا طيبا مباركا فيه كما ينبغي لجلال وجهه الكريم وعظيم سلطانه، والصلاة والسلام على خير خلق الله المصطفى الأمين النبي الكريم سيدنا محمد صلى الله عليه وسلم وعلى آله وصحبه ومن تبعه بإحسان الى يوم الدين وسلم تسليما كثيرا، نعوذ بالله من شرورانفسنا وسيئات اعمالنا، من يهد الله فهو المهتد ومن يضلل فلن تجد له وليا مرشدا وبعد، إن نعم الرب على العباد وافرة لا تعد ولا تحصلى رز قهم اياها بغير حول منهم ولا قوة فالحمد لله على نعمه الظاهرة والباطنة التي ندركها والتي فوق ادراكنا والحمد لله الذي وهبنا السمع والبصر وانار ع قولنا وافئدتنا وهدانا الى دروب العلم ويسر لنا سبل المعرفة وعلمنا ما لم نكن نعلم، نحمد الله ان اعاننا على اكمال هذا البحث في محاولة منا لتوفير حلول لبعض المشاكل التي تواجه المجتمع وتؤر قه ونسأل الله العلي الـ قدير أن يوف قنا للإستفادة من العلم فيما فيه صلاح الأمم وأن تتم الإستفادة من هذا العمل على الوجه الأمثل، وأن يكون عونا لمصممي ومطوري الموا قع الإلكترونية بشكل خاص، جعلنا الله ممن ينتفع بالعلم ويحفظه، والله من وراء الـ قصد وهو نعم المولى ونعم النصير.

الإهـــــــداء

يشرفتا ويسعدنا اهداء هذا البحث الى:

من اضئن لنا الدرب أمهاتنا الحبيبات:

أميرة عمر حمد

صفية العطا عبد الله

مها محمد الهادي

من شدوا على ايدينا دائما اباؤنا الأعزاء:

محمد آدم نجم الدين

محمد علي عمر

مكاوي مبارك ابوزيد

أستاذتنا الفاضلة داليا محمود السر

أساتذتنا في كلية علوم الحاسوب وتـ قاتة المعلومات

أساتذة جامعة السودان للعلوم والتكنلوجيا

إخواننا وصديـ قاتنا و زملائنا

كل من علمتا حرفا

أمنية، فاطمة، مرام

شكر و عرفان

نت قدم بالشكر لله سبحانه وتعالى الذي اعاننا بفضله الكريم على انجاز البحث على اكمل وجه فله الشكر الأعلى وله الحمد اولا وآخرا، كما ونت قدم بالشكر لكل من مد لنا يد العون في اخراج هذا البحث، ونخص بخالص الشكر الأستاذة الفاضلة داليا محمود السر المشرفة ال قائمة على هذا المشروع لحسن اشرافها وكريم مساندتها لنا، والشكر موصول الى الأستاذ الفاضل محمد اسامة حوايذة الله على مساعدته الكريمة لنا خلال مراحل المشروع، والشكر لجميع الأساتذة الأفاضل بكلية علوم الحاسوب وت قانة المعلومات الذين لم يبخلوا علينا بو قت او معلومة و قدموا لنا كل العلون والمساعدة والتشجيع، والشكر كذلك لكل من ساعدنا من زملائنا و زميلاتنا بالكلية ولأسرنا التي جاهدت وتكبدت المشاق في سبيل وصولنا لما بلغنا.فلهم جميعا جزيل الشكر والت قدير واجمل با قات من االثناء والإمتنان.

المستخلص

إن الإنترنت يقود العالم اليوم وهو يحتوي على الملاين من المواقع الإلكترونية لمختلف المجالات بحيث ان معظم الخدمات في الحياة اليومية اصبحت تقدم عن طريق الويب وبالتالي فإن اي اختراق في تلك المواقع من الممكن ان يؤدي الى اضرار قد تتراوح بين تعطل الخدمات الى إزهاق حياة الأفراد. إن اهداف هذا البحث تتمثل في تقديم أداة تقوم بفحص هذه المواقع للكشف عن نقاط الضعف التي يمكن استغلالها من قبل المخترقين وتقديم تقرير بتضمن جميع النتائج وذلك باستخدام تقنية اختبار الإختراق، وتكمن اهمية هذا البحث في ضمان أمن البيانات الحساسة التابعة للمواقع الإلكترونية عن طريق تقنية بسيطة وفعالة لجعل عملية إستخدام المواقع الإلكترونية تتم بطريقة أكثر راحة وأمان.

ABSTRACT

Today many services in people daily life are provided throw the web, so any problems in those websites can lead to damages vary from delay of services to threaten people's lives, the objectives of this research represents in delivering a tool that help in examine these websites for detecting any vulnerabilities that can be exploit by the hackers and provide full report contains all results.the importance of this research is to ensure the security of websites sensitive data through a simple effective technique in order to make the usage of websites more comfortable and safe.

Table of Contents

Table of figure

Table of tables

CHAPTER 1

Introduction

CHAPTER 1: Introduction

1.1 Introduction:

Internet becomes the most important infrastructure for living in this informatics technological world, these days internet is used for satisfying people with various services related to various different fields. One important feature of the internet lies in the ability to access to the network resources from anywhere at any time for 24 hours/7 days. Information related to a wide range of fields can be easily being found with just a few keyboard strokes. So this technology is helpful to get information easily, research, customer support, publishing message to the world, and lots of other services in many different field such as education, business and communication.

Internet contains millions of web sites for different purposes varying from business companies websites to social networking websites; people from all over the world are using them. As a result of this wide usage that involves exchanging, sending and storing sensitive information, many security problems may arise.

The remainder of this research will be organized as follows: chapter tow will provides a general view about the project background related fields and previous studies. Chapter three provides a background and basic information about the tools that used in the stage of project implementation. Chapter four analyzes the system using data modeling diagrams to better understanding for the system.

1.2 problems:

One of the most serious problems in the web is the appearance of the web hackers, who are a group of people that aims to break the security policy of the websites and web applications. Attackers find numerous ways to discover vulnerabilities and flaws in websites to allow them access secure and sensitive data in order to use it for different purposes. Therefore this research comes in an attempt to detect a group of major vulnerabilities that may serve as the entrance to break the security policy for websites.

The main problem of this research is that many website have codes contain various vulnerabilities that may result from injection attacks. This Attack is considered one of the most dangerous types of attacks that may compromise the whole computer system.

1.3 Research Scope:

The project aim to build a tool that scans websites against three types of SQL injection vulnerabilities including Tautologies, Union and Illegal Logically Incorrect Queries following penetration testing technique for websites that building using PHP technique, then display a report that includes the result of the detection scanning.

1.4 Objectives:

- Provide penetration testing tool to check some of SQL injection vulnerabilities on websites an attacker could exploit.
- Deliver a full Report contains various information to the user about the result of scan.
- Develop a tool that is safe, easy to use and don’t need deep knowledge about databases or web security.
- Providing the tool for free public use.

1.5 Research Methodology:

The research will use the descriptive approach as an appropriate approach to the nature of the research and its goals. A tool is developed to scan and detect the website against tree types of SQL injection attacks. To solve our problem we are going to take the attacker role and trying to inject the website and cause it to generate vulnerabilities through developing a simple tool that fallowing the penetration testing technique, Using the tool user Enter the website URL, then it’s possible to choose among a variety of testing options to perform on the code, after the test is done all bugs in the code will be delivered as an optimal report.

CHAPTER 2

Background and Related works

CHAPTER 2: Background and Related works

2.1 Introduction:

This chapter provides a general view about the project background, in the first part we are going to introduce an introduction to our project related fields, then in the second part we will provides a summery for the previous studies and related works.

2.2 Background:

2.2.1 Introduction to penetration testing:

Penetration testing is a comprehensive method to test the complete, integrated, operational, and trusted computing base that consists of hardware, software and people. The process involves an active analysis of the system for any potential vulnerability, It is done by simulating an unauthorized user attacking the system using either automated tools or manual method or a combination of both, It helps confirm the effectiveness or ineffectiveness of the security measures that have been implemented. The main goal of vulnerability assessment is to identify security vulnerabilities under controlled Circumstances so they can be eliminated before unauthorized users exploit them. Computing System professionals use penetration testing to address problems inherent in vulnerability Assessment, focusing on high-severity vulnerabilities. [1]

2.2.1.1 Benefits of Penetration Testing from Operational Perspective:

Penetration testing helps shape information security strategy through quick and accurate identification of vulnerabilities. Also provides detailed information on actual, exploitable security threats if it is encompassed into an organization's security doctrine and processes. [1]

2.2.1.2 Penetration Testing Strategies:

There are three strategies for penetration-testing:

1. **Black box:** In black box penetration testing, the testers have zero knowledge about the test target.
2. **White box:** In white box penetration testing, the testers are provided with all the necessary information about the test target. This strategy is referred to in as targeted testing where the testing team and the organization work together to do the test, with all the information provided to the tester prior to test
3. **Gray box:** Partial disclosure of information about the test target leads to gray box penetration testing. Testers need to gather further information before conducting the test. Based on the specific objectives to be achieved[1]

2.2.2 Introduction to Code injection:

Code Injection is a type of exploitation caused by processing invalid data input. The concept of injection attacks is to introduce or "inject" malicious code into a program so as to change the course of execution. Such an attack may be performed by adding strings of malicious characters into data values in the form or argument values in the URL. [2]

2.2.2.1 Code injection levels:

Code injection can be classified into three major levels as the fallowing:

- **Web level:**

In this form of injection attack, the attackers introduce improper scripts into the web browsers. Dynamic websites are more vulnerable to a type of code injection, called Cross-Site Scripting ("XSS"), than those traditional static websites.

- **Application/Database level:**

This form of injection attack aims to exploit database through read sensitive data from the database, modify database data, and execute administrative operations within the database, two common injection techniques, SQL injection and LDA injection, both fall into this category.

- **Operating System (OS) level:**

This form of injection concerning with the ability of execute OS commands,the attackers can inject unexpected and dangerous commands, upload malicious programs or even obtain passwords directly from the operating system. The common injection in this level called OS Command Injection. [2]

2.2.2.2 Major type of attacks in code injection:

Code Injection is the general name for various types of attacks which inject improper code into the script interpreter. This can be achieved through different dimensions which included:

- **SQL Injection:**

SQL injection attack consists of injection of malicious SQL commands via input data from the client to the application that are later passed to an instance of a database for execution and aim to affect the execution of predefined SQL commands.

- **LDAP Injection:**

Lightweight Directory Access Protocol (LDAP) is an open-standard protocol for both querying and manipulating X.500 directory services. The LDAP protocol runs over Internet transport protocols, such as TCP. LDAP injection is an attack technique of exploiting web applications that use client-supplied data in LDAP statements without first stripping potentially harmful characters from the request. When a web application fails to properly sanitize user-supplied input, it is possible for an attacker to alter the construction of an LDAP statement. (E.g. Database server, Web application server, Web server, etc.).

- **OS Command Injection (“Shell Injection”):**

OS command injection is also known as Improper Sanitization of Special Elements used in an OS Command and is a technique used via a web interface in order to execute OS commands on a web server.

