International Journal of Machine Intelligence
ISSN: 0975-2927 & E-ISSN: 0975-9166, Volume 6, Issue 3, 2015, pp.-466-468.
Available online at http://www.bioinfopublication.org/jouarchive.php?opt=&jouid=BPJ0000231

WEB SITE SECURITY EXTENSION AGAINST ATTACKS

GHODKE A.S.* AND SEN LAKHAN

Head of Department MCA, Sinhgad Institute of Business Administration & Computer Application (SIBACA), Savitribai Phule Pune University, Pune, 411007, Maharashtra
Sinhgad Institute of Business Administration & Computer Application (SIBACA), Savitribai Phule Pune University, Pune, 411007, Maharashtra
*Corresponding Author: Email- ghodke.a@gmail.com

Received: June 30, 2014; Revised: October 23, 2015; Accepted: October 25, 2015

Abstract- Internet is very popular and used all over the world. The use of internet is increasing day by day but it is not much secured. The things on the internet are not secured including a person and the system used for accessing the internet. The security services provide web security to vulnerable websites but still it is not possible to secure every website and the end user always has a risk from hack into their system or missing of their important data and information. In this research, paper we explain the client side security mechanisms in which how one web browser extension increases the security on the web and protect their user from the different types of attack is explained. This extension checks each and every request and response between web server and web client and if any malicious thing is found, it detect and block them and execute the other useful things.

Keywords- Vulnerability, Extension, Malicious script, Web site security

Citation: Ghodke A.S. and Sen Lakhan. (2015) Web Site Security Extension against Attacks. International Journal of Machine Intelligence, ISSN: 0975-2927 & E-ISSN: 0975-9166, Volume 6, Issue 3, pp.-466-468.

Introduction

The use of Internet is the most important need in today's life because everything is related to internet. By this the use of internet is also increased which increases the security risk and security issues. As we see in news the attacks of the hacker's will increase rapidly because of the vulnerability in the website. A security service provider always try to protect the website from the attacks and remove their vulnerability but it is not possible to protect each and every website from every type of attack's or make them that much strong because the development of the web application are commonly increased and the newbie of the website developed are not much aware about the security issues of the web application [1]. For this reason, the new concept is to increase the security on the web is to create a web security extension, which is installed on the internet web browser. The Internet web browser, arguably the most commonly used application on a network-connected computer, is becoming an increasingly capable and important platform for millions of today's computer users [6]. Browser extensions (or "add-ons") are facilities provided to customize the browser. These extensions make the use of interfaces exported by the browser and other plug-ins to alter the browser's behavior [3]. The function of this web browser security extension is to check every request and response between the client and the server and if any malicious script is found then it blocks them and skips to the next one. This web browser extension is smart enough to detect the difference between normal script and the malicious attacking script [12].

It is a new concept for providing security on the web sites in which provide security to each and every website instant its a secure extension which do not secure webpage but secure the user and system from the attacks of malicious websites[5].

This extension is updated continually according to the discourse of new vulnerability on internet.

Preceding effort

Web application security is a major concern in today's era for various organizations and banking sectors. Most of the organizations and banking sectors, which uses internet to provide web, based services so that they protect their sensitive data using firewalls and few access control mechanisms. However, still the organizations data are revealed by internet hackers by some means of purposefully designed java script [6]. No language can prevent insecure code, although there are language features, which could aid or hinder a security-conscious developer [8]. In such a scenario, it is necessary to provide additional protection mechanisms for securing the critical information that are retrieved by SQL queries or java script designed carefully by hackers [6].

Some previous work is done which is little similar to our concept is some web browser extension as follows:-

No Script security suite

HTTPS Everywhere

Hack Bar

SQL Inject me

No Script security suite: - Winner of the "PC World Class Award", this tool gives you with the best available protection on the web. It allows JavaScript, Java and other executable content to run only from trusted domains of your choice, e.g. your home-banking web site, guarding your "trust boundaries" against cross-site scripting attacks (XSS), cross-zone DNS rebinding/CSRF attacks (router hacking), and Click jacking attempts, thanks to its unique Clear Click technology. It also implements the Do Not Track tracking opt-out proposal with their security features there are some disadvantage also that are websites weren't loading or only loaded partially. Due to security reason, some java script code will be blocked and hence the website is not properly downloaded this useful extension become useless.

