IJMRT: Volume (4), Issue 6, 2022

ISSN (Print) : 2663-2381
ISSN(Online) : 2663-4007

International Journal of Multidisciplinary Research Transactions

(A Peer Reviewed Journal)

www.ijmrt.in

A research study on Web Application Security

Kumar Shivam[1*], Mahesh Raval[2], Prof. Nripesh Nrip[3], Dr. Achalesh Sinha[4]

[1,2]Student, Department of Computer Application, Bharati Vidyapeeth (Deemed to be University) Pune. Institute of Management Kolhapur Maharashtra India.
[3]Assistant Professor, Department of Master of Computer Application, Bharati Vidyapeeth (Deemed to be University) Pune, Institute of Management Kolhapur Maharashtra India.
[4]Assistant Professor, Department of Computer Application, T. N. B. College, Bhagalpur, Tilka Manjhi University, Bhagalpur, Bihar, India.

**Corresponding author*

https://doi.org/10.5281/zenodo.6633934

Abstract

This research basically centers on the point of website/web application security. The prime agenda of this research is to verify that how much government websites are protected that is how they are handling the user's data as a part of providing such facility over the data inputted by the user. Vulnerability of websites is a very important aspect on which we are not focusing yet. Might have a security escape clause in it. The world is exceedingly reliant on the Internet. Nowadays, web application security is one of the biggest challenges in this world. It is considered as the principal framework for the worldwide data society. Web applications are prone to security attacks. Web security is securing a web application layer from attacks by unauthorized users. A lot of the issues that occur over a web application is mainly due to the improper input provided by the client. This paper discusses the different aspects of web security and its weakness. The main elements of web application security techniques such as the password, encryption-decryption, authentication and integrity are also discussed in this paper. The anatomy of a web application attack and the attack

methodologies are also covered in this paper. This paper explores a number of methods for shielding this class of threats and assesses why they have not been proven more successful. This paper introduces a better and prospect way for minimizing these type of web vulnerabilities. It also provides the best security mechanisms for the defined attacks.

Keywords: Web application, Security, Threats, Web Vulnerabilities.

1. INTRODUCTION

Web security is an important aspect for web applications. Today web security is a real concern related to the Internet. It is considered as the principal framework for the worldwide data society. Web applications provide a better interface for a client through a web page. The web page script gets executed on client web browser.

As per the report of CERT-in, over fifty-three thousand eighty-one security incidents were handled including twenty-nine thousand five hundred and eighteen website defacements in 2017 [1]. Recent vulnerability notes reported multiple vulnerabilities in phpMyAdmin, remote code execution in WebSphere Application Server, Data breach via malware on IoT that may exploit the SQL injection and cross site request forgery at victim's machine. In recent last year malwares like ransomware, WannaCry comes in account and flare-up the accounts and breach the credentials. In consequence online service providers down for a while. There are more new versions of web site malwares are formed by attackers' day to day. Web applications are a main base of attacks such as cross-site scripting, cookie-session theft, browser attack, self-propagating worms in web email and web sites. These types of attacks are called 'injection attacks' which attacks by the use of malicious code. Injection

attacks have commanded the highest point of web application vulnerability lists for a significant part of the previous decade.

2. Literature Review

The main issue in web security research is in enabling a user a safe and trusted platform for communication with the web application. But some people continue to do business with insecure site. Some organizations or companies don't want to reveal the information about their own security holes. So, it's very hard task to get the reliable information about the state of web security today.

There are two common important security vulnerabilities today: SQL injection and cross-site scripting. These types of vulnerabilities directly affect web servers, application servers, and web application environment.Literature survey has been carried out to explore the existing work and identify the research gap in the field of web application vulnerability analysis, their limitations, future work. Identified future scopes of existing tools and techniques are summarized in next section.

The below graph depicts about the possible vulnerabilities that an attacker or data stealer can perform by using different methodology. The graph illustrates that what percent of motivation are generally seen in attackers while performing the attack on web applications.

