Web Applications: Security Issues and Challenges

Shahriar Arman (17-34875-2)

Department of Computer Science
American International
University-Bangladesh
Dhaka, Bangladesh

Khan Md. Salman (17-34851-2)

Department of Computer Science
American International
University-Bangladesh
Dhaka, Bangladesh

Ilahi, A.B.M Foisal (17-34891-2)

Department of Computer Science
American International
University-Bangladesh
Dhaka, Bangladesh

Rahman, Md. Sufiur (17-34820-2)

Department of Computer Science
American International
University-Bangladesh
Dhaka, Bangladesh

Abstract— the web is totally essential piece of our lives. It is wide stage which is utilized for data sharing and administration over web. They are utilized for the money related, government, social insurance, instruction and numerous basic administrations. Ordinary billions of client buy things, move cash, recover data and convey over web with one another. Despite the fact that the web is closest companion of clients since it give whenever anyplace access to data and administrations simultaneously. Everything is made by human on the planet so it's existence that the things made by man are tad dangerous. So web applications are additionally made by human so it contains an excessive number of provisos. The prevalence of utilizations charm programmers towards them. Presently now a days securing and keeping up the sites against assault is hard and testing task. Discovering provisos in Web application, Computer framework or arrange and abusing them called hacking. New methodologies for web assaults are increasing everyday so the investigation of recognize and avert against web application assault and discovering arrangement is significant part in web world. In this paper we presented all web application based assault including two noteworthy assaults like XSS (Cross Site Scripting) and SQLI.

Keywords— Web Application Attacks, Web Security, Web Security, testing, Vulnerability.

I. INTRODUCTION

Web application security and digital security is Current, demandable and hot profession field subject. The World Wide Web turns out to be most significant and worldwide data medium on the planet. It rapidly turns out to be most predominant approach to give access to online administrations. Client use electronic applications to look through information, trade message, connect with one another, direct business, and perform budgetary task and some more. For some clients the web is extremely simple to utilize and advantageous in light of the fact that it give 24 – hour whenever, anyplace access to data and administration for all concerned a lot is on the line: (A)Business: That get expanding salary from web business. (B)Users: Those who trust web application with touchy data. (C)Criminals: Those who can make enormous cash by taking installment subtleties or trading off financial balances.

II. RELATED BACKGROUND

Problem of web security:

A significant security look into issue is the way to empower client who is running a customer on an untrusted stage to safely speak with the web application. Since certain individuals need to work with unreliable site. Some association or organizations would prefer not to give the data about their own security openings. Along these lines, it's exceptionally hard assignment to get the solid data about the condition of web security today. Such a large number of destinations are there that did not validate client since there was no need. Every client treated in an equivalent manner and was introduced in same data [4]. Any security dangers emerging from facilitating a site were connected to a great extent to vulnerabilities in web server programming. In the event that an assailant bargains a web server he would not access any delicate data in light of the fact that the data hung on the server was at that point open to general visibility. An assailant commonly would change the documents on the server to ruin the site's substance. No client need to utilize web application in the event that she trusts her data will be uncovered with unapproved parties.

Working of web application:

Web applications are PC program enabling site guests to submit and recover information to database over the web utilizing their favored internet browser. The World Wide Web comprises of sites and sites were gathering of website pages [16].

There are for the most part two sorts: 1) Static: a page is one that does not change when a client demand it. The web server sends the page to the mentioning internet browser without adjusting it. 2) Dynamic: It's altered by server before it is sent to the mentioning program. Internet browsers were designed as a methods for recovering and showing these reports. Site page contain HTML, pictures, content code and become easier to understand yet additionally abuses security escape clauses. Each web application is extraordinary and may contain one of a kind defenselessness. Web application is chiefly made to perform essentially valuable capacities you could execute like,

- ☐ Web mail services: Gmail, yahoo, Hotmail
- ☐ Interactive information: Wikipedia
- ☐ Social networking: Facebook, Myspace, hi5.com, twitter, LinkedIn, classmates
- ☐ Shopping: Amazon, flip kart
- ☐ Weblogs: blogger
- ☐ Online calendars: Google calendar, o2 calendar, yahoo calendar
- ☐ Online telephone directory: yellow.com, whitepages.com, anywho.com
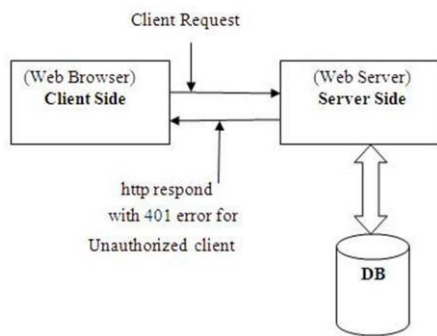
At customer side, customer sends solicitation to specific errand than at server side, customer's solicitation prepared with web server utilizing dynamic HTML pages through execution or interpretation [6]. In the event that client is approved, at that point server gives fitting reaction to the customer demand else it reacts with 401 blunders for no approved customer. It's called http confirmation and after that web application interface with backend database for putting away and recovering information. The programming language, state support, rationale execution and configuration separate web application from others. By and large assailant assaults by means of Application Layer. Aggressor sends assault inside legitimate http demand. Firewall, fixing, IDS and SSL can't distinguish or stop assault inside http demand.