HTTPS Everywhere:- Many sites on the web offers some limited support for encryption over HTTPS, but make it difficult to use. For instance, they

may default to unencrypted HTTP, or fill encrypted pages with links that go .back to the unencrypted site. The HTTPS Everywhere extension fixes these problems by rewriting all requests to these sites to HTTPS.
This extension is used to restrict the all http request and allow only https request to be processed but this is not sufficient to protect the website from XSS and other attack.

Hack Bar: - This toolbar will help you in testing sql injections, XSS holes and site security. It is NOT a tool for executing standard exploits and it will NOT teach you how to hack a site. Its main purpose is to help a developer the security audits on his code. If you know what you're doing, this toolbar will help you do it faster. If you want to learn to find security holes, you can also use this toolbar. This extension is used only for developer and for pen tester to check security holes of web application. But it is not enough you will probably also need a book, and a lot of Google.

SQL Inject me:- SQL Inject Me is the Exploit-me tool used to test for SQL Injection vulnerabilities. SQL Injection vulnerabilities can cause a lot of damage to a web application. A malicious user can possibly view records, delete records, drop tables or gain access to your server. The tool works by submitting your HTML forms and substituting the form value with strings that are representative of an SQL Injection attack. The tool works by sending database escape strings through the form fields. It then looks for database error messages that are output into the rendered HTML of the page.
This extension is also for developer support. It is used to check the vulnerability of sql injection in the web site. It is not able to secure the end user at the use of web site from XSS and other attacks.

Objective

The main objective of this research paper is to highlight the new concept of web site protection by web browser extension [4]. This web browser extension is a type of tools which is added to the web browser as a plug-in which scan each and every web site which is run in that particular web browser. This extension reduces the burden from web developer to provide security to their web applications. This extension is smart enough to detect the vulnerability in any web site and catch any malicious request and response between client and server.
As we describe earlier about previous extension [14] that are not able to difference between normal java script and the malicious java script and it block every java script that is the result web page are not completely loaded but this new extension overcome from that drawback to the main objective of this extension is to create a security extension wall which protect the web site and the client from the cross site scripting (XSS) and other similar types of attack.

Theoretical Revision

In the world of web or internet, static and dynamic web site is developed to interact and provide services and information to the end user. This web site works on request and response between client and the server [7]. So there is establishment of flow between both of them [13] and the attacker will always find the loophole in that flow and then intercept or interact in that flow to attack on that website. We describe both the normal flow and the interpreted flow.

Normal flow of web site: - In general, the work of any web site depends on the request from the user to the server and the response from the server on that request. When the server receives the request from the user it executes that and fetches the data from the database according to the user request and then send it back to the user. It is a normal flow of website work. We describe it clearly by their diagram in [Fig-1].