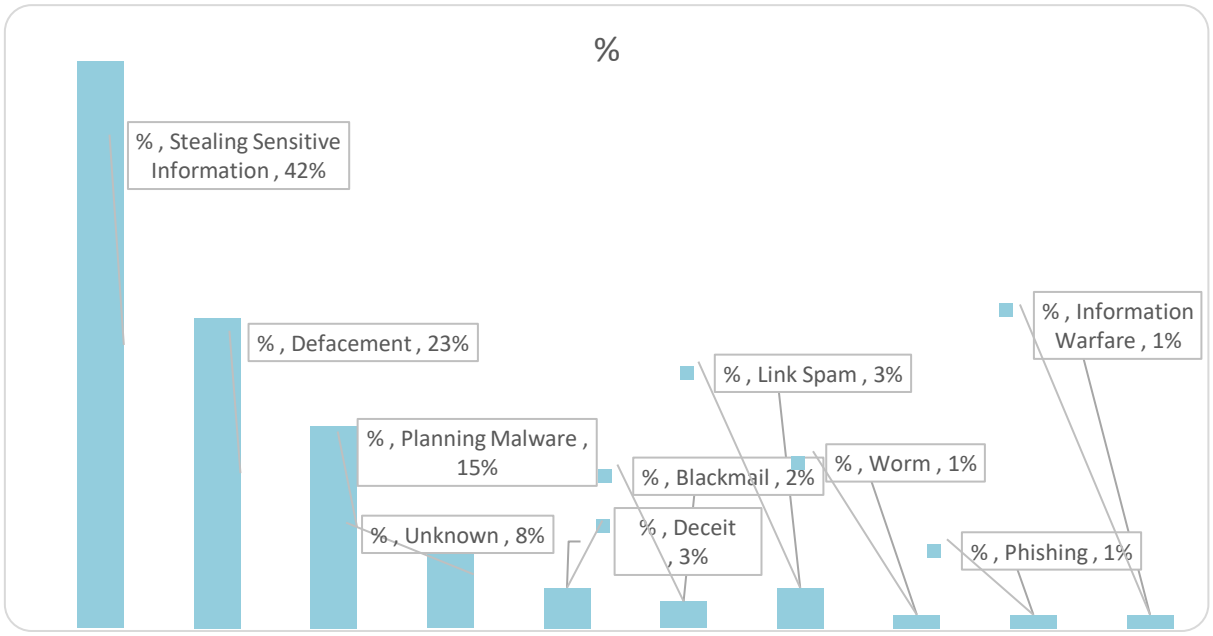


Figure.1 Attacker Intention during WebApp attack

The literature survey study of different vulnerabilities define that two common security vulnerabilities are SQL injection and XSS. Many technology and mechanism are proposed by different researchers to prevent the SQL and XSS attack. During our research we have found out that SQL injection attack and XSS attacks are still possible even after implementing preventing mechanism presently available in the market, and so provide a preventive mechanism we have proposed the architecture shown in figure 2. In this figure we have proposed a scheme through which we will attack any website with SQL injection whether it is prevented by any of current available mechanism.

Client:

The client of a web browser is effectively making client requests for pages from servers all over the web. In this article client login to system normally, client sends request to server and gets response. This happens only in normal scenario.

Attacker:

Attacker is an unauthorized user. Typically, this kind of attacker would be a proficient

programmer or engineer with sufficient technical knowledge to understand the weak points in a security system. In this article Attacker attacks the website through SQL injection and XSS. Uses of SQL injection and XSS by the attacker is mentioned below.

a. SQL Injection Attack:

The common use of SQL injection attack is to abuse web pages that allows users to input data into form fields for database queries. Injection is an unintended command sent to an interpreter. Attackers can enter the modified SQL query for user information. The queries directly communicate with database for operations on data like data delete, create and change. The queries create link of the static part and value intended for attack.

b. URL Injection Attack

Query url is also a way of attack which is a well crafted attack url . If we have a web page with the url. For example: if you get an URL like http://xyz.&.in/word /abc/abc.html
Then it means, we do not have any vulnerable points in the
page. But if the URL is like

http://xyz.s&.com/pro.php?u_id='xxx' then 'u_id=xxx' is a string type query for the url for can be altered by an attacker. The attacker can then enter his query in url which can give him access to the database, causing an attack.

SELECT * FROM obj WHERE u_id='xxx'.

