e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
Volume:03/Issue:04/April-2021 Impact Factor- 5.354 www.irjmets.com

OWASP VULNERABILITY SCANNER

Abhishek kumar [*1], Abdullah Tahir[*2], Mohd Daem Khan[*3], Dr. Amrita[*4]

Affiliation, Computer Science, Sharda University, Greater Noida, Uttar Pradesh, India

Affiliation, Computer Science, Sharda University, Greater Noida, Uttar Pradesh, India

Affiliation, Computer Science, Sharda University, Greater Noida, Uttar Pradesh, India

(Dr. Amrita- Professor, Department of Computer Science Engineering, Sharda University, Greater Noida, Uttar Pradesh, India)

ABSTRACT

OWASP vulnerabilities Scanner is used to scan the web page of the websites. The tool requires regular updating from both users and creators. The whole objective of the project is to find the vulnerabilities in the web page.

Most of the Vulnerabilities are found on users' side through client-side submission of unexpected inputs. It is clear that Vulnerabilities are present since the widespread of WWW (world wide web) but what seem unclear is that why anything is not done to prevent and cure it. Here we will find out current methods and practices to prevent these Vulnerabilities.

In the last two decades, the massive growth of web-based applications has led to increasing security vulnerabilities in the Web app. With the maturity of the dominance of web applications, web applications cover a large number of empirical studies with the solution for the vulnerable web application. However, before we progress towards finding new approaches to web application security detection, existing evidence-based studies in web applications must be analysed and synthesised.

Keywords: OWASP Vulnerability, SQLi injection, XSS.

I. INTRODUCTION

The OWASP is a non-lucrative organisation that enhances software security. The OWASP is an open application security project. With the help of community based open-source software initiatives, many local structures worldwide, large numbers of people, and leading education and training conferences, the OWASP Foundation is the source of Internet developers and technologies.

- Resources and Tools
- Collaboration and Networking
- Training & Education

For web applications, web security is an important aspect. Web security today is a real Internet concern. It is regarded as the main framework for the global data society. A better interface to a client via a Webpage is provided by web applications. The script of the webpage is run on the web browser of the client.

The Scanner for OWASP vulnerabilities is used to detect the bug and vulnerabilities that the websites display about the kinds of vulnerabilities in them. As we all know, over the last decade, organisations have been affected by an ever-increasing number of status data breaches. A large number of them are so-called "injection attacks," in which malicious code is injected into an online application

Tactically and operationally, new kinds of exploitable vulnerabilities are created by the growing reliance of new technological strength on networks and knowledge systems. Secondly, with the evolution of societies of the new era, including the military, they must become increasingly involved in a series of interconnected and increasingly vulnerable 'critical infrastructures' that can function effectively. In addition to significantly enhancing the daily efficiency of almost one part of our society, these infrastructures also require introducing new forms of vulnerabilities.

The two most common vulnerabilities today are SQL and cross-site scripting. An appliance defence security evaluation with over 250 applications, online banking and corporate websites revealed that over 85% of web applications are vulnerable to attacks.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
Volume:03/Issue:04/April-2021 Impact Factor- 5.354 www.irjmets.com

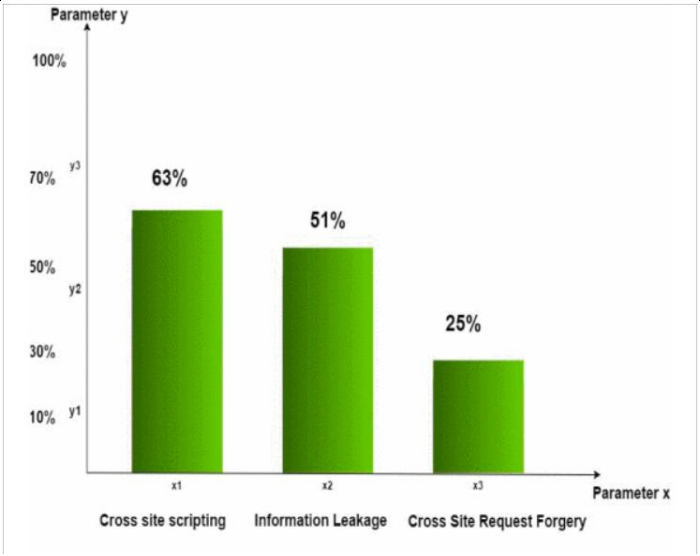

Fig 1: -Bar graph

The main problem in web security research is to allow a user to communicate with the web application on a safe, trusted platform. However, some people still deal with insecure places. Some companies or organisations do not want to disclose their own safety information. So, the reliable information on the state of web safety today is a very difficult task.

