Web Applications and Their Security Perspective

Sumit Sharma
Research Scholar
Department of Computer Science
and Engineering
Lovely Professional University
Phagwara, India

Atul Malhotra
Assistant Professor
Department of Computer Science
and Engineering
Lovely Professional University,
Phagwara, India.

Abstract:

Cyber security is playing a leading role in all possible organization such as in financial organizations, manufacturing industry and other organization sectors. Computers which manage access to a centralized resource or service in a network are dictating assets in all such organizations where business acute sensitive information is stored. These servers include web servers in them through which any business data and operations are performed remotely. Hence, it is obvious that for a secure and well founded operation, security of web servers is very important. Government Sponsored Program like Digital India helps many small-scale employers to scale up and take up their company online, so they can reach as many individuals as possible. With this web application-related risk of digitization also increases. In this article, I have addressed some renowned vulnerability like SQL Injection, Session Hijacking, XSS that can damage online business and its cause and mitigation strategy. A demonstration of vulnerability assessment and penetration test of web application by using open source tools has been presented.

Keyword: Cyber Security, Web Application, Vulnerability testing, digitization.

1. Introduction:

Web servers play a very important role in those services which are mainly focused or based on information technology. The most vulnerable to attacks are unsafe web applications which can cause financial damage and disrupt market reputation for organizations.These vulnerabilities can have a direct effect on the integrity of confidentiality and the accessibility of information on that specific implementation of application. Web application contains a lot of sensitive information, financial information, payment information, business data information in order to secure all of these data from an attacker or unauthorized access so that we can maintain CIA (confidentiality, integrity and availability) triad of security. The developer makes internet apps more user-friendly to run and interact with the application. Ease of use, however, is the main factor making applications vulnerable. It is also no surprise to note that the internet application contains many separate points that can be used to inject vulnerabilities and these injection points may damage the use of the application and the breakdown of information. A weakness may happen because of application design, codification error, operational error or application design safety and may also be described as vulnerability within the application. A vulnerability-free implementation is not feasible, although at some point or in association with some assaults, we can decrease or mitigate the vulnerability. The application's strategy to reduction and vulnerability tracking is penetration testing. In this phase the penetration test scans the application, tries to detect or evaluate the vulnerabilities in the application, takes advantage of the vulnerability and provides a technology to mitigate and secure the application. After the completion of the entire testing phase the tester produces a report describing the entire test outcome, including value, risks and resources, which could be threats to web application.

1.1 Web application technologies

Each web applications contains some technologies for proper functionality of application. These technologies could be application specific but there are some common protocols, technologies, terminologies which is being used by all web applications.

1.1.1 HTTP Protocol

HTTP (Hyper Text Transfer Protocol) is used for performing transmission between user and attendant, it works as request-response order in between the user and server. User could be a web browser and a hosted website could be a web server. HTTP could be used for caching, Authentication, Proxy and tunneling and for maintaining the user session.

