ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 12, December 2017

Web Security: A Review

[1]Devraj

[1]Department of Computer Science and Engineering, Galgotias University, Yamuna Expressway Greater Noida, Uttar Pradesh

[1]devraj@Galgotiasuniversity.edu.in

Abstract: Web apps are designing and evaluating vulnerability removal measures with very short turnaround time. The security of the website requires the assurance of privacy and data protection. This paper proposes a research approach in the web application system. The World Wide Web offers a wide range of advanced software. The security test methodology is based on an understanding of the interaction between the user and the server via HTTP. In this section, the author will discuss the mechanisms for the creation of web applications throughout order to recognize weak web application coding practices. In this section, the author discusses frames for web application security evaluation in order to identify bad coding practices for attacks such as SQL injecting and cross-site scripting that vulnerable web applications may have. SQL injection and XSS attacks are extremely dangerous, since the database is a key information source for the attacker. The suggested approach consists of creating a searchable research suite based on the heuristic genetic user session. The main goal of this article is to clarify the protection of a cloud-based framework for online testing.

Keywords: Web Application Testing, Security Assessment, Gray Box Testing, White Box Testing, Black-Box Testing.

INTRODUCTION

The development of web applications is a very expensive process due to the time and energy nature of a web application. Research, development and production cases. The detection of network security vulnerabilities worldwide shows a dramatic increase in the number of attacks on Web applications. Developers are increasingly skilled in writing and designing and distributing secure code. Based on the injection input from the first injection and then extend the knowledge base as other pages crawl the knowledge base using the proposed theme model. Knowledge and knowledge extension lead to better patterns of injection..

It also offers a new analysis approach to vulnerability, including the advantages of dynamic and static analysis. This approach is effectively implemented through the expanded web application protection assessment framework. One of the distributed systems is a Web device with a client and server architecture or multi-level architecture. Web applications continue to operate in different environments such as computers, network connections, operating systems, web servers and web browsers. [1].

World Wide Web is one of the most popular internet access software information and services, which offers static page access to a network that facilitates web applications. There are numerous factors, including remote accessibility, cross-platform compatibility and fast growth that contribute to the growing popularity of the web application. The AJAX (Asynchronous JavaScript and XML) architecture also allows users to gain greater performance and flexibility on web applications. As the use for critical security services of Web applications increases, they are a valuable tool for security attacks. [2].

In general web applications the backend systems communicate with which sensitive information (e.g. financial and health) can be stored. The compromise of web applications will lead to a systemic breach that leads to serious economic, ethical and legal damage. The Verizon violation report showed that web devices have now had a large number of infringements and a large amount of data. [3].

In this article, the author discusses the state of the art in the protection of web applications as displayed in Figure 1 to systematize current technologies in a

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 12, December 2017

broad picture which promotes future research. Based on the theoretical safety paradigm of the some researcher surveys, structure our surveys into three web application safety assessment parts: a system model, a risk model and a defense mechanism. The process model defines the operation of a web application and the unique characteristics of the threat model. The danger model describes the power and resources available to assailants. [4].

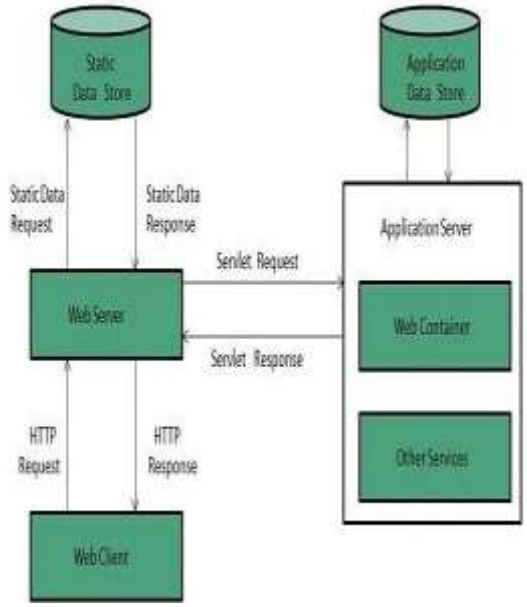

Figure 1: Block representation of web server

Considerations In Web Security:

The World Wide Web is primarily an internet-and TCP / IP client / server application. Therefore in this book, the security tools and strategies mentioned so far apply to web security as displayed in Figure 2. But in computer and network security, the Web presents new challenges which are generally unknown:

There are two Internet routes. In contrast to traditional publication systems, even digital publishing systems including teletexts, voice makers or fax back can make Internet attacks against web servers.

The internet primarily serves as a highly visible way to provide business information and a trade forum. The reputation of web servers can be hurt and the cash can be lost.

The underlying code is extremely complex, as web-browsers are very simple to use, web-servers are relative amentia easy to configure and manage.

A web server launch pad in the entire organizational or departmental computer complex. Upon subversion, an attacker can access non-web-based data and structures that are linked to local website databases.