Today there are two major common security vulnerabilities: injection with SQL and script cross-site. These vulnerabilities affect web servers, application servers and the environment of web applications directly.

In this paper, OWASP explores various reasons for attacking threats. This paper proposes a better mechanism to reduce such web vulnerabilities. In web applications, there are currently many privacy risks. Today, anonymous people hack too many websites. For different reasons, they target the website.

II. METHODOLOGY

In this project our team is building a software that can detect vulnerabilities in web pages and give results on which vulnerability your webpage is lacking in security and you need to secure it.

Requests Security and software is only one of the main development planning steps. The extent of reliability is, after all, what will determine your success, as an example for the number of active users in the application. And without mentioning OWASP, there is no reason to debate security.

In order to combat safety violations, systems to protect against unauthorised infringements and wind leaks of users and corporations, IT professionals work together. This makes monitoring and participation in OWASP essential.

Attack Goal	%
Stealing Sensitive Information	42%
Defacement	23%
Planning Malware	15%
Unknown	08%
Deceit	03%
Blackmail	02%
Link Spam	03%
Worm	01%
Phishing	01%
Information Warfare	01%

Fig 2: -Table

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
Volume:03/Issue:04/April-2021 Impact Factor- 5.354 www.irjmets.com

SQl Injection Attack

Sql injection attacks for example the weakness of a bank application is used in SQL injections to mislead your application to run a backend query or command in a database. Usually, there is a menu used to search the personal detail of customers, like a telephone number, in the application of a bank.

This software will run a sql script in the database for example: -

Select customer name, gender, address, DOB;

It passes if the user enters "xxxxx or 1=1";

