Vulnerabilities and Security of Web Applications

Conference Paper · December 2018

DOI: 10.1109/CCAA.2018.8777558

5 authors, including:

Dhananjay Singh

2 PUBLICATIONS **17** CITATIONS

SEE PROFILE

Devendra Kumar

ABES Engineering College

1 PUBLICATION **17** CITATIONS

SEE PROFILE

Upasana - Sharma

Amity University

24 PUBLICATIONS **67** CITATIONS

SEE PROFILE

Vulnerabilities and Security of Web Applications

DivyaniYadav[1], Deeksha Gupta[2], Dhananjay Singh[3],Devendra Kumar[4], Upasana Sharma[5]
Students[1,2] Department of Computer Science & Engineering at GCET, Greater Noida
divyaniyadav1851@gmail.com,deekshagupta19979@gmail.com
Students[3] Department of Information Technology at GCET, Greater Noida
dhananjay0397@gmail.com
Associate Professor[4] Department of Computer Science & Engineering at GCET, Greater Noida
devendra.arya@gmail.com
Assistant Professor[5], Department of Information Technology at AIIT, Noida
usharma2@gmail.com

Abstract: **Web applications are active websites which are composition of server based programs serving user interaction and various other functionalities. Web Server security is thus an important aspect for any organisation having web server connectivity with the internet and also to ensure customers using their websites, for a secure online portal.**

In this age of digital revolution, there has been a rise in demand of web developers who can produce user friendly web platforms such as mobile applications, web applications. The user base for online web applications is on a rise too. We have seen a huge emphasis on creating visual and catchy web applications but with large amount of sensitive user data at stake there should be more focus on providing web security to the applications developed.

Keywords-Software Development Lifecycle, Web Applications, Security Vulnerabilities, Threat Modules, Application Security Risks

I. INTRODUCTION

As a result of enormous amount of data being used online several vulnerabilities such as fraud and online attacks has been exposed. Also, hackers in recent years are increasingly targeting web applications, as majority of networks are governed through Intrusion detection. Therefore, the security of web application layer is necessary from unauthorized users, by building security mechanisms as follows-

In this paper, we have reviewed several evolving trends and preventions from unauthorised attacks on web .We discussed about prevention from various vulnerabilities by providing suitable data types to inputs, restricting uses of the web server, http request and restricting users from accessing files from the root directories. We have illustrated about security in academia as well as in e-commerce by assuring preservance of the various sensitive credentials such as passwords and id information. Finally we discussed about the overall security preventions for operating system and mobile applications and also discussed about operating system hardening and privileged access to promote total security of our applications and data.

II. LITERATURE SURVEY

There has been a lot of research in the field of security testing of web applications.

Clifton[6] discuss about the main building blocks of e-commerce and web security and these are tools and mechanisms supporting access control policies for the e-commerce environment, secure federations of collaborating organisations and secure workflow management systems .he believes that the XML language can play a key role in access control for e-commerce applications.

Ibrahim [7] focuses on the vulnerabilities present in the websites of the Academic Institutions ranging from high to low and also suggests some counter methods to overcome these threats. This measures the differences among the private and government educational institutions by the consideration of information like budget, expertise in order to provide security to their web applications.

Vulnerabilities present in web application

Now, we will discuss the various vulnerabilities present in the websites and also how we can prevent them.

These vulnerabilities affect the web servers, application servers and web applications. These vulnerabilities are also referred as application security risks.