- **Cross-site Scripting (“XSS”):**

Cross-site Scripting (“XSS“) is a type of injection attack, in which malicious scripts are introduced into the trusted websites. This exploitation would occur when a web application uses user-supplied inputs as an output without validating or encoding it. [2]

2.2.3 Introduction to SQL injection:

Structured Query Language injection (SQL injection) is a hacking technique and one of the top most threats against web applications. It's class of code injection attacks and has known as one of the most common threats to the security of database-driven applications. The main goal is to execute SQL codes and commands directly on the victim's back-end database through a web application via a form or URL parameters and gain unlimited and unauthorized access or makes changes to data. The main reason for rising SQL injection is the lack of user input validation.

2.2.3.1SQL injection attack types:

There are different methods of attacks that depending on the goal of attacker and they are performed together or sequentially. So SQLIAs are classified in various categories which are given below:

- **Tautologies:**

This type of attack is mainly used to inject conditional query statement with SQL tokens so they always evaluates true. Tautology attack is used to bypass authentication control and access to data by exploiting vulnerable input field which use WHERE clause.

- **Illegal/Logically Incorrect Queries:**

When any query is rejected, an error message is returned by SQL Oracle engine including useful debugging information. In this type of attack the attacker is exploiting this error messages and use it to find vulnerable parameters in the Database.

- **Union Query:**

This technique is used to join the result of the original query with result of another query; the attackers join SQLIA to safe query by using keyword UNION and then can get data about other tables from the application.

- **Piggy-backed Queries:**

In this type of attack, intruders exploit database by using query delimiter, such as ";" and appending extra query to the original one. In this attack database receives and execute a multiple distinct queries. It's very dangerous attack which could damage or completely destroy the table. If this attack is successful then there could be huge loss of data.

- **Stored Procedure:**

Stored procedure is a part of database that programmer could set an extra abstraction layer on the database. By using stored procedure a user can store its own function according to the need. In stored procedure, a collection of SQL

queries are included. As stored procedure could be coded by programmer, so, this is also one of the causes of SQLIA.

- **Alternate Encoding:**

In this type of attack the regular strings and characters are converted into hexadecimal, ASCII and Unicode. Because of this the input query is escaped from filter which scans the query for some bad characters which results in SQLIAs i.e. the converted SQLIA is considered as normal query.

- **Inference:**

In this type of attack, intruders change the behavior of a database or application. There are two well-known attack techniques that are based on inference: blind injection and timing attacks.

  - **Blind Injection:**
    Sometimes developers hide the error details which help attackers to Compromise the database. In this situation attacker face to a generic page provided by developer, instead of an error message.

  - **Timing Attacks:**
    A timing attack lets attacker gather information from a database by observing timing delays in the database's responses. This technique by using if-then statement cause the SQL engine to execute a long running query or a time delay statement depending on the logic injected.[5][6]

2.3 Related works:

2.3.1 A hybrid technique for SQL injection attacks detection and prevention:

Omer and Jibril present a hybrid technique that can secure systems from being exploited by SQL injection attacks, this hybrid technique combines static and runtime SQL queries analysis to create a defense strategy that can detect and prevent various types of SQL injection attacks.

The suggested approach is based on different stages to reject any malicious query from being passed through the database engine before its execution process, and those stages :for each database to be secured from SQLIAs, there should be a new replication database and it should contain a small amount of sample data, Creating “database_Behaviors” database ,that contains all system database queries and their expected behaviors that have resulted from SQL queries execution in normal cases, all SQL queries that are passing through the replicated database to monitors and traces the behaviors of the SQL query ,should also pass through multiple check processes to checking syntax, detect whether the received SQL query is valid and expected query or not. The idea here is to catch the objects that have been affected by the current SQL query whatever the type of such objects and create a list of these objects; the resulted list of affected objects will be compared with the “database_Behaviors”. If there is a query that handles all of the listed objects with the same type of behavior that is detected from the previous step then this behavior query will be added to a new list (Expected Queries). Any resulted behavior that is detected as a suspicious should be rejected and deleted from the actual database instance execution queue, otherwise the query will be transferred to the actual database instance for being executed.

This hybrid technique, can detect and prevent SQLIAs that are performed through the system or through a direct SQL query to the database, however occur time delay that the database recovery takes after the SQLIA is detected, that is leads to decreasing performance and many steps to execute this approach that is makes technique is complex. [8]

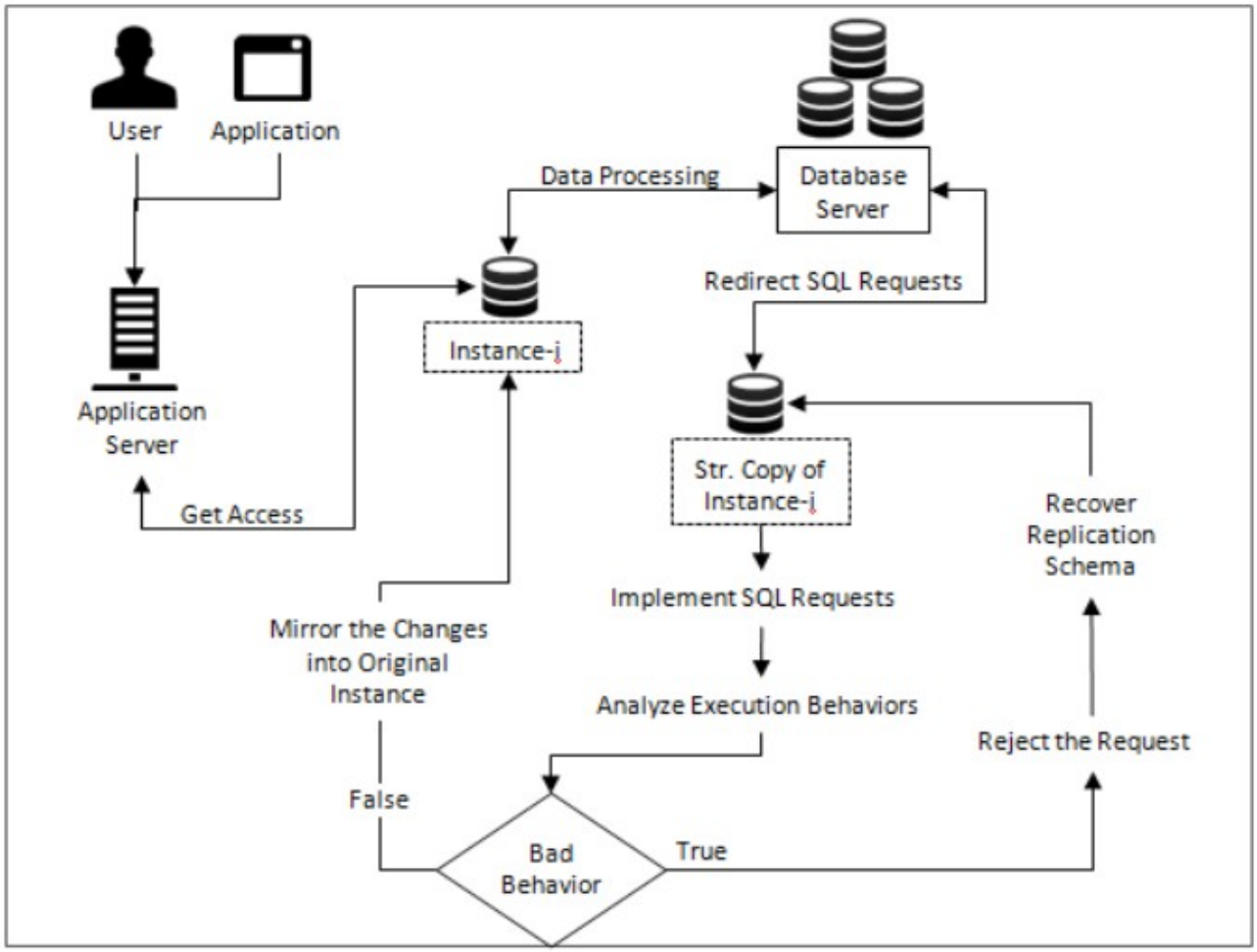


Figure2.1 Process Flow Diagramfor Suggested Approach

2.3.2 An analysis on Blocking of SQL Injection Attacks by Comparing Static and Dynamic Queries:

Whereas Minhas and Kumar discuss a technique to detection and prevention from SQLIAs which uses combined static and dynamic analysis as a solution for the problem of the increase needs to store secure and sensitive data in databases that are unsafe and able to be attacked.

The Proposed method is based on combining static and dynamic analysis, the static query structure is compared with dynamic query. In this database is maintained to store the valid query structure. These valid queries are also known as static queries; the attribute values of dynamic queries will be removed during the run time and compared with previously stored static queries having same number of tokens as in dynamic query. After that the

method locates for static queries having same number of tokens as in dynamic query. Then the dynamic query is compared character by character only with that static queries having same number of tokens. If match is found requested dynamic query is valid query otherwise it is SQL Injection.

This technique is reduce false positives and false negatives, very simple because not contain many steps to execute this approach , however there is a time delay that method locates static queries having same number of tokens as in dynamic query. [7]

2.3.3 A method of detecting SQL injection attack to secure web application:

Another solution to solve this problem, Manmadhan and Manesh proposes a method of detecting SQL injection attack to secure web applications. The basic idea is to check before execution, the intended structure of the SQL query. For this use semantic comparison .This Solution is based on the principle of dynamic query structure validation.

The idea requires that the application will not allow the user to enter any part of SQL query directly. Benign Query is contents valid Query, Original Query is generated by the application. Benign Query is generated from Original Query,This is done by replacing user inputs to the query with benign inputs, Check the syntax of the Benign Query to ensure its validity while doing the replacement, put Benign Query and Original Query in stack, Get the count of stacked queries in both original SQL query and Benign Query, Compare the count of stacked queries. If both counts are different, then we can directly report SQL injection attack and prevent that query from execution without going for semantic checking, otherwise construct a syntax tree of both Original Query and Benign Query and compare them. Here, syntax trees are created using java ArrayList structure, finally Compare the syntax trees. If they are equal, the query is valid and allows its execution. Otherwise, report injection and block the query.

This technique is efficient approach to prevent vulnerability because not consume big part of memory and use syntax tree to construct structure, this is make discover vulnerability is very easy. But this method for preventing SQL injection attacks in JSP web applications not all web applications. [4]

2.3.4 A Novel Approach to detect SQL injection in web applications:

Whereas Kumar et.al present a method to detect SQL injection in web applications, this approach based on grammatical structure of an SQL statement and validation. This method detects various types of SQL injection attacks.

Propose method to detect SQL injection attacks based on static and dynamic analysis. Identify un trusted user input and security sensitive operation in the web application, wrap every un trusted input and security operation with sql_Validator() Function , if input user not valid Block execution and redirect to error page, Separate the input from dynamic query(from user) , Compare the structure of dynamic query(dynamic query after removing input)with the structure of query generated by application(template query),if checksum () Function, of template query equal dynamic query structure is valid , then Validate the user input which parsed from query check whether attack pattern present in input, If no attack pattern is present in input then input is valid otherwise Input is malicious , finally If structure of dynamic query AND input is valid No SQL injection attack is there otherwise report injection.