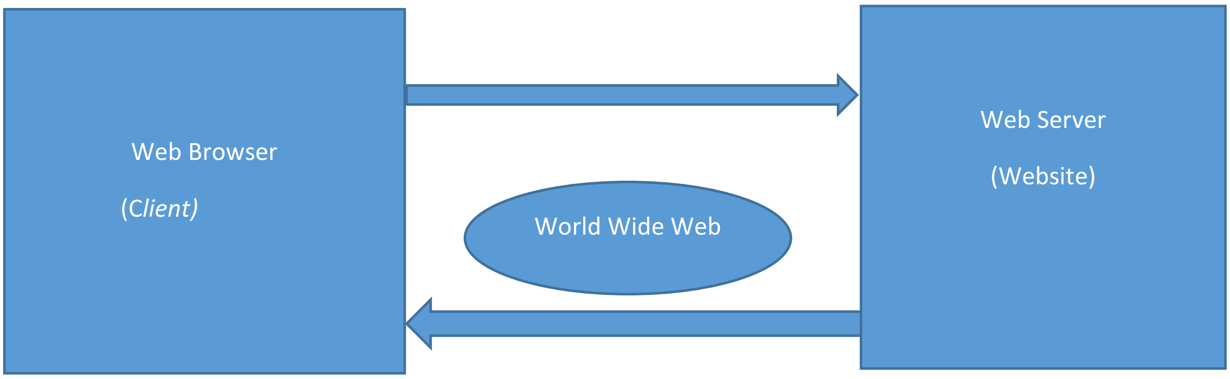

Fig 1: Hyper Text Transfer Protocol

1.1.2 HTTP Request

A simple HTTP request is sent by client to the web server for accessing the web resources. When client sends a HTTP request it mainly contains a request line to get the resource, Request Header, An empty line and a message body. Whereas when server response for that particular request it contains HTTP Status code, Headers, An empty line and a message body which is optional.

1.1.3 Cookies

Cookies are small text file is generated by website and that is stored in client system either temporary for that particular session or permanently on the disk. Cookies plays an important role in maintaining the application state. It is mostly used for storing user preferences websites, authentication and with all other resources which can help to client for accessing server. Cookies are very important according to security concerns of users as only that particular website can see that particular cookie which is being used by user so other don't have permission for check the information provided by user.

1.1.4 Server Side Functionality

As Web application content is dynamic so for handling the all queries being requested by client we need server side to perform the functionality .Server side mainly contains Application and Database server. These are set of programs run on server which is mainly deal with generation of content of web pages. Server side mainly performs function like Process the input given by user, Querying the Database, Simultaneously interact with other servers too, Providing structure to the web application and many more. All these function is done by making use of programming language like PHP, PYTHON, ASP.NET. Which mainly works on Server side of application.

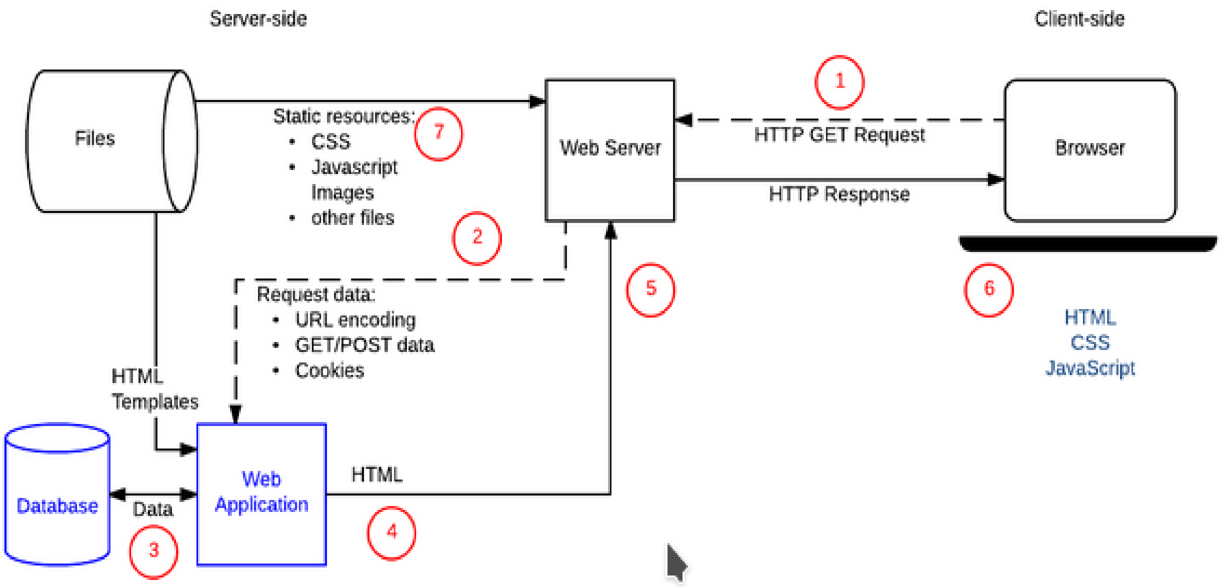

Fig 2: Client and Server Side Functionality

1.1.5 Client Side Functionality

As compare with server side client side programs are embed on the client web page and process on the clients browser. These are set of programs which runs on end user system and mainly deal with the User interaction of application. Client side mainly perform functions like interacting with user ,making interactive web content, local storage interaction ,works as bridge between client and server. All these function is done by using client side programming language like JavaScript, HTML, CSS.