'u_id' is parameter of this query and xxx is its value .It is fixed type of parameter but attacker can modify its value, which makes it vulnerable. For Example:-

http://localhost1/?E_Id='xxx';

String E_id= "DROP TABLE EmpTable"

Another type of attack is when the attacker uses a UNION query and merges the special crafted query with the original query used by the user. **http://localhost/?EmpId='UNION' .** This url will change the following SQL statement **SELECT e_info FROM E_Table WHERE E_ID = '' UNION.**

c. Cross Site Scripting Attack (XSS)

Cross site scripting (XSS) is also serious problem of web application that can be used by an attacker. The attacker can insert the malicious script in web application through any external resource.

The web browser executes the malicious code as a legitimate code.For example:

The hacker can modify the URL and execute the malicious code in URL box.

http://xyz1.com/index23.asp?search=

The attacker can add modify statement to the URL and hijack the client to his domain.

1. {get Element sByTagName("formpage"[02].act io =}
2. ">><script>document.location=' http://www.xyz.com/bin1/cookies.cgi_?' +document.cookies</script>"
3. varmsg = '<p tyle="color: red </p>'; msg.addInfoMessage(msg);

The attacker uses this type of script code for cookie theft with the stolen cookie and it helps in accessing the user's account.

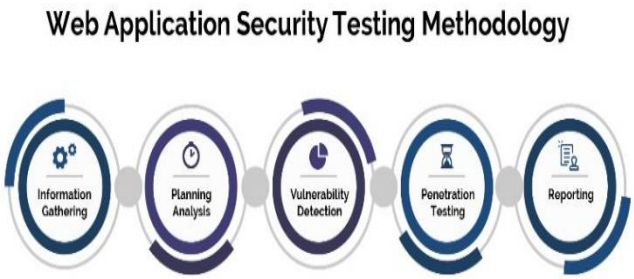
Server:

A server is a program that uses HTTP to serve the files that form web pages to users, in response to their requests, which are forwarded by their system HTTP client. In this article client sends request to server and gets a response. Attacker tracks the session id of user by

sending http request to server. (eg:GET/user/profie_session_id="xyz") using several malicious code.After this request, server will respond to the user's session_id (eg: _session_id="xyz"). Finally, attacker will attach malicious script into a database(commands) and gets response for the query accordingly.

3. **Future Scope of Existing Scanners and Approaches**

Web application analysis tools and techniques are used to identify web vulnerabilities in web pages with or without running the source code. These techniques are useful to write secure code during SDLC. Solution of vulnerabilities during development life cycle saves the testing time and cost. Most of the static web analysis scanners suffer from false positive and false negative cases due to unavoidable conditions. Such conditions can be resolved by the developers during development. Hence, web application scanners during SDLC help most to the developers to write secure code.



4. Protection Against SQL Injection Attacks

Malicious attacks make web applications less secure because the intruder can harm the integrity of the database by applying malicious queries

Binding variables is one more way for control SQL injection attacks and through binding variables we can improve web applications performance. The developer should use this type of variable in all SQL statements and also to Java language which provides better method called prepared statement. Prepared statement also uses bind variables. To defend against the SQL injection attacks, we should avoid passing the input directly into SQL queries. Instead, user should use parameterized statements or sanitized input filtered carefully. In order to sanitize the provided user input, it should be bound to a parameter and input must be done through a filtering or sanitizing method .The main purpose of this method is that it adds a back slash('\') against all malicious code.

Web application penetration testing is a process that is used for analyzing the security of the website. It is used to find out the vulnerabilities of the website or its web applications. It can be used for a white hat or black hat purposes.

The web application penetration testing is done to find out the loopholes of the website before malicious hackers can find it. Penetration testing is generally done to find out the security weaknesses of the website, which are then reported to the concerned team.

5. **Protection Against Cross-Site Scripting Attacks**

Nowadays cross-site scripting attacks occur because the developers add some vulnerability to the code. Every developer is responsible for attacks because developer should understand what kind of attacks are possible on web application. Never trust user input because the user can insert any type of characters and always use filter metacharacters as it reduces the XSS attacks. Developers should convert what's written between any two tags, which are enclosed in '<' and '>'. XSS holes can damage your application because the attackers will disclose

these types of holes to the public and often everyone can see your personal information. Filtering does not provide a proper solution for cross site scripting attacks. But if developers use) and (, to &quot ; , ' to ' and convert # and & to #(#) and & (&).