Application Security risk is a risk involving attackers where attackers can use various illegal means to cause harm to the business and suppressing huge losses on the organisations. Attackers can potentially use various means through your application to do harm to your business or organization. It is represented as shown

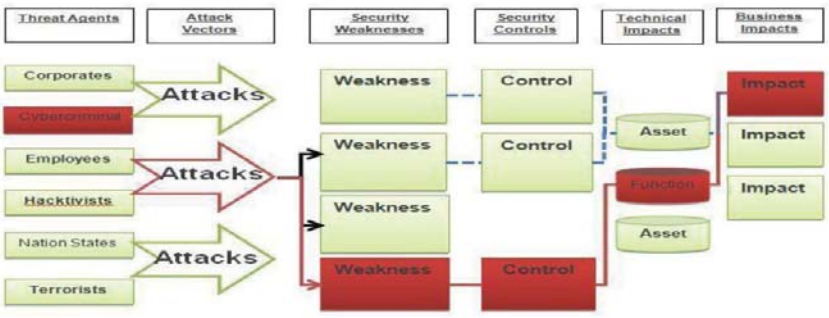

Fig. 1 Web Application

Un-Validated Input

The web application development is based on the client-server communication process where the server receives the request in the form of input which is processed through the web application from the client.

The web applications are unable to check the appropriateness of the input for the request. Due to this vulnerability, the attackers can take undue advantage by entering malicious information in the application, thus bypassing the security of the website.

Prevention and Security

- The parameters inputted have to be checked for their validity based on their data types, length of fields.
- The legality of the parameters is checked by patterns and values for presence of null values, duplicate values etc.

Improper Error Management

The attackers intentionally put errors inside the web application which are displayed in the form of error messages as output after the application is processed.

Prevention and Security

- The application should have the capability to display proper error message for informing the user.
- The error message should be restricted to sensitive user credentials (i.e. userid, password), Card Details etc.

III. WEB SECURITY IN ACADEMIA

The academic data continues to grow both in terms of volume and variety. In todays smart world it is crucial for all academic institutions to have a secure and informative web portal which can store large databases of students, professors which should have an authorised access. As we can see in figure3 depicts a real time example of an university web portal.

Unnecessary access makes the job of security professionals almost impossible because it introduces an uncontrollable number of security vulnerabilities. Such power is limited even for the system administrators and the principal themselves, due to the insider threat concerns.

Many security incidents results from a lack of visibility. It is the users' responsibility to notify IT staff before taking any security relevant actions.