In the database 1=1 is always true therefore returning all the data in table

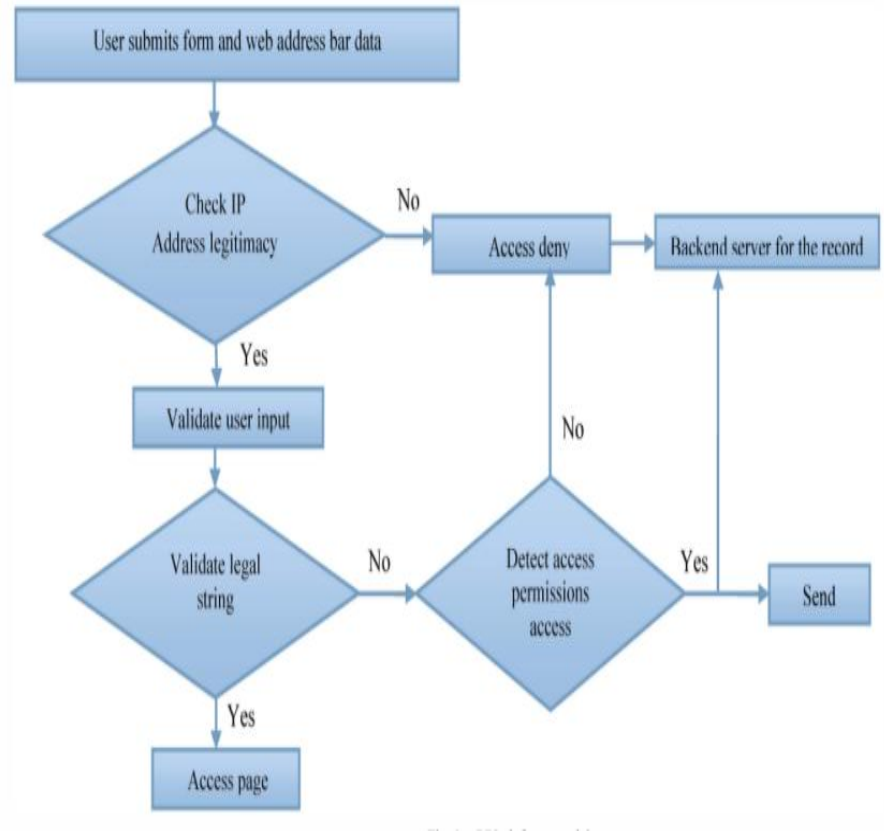

Fig 3: - Flow Chart

III. MODELING AND ANALYSIS

The design of software sits on the software system technique kernel and is applied irrespective of event paradigm and application space. Style is that any built product or system begins during the development phase. The designer's objective is to provide a model or illustration of an entity that is to be developed later. Initially, once the demand for the system is fixed and the style of the system is analysed, the first of three technical activities is to design, code and take a look at software system design and verification.

- Sql py module
- Xss module
- Broken authentication module

.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
Volume:03/Issue:04/April-2021 Impact Factor- 5.354 www.irjmets.com

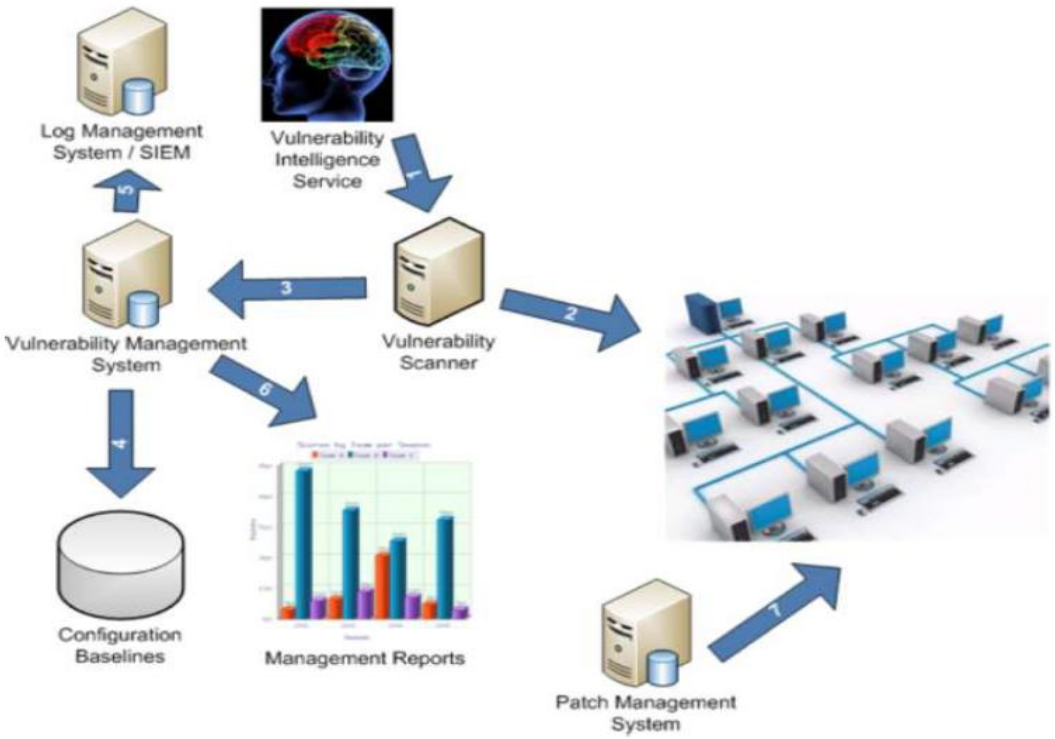

Fig 4: -ER Diagram

USECASE DIAGRAM:

It is important to consider use case diagram in the planning of an economical and efficient healthcare partner system. The case diagram for use is one of the 5 YML diagrams or modelling the system dynamics. Case diagram for modelling a system, system or category comportment is central. Use case diagrams are very important for the visualisation, specification and creation of approachable systems, systems and subsystems and categories, and they can be used in context.