Risk Assessment and Entry Assessment Must be regardless of the type of industry your organization falls into. It is about verification and evaluation of your organization's security status.

In simple terms, we can say it is a way to test whether your company is secure to external attacks or not. In these modern times, we hear a lot of stories of robbery and cyber-attacks. We all need to protect our systems and networks. Risk assessment and entry assessment will inform you of the attacks and security loopholes and how to fix them.

Additionally, enabling VAPT also enables compliance with data security by storing customer data on networks and applications and protecting it from any risk of cybercrime.

5. Result Analysis

In this study vulnerability assessment is performed the on few government of India websites (Indiagovtjobs, mahadbt, morth, nadakacheri, ncs). We have accessed the website through a Vulnerability assessment tool **sitecheck.sucuri.net**. According to the data the researcher found that most of the government websites are not much secure. There may always be the threat of cyber application attack.

Below data stats represents the result of assessment of selected government websites on which vulnerability testing is performed the. As result it is found most of the government

websites are not as much secure as expected. The website handling team needs to pay attention about the vulnerability.

The below data set represents that indiagovtjobs, mahadbt and ncs websites are having the chances to get attacked by any of means.

The researcher also taken the scanning assessment of privately owned websites the results is quite good, that almost of them are having the vulnerability status low as they are much secure.

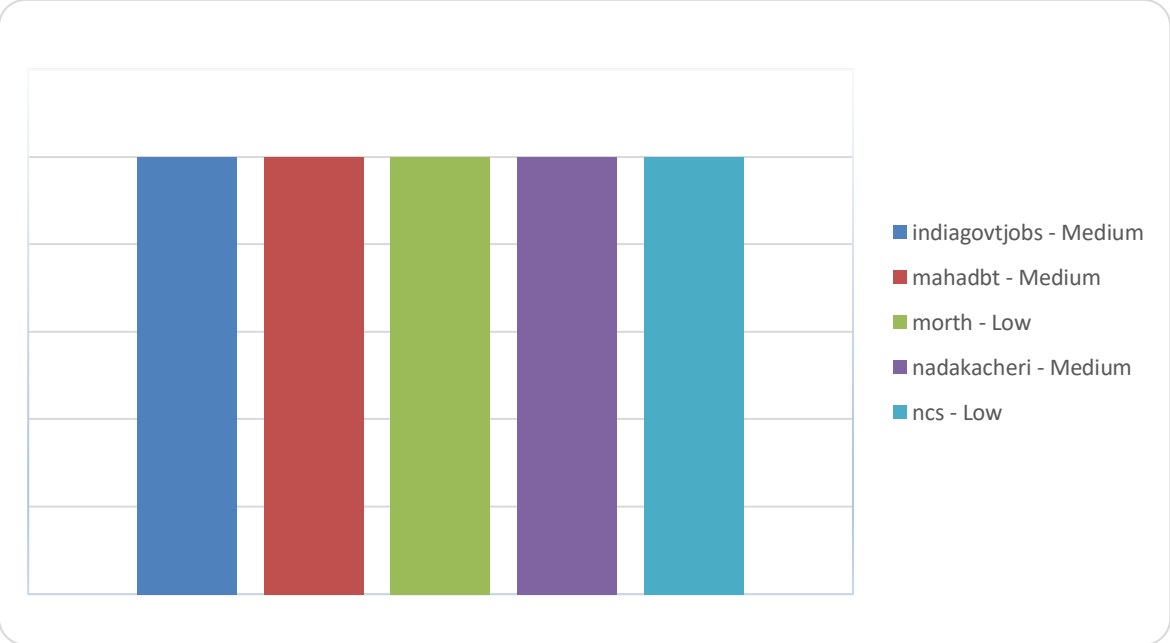


Figure.2. Details of attack

6. Conclusion

In today's era one of the roles of web applications is to provide graphical user interface to the end users for communicating the devices through internet. Development and hosting of web application is too easy. Hence, new attack vectors are encountering frequently to breach the end user's information. Literature survey of this paper concluded that there is a need of an AI engine to update instructional database of vulnerability scanner automatically for newly encountering attack vectors.

Hence, in this paper a framework to identify the taint style attacks has been proposed. It performs several types of scanning like taint type, ontology based, etc. to detect security vulnerabilities.