The proposed method is simple comparing to other methods,for use functions very simple ,and not occurs delay time .however it is a good technique with fewer experiments that does not assure it accuracy and efficiency. [5]

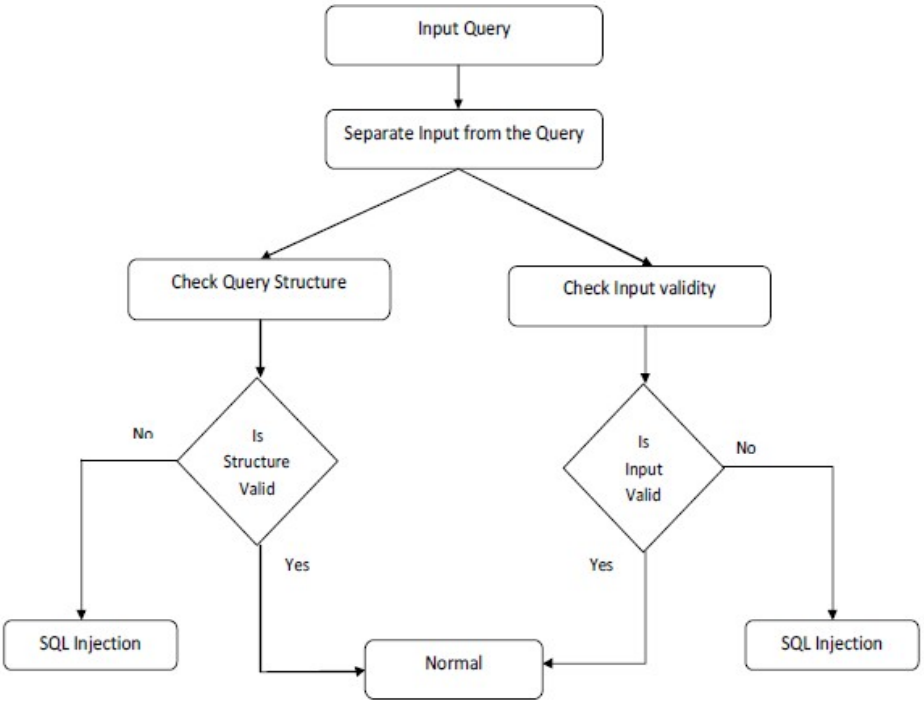


Figure 2.2 Architecture of proposed model

.

CHAPTER 3

Tools and Techniques

CHAPTER 3: Tools and Techniques

3.1 Introduction:

This chapter provides a background and basic information about the tools that used in the stage of project implementation, in the first thing we are going to introduce an introduction to our programming language python, its features and implementation, and then we will discuss the reasons for choosing python, after that will bravely provide an introduction to code editor we used in writing and developing the code, and we are going to give a basic concepts about the other tools and techniques we used in developing the project.

3.2 Python:

3.2.1 Introduction to python:

Python is an open source very high-level programming language for general-purpose created by Guido van Rossum in 1991, It is implemented in C, and relies on the extensive portable C libraries. It is a cross-platform language and runs on all major hardware platforms and operating systems, including Linux, Mac OS X and Windows. It is widely used and actively developed because of its vast array of code libraries and development tools, and integrates well with many other programming languages, frameworks and musical applications.

Python has an easy-to-use syntax and is quite easy to learn, making it suitable for those who are still learning to program. Python has a rich set of supporting libraries, and many third-party modules are available for it. Python is a programming language that also supports scripting, making it suitable for rapid application development. Python comes with a powerful and easy to-use graphical user interface (GUI) toolkit that makes the task of developing GUI applications in Python quite easy. [9]

3.2.2 Python features:

1. Following are a few of the most important python features:
2. It is a mature language and allows for programming in different paradigms including object orientated and functional styles.
3. The clean and simple syntax puts an emphasis on producing well-structured and readable code.
4. Documentation can be generated automatically from the comments and source code.
5. Python is free. Anyone can download and install any version of Python and use it to develop software for commercial or personal applications without paying a penny. Python is developed under the open-source model. You can copy Python, modify it, and even resell it.
6. It comes with a large number of libraries included, and there are many more that anyone can download and install.
7. Python can be integrated with other languages, like C, C++, and Java. That is, the components written in these languages can be embedded with Python programs, thus making it easier to develop complex solutions.
8. Python is an interpreted language; therefore it supports a complete debugging and diagnostic environment making the job of fixing mistakes much faster. Also, the software development is quite rapid and flexible in it.
9. Python supports exception handling. That is, errors are raised as exceptions so that you can take corrective measures.[9]

3.2.3 Why python?

There are many good programming languages but three reasons makes python the best choice for this project:

1. Python known as a hacker language so it's widely used for security related projects.

2. Python is a good choice for web development, networking, games, data processing, and business applications.
3. Efficient memory management, because of using garbage collection, so you don’t have to worry about memory leaks in the case of limited resource.

3.3 Eclipse:

3.3.1 Introduction to eclipse:

The Eclipse Platform is open source, designed for building integrated development environments (IDEs), and arbitrary tools. Eclipse is written in Java and will thusneed an installed JRE or JDK. [10]

3.3.2 Eclipse Platform Technical Overview:

The Eclipse Platform is designed and built to meet the following requirements:

- Support the construction of a variety of tools for application development.
- Support an unrestricted set of tool providers, including independent software vendors (ISVs).
- Support tools to manipulate arbitrary content types (e.g., HTML, Java, JSP, EJB, XML, C, C++, Python, PHP, Ruby and GIF).
- Facilitate seamless integration of tools within and across different content types and tool providers.
- Support both GUI and non-GUI-based application development environments.
- Run on a wide range of operating systems, including Windows®, LinuxTM, Mac OS X, Solaris AIX, and HP-UX.[10]

3.4 Enterprise Architect:

Enterprise Architect is a comprehensive UML analysis and design tool, it Covers all aspects of software, business and systems modeling and design. [11]

3.4.1 Enterprise features:

- Suitable for requirements gathering through analysis, design, construction, build, debug, simulation, testing, change management and maintenance to implementation, with full traceability, Combines the power of the latest UML specification (www.omg.org) with a high performance, intuitive interface, to bring an integrated and advanced toolset to the whole development team .

- Scalable, multi-user, visual tool with a rich feature set, Helps build and document robust, maintainable systems and processes.
- Proven, highly popular tool for analysts, developers, consultants and managers in over 130 countries, is used in the development of many kinds of application and system in a wide range of industries.
- Covers multiple domains, including: aerospace, banking, web development, engineering, finance, medicine, military, research, academia, transport, retail, utilities and electrical engineering , It also has a long history of being used by standards organization worldwide to structure and organize their domain specific knowledge and communication channels.
- Supported by many partners, consultants, colleges and other organizations that provide training and consulting services based around Enterprise Architect.[11]

3.4.2 Key benefits of Enterprise Architect:

Enterprise Architect is a powerful tool for specifying, documenting and building your software and business process projects. Using Enterprise Architect'ssupport for UML and its related standards, you can model new complex software and business systems, or visualize and maintain existing systems. [12] Enterprise is used in this project to design data modeling diagram.

3.5 PHP:

PHP is the most powerful phrase in web development industry from last number of years. is an acronym for "PHP: Hypertext Preprocessor”Invented by Rasmus Lerdorf in 1994 .iswidely-used and open source, which commonly used scripting language for most eye-catching website. The scripting language can easily make communication with dynamic data coordination in web applications as well also supports all commonly used databases like My-SQL, Oracle and more. PHP is used in this project as a scripting language for website as a case study. [13][14] PHP is used in this project as a scripting language for a case study website.

3.6 MySQL:

Database is a separate application that stores a collection of data. Each database has one or more distinct APIs for creating, accessing, managing, searching and replicating the data it holds. Other kinds of data stores can be used, such as files on the file system or large hash tables in memory, but data fetching and writing would not be so fast and easy with those types of systems. So nowadays, we use relational database management systems (RDBMS) to store and manage huge volume of data. This is called relational database because all the data is stored into different tables and relations are established using primary keys or other keys known as foreign keys**.** MySQL database is a fast, easy-to-use RDBMS being used for website as a case studyit works on many operating systems and with many languages including PHP, PERL, C, C++, JAVA, etc. [15]

3.7 HTML5:

HTML stands for Hyper Text Mark-up Language. HTML5 is a revised version of the original HTML standard created in 1990 by the World Wide Web Consortium to define an Open Web Platform. HTML is a language used for structuring and presenting content on the Web consistently, across web browsers. HTML5 is the evolution of that standard to meet the increasing demands presented by today's rich media, cross device and mobile internet access requirements. As such, it is a great candidate for cross-platform mobile application development, as many of its features have been adapted with the consideration of running on low powered devices, such as Smart Phones and Tablets and providing web developers with tools like CSS3**.** [16]HTML5 is used in this project for structuring and presenting content on a case study website**.**

3.8 JavaScript:

JavaScript is one of the most simple, versatile and effective languages used to extend functionality in websites. Uses range from on screen visual effects to processing and calculating data on web pages with ease as well as extended functionality to websites using third party scripts among several other handy features. [17]JavaScript is used in this project to extend functionality in websites.

3.9 Bootstrap:

Bootstrap is an open source project originally created by Twitter to enable creation of responsive, mobile first web pages. Bootstrap has a standard set of classes that allow developers to quickly create applications that scale to devices of all sizes, and incorporate common components such as dialog boxes and validation. Bootstrap has become a de facto standard for web design. [18] Bootstrap is used in project to creating flexible and responsive web layouts.

3.10 UML:

UML, the unified modeling language, is a standard used to visually describe a program, specifically an object-oriented program. UML helps to organize, plan and visualize a program. In addition, being a standard, it is widely used and accepted as the language for outlining programs. UML is used in a variety of purposes and its readability and re-usability make it an ideal choice for programmers. [19] UML is used to describe and analyze the tool.

3.11WAMP:

Acronym for Windows/Apache/MySQL/PHP, Python, (and/or) PERL, The acronym WAMP refers to a set of free (open source) applications, combined with Microsoft Windows, which are commonly used in Web server environments. The WAMP stack provides developers with the four key elements of a Web server: an operating system, database, Web server and Web scripting software. The combined usage of these programs is called a server stack. In this stack, Microsoft Windows is the operating system (OS), Apache is the Web server, MySQL handles the database components, while PHP, Python, or PERL represents the dynamic scripting languages.[20]Wamp is using as web server for case study website.

CHAPTER 4

Analysis

CHAPTER 4: Analysis

4.1 Introduction:

This chapter analyzes the system operations, components and environment using (UML) data modeling diagrams with brave description to better understanding for the system.

4.2 UML diagrams:

4.2.1 The Use Case Diagram:

This Diagram is Functional description of a tool and its major processes, provides a graphic description of who will use a system and what kinds of interactions to expect within that tool.[21]

Processes that occur within the tool area are called use cases.

- ***Use cases:***

  - **Enter URL :**

Table4.1 Enter URL use case specification

Enter URL	**Name**
_____	**Precondition**
Load source code	**post condition**
The user enter URL for the website to check the vulnerabilities	**Description**

- **Load source code :**

Table4.2 Load source code use case specification

Load source code	**Name**
Enter URL	**Precondition**
select vulnerability	**post condition**
The tool will download the source code of the targeted website	**Description**

- **select vulnerability :**

Table 4.3 select vulnerability use case specification

Select vulnerability	**Name**
_____	**Precondition**
inject queries	**post condition**
The user select vulnerability to be scan	**Description**

- **inject queries:**

Table4.4 inject queries use case specification

Inject queries	**Name**
select vulnerability	**Precondition**
_____	**post condition**
inject SQL commands into an SQL statement, via web page input	**Description**

Entities outside the area that are going to use the tool are called actors.

