SQL Injection Detection and prevention

DIKSHA PATIL, SHEETAL SONKAMBLE, PROF. V. M. KHARCHE

Abstract— Complete Web Vulnerabilities Scanner is developed for creating scanning whole webpage of websites. This web application is to be conceived in its current form as a dynamic site- requiring constant updates both from the clients as well as the developer. On the whole the objective of the project is to remove the vulnerabilities which is founded by this application. A great number of web application vulnerabilities are leveraged through client-side submission of unexpected inputs. While it is clear these vulnerabilities are complex and widespread, what is not clear is why after over a decade of effort they remain so prevalent.

Index Terms— SQL, crawling, spiderlogs, workinglogs, coding, type of sql, prevention, conclusion.

1 INTRODUCTION

Complete web vulnerabilities scanner is used to find the websites bug and after that it shows the types of bug on that websites. This project is developed in JAVA and MYSQL .As we know an ever-increasing number of high profile data breaches have plagued organizations over the past decade. A great number of these come about via so called 'injection attacks'; the submission of malicious code to a web application. Indeed, the Open Source Web Application Security Project (OWASP), the leading organization in the field of web app security states; "How data input is handled by Web applications is arguably the most important aspect of security." Two factors increase the stakes of the cyber struggle. Tactically and operationally, theincreasing dependence of modern technologically advanced forces onnetworks and information systems create new kinds of exploitable vulnerabilities. Second, asmodern societies including the militaries that mirror them have continued to evolve, they havebecome ever more dependent on a series of interconnected, increasingly vulnerable "critical infrastructures" for their effective functioning. These infrastructures not only have significantlyincreased the day-to-day efficiency of almost every part of our society, but they have al sointroduced new kinds of vulnerabilities.

2 SYSTEAM ANALYSIS

2.1 Existing System

This project is aimed at developing a web-based for a company. This document provides details about the entire software requirements specification for the CWVS. The project Complete Web Vulnerabilities Scanner(CWVS) is aimed at developing a web-based and more efficient crawler and Scanner form.

2.2 Proposed system

This system tends to replace the existing manual system for the scanning process which is a time consuming, less interactive and highly expensive. The main features of this system will be creating report and find various types of vulnerabilities, storing Scanning data, process initiation, and after that it generates a report of whole scanned websites

Advantages of the Proposed System:

- User friendly registration System
- Fastest Wed Spider/Crawler
- Easy to control Session
- Free Registration
- Search for a particular Websites if Once it is used

3 SYSTEM REQUIREMENT SPECIFICATION

Purpose: The main purpose for preparing this document is to give a general insight into the analysis and requirements of the existing system or situation and for determining the operating characteristics of the system. This document provides details about the entire software requirements specification for the Complete Web Vulnerabilities Scanner. The project Complete Web Vulnerabilities Scanneris aimed at developing a web-based Scanner of a all company and organization.

Scope: This Document plays a vital role in the development life cycle (SDLC) and it describes the complete requirement of the system. It is meant for use by the developers and will be the basic during testing phase. Any changes made to the requirements in the future will have to go through formal change approval process.

3.1 Functional Requirements

Output Design

Outputs from computer systems are required primarily to communicate the results of processing to users. They are also used to provide a permanent copy of the results for later consultation. The various types of outputs in general are:

- External Outputs, whose destination is outside the organization,
- Internal Outputs whose destination is with in organization and they are the
- User's main interface with the computer.
- Operational outputs whose use is purely with in the computer department.

Input Design
Input design is a part of overall system design. The main objective during the input design is as given below:

- To produce a cost-effective method of input.
- To achieve the highest possible level of accuracy.
- To ensure that the input is acceptable and understood by the user.