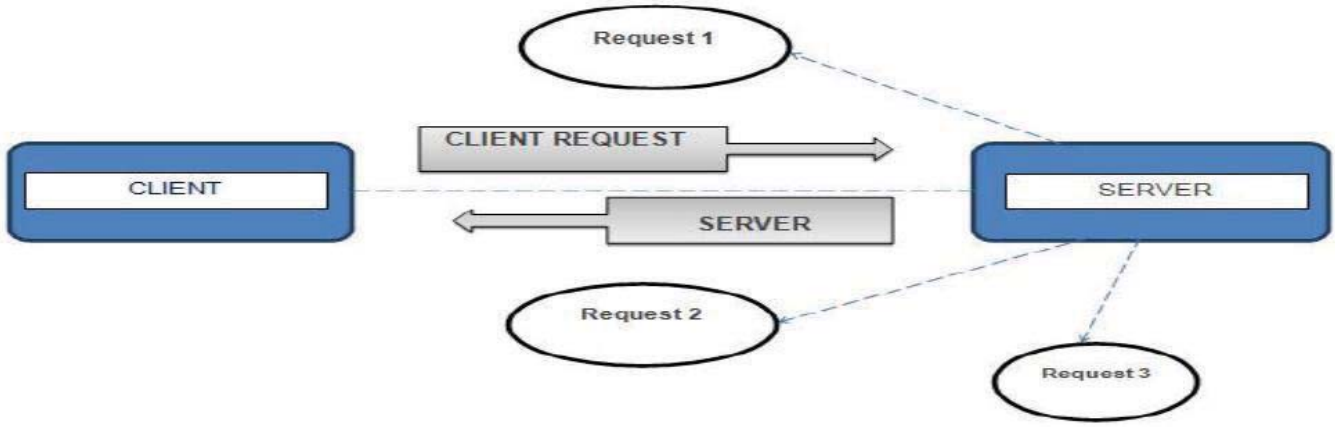

Fig. 2 Client Server Model

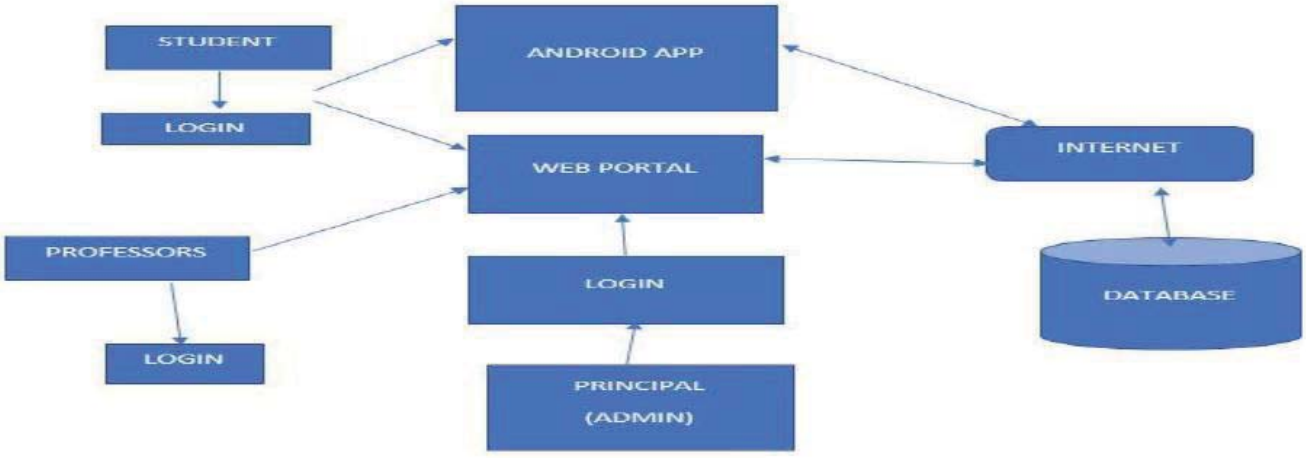

Fig. 3: Securities in Academics

Fig. 4: E-Commerce Securities

E-Commerce application security

There are many policies which provide security to e-commerce, one of them is to provide information based on authorization to the user. This can be explained using three variables<s r b>, this triplet specifies that user 's' is authorized to exercise privilege 'r' on
object 'b'. according to the reference [3] we see the actual working of E-commerce right from the buyer connecting a secured connection, retrieving the information of buyer, checking the product on a fraud free store, the items are then bought by the buyer using online payment gateways finally completing the whole transaction [6].

Database security

Data security is very difficult for most computer users and business. All the personal data related to the Client such as bank account, payment information. All of this information is very difficult to protect when it is accessed by attackers.

Securing Data

With amount of sensitive data available online increasing day by day, the need for ways to protect the same is increasing too. Following are a few ways of securing the web data:

1. Avoid creating database on the same server on which the application is installed as administrator accounts can easily be attacked.
2. The files and backup information should be stored in an encrypted format as plain text data can be easily decoded.
3. Database can be secured by implementing firewalls as the attackers can vandalise the websites by SQL injections.

Operating system security

Operating System security provides more securable environment to the enterprise level as compared to security provided by its tools. OS security authenticates and permits different applications and program enabling them to run various tasks and prevent unauthorised disturbances. Following are the common ways to secure operating system:

1. Security of the system begins with utmost careful and secure installation.
2. System Configuration to identify and counter, security needs by eliminating insignificant applications, services.
3. Software like intrusion detection system should be installed which integrate various mechanisms to identify and respond to attacks.

