International Journal of Information Technology and Management
Vol. 12, Issue No. 1, February-2017, ISSN 2249-4510

Integrated Web Applications: Improving Security and Privacy

Dr. A. S. Saxena[1]* Jitendra Singh Chouhan[2]

[1] Co-Supervisor

[2] Research Scholar, Mewar University, Chittorgarh, Rajasthan

Abstract – Web Application Security Web applications are universal these days. Therefore, the field of Web application security is of regularly rising essentialness. One of the worries of security testing of web applications is the improvement of mechanized devices for testing the security of web applications. Increment in the utilization of Rich Internet Applications (RIAs) likewise represents a test for security testing of web application. This is because of the way that the slithering methods which are utilized for investigation of the web applications utilized for before web applications don't satisfy the necessities.

Keywords: Web Applications, Security, Browser Design, Distributed Applications

- - - - - - - - - - - - - - X - - - - - - - - - - - - - -

INTRODUCTION

To battle the attack and the potential for data loss, web applications must have dynamic security—like the way arranges must be effectively ensured by IDS, IPS and stateful firewalls. Notwithstanding avoiding attack, the viability of a present day application conveyance arrangement additionally relies on upon its capacity to convey execution, dependability and lower cost of possession. Application deliver controllers (ADCs) give the capacities important to quicken enhance and secure web applications and web administrations. Application conveyance, a basic for associations, includes an adaptable arrangement of administrations that can effectively oblige changing application and client factors while reliably guaranteeing the largest amounts of execution, security and accessibility, and lower add up to cost of proprietorship. As opposed to regular ways to deal with application administration, application conveyance conquers any hindrance between conventional systems and present day applications, in this manner staying away from the need to persistently include assets or hard code changes to basic parts and frameworks as abnormal state business necessities develop.

THE APPLICATION DELIVERY IMPERATIVE

Applications are pivotal to business achievement. The level of reliance on these devices of robotization has consistently ascended over the previous decade and this pattern will proceed. A few patterns influence its capacity to keep up the openness, execution and, hence, general helpfulness of these applications to their clients. The ascent of distributed computing has amplified the web application show, breaking the customary security display by giving multi-occupancy on shared gear and administrations. Versatility, globalization and off-shoring are moving clients promote far from base camp, while data enter union, security and administrative consistence are driving centralization of data assets, frequently presenting hindrances that make the related applications less available. Exacerbating matters are an expanding dependence on web applications and different innovations which are famously shaky and execution tested, and rising desires among clients and business chiefs. Exchanges must be executed about promptly. At the point when confronted with changing business necessities, IT should have the capacity to take off new applications rapidly. Distributed computing suppliers regularly refer to these snappy reaction time advantages and they depend on quick outcomes significantly more than customary undertakings. Tending to these difficulties with customary systems administration, security and administration arrangements is inadequate. They do not have the application mindfulness expected to make up for a system framework not planned in light of present day applications. Organize firewalls are tuned to the particular needs of systems administration. Web application firewalls are tuned to meet the particular needs of dynamic web applications.

SECURITY REQUIREMENTS FOR APPLICATION DELIVERY

Application conveyance requires security that is powerful, versatile and thorough. Associations have

made a generally decent showing with regards to with system security. Gone up against with sensibly solid protections at the system layer, programmers have depended on assaulting shortcomings at higher layers of the registering stack. A considerably greater component has been a move in aggressor inspiration. Instead of endeavouring to pick up reputation, assailants now concentrate decisively on getting important data including passwords, MasterCard subtle elements and Social Security numbers, and the subsequent money related prizes. The more noteworthy accentuation being put on application-layer attack relates to the way that applications are an immediate and helpful course to this kind of data. Application Security Organizations ought to make a comparing shift in their security methodologies and models. The agreement of driving security specialists and controllers is that more consideration should be paid to setting up vigorous, application-layer resistances. For no situation is this need more prominent than for web applications. Are web applications exceedingly powerless, as well as the essential vehicle for internet business and client entrances and a front way to possibly lucrative data.

REVIEW OF LITERATURES:

Hassan Doaa et al. (2008) discusses about the broken access control vulnerability which exploits the fragility of the access control and is able to fetch the sensitive and confidential information.

Turpe Sven et al. (2008) mentions about various issues like path traversal, command injection, cross site scripting, content spoofing, SQL injection, LDAP injection. Noiumkar Preecha et al. (2008) discusses about session hijacking, sidejacking, cookie cloning and sniffing cookies.