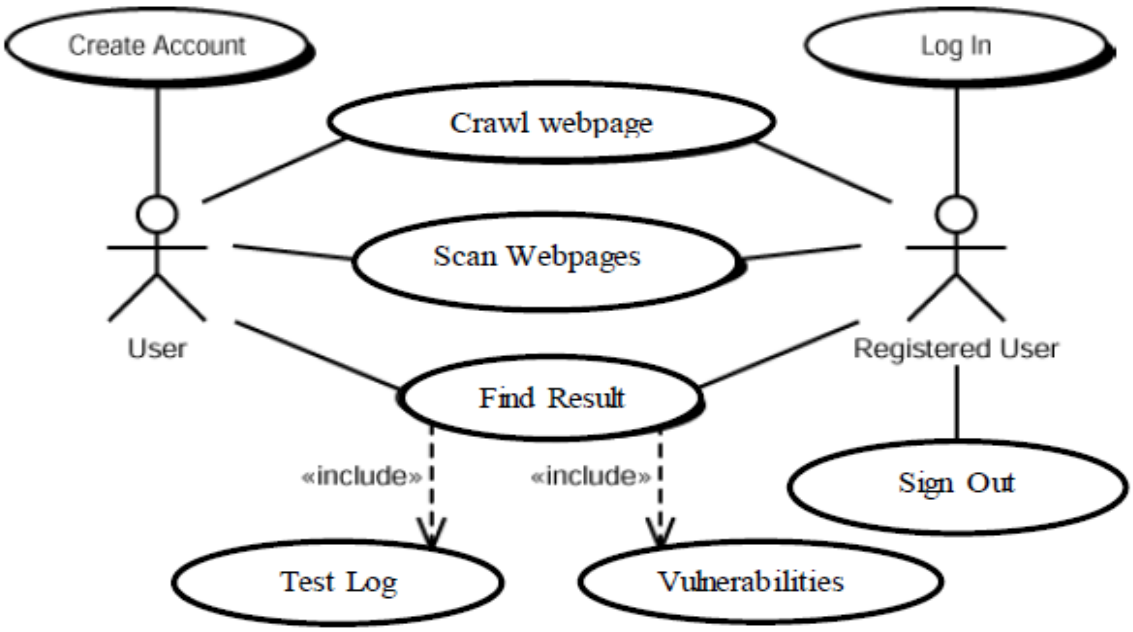

Fig 5: - Use Case Diagram

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
Volume:03/Issue:04/April-2021 Impact Factor- 5.354 www.irjmets.com

PHYSICAL SYSTEM DESIGN

The work system is created by defining design requirements that tell the programmers precisely what the applicant system has to do.

ARCHITECTURAL DESIGN

Architectural style can be an overview of its type and structure and the ways in which its components match. The style of study can be a package element, one thing as easy as the programming module, but it could be extended to include information and middleware that changes the shopper and server network configuration. There are several modules in this project. The Admin module supports the management of the entire website. The manager may decide that the complaint should be read by the department.

INTERFACE DESIGN

An effective communication media between a human and computer is created by the interface design. The communication between the administrator and the commissioning station is part of this project. As a database is necessary for this project, clients' machines have to be connected to the server host. Through the user-friendly web pages, users interact with the software.