1.2 Working of Web Applications

Website are an application installed on computers has an operating system and it also has a number of application to allow to act as web server so the main two applications it probably has a web server and a database server. Web server is like Apache, IIS, Nginx etc. which basically understand and execute the web applications. Web application mainly used combination of server side and client side scripting programming language to develop and execute. Database server like MySql, Mongo DB etc. contains the data used by the web applications and all of this stored on a server and which is connected to internet with some IP address associated with it so any one can access those services. The invention of web browsers was used as a means of retrieving and displaying web pages. Web page contains hypertext markup language, images, script code and become a lot of user-friendly but additionally exploits security vulnerabilities. Each web application is completely different and may contain distinctive vulnerabilities. The main purpose of the web application is to perform a lot of useful functions that you are likely to implement like:

Mail Services : Gmail, Yahoo, Outlook

Social Networking: Instagram, Facebook, Twitter

Shopping: Flipkart, Amazon, Alibaba

1.3 Architecture of Web Applications

The connectivity pattern between various components of web based applications is define as web application architecture. The architecture of the Web app depends on the distribution of the program logic between the user and the server side code. The architecture of web applications mainly consists of three types and each is separated into a working base. These areas are divided according to the source and purpose of the information that is being communicated. The following three fields are:

1. Single Page Application
2. Micro-services
3. Server-less architecture

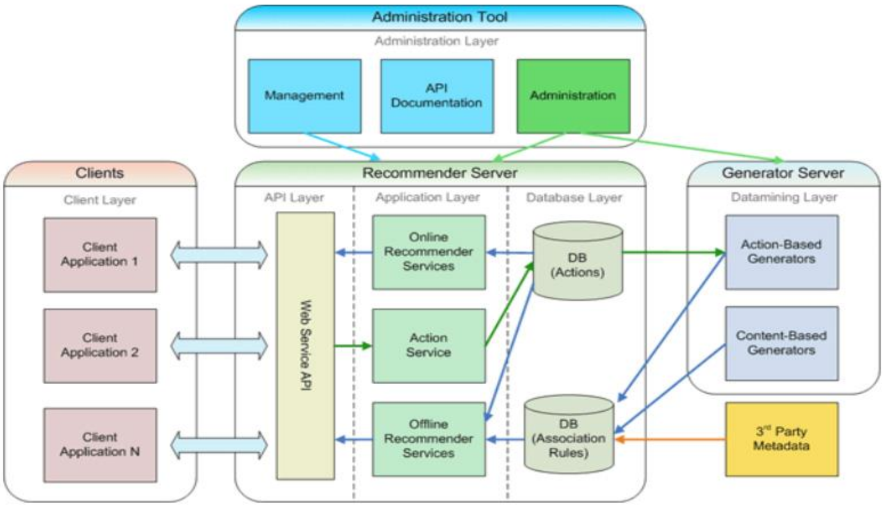

Fig 3: Full Stack Web Application Architecture

1.3.1 Single Page Application

Single Page application or single page interface is kind of modern type approach for handling the web request and serving content to the client. As previously when server was not smart and performance of JavaScript also not good, every page request coming from the server. SPA mainly works in the browser and it does not require page reload .The web page doesn't need to be updated since all page information or content is downloaded automatically. There are some advantage related with SPA as follows it is fast, Easy to debug, Can easily cache local storage more effectively.

1.3.2 Micro-services

Small and lightweight resources that provide a single task. The architecture for Micro-services Architecture has a number of advantages that allow developers not only to improve productivity, but also to speed up the entire deployment process. The components used by the Micro-services Architecture to create an application are not directly dependent on each other. As such, they do not need to be designed using the same language of programming. As shown in fig there is one gateway and that decides where it has to forward a user request. The individuals system (ORDER, CART, USERS) have been taken out and developed in parallel by individual development team. So Order system is developed by another team with its own Database and Cart system team don’t have any access to the order system database. After that an integration testing is performed to check that whether everything is working fine together or not. Now if developer want to update Order system than there is no need to update cart or user system which means all system are decoupled and can be updated individually. Individual service of micro services communicate through dumb pipes (REST API), these system can create a HTTP request and forward to another system for communication.