- ***The actors :***

- **End user :**

Table4.5 End user actor specification

End user	**Name**
The end-useris the onlyuser whouses thetool in orderto discover vulnerability inspecific Website	**Description**

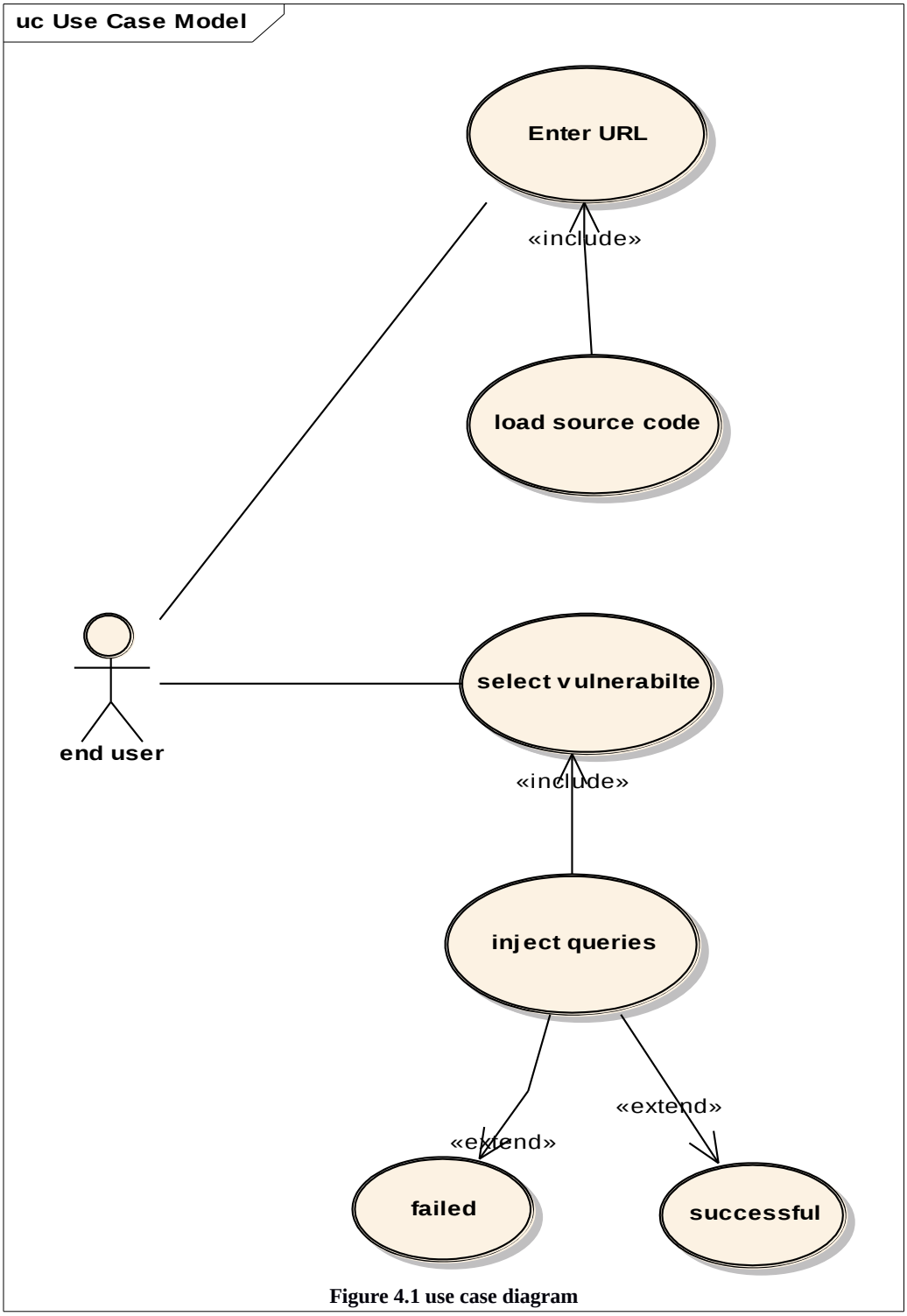


Figure 4.1 use case diagram

4.2.2 The Sequence Diagram:

This diagram is a model describing how groups of objects collaborate in some behavior over time. The diagram captures the behavior of a single use case and shows objects and the messages that are passed between these objects in the use case.[22]

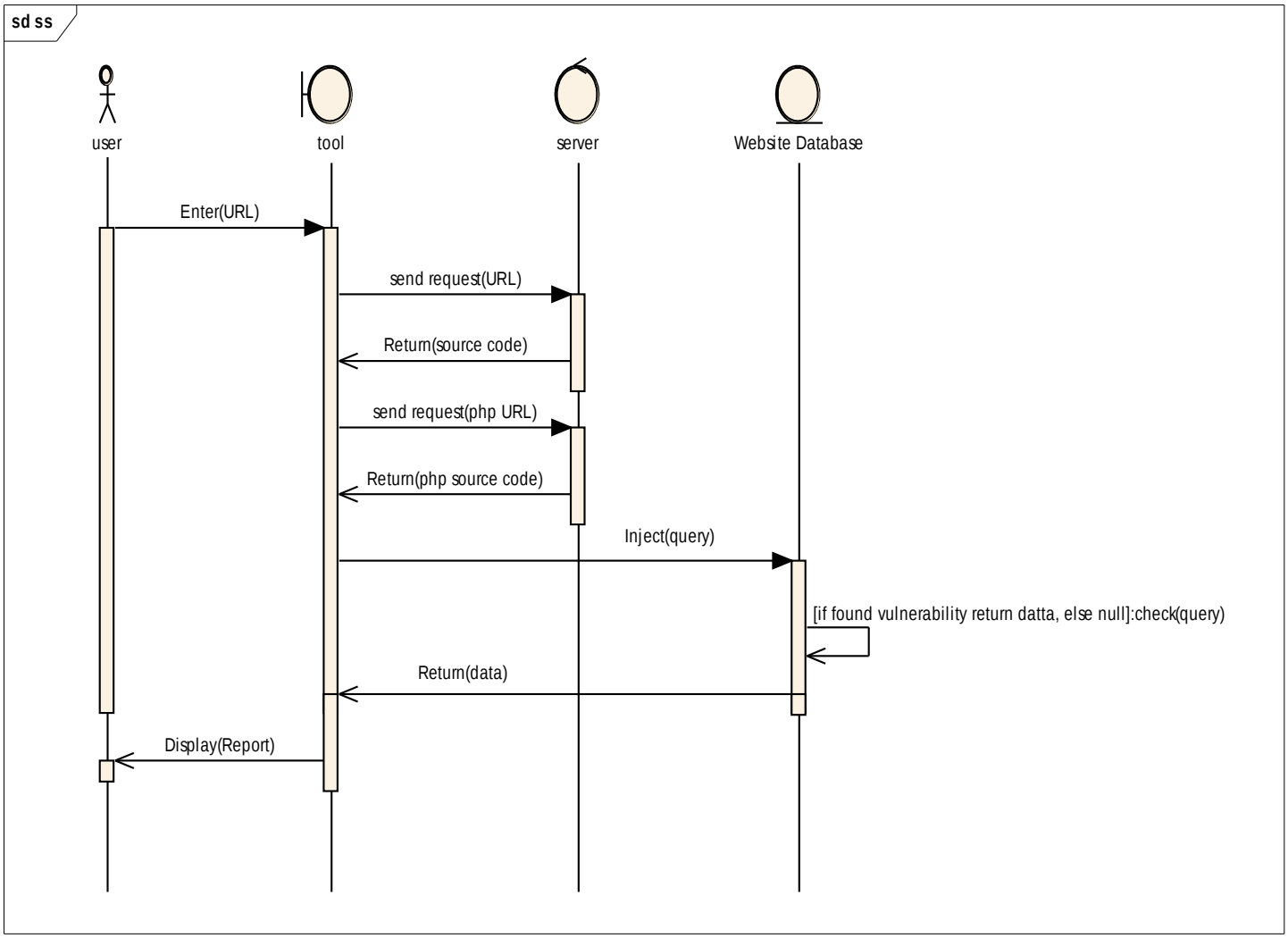


Figure 4.2 sequence diagram

4.2.3 The Activity Diagram:

This diagram is Describes activities and flows of data or decisions between activities and provides a very broad view of business processes and good for showing parallel threads, shows different activities that will be handled by lots of different symbols[23]

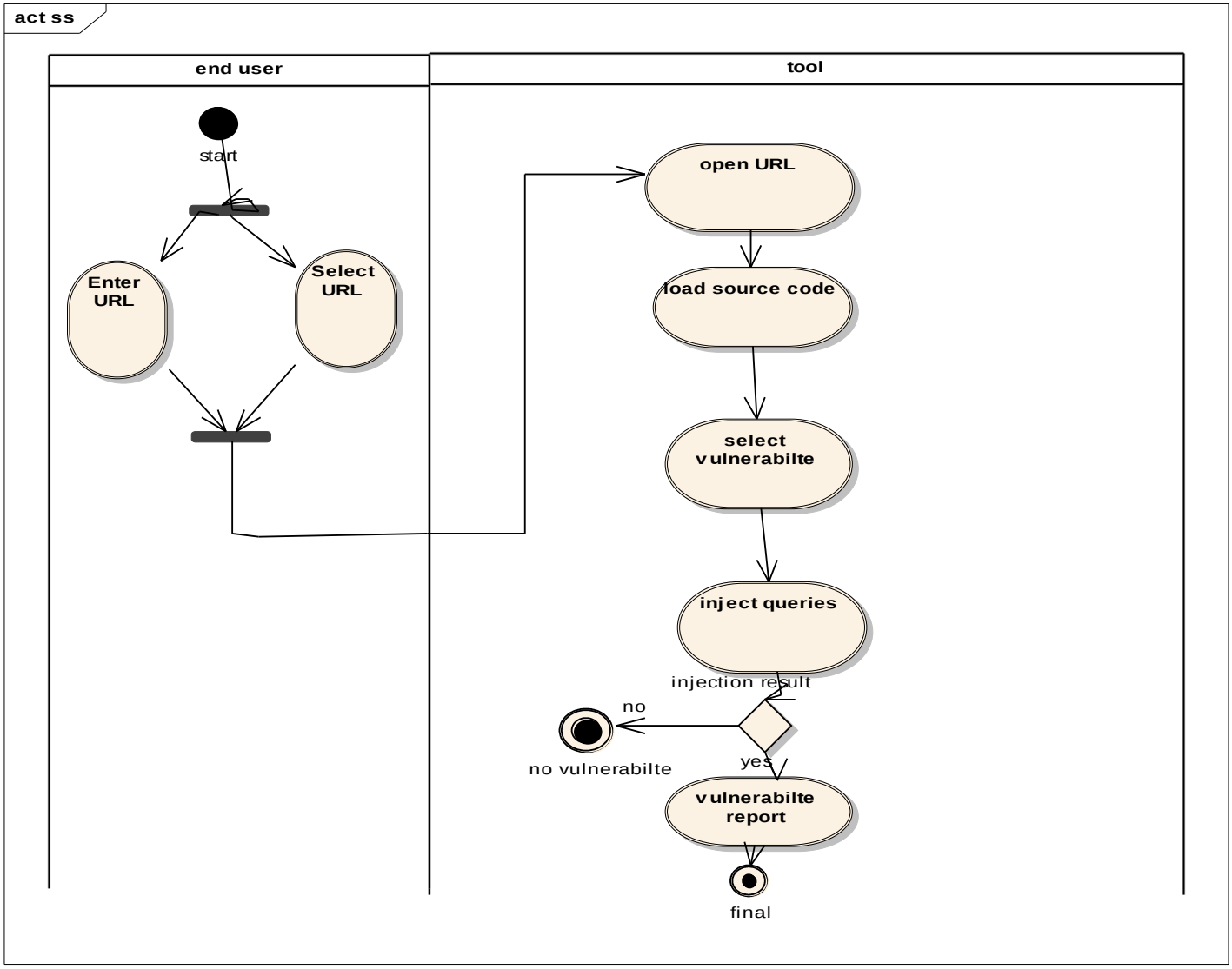


Figure 4.3 Activity Diagram

4.2.4 The Class Diagram:

This diagram describes the static structure of the symbols in tool. This model allows to graphically representing symbol diagrams containing classes. Classes are arranged in hierarchies sharing common structure and behavior and are associated with other classes.[24]