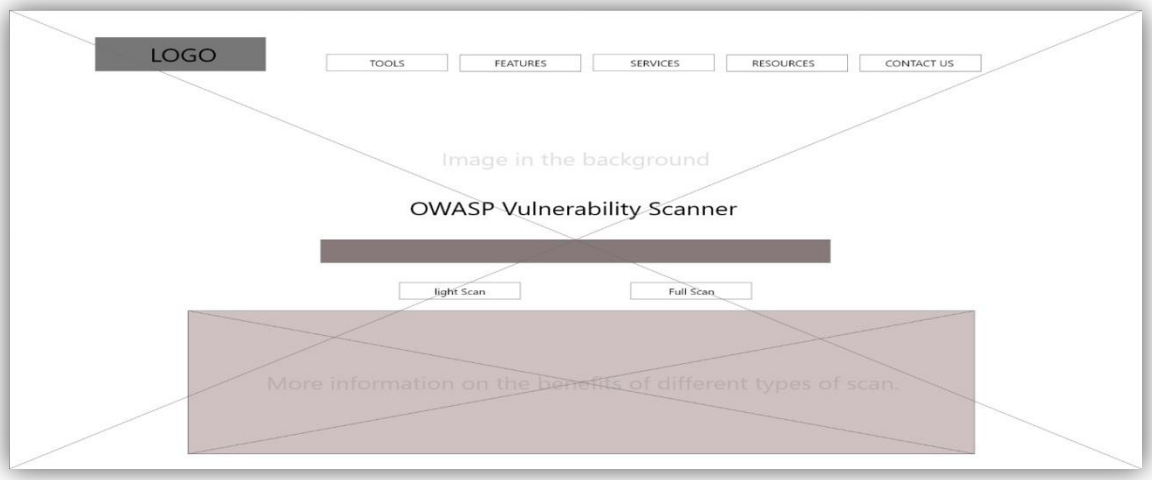

Fig 6: -Output Design

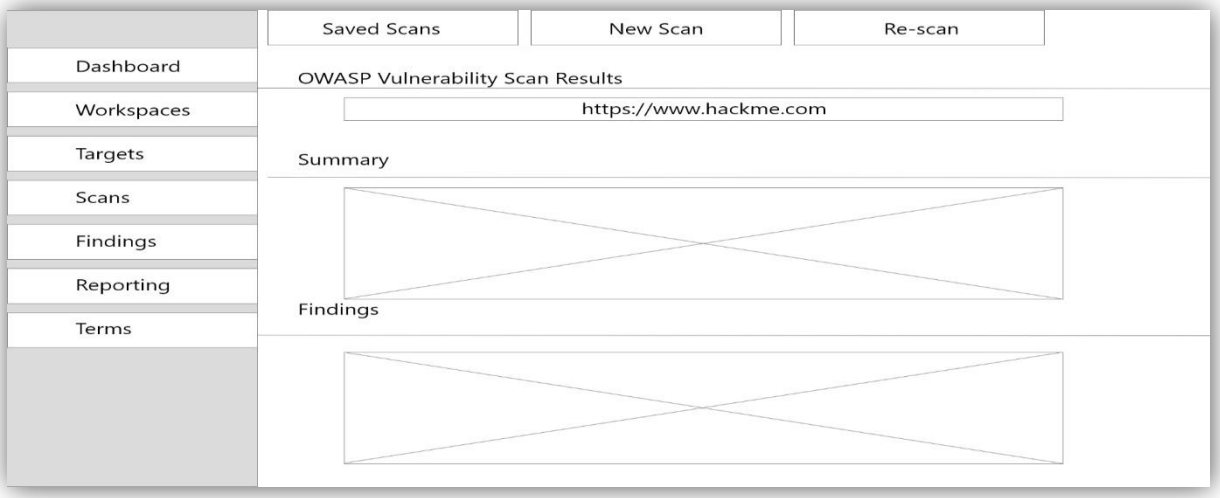

Fig 7: - Report Design

IV. RESULTS AND DISCUSSION

In one step, nothing can be achieved. It's just that during this world nothing is permanent. In addition, this project has further improvements in the evergreen and booming trade in IT. Change is unavoidable. The

"OWASP Scanner of Vulnerabilities" project was developed and tested successfully. The system and thus the design square are compatible and can therefore lead to abundant problems by adding the latest modules. Since this module has its characteristic characteristics, it can extend it to make a whole technique.

It gives the security analyst all the security issues and resolves them by the hackers.

It gives users access and modifies the information intended for them to all the privileges they need.

The present system will not be completely replaced, but the Scanning method and the information used will be largely automated.

It automates the manual method of scanning. We are inclined to believe that the organisation will finally recognise the value and necessity of this technique when it chooses to use that technique and will perceive the questions in question under the manual procedure.