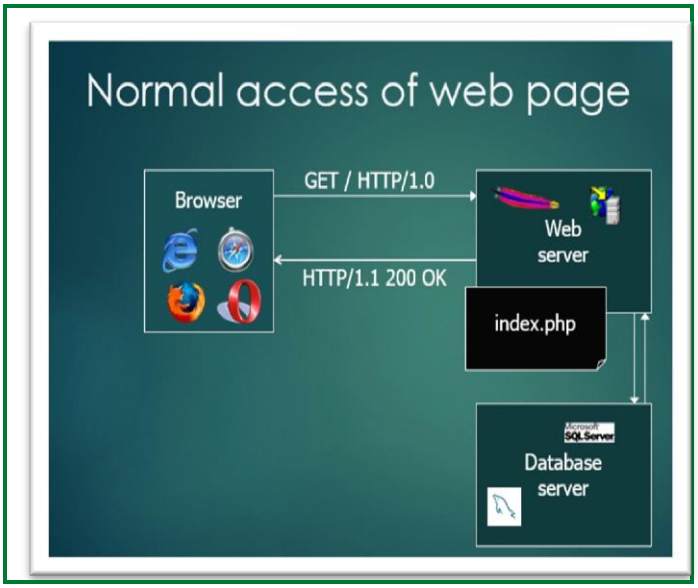

Fig. 1- An example of the normal flow of web site

Web site is basically work on the three layer, first is application layer which is the top most layer then second is logical layer which are middle layer and last third is database layer it is the last layer of that architecture. As we discuss about the working of web site and their flow, the web browser is work on the application layer then this browser sends a request to the web server which work on the logical layer. On that layer it work for executing the command provided and then execute that command logically and at last it fetch data from the database. Database works on the data layer and its function is to store data in required format and provide to the upper layer according to the requirement.

Loophole in web site: - Web applications do raise a number of security concerns stemming from improper coding. Serious weaknesses or vulnerabilities, allow hackers to gain direct and public access to databases in order to churn sensitive data. Attacker always find vulnerability or a loop hole in the web application or web server and then force fully inject there malicious code to that web site and save them[14]. So when any victim visit to that web site then that malicious code will be downloaded to that victim's computer and execute their web browser without any knowledge of the victim. We can describe it with the help of diagram as mention in [Fig-2].

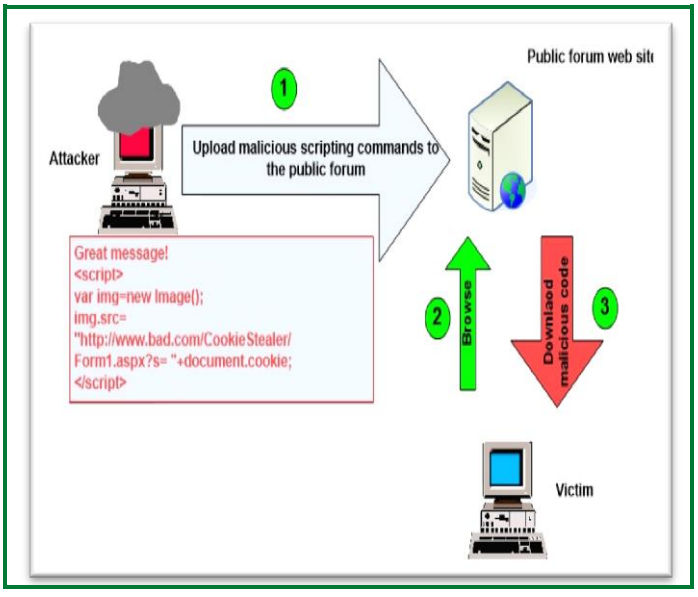

Fig. 2- Example of vulnerability exploitation in web site

As we mention in the diagram an attacker can find a vulnerability in the web server so attacker can inject a malicious script behind any attractive advertisement so when any victim user go through that web server and click on that advertisement then that malicious script will downloaded to that victim's computer and it is run by their web browser with the knowledge of the Victim and then attacker is able to do whatever he want to do with that system [11].

Extension for web security

In all the previous research all attention has been given on the vulnerable code of the web application that means where the loop hole is present on the web application and how to protect this loop hole or a vulnerability of the web application. But the web application developer will not been aware of each and every security concept of the web application at every level. As web attacks are increased in very far manner and now web security is not just a part of web application development. These both are different and much extensive fields. So we develop one smart extension which works a security wall in web browser.

As we know that web browser extension is used to extend the feature of the web browser so we develop one new extension with the security point of view by which the security of the web site and their client will increase. This extension will be installed in the web browser and scan each and every web site before downloaded it to the system. It also scan every request and responses between the client and the server and if it find any malicious script or data are come from outside then it block that [8]. This extension is smart enough to differentiate between the normal web page script and any other malicious script, and block only malicious script before downloading on the system.