3.2 System Configuration

Hardware Requirements:

Machine	: Pentium IV or higher
Clock Speed	: 500 MHz or higher
System Memory	: 512 MB and above
Hard Disk Space	: 20 GB and above

Software Requirements:

Operating System	: Windows XP / 7 or higher
RDBMS	: MySQL
Web Server	: Xampp server, Wampp Server
Front-end	: JAVA, JAVASCRIPT,HTML, CSS

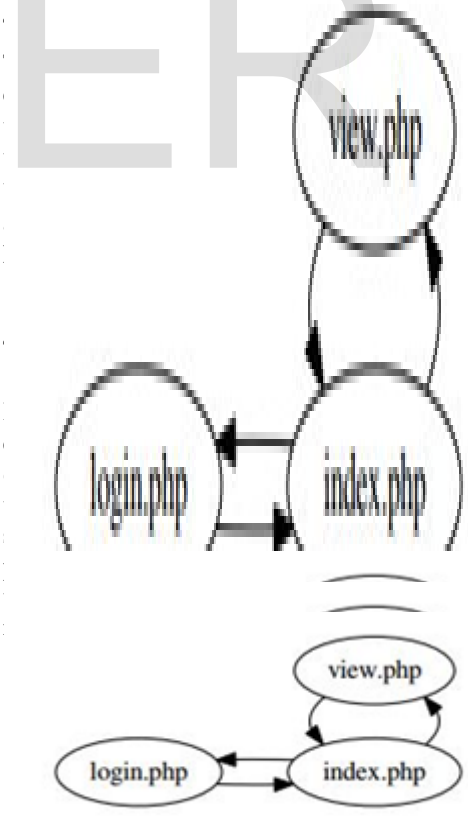
Communication Requirements: -
Web Browser: IE-9, Chrome 28, Firefox 18 or higher version.
Local intranet and internet protocols.
Supports all HTTPS, SMTPS and POP3 services.

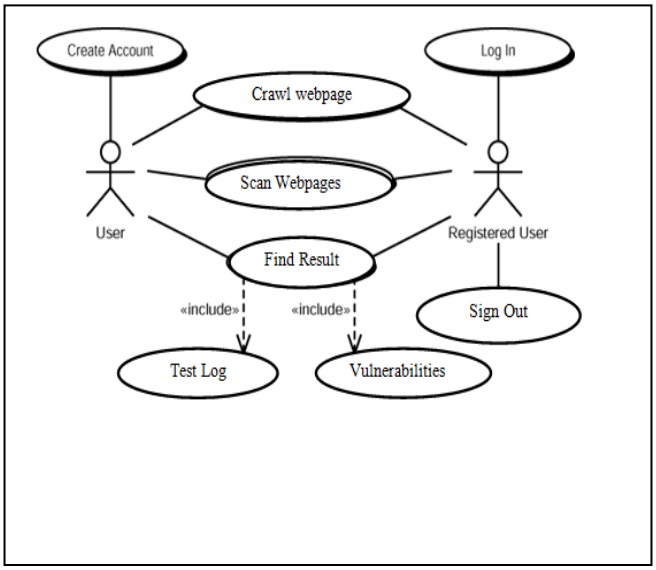
4 SYSTEAM DESIGN

4.1 Modules of project

Software design sits at the technical kernel of the software engineering process and is applied regardless of the development paradigm and area of application. Design is the first step in the development phase for any engineered product or system. The designer's goal is to produce a model or representation of an entity that will later be built. Beginning, once system requirement have been specified and analyzed, system design is the first of the three technical activities - design, code and test that is required to build and verify software.
The importance can be stated with a single word "Quality". Design is the place where quality is fostered in software development

During design, progressive refinement of data structure, program structure, and procedural details are developed reviewed and documented. System design can be viewed from either technical or project management perspective. From the technical point of view, design is comprised of four activities – architectural design, data structure design, interface design and procedural design.





4.4 Physical System Design

This produces the working system by defining the design specifications that tell the programmers exactly what the candidate system must do.