Security in mobile applications

Mobile application security evaluates the basic building block of mobile apps and its functioning. Its scope can include databases, configuration files and operating system. Some security evaluation methods are shown below:

1. Validation
2. Controlled Access
3. Session Monitoring
4. Encryption
5. Error Management
6. Data Security

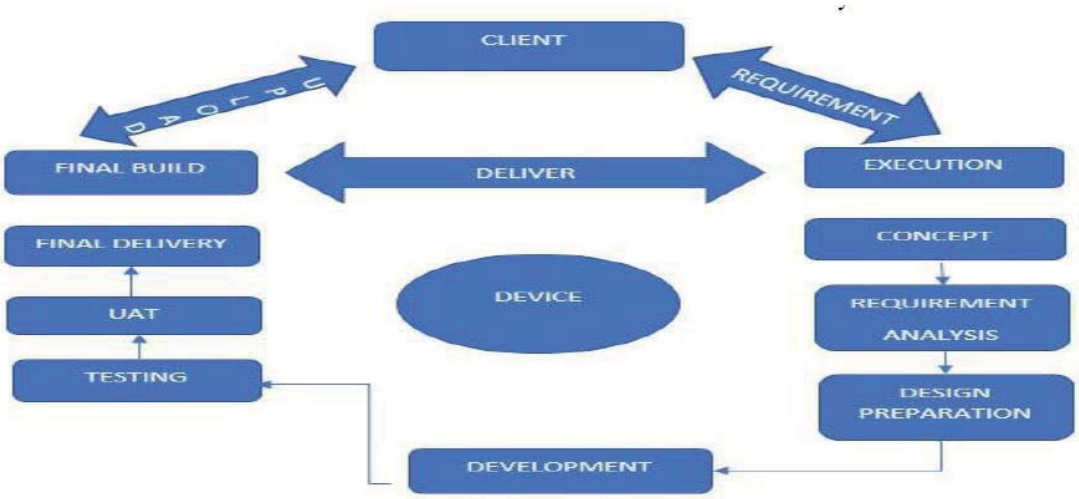

Fig. 5: Mobile Security

IV. CONCLUSION AND FUTURE DIRECTION

This paper provided a comprehensive knowledge of web application security and vulnerabilities present in it. It also covers various aspects of security models which are extensively used in the field of academics, e-commerce and present scenario of various tools like operating system, databases and mobile applications.

We propose that, the government along with promoting digitalisation should also focus on devising strict rules and regulation to protect against malicious attacks and frauds. In order to enforce these rules there have to proper punishments for the ones breaking them. Large companies have supported the cause of digitalisation by updating large databases online and also developed web and mobile applications for users to access these data and where users enter sensitive data. Thus, the companies also have their responsibility to ensure web security by employing the hackers in a good cause of identifying loopholes in the web applications and providing ways to rectify them.

Another proposal we want to give as per our observation is that as the demand of visual and catchy websites is increasing developers in order to save time and maintenance costs have consorted to use PHP, Html, CSS, Bootstrap, AJAX for developing websites. These are good platforms to develop user friendly websites but not for secure websites. This is the reason that the importance of basic OOP based languages such as JAVA never decreases. Thus the web applications which primarily deal with sensitive user credentials such as personal information, user id, passwords should be developed on more secured platform like JAVA rather than on less secured platforms. Web Security is one major thing which if provided properly will build the trust of users on online web applications and also influence more and more people using them with ease and comfort. Finding loopholes is like finding needle in a haystack, thus complete web security cannot be actually achieved but we can do our best to ensure web security and win the trust of users. As digitalisation is a very big step towards a bright, better and a fast paced future, Web Security is the prime requirement to achieve it.

REFERENCES

[1] A Jaiswal, G. Raj, D. Singh, "Security Testing of web applications and issues", International journal of computer applications, 2014.

[2] AXCENSION INC. "Mobile Application Development." *axcension.com.* 2013. http://www.axcension.com/mobile-applications.htm.

[3] B. Thuraisingham, C. Clifton, A. Gupta,"*Directions for Web and E-Commerce Applications Security",* Massachusetts, October 2002.

[4] Entersoft."MobileappSecurity."*entersoftsecurity.com.* 2018. https://entersoftsecurity.com/mobile-app-security.

[5] Katkar Anjali S., Kulkarni Raj B. "Web Security." *International Journal Of Innovative Research & Developement*, 2012.