Misconception regarding security:

Some security misunderstandings are there
☐   Firewall protects my web server and database.
☐   The IDS protects my server and database.
☐   IDS configured to detect attacks.
☐   Honey pot catches the attackers.
☐   SSL secure my site.
☐   SSL secure transaction of data between web server and browser of user.

These all misguided judgments ain't right. SSL does not ensure against the server and applications but rather SSL is the programmer's closest companion because of misguided sensation that all is well and good. There is one lovely sentence said by John Viegel and Gary McGraw that "Vindictive programmers don't make security gaps; they just endeavor them. Security gaps and vulnerabilities – the genuine underlying driver of the issue – are the consequence of terrible programming structure and usage."

Review process:

Planning:

4.1.1   Identification of the requirement for a survey:

This survey has been led in order to pick up learning about the issues and moves identified with the security testing of web applications. It has fundamental importance as it will furnish us with the learning and update our data in regards to upgrade of security of the web applications.

4.1.2   **Identifying Research Questions:**

Ques. 1: What are the vulnerabilities related to security of web Applications?
Ques. 2: What are the challenges faced by web Application security?
Ques. 3: What are the possible issues related with security aspect of web Applications?
Ques. 4: Does the challenges faced identify the risk associated with the secure web Applications?
Ques. 5: Does the outcomes relate to factors of importance to practitioners?
Ques. 6: Is automated security process helpful for security of web applications?

Conducting the review:

4.1.2   Selection of essential investigations

Security is a significant part of value. Because of expanding heterogeneity and multifaceted nature of the web, testing of web applications for security remains a subtle assignment. Security of web applications undermines different assaults like SQL infusion, content infusion, treat control and so forth. Likewise it features different dangers and vulnerabilities which may bring about security breaks and may block the protection of the application prompting the absence of reliability of the web administrations.

4.1.3   **Criteria for study determination**

A model for the examination choice procedure was to incorporate each one of those papers which furnish us with significant data about the security of web applications. There are different issues and difficulties related with secure web. Numerous instruments have been researched for improving the security of web applications. Dangers and dangers are regularly connected with web security.

4.1.4   **Selection of essential investigations**

For the overview, papers were gathered from different sources including IEEE, Springer, Elsevier, ACM, and so on. Aside from this, different articles, distributions and so on were additionally included during investigation. Additionally it incorporates the investigation of different devices which are utilized for security of web applications. It prohibits investigation of different structures and technique which are utilized for performing web security.

5. **Issues and challenges:**
Security is one of the pivotal parts of nature of any product or any application. Security of web applications endeavors to make sense of different vulnerabilities, assaults, dangers, infections and so forth identified with the individual application. Security should endeavor to consider however many as potential assaults as would be prudent. So we endeavor to recognize different issues and provokes identified with the security of web application.

Issues related with web application:
i. *Authentication* [9]: this involves confirming the identity of an entity/person claiming that it is a trusted one.

ii. *Authorization* [9]: it is a process where a requester is allowed to perform an authorized action or to receive a service.

Challenges by web app:

One of the worries of security of web applications is the improvement of computerized apparatuses for the security of web applications [3]. Increment in the utilization of Rich Internet Applications (RIAs) likewise represents a test for security of web application. This is because of the way that the creeping systems which are utilized for investigation of the web applications utilized for before web applications don't satisfy the necessities for RIAs [3]. RIAs being more clients well-disposed and responsive because of the use of AJAX advances. Another test could be the use of unintended invalid sources of info which may bring about security assaults [1]. Also, these security ruptures may prompt broad harm to the respectability of the information.

While working the freaks, one ought to be earnest enough to fuse them as infusing && (and) rather than || (or) or any such other adjustment may prompt flaw infusion which could bring about a security powerlessness as vulnerabilities don't think about semantics [1]. This may even represent a test to the security of any such web application. Use of shaky cryptographic capacity may even represent a test to the web application security [1]. Security of web applications may confront renouncement assaults where any beneficiary can't prove that the information got originated from a particular sender or from some other unintended source [1]. Likewise the web improvement dialects which we use may need upholding the security approach which may even abuse the uprightness and privacy of the web application [11]. This may even represent a security risk. Now and again it is likewise conceivable that a

Trespasser can wash more data than expected, in such a case again this may prompt the set back to the trustworthiness of the information which could be another test for a security analyzer.

Results and Analysis:

1. Initial Web Development Requirements

Sometimes before hiring a web development company, client's may not thoroughly clear and specific about the final finished look and working of a website. Unluckily some of the requirements that client want are not actually favor the client's need. They don't bother to prioritize their web requirements and this may substantially change the overall cost of the project.

Solution: A business examiner should unmistakably think about the significant customer's prerequisites before beginning any web advancement venture. Comprehend the customer's task work process and its related issue to discover ways for its answer next to advancing other work processes. Prior to beginning the undertaking, compose the customer's prerequisites record and get it marked by the customer and disclose it to the advancement group.