4.5 Architectural Design

Architectural design is a comprehensive framework that describes its form and a structure its components and how they fit together. Architectural design is a software component that can be something as simple as program module, but it can also be extended to include database and middleware that enable the configuration of a network of client and servers. This project consists of different modules. The Administrator module helps the administration of the entire site. The administrator will decide which department should view the complaint.

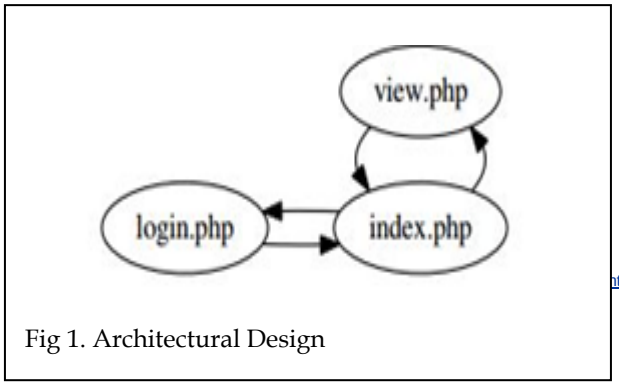


Fig 1. Architectural Design

5. SYSTEM TESTING

Testing is the process of executing the program to find if there are any errors. It is the final verification and validation activity. In testing phase, we have tried to affirm the quality of the product. We have also tried to eliminate errors in the previous stages.

5.1 STRATEGIC APPROACH TO SOFTWARE TESTING

A strategy for software testing may also be viewed in the context of the spiral. Unit testing begins at the vertex of the spiral and concentrates on each unit of the software as implemented in source code. Testing progress by moving outward along the spiral to integration testing, where the focus is on the design and the construction of the software architecture. Talking another turn on outward on the spiral we encounter validation testing where requirements established as part of software requirements analysis are validated against the software that has been constructed. Finally, we arrive at system testing, where the software and other system elements are tested as a whole.

6.SECURITY ANALYSIS OF WEBSITE:

Security is the most important part of any website or development process which is related to internet. We have done a lot of studies on different kinds of websites related to JAVA, HTML, Java –Script and CSS to make our website more and more secure. In context of that we found a lot of vulnerabilities and traced several me thods for securing this. For that we made some protections and developments in it.Secured from:-

- Sql injection
- XSS
- File upload

7. FUTURE ENHANCEMENT

Nothing can be ended in a single step. It is the fact that nothing is permanent in this world. So this project also has some future enhancements in the evergreen and booming IT industry. Change is inevitable. The project entitled "Complete Web Vulnerabilities Scanner" was successfully designed developed and tested. The system and the architecture is a compatible one, so addition of new modules can be done without much difficulty. Since this module has its unique properties it can extend further to make this system a

complete one.

7.1 Scope

It provides the Security Analyst with all the necessary security issues and its solution to prevent by the hackers.
It provides the users with all the necessary privileges to access and modify the data intended for them.
It doesn't entirely replace the existing system but it mostly automize the Scanning process and all the data used.

7.2 Success Criteria

This softwareautomates the manual Scanning process. We believe that once the organization chooses to use this system, it will eventually recognize the value and necessity of this system and understand the problems involved in the manual process.

CONCLUSION

The project provides much security. The simplicity and friendliness are the advantages of this project. The Software is made user friendly to the maximum so that anyone can run the software provided he could access to the system via the login password.
This project manages all details without any risk. All the objectives were met with satisfaction. The performance of the system is found to be satisfactory.

References

[1] K. Bagchi and G. Udo, "An analysis of the growth of computer and internet security breaches," Communications of the Association for Information Systems, vol. 12, no. 1, p. 46, 2003.

[2] M. Howard and D. LeBlanc, Writing secure code. Pearson Education, 2003.

[3] W. G. Halfond, J. Viegas, And A. Orso, "A Classification Of Sql-Injection Attacks And Countermeasures," In Proceedings Of The Ieee International Symposium On Secure Software Engineering