[6] K. Singh, Vikas. "Analysis of Security Issues in Web Applications through Penetration Testing."*International Journal of Emerging Research in Management &Technology*, 2014.

[7] L. Desmet, M. Johns, "*Web ApplicationSecurity",* Seminar Report, Germany: Dagstuhl Publishing, 2012.

[8] Matelski, John. "5 Best Practices for Securing Databases." *Database trends and applications.* 25 March 2015. http://www.dbta.com/Editorial/News-Flashes/5-Best-Practices-for-Securing-Databases-101930.aspx.

[9] M. Al-Ibrahim, Y. Shams Al-Deen. "The Reality of Applying Security in Web Applications in Academia", *International Journal of Advanced Computer Science and Applications*, 2014.

[10] K.Naveen Durai, K.Priyadharsini. "A Survey on Security Properties and Web Application Scanner", *International Journal of Computer Science and Mobile Computing*, 2014.

[11] P. Mutchler, A. Doupe, J. Mitchell, C.Kruegel, G. Vigna. "A Large-Scale Study of Mobile Web App Security."

[12] P. De Ryck, L. Desmet, F. Piessens,"Improving the Security of Session Management inWeb Applications", Belgium: iMinds-DistriNet.

[13] S. Rafique, M. Humayun, Z. Gul, A. Abbas,

[14] H. Javed. "Systematic Review of Web Application Security Vulnerabilities Detection Methods."*Journal of Computer and Communications*, 2015.

[15] Samir,"ContentDeliveryBasics."*contentdeliverance.com,* May 2011, http://contentdeliverance.com/2011/client-server-architecture/.

[16] Scarpino, John J. "Web application security testing: an industry perspective on how its education is perceived." Pittsburg, 2010

[17] Shkoukani, H. Abusaimeh, "Survey of Web Application and Internet Security Threats", IJCSNS International Journal of Computer Science and Network Security, 2012.Techopedia Inc. "Operating System Security(OS Security)." techopedia.com. 2019. https://www.techopedia.com/definition/24774/oper ating-system-security-os-security.

[18] Threatpost.com/google-chrome-bug-opens-access-to-private-facebook-information/136573/.
"CURRENT SECURITY INFORMATIC", 2018. https://seguridadinformaticaactual.blogspot.com/20 17/11/owasp-publica-la-edicion-2017-%20de-su-top.html.

[19] Vina M. Lomte, Prof. D. R. Ingle, Prof. B. B.Meshram. "A Secure Web Application: E-Tracking System." International Journal of UbiComp, 2012.

[20] Xiaowei Li, Yuan Xue. "A Survey on Web Application Security.

[21] Arunima Jaiswal, Gaurav Raj,Dheerendra Singh. "Security Testing of Web Applications: Issues and." International Journal of Computer Applications, 2014.

[22] AXCENSION INC. "Mobile Application Development." axcension.c. 2013. http://www.axcension.com/mobile-applications.htm.

[23] Bhavani Thuraisingham, Chris Clifton, Amar Gupta, Elisa Bertino, Elena Ferrari. Directions for Web and E-Commerce Applications Security. Massachusetts, October 2002.

[24] Entersoft."MobileappSecurity."entersoftsecurity.com. 2018. https://entersoftsecurity.com/mobile-app-security.

[25] Katkar Anjali S., Kulkarni Raj B. "Web Security." International Journal Of Innovative Research & Developement, 2012.

[26] Khushal Singh, Vikas. "Analysis of Security Issues in Web Applications through Penetration Testing." International Journal of Emerging Research in Manement &Technology, 2014.

[27] Lieven Desmet, Martin Johns, Benjamin Livshits, Andrei Sabelfeld. Web Application Security. Seminar Report, Germany: Dagstuhl Publishing, 2012.

[28] Matelski, John. "5 Best Practices for Securing Databases." database trends and applications. 25 March 2015. http://www.dbta.com/Editorial/News-Flashes/5-Best-Practices-for-Securing-Databases-101930.aspx.