When attacker try to attach any victim he sends a malicious link to the victim or store malicious script to the web server and target the victim to hack into their system but when the victim go through that web server or link so at the time of downloading the page on victim system this extension catch that malicious code and block them. That extension is that much smart that it protect the user from XSS and other similar types of attacks [9]. The development of this extension is the newly concept to protect the user from cyber-attacks [10]. This extension also reduces the security providing efforts of the web developer. This extension is able to detect all the previous vulnerability, which was discovered previously, and the newly discovered vulnerability will be added to their update version by which it is automatically updated when the new vulnerability will be discovered and added to this extension by which this extension is able to provide better security to the end user.

Conclusion

As we see in our today cyber world that the number of net or web user will be increasing rapidly and the use of the web site will also be increased so the users will trust on the web site and do there transaction by this web site so the risk will also be increased for which company spend their lots of money to secure their web sites.

This research paper gives a new way to provide security to the end user of the cyber world and protect them from the cyber attacks. The main purpose of our research paper is to develop the most secure extension and install it to our web browser. This extension work acts as a middleman between the client and the web server. It protects the client from the different types of web attack. Its a simple, easy and effective way to protect the user in the cyber world from different types of attacks.

References

[1] Jonathan R. Mayer (2009) *Any person…a pamphleteer":Internet Anonymity in the Age of Web 2.0. PhD thesis, Princeton University*.

[2] Clark D.D. and Wilson D.R. (1987) *In: IEEE Symposium on Security and Privacy*, 184-194.

[3] Douceur J.R., Elson J., Howell J., Lorch J.R. (2008) *In Proceedings of Operating Systems Design and Implementation (OSDI)*.

[4] Reis C. and Gribble S.D. (2009) *Proceeding EuroSys '09 Proceedings of the 4th ACM European conference on Computer systems, 219-232, ISBN: 978-1-60558-482-9, doi: 10.1145/1519065.1519090*.

[5] Saint-Jean F., Johnson A., Boneh D. and Feigen Baum J. (2007) *In Proc. of the 6th ACM Workshop on Privacy in the Electronic Society (WPES)*.

[6] Hallaraker O. and Vigna G. (2005) *In Proceedings of the IEEE International Conference on Engineering of Complex Computer Systems(ICECCS), Shanghai, China, 85–94*.

[7] Reis C., Dunagan J., Wang H., Dubrovsky O. and Esmeir S. (2006) *In Proceedings of The 7th USENIX Symposium on Operating Systems Design and Implementation (OSDI-2006)*.

[8] Grier C., Tang S., King S.T. (2008) *In Proceedings SP '08 Proceedings of the 2008 IEEE Symposium on Security and Privacy, 402-416, ISBN:978-0-7695-3168-7, doi: 10.1109/SP.2008.19*.

[9] Vogt P., Nentwich F., Jovanovic N., Kirda E., Kruegel C. and Vigna G. (2007) *Cross site scripting prevention with dynamic data tainting and static analysis. In Network and Distributed System Security Symposium (NDSS), San Diego*.

[10] Jackson Collin, Barth Adam, Bortz Andrew, Shao Weidong, and Boneh Dan (2007) *Proceeding CCS '07 Proceedings of the 14th ACM conference on Computer and communications security, 421-431, ISBN: 978-1-59593-703-2, doi:10.1145/1315245.1315298*.

[11] Takahashi H., Yasunaga K., Mambo M. and Kwangjo K. (2013) *IEEE Eighth Asia Joint Conference on Information Security (Asia JCIS),Seoul*, 85-89, DOI: 10.1109/ASIAJCIS.2013.20.

[12] Wahbe R., Lucco S., Anderson T., and Graham S. (1993) *Efficient software-based fault isolation.In Proceedings of the Symposium of Operating System Principles*.

[13] Ismail O., Etoh M., Kadobayashi Y. and Yamaguchi S. (2004) *Proceeding AINA '04 Proceedings of the 18th International Conference on Advanced Information Networking and Applications - Volume 2, 145, ISBN:0-7695-2051-0.*

[14] Shalini S., Usha S. (2011) *International Journal of Computer Science Issues (IJCSI) 8(4), 650-654.*.