1.3.3 Server-less architecture :

As suggested by the name Server-less architecture but not a server less. In this type of web application, web developers focus mainly only on their web application and contact different service providers for infrastructure. Since there is no different service provider, they provide their client with complete infrastructure and maintained server and help them to work and focus on it.

2 Literature Review

Different authors have discussed about different vulnerability aspects in Web Application security in their respective research,including modification of data,user privacy and others.There are some well know vulnerabilities discussed and proposed their possible solution .

2.1 Security Triad in Web Application

Mainly security of web application is concern about three factors which are Confidentiality, Integrity and Availability.

Confidentiality can however refer to privacy. It could be characterized as an individual-sensitive data is proprietary to that particular and authorized user only so that no other person or attacker can access it. Encryption method is used to accomplish this objective.

Integrity could be define as that there will be no change of data when client server communication is being communicated. So that sender and receiver will receive same value of data on the both end. Hashing mechanism is used to accomplish this objective.

Quality could be characterized as data should be accessible to the client. Availability refers to the device as well as data. Attacks such as DOS and DDOS could directly affect the quality of information for legitimate users, so a network administrator must take care of proper implementation and protection measures to avoid such attacks.

The rest of the paper is in order as follows. Section 2 write-up the current literature about web application security and attacks. Section 3 constitute the methodology of vulnerability assessment and penetration testing 4 conclude the paper.

2.2. Different threats in web security

There are different types of threats, vulnerabilities and attacks related web application. OWASP (The Open Web Application Security Project) Top-10 represent an agreement in the middle of security resource persons of the ten all of censorious web weaknesses on the global medium now a days.

Different web applications are different in terms of its working and functionality so weakness depends upon the functionality of application.

Different application have contrasting security requires supported on the reactivity of the facts and figures stockpiled and the sequel of the proceeding the solicitation is used for. Some request can receive a high level endanger than others. To assess this we cannot only consider at the technical facet or side, but require to contemplate the ultimatum (threats) and the market utility of the system. There needs to be in way that requires by the things between the security requirements and the security reached. In literature, we will try to interpret or view of some well-known web attacks and their reduction strategy.

OWASP TOP-10

1. Injection
2. Broken Authentication
3. Sensitive Data Exposure
4. XML External Entities
5. Broken Access Control
6. Security misconfiguration
7. Cross Site Scripting (XSS)
8. Insecure Deserialization
9. Using Components with known vulnerabilities
10. Insufficient logging and monitoring

Table 1: OWASP Top 10 vulnerabilities.

2.3. SQL Injection

All web applications have a database server to manage client requests. Whenever a user sends a request to get some information from the web page or to sign in to any web application that is handled by the application's database server.SQL injection is attack which abused web pages by inserting SQL queries and allows an attacker to fetch data from the Database server.

The web submission originator does not sort sure that principles acknowledged from a snare form, cookie and input limitation, at that time SQL injection exposure commonly arisen. These SQL injection liabilities are legitimate or determined formerly transient them to SQL requests that will be accomplished on a databank attendant [8] change the invader to repossess workable data or even adjust database chronicles.

An SQLi censure can be reposing for a period and be activated by a particular occurrence, such as the recurrent performance of some course of action in the collection of data (e.g., the scheduled database record cleaning function). [4]

For example: assume there are two form

Fields are as follows-

- username and
- password

The authentication is done as:

1.

String strr ="select count(*)"Form(user) Where uname='

" ?? "'& Password='" ? " ' ";

2.