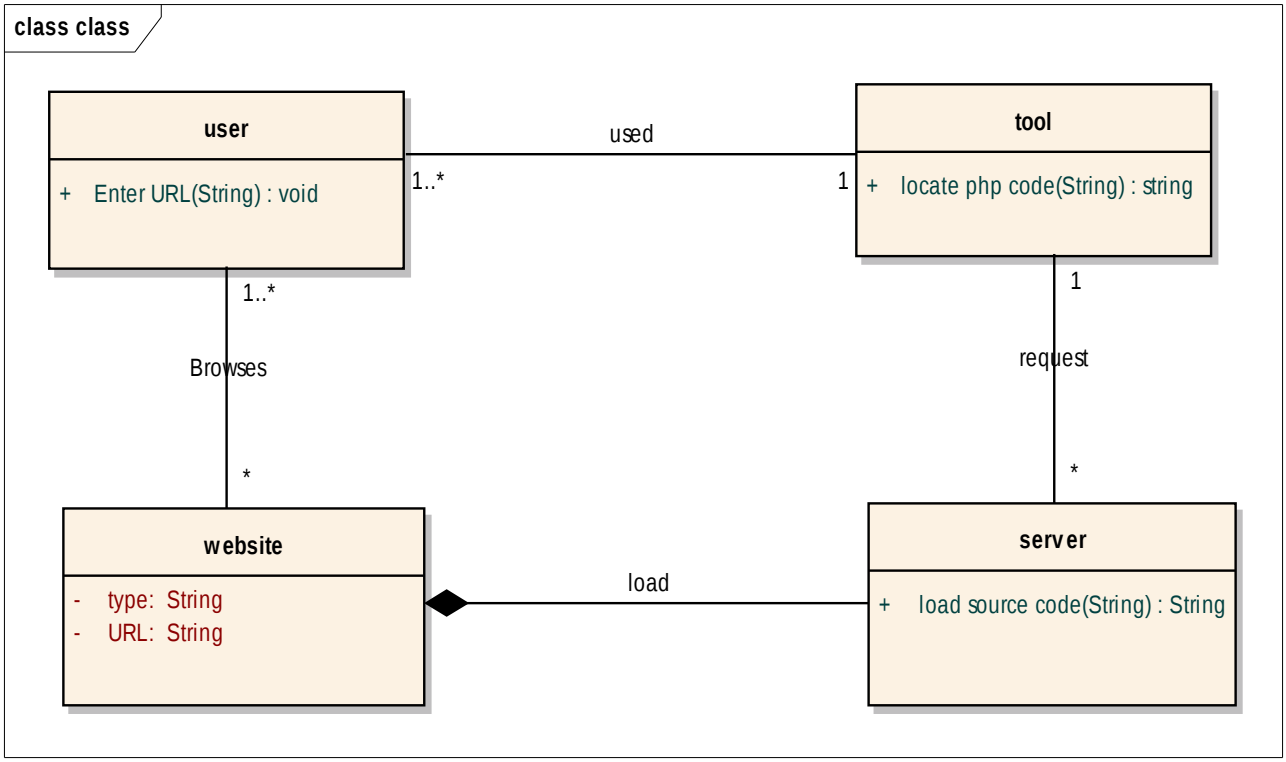


Figure 4.4 Class Diagram

CHAPTER 5

Implementation

CHAPTER 5: Implementation

Execution screen:
It's the main screen appears to user after executing the tool to detect vulnerabilities in the site.

Enter the URL address of the desired website.

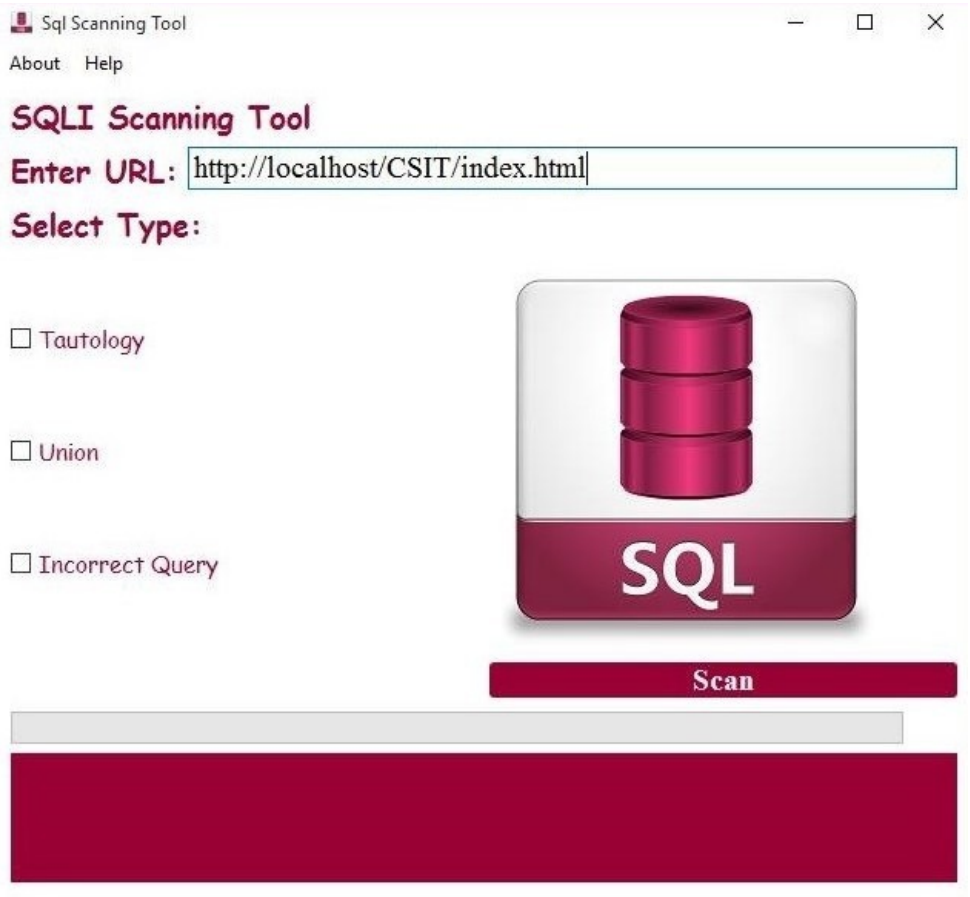


Figure 5.2 Entering URL in execution screen

Select the type to check, choose one or more type.

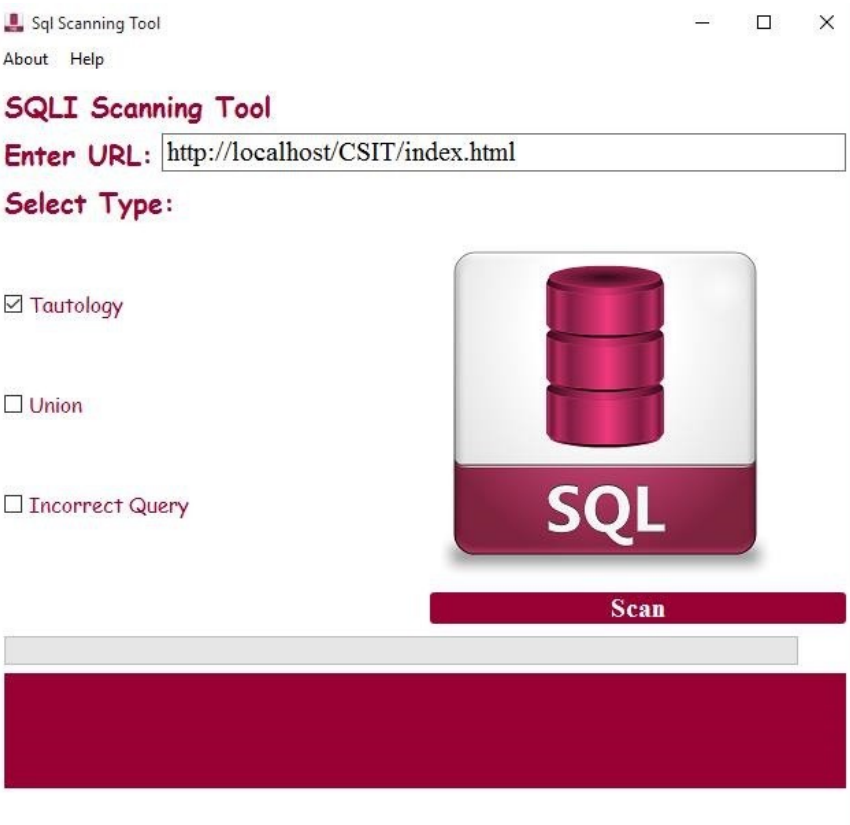


Figure 5.3 Choosing SQL injection type

Progress bar appears after pressing the SCAN button. In this case user must wait until the end of the examination

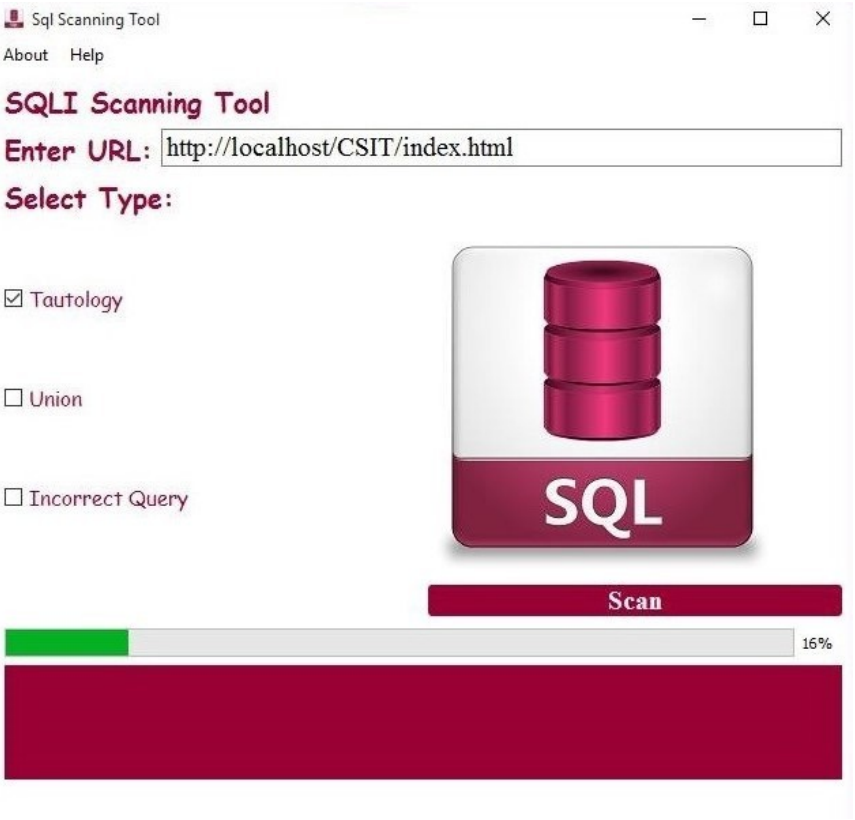


Figure 5.4 Wait for detecting vulenerability

Report window appears when the examination ends and a report of vulnerabilities is delivered.