Typical consumers are casual and untrained web-based service users (in security cases). Such users are not necessarily aware of safety risks and they have no active tool or know-how countermeasures. [5]

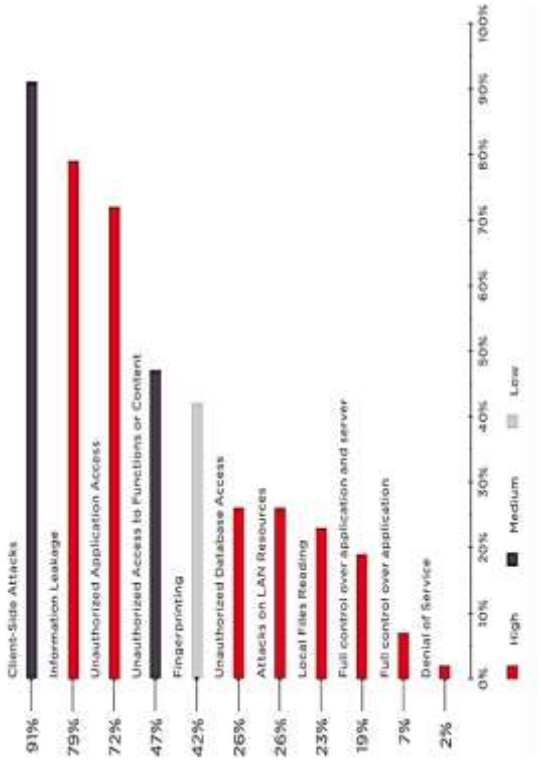

Figure 2: Comparison of threats on web

Security Techniques of the web application:

CI4A (Confidentiality, Privacy, Authentication, Authorization, Availability, Accountability) as key security services are subject to Web security evaluation requirements. Non-repudiation is another security service commonly associated with transparency. Confidentiality of data transmitted or stored within the web application is considered for business web applications. [6]

Integrity means that no intentional or accidental modification of information used may be possible.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 12, December 2017

Authentication involves searching for identity. Integrity encryption can also be taken into account in the scope of origin. The security company actively develops automated solutions to detecting security vulnerabilities. [7]
Nonetheless, the most effective way to identify web-based vulnerabilities is to manually test applications:
Testing black boxes, and
Testing white boxes.

Testing Black Box:

This research approach examines the applications available and the expected results of each input. Most blackbox analyzes utilize either the GUI or image recovery software as co-ordinates. An example of a black-box system would be a search engine. In the search bar, you enter text to be searched by clicking on "Search" and returning results. If you do this, you clearly see that you give the results of your quest an annotation–a search word–and you obtain an output. The precise process used to achieve the search results is not known or seen. The way the algorithm produces a certain result does not contribute to the internal function of the system. [8]

White box testing:

This approach explores the subsystem of the application. While black-box testing only codes inputs and outputs are checked, white-box tests let you see what's going on in the system. White box testing provides a certain degree of complexity not available for black box testing because the tester can define and communicate with software rather than the user's interface. An example of a white box system is an in-circuit test when someone considers the interconnections between individual elements and tests that every internal connection functions correctly. An automatic machine control from a different area may serve as an example to ensure that all individual parts function properly to ensure the machine is properly operated. The system is automatic.
Considering the requirements for the web security
A different set of security protocols are required for every application, so for a minimum standard, the NIST SP 500-269 recommends a security web application scanner.
Recognize such web application vulnerability types.
Build an attack text report for each vulnerability found.
Fake positive results are identified at an acceptable low rate. [9], [10]

CONCLUSION

The aim of this paper is to test web applications for security on the basis of a machine approach. Some website vulnerabilities have been reported in cases of phishing and defacement. Mostly because of inaccurate coding or no validation data for web applications. This paper also introduced a new approach to predictive penetration testing using skills in quantitative analysis. The data analysis is carried out via stored procedures and triggers via other software storage types and special attention is given to developing automatic ratcheting mechanisms. Automatic filling of a form is the main problem. Statically analyzed data flows can be identified from HTTP parameters in the server area. The work should also be carried out to supplement the generated test suit to achieve a full coverage through a structural analysis.

REFERENCES

[1] "Web application firewalls for security and regulatory compliance," 2017.

[2] Z. Ghanbari, Y. Rahmani, H. Ghaffarian, and M. H. Ahmadzadegan, "Comparative approach to web application firewalls," in *Conference Proceedings of 2015 2nd International Conference on Knowledge-Based Engineering and Innovation, KBEI 2015*, 2016, pp. 808–812, doi: 10.1109/KBEI.2015.7436148.

[3] *2012 Trends Report: Application Security Risks*. Cenzic, Inc., 2012.

[4] "The Basics of Web Application Security." .

[5] "OWASP Top 10 - 2017: The Ten Most Critical Web Application Security Risks," *Open Web Appl. Secur. Proj.*, 2017.

[6] "6 Ways To Strengthen Web App Security." .

[7] *WHID Project is now a Joint WASC/OWASP Project*. WASC, 2014.

[8] B. Musa Shuaibu, N. Md Norwawi, M. H. Selamat, and A. Al-Alwani, "Systematic review of web application security development model," *Artif. Intell. Rev.*, vol. 43, no. 2, pp. 259–276, 2013, doi: 10.1007/s10462-012-9375-6.

[9] "Web Application Vulnerability Scanners."

[10] "Source Code Security Analyzers."