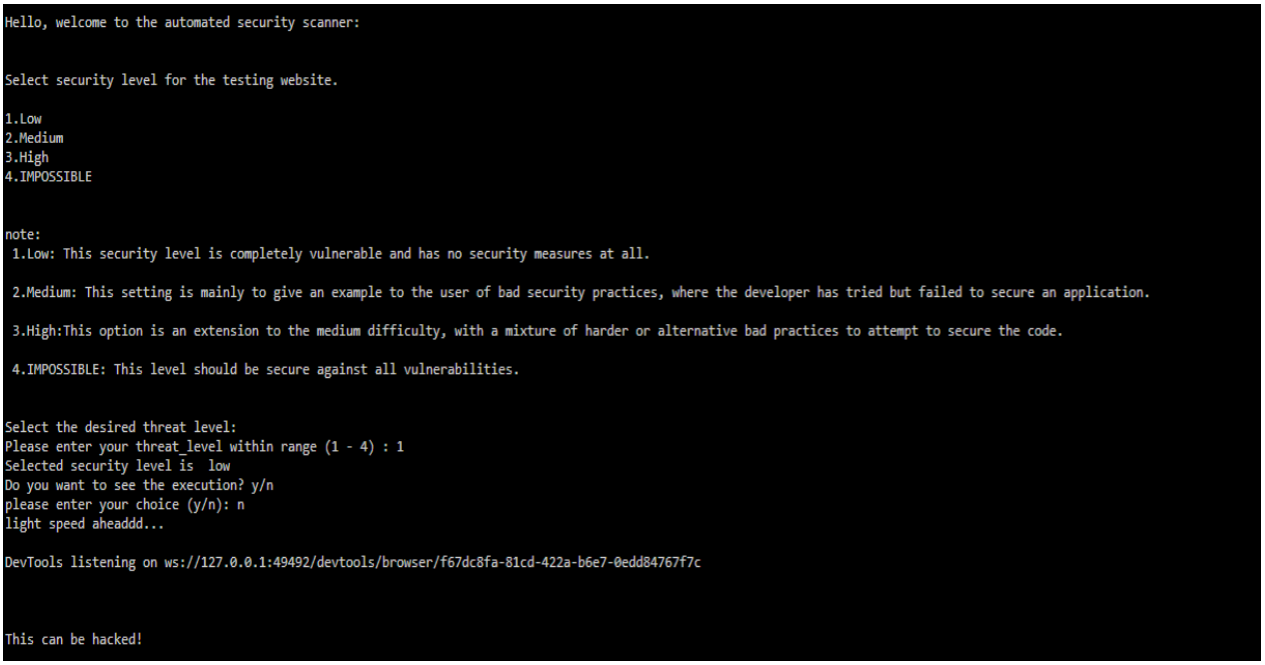

Fig 8: - Code Output

Fig 9: - Code Output

V. CONCLUSION

There is a great deal of security in the project. The simplicity and simplicity of this project unite the advantages. The user-friendly code for pc is created in the first place so that anybody can execute the pc code provided by the login word.

All details with no risk are managed in this project. All goals have been met with pleasure.

VI. REFERENCES

[1] A Study On Sql Injection Techniques Rubidha Devi. D,R. Venkatesan, Raghuraman. K

[2] Broken Authentication and Session Management Vulnerability: A Case Study Of WebMD. Maruf Hassan, Shamima Sultana Nipa1, Marjan Akter, Rafita Haque, Fabiha Nawar Deepa, Mostafijur Rahman, Md. Asif Siddiqui1, Md. Hasan Sharif1

[3] Static Analysis on Interactive Sensitive Data Exposure Detection A. Obaida, Eric Nelson, Rene V. Ee1, Israt Jahan, Sayeed Z. Sajal

[4] A Guide to XML eXternal Entity Processing Rachel Hogue, Tufts University.

[5] Kuhlman, Dave. "A Python Book: Beginning Python, Advanced Python, and Python Exercises". Section 1.1. Archived from the original (PDF) on 23 June 2012.

[6] Complete Web Vulnerabilities Scanner: Vikas Kumar