Mendes Naaliel et al. (2008) focus on the issues and vulnerabilities which are caused due to mis-configurations or by absence of any intrusion detection mechanism or firewalls. Also they mention about the threats which may occur due to the usage of the off the shelf components.

Saleh Kassem et al. (2008) discuss about the comprehensive modeling of security requirements and introduce the security requirements behaviour model to obtain secure and trustworthy web services and applications.

Fonseca Jose et al. (2008) focuses on the root cause of most security attacks are the vulnerabilities created by the software faults, and most critical web vulnerabilities are SQL injection and cross site scripting.

Haixia Yang (2009) discusses about the SQL injection vulnerability which occurs in the presentation layer (user layer) of web application.

Bau Jason et al. (2010) discusses about the Cross Channel Scripting vulnerability which allows an attacker to inject malicious code into the web server which will thus manipulate the client or a server browser.

Salva Sebastien et al. (2010) mentions about the vulnerabilities which are related to the security testing of web applications like xml injection, authentication, and authorization.

Zhang Lijiu et al. (2010) discusses about the issues like cross site request forgery, cross site scripting, malicious file execution and SQLi injection related to the web application security testing.

Terri Oda et al. (2011) discusses about the web security issues like script injection, content injection, information leakage, cross site request forgery and Click jacking.

Avancini Andrea et al. (2011) mentions about the content injection, file injection and cross site scripting attack.

Choudhary Suryakant et al. (2012) focus on the crawling as essential for security testing of web applications. Crawling is automatic explorations of web application. Andrea

Avancini (2012) discusses about a research plan to address problems of potentially attackable code. Also it speaks of cross site scripting vulnerabilities in which missing input validation can be exploited by attackers to inject malicious code into the application.

Avancini Andrea et al. (2012) mentions about the issues like cross site scripting vulnerabilities, missing or inadequate validation of input data, and disclosure of any sensitive information or hijacking of user session.

Andrea Avancini et al. (2012) discuss about cross site scripting and SQLi vulnerabilities involved with many of the web applications build in java.

ISSUES RELATED TO SECURITY TESTING OF WEB APPLICATIONS

i. Authentication: this includes affirming the personality of an element/individual guaranteeing that it is a put stock in one.

ii. Authorization: it is a procedure where a requester is permitted to play out an approved activity or to get an administration.

iii. Cross webpage scripting: it is a basic assault where an aggressor may infuse any

malignant code into the page and these vindictive code/scripts can get to secret data, or may even change the substance of any html page and so forth.

iv. SQLi: it is an assault where any vindictive script/code is embedded into an example of SQL server/database for execution which in the end will attempt to bring any database data.

v. Cross webpage ask for fabrication: it is a powerlessness which incorporates misuse of a site by transmitting unapproved summons from a client that a site trusts. Along these lines it abuses the trust of a site which it has on its client program.

vi. Xml infusion: it is an assault where an aggressor tries to infuse xml code with point of adjusting the xml structure in this manner damaging the trustworthiness of the application.

vii. Malicious record execution: web applications are frequently powerless against malevolent document execution and it ordinarily happens the code execution happens from a non confided in source.

viii. Cookie cloning: where an assailant in the wake of cloning the client/program treats tries to change the client records or information or may even damage the infused code.

ix. Xpath infusion: it happens at whatever point a site uses the data given by the client to build a xml question for xml information.

x. Content satirizing: is an assault where an aggressor tries to disguises another program or client by distorting the substance/information.

xi. Cookie sniffing: is a session capturing defencelessness with the point of blocking the decoded treats from web applications.

xii. Cookie control: here an assailant tries to control or change the substance of the treats and therefore can make any damage the information or he may even change the information.

xiii. Sidejacking: is a hacking helplessness where an assailant tries to catch every one of the treats and may even access the client letter drops and so forth.

xiv. Broken get to control: misuses the delicacy in the get to control system of the web applications with a specific end goal to get significant and touchy data.

xv. Missing or deficient approval of information: because of some absent or insufficient approval of information, assailant may give information having the scripts and so forth which when infused into a website page may prompt the divulgence of the touchy data.

xvi. Information or touchy information divulgence: security ruptures may prompt the exposure of any secret or delicate information from any web application. xvii. Social weakness (hacking), session capturing: is a well known commandeering instrument where an assailant increases unapproved access to the data.