2. Incorporating Web Application :

In present world, most business applications are progressively broadened and want to live outside the firewall. These organizations may use in-house BI instruments, SaaS-based CRM framework or facilitating sites on the cloud. In spite of the fact that this may improve adaptability, still it makes a test for web designers make a web application that can undoubtedly coordinate with different applications.

Solution: An assortment of cloud facilitated administrations are presently accessible as a twofold edged sword. Coordinate site with the cloud administrations for arrangements for example mail, stockpiling, repeating membership installments, and systematic.

Each joining point ought to include understanding the coding, API, testing, and logging to investigate any test.

3. Web Site Loading:

A site page stacking time (full-page, beginning, TTFB, and so forth) for the most part relies upon a lot a bigger number of things than simply the media size. Just packing the pictures won't unravel the reason.

It is assessed that roughly 50% of absolute clients incline toward a site to stack inside 2 seconds, and in the event that it takes over 3

Seconds to stack, at that point they will in general desert this site.

Solution: Make sure to load site with just what is required. JavaScript documents and External templates must be utilized. Lessening and pack JavaScript and CSS for better execution. Pictures must be streamlined for the web. Page load and unforeseen mistakes can be diminished by cleaning codes. Check for any divert issues. Keep number of sidetracks to absolute minimum and in the best case is none by any stretch of the imagination. On overwhelming sites on account of moderate begin TCP, TTFB (Time-to-First-Byte) times can be high. Along these lines, attempt to keep the site page light. Utilization of substance conveyance and reserving systems ought to be supported.

4. Responsive Website:

In year 2015, versatile traffic has as of now surpass work area traffic. Thus, an inert site for versatile clients may lose its gigantic client base and income.

Solution: Continuously make a responsive web architecture to serve the correct client with the correct page rendition. Break down what data the greater part of the portable

clients are searching for and give it to them as ahead of schedule as could be allowed.

5. Creating the Multi-platform app: Nowadays, we're viewing another flood of brilliant gadgets, for example, glasses, watches, TVs, and parcels more. In this way, it would challenge for any web advancement application to adjust and fit every one of these gadgets and stages.

Solution: While growing new application, consider the wide assortment of gadgets for cross-program similarity, screen sizes, pixel, proportions and thickness that may fluctuate between gadgets. Evade absence of cautious idea or it might break gadget highlights and the client experience may get impeded.

REFERENCES

[1]Allen Harper, Jonathan Ness, Gideon Lenkey. "Gray Hat Hacking – Third Edition" – 2011.

[2]Ashwani Garg and Shekhar Singh. "A Review on Web Application Security Vulnerabilities". International journal of advanced research in computer science and software engineering" , Volume 3, Issue 1, January- 2013.

[3] Bhavani ThuraisI ngham, Chris Clifton, Amar Gupta, Elisa Bertino, Elena Ferrari. "Directions

[4]Dafydd Stuttard and Marcus Pinto. "The Web Application Hacker's Handbook – Second Edition" – 2014 for Web and E-Commerce Applications Security. http://ssrn.com/abstract_id=333682 October 2002.

[5]Dafydd Stuttard and Marcus Pinto. "The Web Application Hacker's Handbook – Second Edition" – 2014 for Web and E-Commerce Applications Security. http://ssrn.com/abstract_id=333682 October 2002.

[6]Gary Wasserman and Zhendong Su. "Sound and Precise Analysis o f Web Applications for Injection Vulnerabilities*, University of California, Davis.

[7]Gopal R. Chaudhary and Prof. Madhav V. Vaidya. "A Survey on Security and Vulnerabilities of Web Application". International Journal of Computer Science and Information Technology, Volume 5(2), 2014.

[8]Hesham Abusaimeh and Mohammad Shkoukani. Survey of Web Application and Internet Security Threats", International journal of computer science and network security, Volume.12, No.12,December – 2012.

[9]Katkar Anjali S. and Kulkarni Raj B."Web Vulnerability Detection and Security Mechanism",International Journal Of Soft Computing

and Engineering, Volume 2, Issue 4, September – 2012.

[10]Martin Szydlowsi, Christopher Kruegel and Engin Kirda. "SecureI nput forW eb Applications"

[11]Mr. K.Naveen Durai and K.Priyadharsini. "A Survey on Security Properties and Web Application Scanner", International journal of computer science and mobile computing, Vol.3.Issue.10, October – 2014.

[12]Nadya EIBachir EI Moussaid and Ahmed Toumanari. "Web Application Detection: A Survey and Classification. International Journal of Computer Applications", Volume 103 – No.12, October – 2014.

[13]Rahul Johari and Pankaj Sharma."A Survey on Web Application Vulnerabilities (SQLIA, XSS) Exploitation and Security Engine for SQL Injection, International Conference on Communication System and Network Technologies. 2012

[14] Swarnaprabha Patil, Prof. Nitin Agrawal. "Web Security Attack and Injection- A Survey* International Journal of Advancements in Research & Technology, Volume 4, Issue 2 February – 2015.