[29] Mohamed Al-Ibrahim, Yousef Shams Al- Deen. "The Reality of Applying Security in Web Applications in Academia." International Journal of Advanced Computer Science and Applications, 2014.

[30] Mr. K.Naveen Durai, K.Priyadharsini. "A Survey on Security Properties and Web Application Scanner." International Journal of Computer Science and Mobile Computing, 2014.

[31] Patrick Mutchler, Adam Doupe, John Mitchell, Chris Kruegel, Giovanni Vigna. "A Large-Scale Study of Mobile Web App Security."

[32] Philippe De Ryck, Lieven Desmet, Frank Piessens, Wouter Joosen. "Improving the Security of Session Management in Web Applications."Belgium: iMinds-DistriNet.

[33] Sajjad Rafique, Mamoona Humayun, Zartasha Gul, Ansar Abbas, Hasan Javed. "Systematic Review of Web Application Security Vulnerabilities Detection Methods." Journal of Computer and Communications, 2015.

[34] Samir."ContentDeliveryBasics."contentdeliverance.com. 8 May 2011. http://contentdeliverance.com/2011/client-server-architecture/.

[35] Scarpino, John J. "WEB APPLICATION SECURITY TESTING: AN INDUSTRY PERSPECTIVE ON HOW ITS EDUCATION IS PERCEIVED." Pittsburg, 2010.

[36] Shkoukani, Hesham Abusaimeh and Mohammad. "Survey of Web Application and Internet Security Threats." IJCSNS

International Journal of Computer Science and Network Security, 2012.
[37] Techopedia Inc. “Operating System Security (OS Security).” techopedia.com. 2019.https://www.techopedia.com/definition/24774 /operating-system-security-os-security.
[38] threatpost.com/google-chrome-bug-opens-access-to-private-facebook-information/136573/. “CURRENT SECURITY INFORMATIC .” 2018. https://seguridadinformaticaactual.blogspot.com/20 17/11/owasp-publica-la-edicion-2017-%20de-su-top.html.
[39] Vina M. Lomte, Prof. D. R. Ingle, Prof. B. B. Meshram. “A Secure Web Application: E-Tracking System.” International Journal of UbiComp, 2012.
[40] Madhusudan Chandok, Devendra Kumar, Upasana Sharma, Sandeep Mathur D-Crush: A Stronger Approach Towards Web Security”, Dec.2017, Volume No.-3, issue - 2 in International Journal of Software Computing and Testing,eISSN-2456-2351
[41] Devendra Kumar “Models and Techniques of Privacy Preserving Data Mining and its important aspects” June-2013, published in the International Journal of Advances Research in Computer Science ISSN No. 2026-6839, URL: http://www.ijictm.org/admin/html/mail/attach/2 013-07-30-08-44-29.pdf
[42] Devendra Kumar “Analytical Study on Privacy Preserving Data Mining Models and Techniques”, Volume-2, Issue-2, Year – 2012, published in the International Research Journal of Science Engineering and Technology, ISSN-2454-3195(O)
[43] Devendra Kumar, Ruchi Bhatnagar “Getting Better Security by Embedded RFID” Feb. 6, 2010, Published in the proceeding of International Conference on “Computing: Update and Trends
[44] Devendra Kumar “Study of Privacy Preserving Data Mining Techniques for Securing Web Services” 27-April, 2013, proceeding of National Conference on “Role of ICT in Inclusive Sustainable National Development
[45] Devendra Kumar,Himani Pandey,Cahnchal Bhardwaj,Akanksha Sharma “Analytical Study of Cloud Computing and its Services” 22-23 March, 2013, published in the proceeding of National Conference on Next Generation Computing and Information Security: ”Emerging Trends & Challenges
[46] Devendra Kumar, Upasana Sharma “Information Security Risk Assessment”Nov.-7, 2009 Published in the rocessing of National Conference on “Next Generation Technologies for Information & Management”