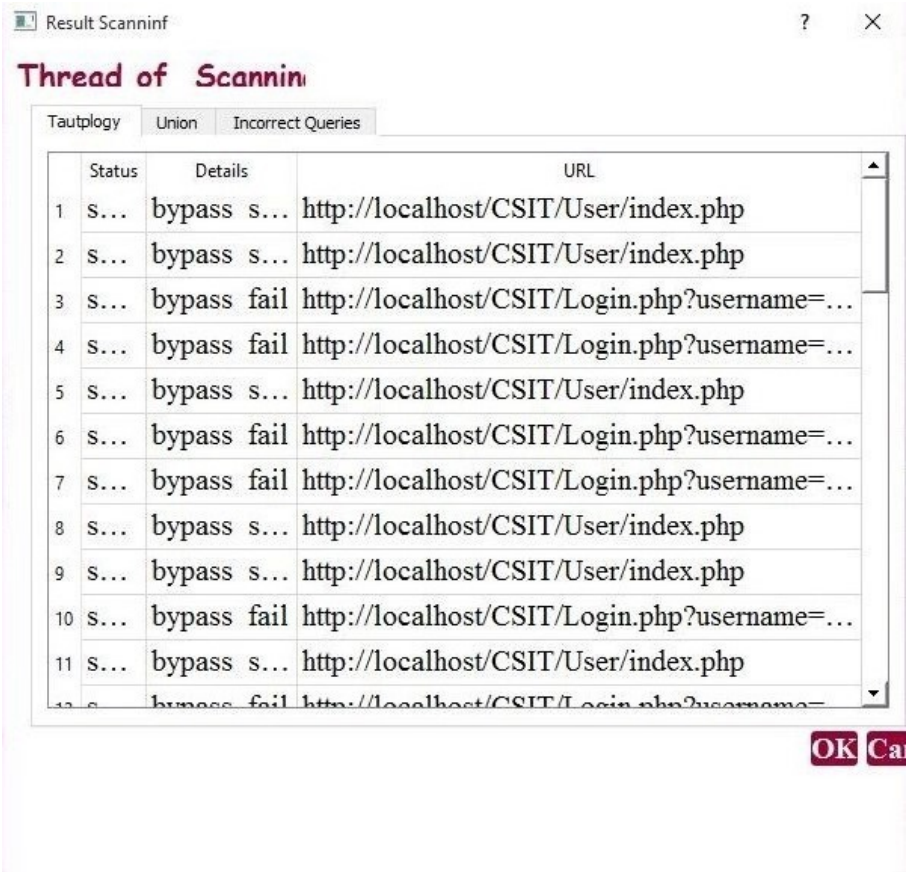


Figure 5.5 Report window

Home page of the website that designed to check SQL injection types.

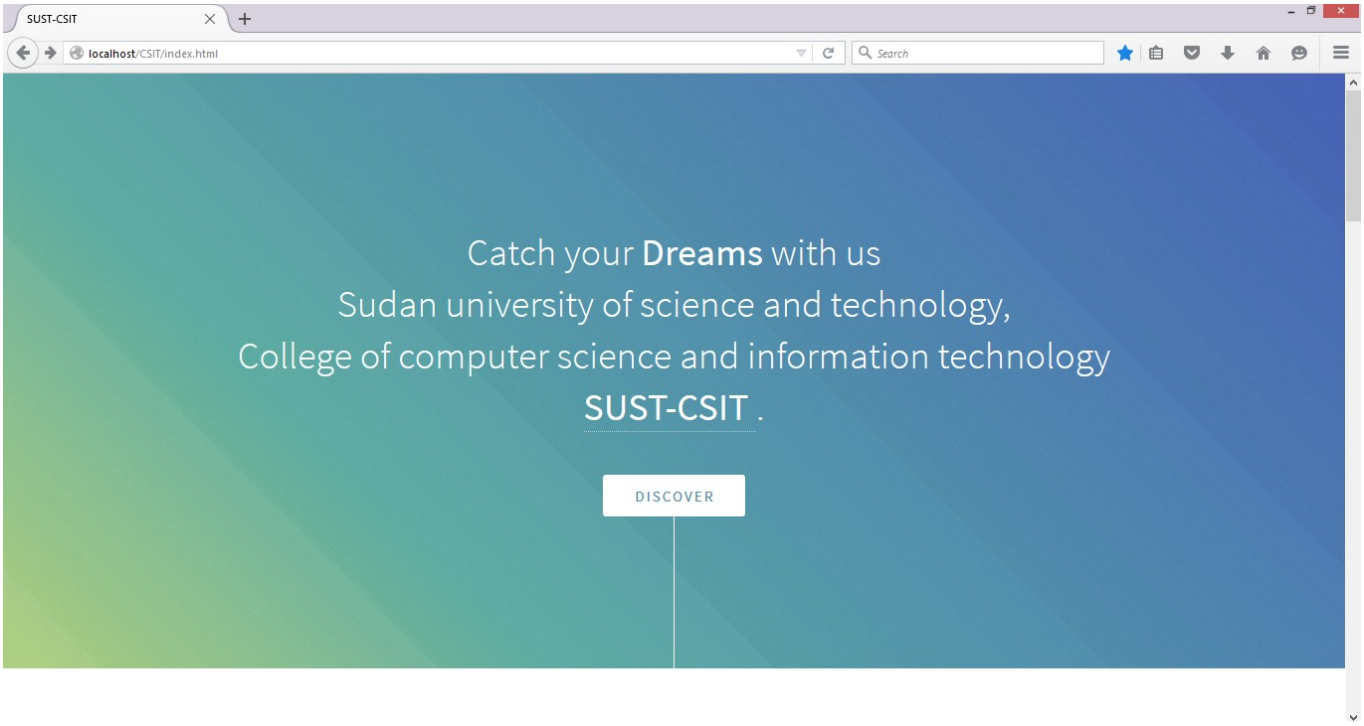


Figure 5.6 Website home page

Website Login form used for entering the data to access user account.

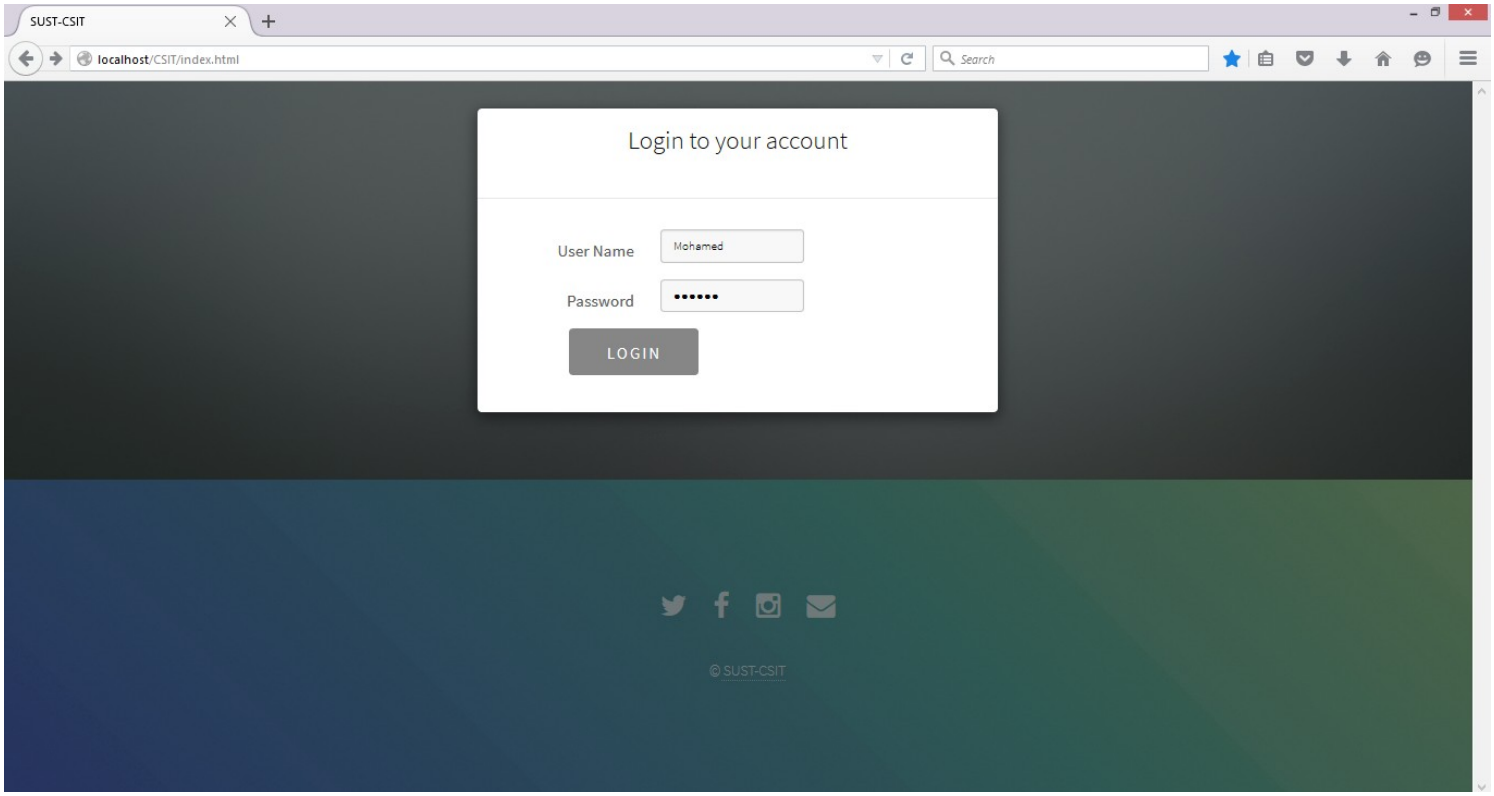


Figure 5.7 Website login form

User profile page that contains all user's data.