SELECT * FROM users WHERE email = 'xx?@x?x.x?x'

AND password = md5('???') OR 1 = -1]');

If user has to be allowed to enter apostrophe(') ,use replace

functions of String class:

“string strrr = UserInput.Replace(" ? ", " ? ");” [2]

2.4. Cross Site Scripting

Cross-Site Scripting (XSS) censures are categorized of injection, in which malevolent scores are introduces into or else benign and reliable or truthful web sites. XSS censures transpire when an unauthorized person utilizes a web solicitation to send malevolent program instruction, generally in the form of a search engine side scores, to a non-identical end clients. Defects that permit these censures to take the place of are entirely extensive and happen anywhere a web solicitation uses input from client side within the output it creates without validating or encoding it.

The unauthorized persons can add alter statement to the URL and seizure the consumer to his province.

1. {get Element sByTagName(“formpage”[02].act io =}

2. ">><script>document.location='http://www.xyz.com/bin1/cookies.cgi_?'+documentcookies</script>”

3. varmsg='<b><em><pstyle="color:red</p></b></em>';msg.addInfoMessage(msg);[2]

3. Methodology:

Vulnerability assessment is a security approach to find critical bugs or vulnerabilities present in the applications. Vulnerability assessment could be state as process of specify, recognize, segregate and compute different-different vulnerabilities and bugs presents in the web applications which could lead to be a bad impact on application. Vulnerability assessment could be performed through different automated testing tools and generate a security report which listed all present vulnerability in the system with their risk assessment level and their mitigation strategy.

Penetration Test approach done after the phase of vulnerability assessment phase. Mainly, Penetration Testing approach follows the exploitation of those vulnerability which are found in assessment phase by using tools like metasploit. Penetration Testing is lawful and legitimate process which actually qualify in the level of security mechanism of the application.

Manual VAPT:

Many bugs can only be detected by manual scanning. Penetration testers can use their skills and knowledge of the penetration process to conduct effective attacks on applications.

Automated VAPT:

In the Process of Automated VAPT penetration tester use tools like Acunetix, Nessus, Metasploit and which automatic perform scanning and testing on application and generate security reports

4. Conclusion

Web application will be an important and valuable asset on this digital surface. As technology is enhancing day by day and new web development framework is being introduced for making application more interactive and user friendly. New framework also invites new types of vulnerability on web surface. Companies should start implement OWASP Top-10 on their web applications and should follow web application security check list provided by OWASP. However as new defense mechanism is being introduced in web but now a days intruder is also getting smart to break those mechanism. Future study on web applications could introduces techniques like Artificial Intelligence, which can help organization to detect web attacks like Sqli, XSS, and DOS. And implementation and study of new techniques in detection of web attacks will help to security researcher to come up with more mature practices and techniques.

5. Reference

[1] Sajjad Rafique,Mamoona Humayun, Bushra Hamid,Ansar Abbas, Muhammad Akhtar,Kamil Iqbal (2015),Web Application Security Vulnerabilities Detection Approaches: a Systematic Mapping Study

[2] Sandeep Kumar,Renuka Mahajan,Naresh Kumar,Sunil Kumar Khatri (2017),A Study on Web Application Security and Detecting Security Vulnerabilities

[3] Tanjila Farah,Moniruzzaman Shojol, Md. Maruf Hassan, Delwar Alam (2016),Assessment of vulnerabilities of web applications of Bangladesh: A case study of XSS & CSRF

[4] Jose Fonseca, Marco Vieira, and Henrique Madeira (2014),Evaluation of Web Security Mechanisms Using Vulnerability & Attack Injection

[5] Priya. R. L,Lifna. C. S,Dhanamma Jagli,Anooja Joy (2014)Rational Unified Treatment for Web Application Vulnerability Assessment

[6] Sonakshi,Rakesh Kumar, Girdhar Gopal (2016) ,TECHNOLOGY CASE STUDY OF SQL INJECTION ATTACKS

[7] Rohan Vibhandik,Arijit Kumar Bose (2015),Vulnerability Assessment of Web Applications -A Testing Approach

[8] Sangeeta Nagpure,Sonal Kurkure (2017),Vulnerability Assessment and Penetration Testing of Web Application

[9] Ashikali M Hasan, Divyakant T. Meva, Anil K Roy, Jignesh Doshi (2017),Perusal of Web Application Security Approach

[10] https://stackify.com/web-application-architecture/