It updates its instructional database by the record gathered from the data flow analysis phase. It can identify the web vulnerabilities like XSS and SQLIAs, Frame-Jacking, Zero-day vulnerabilities, etc. Proposed framework facilitates deeper understanding about attacker's behavior/ intention on web application. It also facilitates to security experts and developers to easily update detection database as per new requirements. Finally, it generates a detailed report which contains a detailed explanation of each potential vulnerable function that represents security vulnerability in web application.

This research paper provides a complete survey of current research results under web application security. We have covered all properties of web application development, understood the important security functions and properties that secure web applications should use and divided existing works into three major classes. we also discuss a few issues that still need to be considered.

To access a few out of the box features in web applications various programming concept and tools are taking place that cause essential security aspects to our applications. Apart from these security researchers applying required efforts to extend security features to web applications by several tools and techniques.

Generally, our logics and crucial codes resides at client side that is our browser that exposes programmer concepts. Thus, for attackers it becomes easy to intercept the logics and cause total damage to the server-side state of the application.

As the number of data breaches grows, companies are urgently looking for new ways to protect their data. The Internet is full of information on how companies can protect their data. The fact is that businesses of all sizes need to use the best VAPT solution to protect data. In

this paper, we have discussed the importance of a VAPT solution and how we can help protect the right business from malicious attacks. The best part is that it is affordable for all businesses.

REFERENCE

[1] Tajpour,Atefeh, Maslin Masrom, Mohammad Zaman Heydari, and Suhaimi Ibrahim. "SQL injection detection and prevention tools assessment" In Computer Science andInformation Technology (ICCSIT), 2010 3rd IEEE International Conference on, vol. 9, pp. 518-522. IEEE,2010.

[2] Ali, S., Shahzad, S.K., and Javed, H., SQLIPA: An Authentication Mechanism Against SQL Injection.European Journal of Scientific Research, Vol. 38, No. 4, 2009, pp. 604611.

[3] Sadana, S. J. and Selam, N. "Analysis of Cross Site Scripting Attack," Proc. International Journal of Engineering Research and Applications (IJERA), vol. 1, no 4, pp 1764-1773, 2011.

[4] Kumar, R. "Mitigating the authentication vulnerabilities in Web applications through security requirements," Information and Communication Technologies (WICT), vol. 60, pp 651–663, 2011.

[5] Avancini, A. and Ceccato, M. "Towards Security Testing with Taint Analysis and Genetic Algorithms," ICSE Workshop on Software Engineering for Secure Systems, vol. 5, pp. 65–71, 2010.

[6] Shar, L. S. Tan, H. B. K. and Briand, L. C. "Mining SQL injection and cross site scripting vulnerabilities using hybrid program analysis," Proc. of Int. Conf. on Software Engineering (ICSE '13) IEEE Press, pp 642- 651, 2013.

[7] Li, Y. Wang, Z. and Guo, T. "Reflected XSS Vulnerability Analysis," International Research Journal of Computer Science and Information Systems (IRJCSIS),vol. 2, pp 25-33, 2013.

[8] Shar, L. K. and Tan, H. B. K. "Automated removal of cross site scripting vulnerabilities in web applications," Inf. Softw. Technol., vol. 54, pp 467–478, 2012.

[9] Yang Haixia And Nan Zhihong , "A Database Security Testing Scheme Of Web Application" , 4th International Conference On Computer Science And Education,2009 , IEEE, PP .953- 955.

[10] Meijunjin ,"An Approach For Sql Injection Vulnerability Detection" , 2009 Sixth International Conference On Information Technology :New Generations IEEE , PP 1411- 1414.

[11] A. Azfar, K.-K. R. Choo, and L. Liu, "A study of ten popular Android mobile VoIP applications: are the communications encrypted?" in Proceedings of the 47th Hawaii International Conference on System Sciences (HICSS '14), pp. 4858–4867, IEEE, Waikoloa, Hawaii, USA, January 2014

[12] Muturi, Isaac. (2017). WEB APPLICATION SECURITY. 10.13140/RG.2.2.24963.20000.

[13] Inamdar, Danish & Gupta, Shyam. (2020). A Survey on Web Application Security. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 223-228. 10.32628/CSEIT206543.