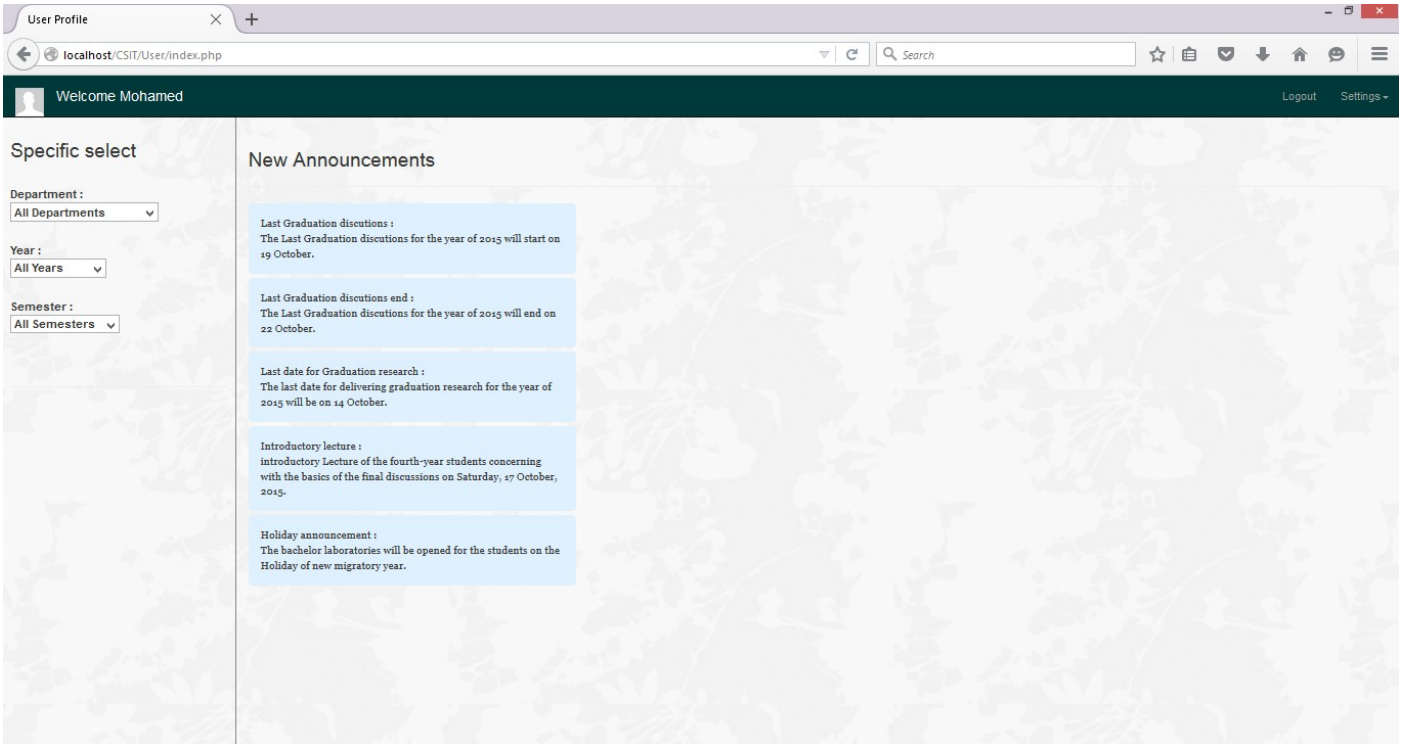


Figure 5.8 Website user page

User profile settings that allow user to change group of settings.

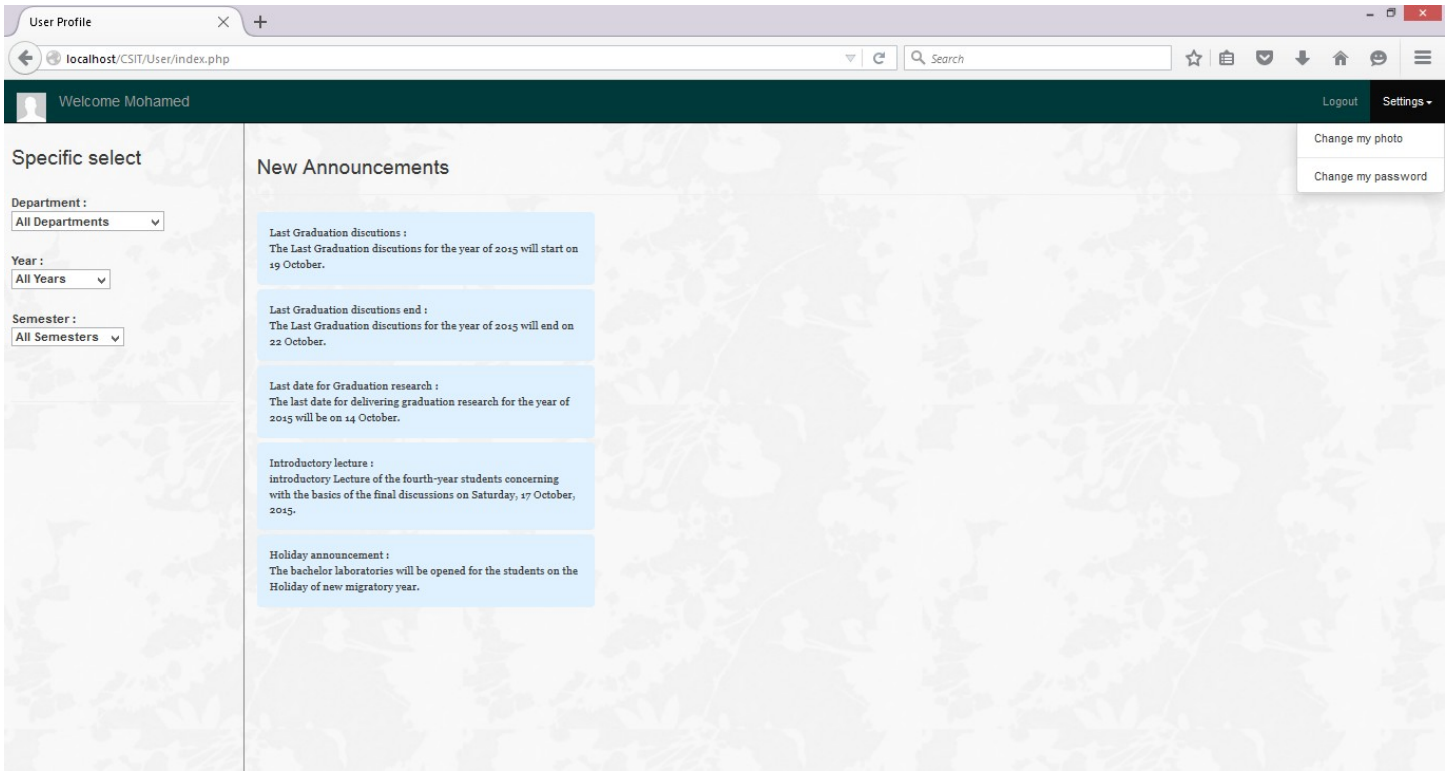


Figure 5.9 Website user profile settings

CHAPTER 6

Conclusion

CHAPTER 6: Conclusion

6.3 Conclusion:

Proportion to the steady increase in the number of Internet users and websites and needs of those websites to deal with sensitive personal data, fears have grown in relation to the web confidentiality and data security so the community has suffered many difficulties with regard to these issues. Therefore it was necessary to develop solutions for the treatment of the causes leading to security breaches, and here was this project in order to help provide the environment and the safe structure that secures the use of these websites.

6.1 Results:

- Provide a tool to check websites using penetration testing technique that tested on 20 sites aginest three types of SQLI using 24 qurey for Tutology, 15 qurey for Union and 17 qurey for Incorrect inlegal qureies, and the final results proof that test success in 7 sites for Tutology, 7 sites for Union and 6 sites for Incorrect inlegal qureies.
- Provide a simple and easy to use interface.
- Provide user with an integrated and simplified report for use it in securing the site.
- Provide a user manual with a number of instructions and guidelines to facilitate the use and helping to solve the problems that may face user.
- Providing specially designed website to experience test the tool on.

6.2 Recommendations:

- Test the remaining types of SQL injection.
- Apply penetration testing Technology in all web applications not only PHP web applications.

- Enable tool to prevention SQL injection.

References

[1] 1Aileen G. Bacudio, 1. Y.-T. (2011). AN OVERVIEW OF PENETRATION TESTING. Greensboro, North: International Journal of Network Security & Its Applications (IJNSA).

[2] *code injection*. (2015, July 5). Retrieved from http://www.owasp.org/index.php/Code_Injection

[3]Atefeh Tajpour, S. I. (2012). Web Application Security by SQL Injection DetectionTools. Malaysia: IJCSI International Journal of Computer Science Issues,.

[4] T2, S. M. (2012). A METHOD OF DETECTING SQL INJECTION. kalady: International Journal of Distributed and Parallel Systems (IJDPS).

[5] Baranwal, A. K. (2012). Approaches to detect SQL injection and XSS in web applications. Canada: EECE 571B, TERM SURVEY PAPER.

[6] Jaskanwal Minhas, R. K. (2012). An analysis on Blocking of SQL Injection Attacks by Comparing Static and Dynamic Queries. India: International Journal for Science and Emerging Technologies with Latest.

[7] Qaralleh, J. O. (2014). A HYBRID TECHNIQUE FOR SQL INJECTION. Amman, Jordan: International Journal of Database Management Systems (IJDMS).

[8] Kuldeep Kumar1, D. D. (2013). A Novel Approach to detect SQL injection in web applications. Bangalore: International Journal of Application or Innovation in Engineering & Management (IJAIEM).

[9] Introduction to Python® Programming and Developing GUI Applications with PyQT2012Ajmer, IndiaStacy L. Hiquet.

[10] (2015, August 10). Retrieved from Eclipse Platform Technical Overview: http://www.eclipse.org/articles/Whitepaper-Platform-3.1/eclipse-platform-whitepaper.html

[11] (2015, August 11). Retrieved from Enterprise Architect: http://www.sparxsystems.com/enterprise_architect_user_guide/12/introduction/introduction.html

[12] (2015, August 11). Retrieved from key benefits of Enterprise Architect: http://www.sparxsystems.com/enterprise_architect_user_guide/11/introduction/what_can_i_do_with_ea.html

[13] (2015, August 15). Retrieved from PHP Web Development: http://phpdevelopmentoutsourcing.blogspot.com/2011/07/characteristics-of-php.html

[14] McCown, D. F. (2012). Introduction to PHP.

[15] (2015, August 17). Retrieved from MySQL Introduction: http://www.tutorialspoint.com/mysql/mysql-introduction.htm

[16] (2015, September 5). Retrieved from How can HTML5 & CSS benefit your business: http://www.thebyte9.com/news/how-can-html5-css-benefit-your-business

[17](2015, September 5). Retrieved from Javascript: advantages and disadvantages: http://www.jscripters.com/javascript-advantages-and-disadvantages/

[18] (2015, September 6). Retrieved from Introduction to Bootstrap – A Tutorial: https://www.edx.org/course/introduction-bootstrap-tutorial-microsoft-dev203x-0

[19] (2015, September 6). Retrieved from List of Advantages of UML : http://www.ehow.com/info_8584011_list-advantages-uml.html

[20] (2015, September 9). Retrieved from WAMP: http://www.webopedia.com/TERM/W/WAMP.html

[21] (2015, June 17). Retrieved from Use case Diagram: http://www.csee.wvu.edu/~ammar/rts/Chapter4-Use%20Case%20Diagram.pdf

[22] (2015, june 19). Retrieved from Sequence Diagram: http://www.csee.wvu.edu/~ammar/rts/Chapter8-Sequence%20Diagram.pdf

[23] (2015, june 17). Retrieved from Activity Diagram: http://www.csee.wvu.edu/~ammar/rts/Chapter10-Activity%20Diagram.pdf

[24] (2015, June 20). Retrieved from Class Diagram: www.csee.wvu.edu/~ammar/rts/Chapter6-Class Diagram.pdf

CHAPTER 7

Supplements

CHAPTER 7: Supplements

7.1 User manual Supplement:

User Manual

Thank you for choosing our product and we hope to be able to provide you with the best performance levels.