xvii. Mis-setup: in suitable or insufficient design of the web application may even prompt the security ruptures.

xviii. Absence of secure system foundation: nonattendance of any interruption discovery or insurance framework or failover frameworks and so on may even prompt infringement of the security breaks.

xix. Off the rack segments: these segments are acquired from outsider merchants so there happens a doubt about their security viewpoint. xxi. Firewall interruption identification framework: a firewall assembles a secured divider between the outside/outer system and the inward system which is kept to be trusted.

xx. Path traversal: is defencelessness where malevolent untrusted input causes non attractive changes to the way.

xxi. Summon infusion: is the infusion of any info esteem which is generally installed into the order to be executed.

xxii. Parameter control: it is like XSS where a trespasser embeds malevolent code/script into the web application.

CONCLUSION:

In this paper, we have attempted to identify various issues and challenges faced by security testing of web based applications. A security tester thus should

keep track of all the issues while conducting testing of web application for security.

REFERENCES:

A Database Security Testing Scheme of Web Application, Yang Haixia, Business College of Shanxi University, Nan Zhihong, Scholl of Information Management, Shanxi University of Finance & Economics, china. Proceedings of 2009 4th International Conference on Computer Science & Education.

An Approach Dedicated for Web Service Security Testing, S´ebastien Salva, Patrice Laurencot and Issam Rabhi. 2010 Fifth International Conference on Software Engineering Advances.

Assessing and Comparing Security of Web Servers. Naaliel Mendes, Afonso Araújo Neto, João Durães, Marco Vieira, and Henrique Madeira CISUC, University of Coimbra. 2008 14th IEEE Pacific Rim International Symposium on Dependable Computing.

Challenges for Security Typed Web Scripting Languages Design. Doaa Hassan, National Telecomm. Institute, Sherif El- Kassas, American University in Cairo, Ibrahim Ziedan, Faculty of Engineering, Zagazig University. 2008 IEEE, The Fourth International Conference on Information Assurance and Security.

Enhancing web page security with security style sheets Terri Oda and Anil Somayaji (2011) IEEE.

Grammar Based Oracle for Security Testing of Web Applications by Andrea Avancini and Mariano Ceccato, Fondazione Bruno Kessler, Trento, Italy. 2012 IEEE, AST 2012, Zurich, Switzerland.

Mapping software faults with web security vulnerabilities. Jose Fonseca and Marco Vieira. International conference on Dependable Systems & Networks : Anchorage, Alaska,june 2008 IEEE.

Security Testing of Web Applications: A Research Plan by Andrea Avancini, Fondazione Bruno Kessler, 2012 IEEE,ICSE 2012, Zurich, Switzerland , Doctoral Symposium.

Security Testing of Web Applications: a Search Based Approach for Cross-Site Scripting Vulnerabilities, Andrea Avancini, Mariano Ceccato , 2011- 11th IEEE International Working Conference on Source Code Analysis and Manipulation

Security Testing: Turning Practice into Theory. Sven Türpe, Fraunhofer Institute for Secure Information Technology SIT. 2008 IEEE International Conference on Software Testing Verification and Validation Workshop (ICSTW'08) 978-0-7695-3388-9/08 $25.00 © 2008 IEEE.

Solving some modelling challenges when testing rich internet applications for security Suryakant Choudhary, Mustafa Emre Dincturk, Gregor v. Bochmann, Guy Vincent Jourdan, Iosif Viorel Onut, Paul Ionescu. 2012 IEEE Fifth International Conference on Software Testing, Verification and Validation.

State of the Art: Automated Black-Box Web Application Vulnerability Testing. Jason Bau, Elie Bursztein, Divij Gupta, John Mitchell, Stanford University 2010 IEEE Symposium on Security and Privacy

Testing of Web Applications: A Research Plan. Andrea Avancini Fondazione Bruno Kessler, Trento, Italy. 978- 1-4673-1067-3/12/$31.00c 2012 IEEE.

The Security Requirements Behavior Model for Trustworthy Software Kassem Saleh1 and Maryam Habil2. 1Kuwait University, Dept. of Information Science, 2American University of Sharjah, Dept. of Computer Science. 0-7695-3082-6/08 $25.00 © 2008 IEEE. 2008 International MCETECH conference on etechnologies.

Corresponding Author

Dr. A. S. Saxena*

Co-Supervisor