Caution:

Please read the user manual before you start using the product.

What are the SQL injection attacks?

SQL injection attack consists of injection of malicious SQL commands via input data from the client to the application that are later passed to an instance of a database for execution and aim to affect the execution of predefined SQL commands.

Product function:

The product used as a tool to examine the websites against three types of SQL injections.

Product output:

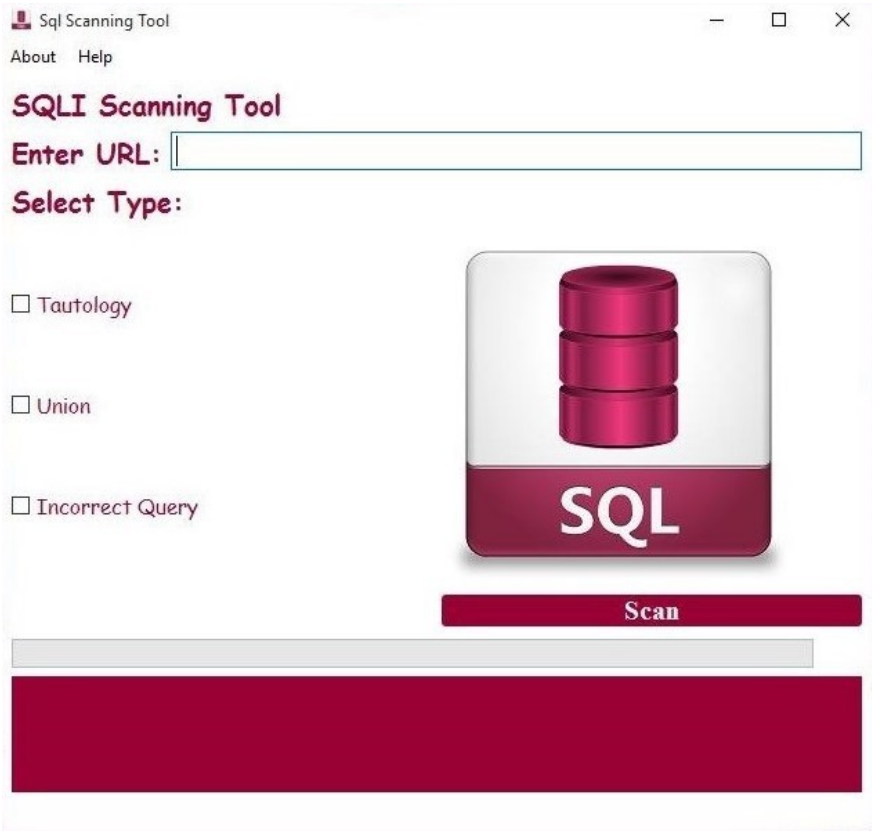
After using the Product a comprehensive report of all vulnerabilities on the site is delivered and can be used as a basic guidance to secure the website.

How to use:

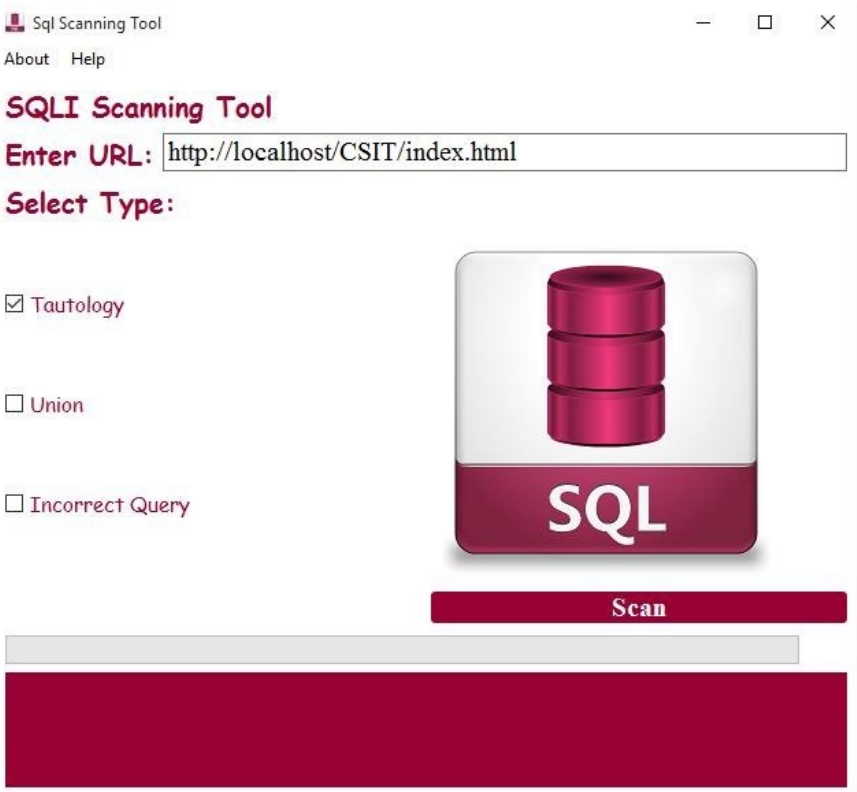
Execution screen:

It is the screen from which you can use the product for the detection of vulnerabilities in the site, and you can start using the product by following the next instructions:

1. Enter the URL address of the desired website as described below.



2. Select the type to check for as in the figure below, and remember you can choose one or more type.

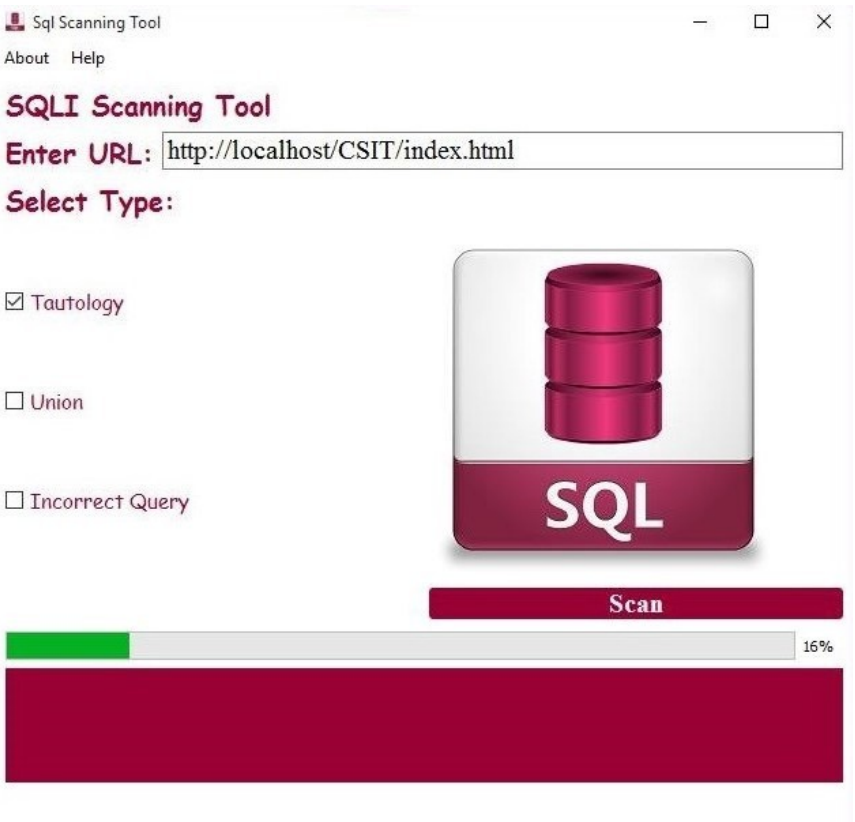


3. Press the SCAN button to start the process of searching for vulnerabilities.
4. Wait until the end of the Scanning process and get a full vulnerabilities report.

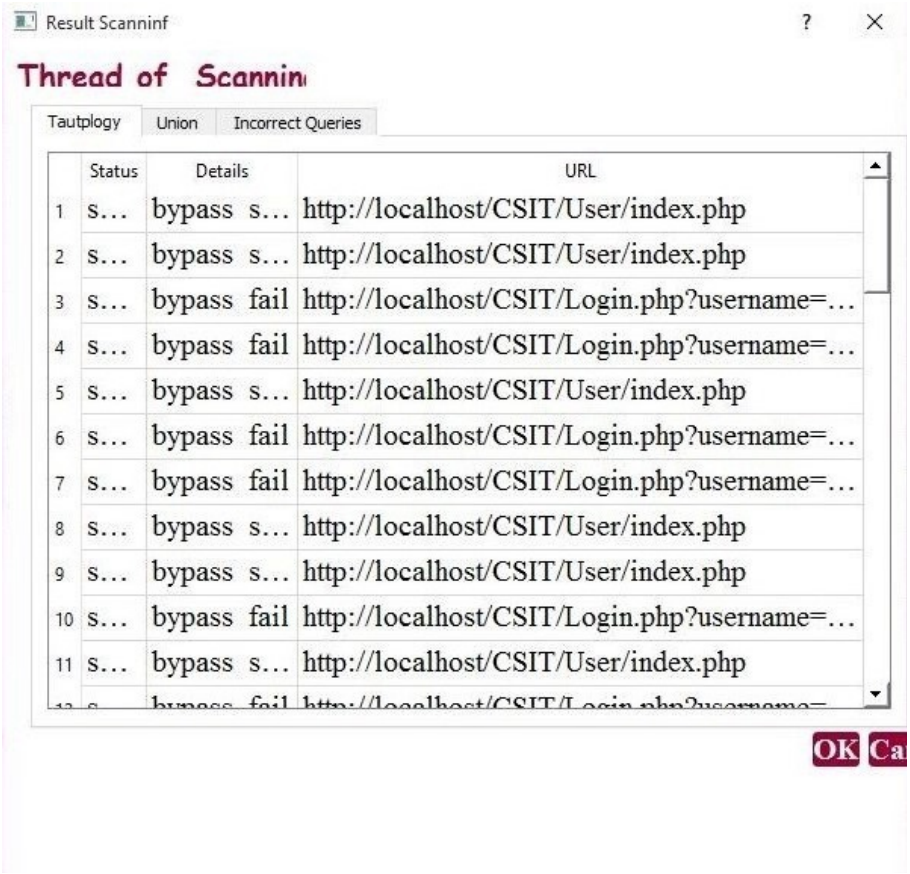
Status and notifications:

You can deal with notifications and pop-up windows through following the next guidelines:

- Progress bar appears after pressing the SCAN button. In this case you must wait until the end of the examination.



- The following window appears when the examination ends and a report of vulnerabilities is delivered.



Support and safety instructions:

The process of using the product:

- If you face any difficult in using the tool, you should re-read user manual for efficient use.
- If you get a notice of an incorrect URL Check the URL you entered and re-entry again.
- If you get a notice to choose a type make sure you choose at least one type of the SQL injection types on the screen.
- In the case of a sudden interruption of the scanning process and get notice of error make sure of a good network connection and make sure to not interrupt scanning by clicking buttons on the interface during the operation.
- If scanning took a period of time exceeding ten minutes make sure of your network connection and try to scan again.

Legal information: