ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

Design of a Security Framework andMulti-Language Implementation in PHP Web Applications

Kavin D[1] Sasireka K[2]

PG Student, Dept. of I.T, Muthayammal Engineering College, Rasipuram, Tamilnadu,India

Associate Professor, Dept. of C.S.E, Muthayammal Engineering College, Rasipuram, Tamilnadu,India

ABSTRACT: Nowadays websites are developed as basic needs of most of the people's life and it was needed by most of the business people to develop their business and every one need website for some special purpose. Anyone can learn anything from anywhere in websites using internet. By using this opportunities many self-learning peoples emerged in this world. They start their own business in internet online. From this, one of the fastest development businesses is web development. A web developer with his basic knowledge developing a web application without practicing security guidelines, improper validation of user inputs, and direct source code deployment in web server leads to various source code attacks and vulnerabilities. Several open source vulnerabilities & attack injector tools which automate the entire testing process are available in Github, Sourceforge to identify vulnerabilities in web applications. Web applications in sense of online, it is available in worldwide. Access at anywhere anytime by anyone and it is involved in companies, education, business, research etc. But the problem is language. Multi-Language implementation is required to solve this problem. In this paper we proposed a new security framework to identify and prevent attacks, user action time based session management technique to maintain session, cookies and other information related to web pages and implementation of multi-language independency framework which helps to implement multi-language in PHP web applications.

KEYWORDS: Web security framework, Multi-language, Injection, Attacks prevention, Vulnerabilities.

I. INTRODUCTION

Nowadays website plays a vital role in everybody's life. Banking, Education, Shopping etc., most of the industry switching to online to market and develop their business. There are many web developers and web development companies are available to develop their website. To develop a secured website the developer must understand background logic and process of websites. The Hypertext Transfer Protocol (HTTP) is an application-level protocol for distributed, collaborative, hypermedia information systems. This is the foundation for data communication for the World Wide Web (i.e. internet) since 1990. HTTP is a generic and stateless protocol which can be used for other purposes as well using extensions of its request methods, error codes, and headers. Basically, HTTP is a TCP/IP based communication protocol, that is used to deliver data (HTML files, image files, query results, etc.) on the World Wide Web. It provides a standardized way for computers to communicate with each other. HTTP specification specifies how clients' request data will be constructed and sent to the server, and how the servers respond to these requests. The HTTP protocol is a request/response protocol based on the client/server based architecture where web browsers, robots and search engines, etc. act like HTTP clients, and the Web server acts as a server. The HTTP client sends a request to the server in the form of a request method, URI, and protocol version, followed by a MIME-like message containing request modifiers, client information, and possible body content over a TCP/IP connection. The HTTP server responds with a status line, including the message's protocol version and a success or error code, followed by a MIME-like message containing server information, entity Meta information, and possible entity-body content.

II. RELATED WORK

Nowadays there is an increasing dependency on web applications, ranging from individuals to large organizations. Almost everything is stored, available or traded on the web. Web applications can be personal websites, blogs, news,

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

social networks, web mails, bank agencies, forums, e-commerce applications, etc. [1].There are several emerging technologies was used by the people in daily life. One of the fastest emerging technology is the web development. There are many new freelancers are available in internet to do the several web projects. Web security is most essential for banking and e-commerce web applications. Most of the information systems and business applications built nowadays have a web front end and they need to be universally available to clients, employees, and partners around the world, as the digital economy is becoming more and more prevalent in the global economy. These web applications, which can be accessed from anywhere, become so widely exposed that any existing security vulnerability will most probably be uncovered and exploited by hackers [2].Regarding the programming language perspective, we considered some of the most relevant in the context of web applications. First, we focused on the most widely used weak typed language, PHP. Then, we analyzed strong typed languages, namely Java, C#, and VB. Recall that our goal is not to analyses each programming language in what concerns their ability to prevent security vulnerabilities, but to analyze the vulnerabilities and their relation with some language characteristics, like the type system [2].Web services are a key element in service oriented architectures (SOA) and consist of standard-based self-describing components that can be used by other software across the web in a platform- independent manner. This makes web services the lingua franca for systems integration. Web services are so widely exposed that any security vulnerability will most probably be uncovered and exploited by hackers [3].Various techniques are used to perform phising attacks, ranging from technical subterfuges (DNS cache poisoning, e-mail spoofing, Web server takeover, etc.) to social engineering. In addition various goals are sought: data, money or credential stealing through fake Web sites, drive-by download of malware, etc. Despite this diversity, one common feature is the use of obfuscated URLs to misdirect users to fake Web sites or drive-by downloads [4].Distributed denial of service (DDoS) attacks have been a continuous critical threat to the Internet since ten years ago. Their implementation keeps on evolving and becomes more subtle. Anew attack pattern that utilizes the edge servers of content delivery networks (CDNs) to launch DDoS attacks to the Web servers was introduced [5].The Web proxy-based HTTP attack is more flexible and covert than most of existing DDoS attacks.

The difficulty of detection lies in three aspects: (i) real attacking hosts are unobservable to the origin server since they are shielded by the hierarchical Web proxies; (ii) a Web proxy may be passively involved in an attack event and may unconsciously act as an attacker; (iii) observed from the victim server, both legal and illegal traffic comes from the same sources (i.e., Web proxies) [5].Security Testing is related to verify the application security services and to identify potential safety defects. A complete WEB safety testing should cover deployment, infrastructure, input validation, authentication, authorization, configuration management, sensitive data, encryption, session management, operating parameters, exception management, auditing and logging, and several other aspects [7].There are many ways to protect a web application, such as implementing a secure coding practice, managing secure configuration, performing vulnerability assessment and deploying a web application firewall, but there is no silver bullet that it will protect the application entirely. Web applications need a defense-in-depth approach to avoid and mitigate security vulnerabilities. This approach assumes that every security precaution can fail, so security depends on having several layers of mechanisms that cover the failures of each other [9].Penetration testing and static code analysis may be used to assess the vulnerabilities of web applications. Penetration testing is a method of security testing through the simulation of an attack. Static code analysis, also known as source code analysis is a code review process that examines the software's source code for common coding errors and defects without execution [10].“A security threat has been known as a situation, or event with the potential to effect economic adversity to data or network resources in the form of destruction, disclosure, modification of data, denial of service, and/or fraud, waste, and abuse Security, then, is the protection against these threats”[9].A large numbers of developers start to use the Ajax technology to develop web applications. By using this technology, the web application can own a more elegant user interface to offer the more fluent service for the user. Ajax is a short term of 'Asynchronous JavaScript and XML', which can send asynchronous requests to the server and handler the response in the background without reloading the client page. Instead, the current Document Object Model is modified directly by client-side code and produces the next client state.

This is not only a technical difference for web-based application development, in fact, a very deep impact on the way of automatically testing the web applications. It is not anymore one URL represent one state of client side. The current DOM can be modify by the JavaScript code in client side without interact with the remote server. Many popular websites, such as twitter and Facebook are based on asynchronous server communications after the first page, meaning that the entire application has a single URL [10].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

III. PROPOSED ALGORITHM

A. *Design Considerations:*

- Prevent SQLi injection, XSS- XSRF/CSRF and other attacks
- Authentication and Authorization bypass prevention(same user role)
- Safe Sessions and Cookies management Techniques
- Support to crawl all pages(HTML results)
- Language independency implementation
- Performance and statics of vulnerabilities prevention

B. *Description of the Proposed Algorithm:*

Aim The browser communicated with a name server to translate the server name "www.domainname.com" into an IP Address, which it uses to connect to the server machine. The browser then formed a connection to the server at that IP address on port 80.The Internet is a gigantic collection of millions of computers, all linked together on a computer network. The network allows all of the computers to communicate with one another. A home computer may be linked to the Internet using a phone-line modem, DSL or cable modem that talks to an Internet service provider (ISP). A computer in a business or university will usually have a network interface card (NIC) that directly connects it to a local area network (LAN) inside the business. The operation of a DNS is never really seen or known of, since they work in the background. When you enter a domain name like www.google.com into your browser (Internet Explorer, Firefox, Google Chrome, Etc.) that Domain Name is first sent to a DNS, the DNS will then tell your Browser the actually IP address for that Domain Name.

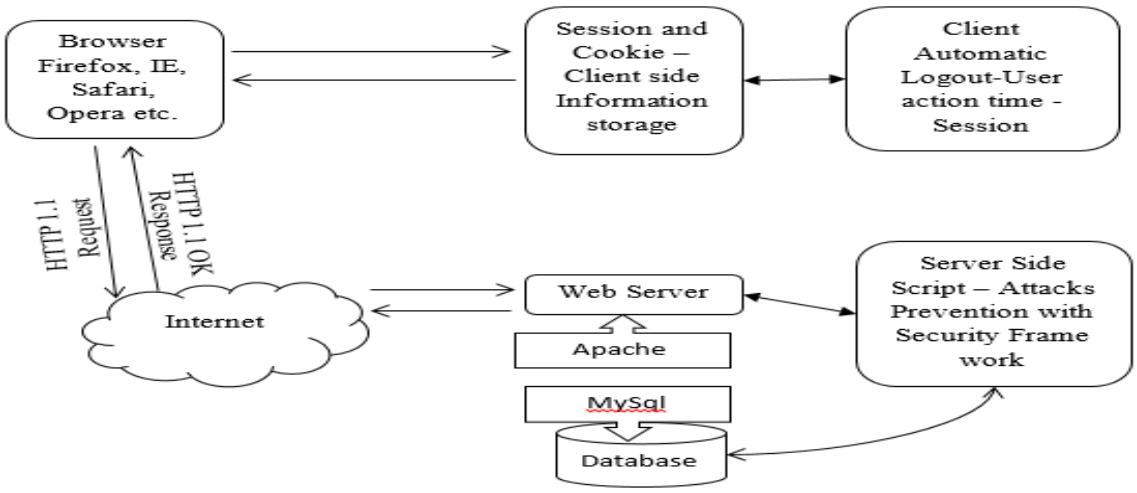

Fig.1 Data Flow Diagram

In general, all of the machines on the Internet can be categorized as two types: servers and clients. Those machines that provide services (like Web servers or FTP servers) to other machines are servers. And the machines that are used to connect to those services are clients. When you connect to Yahoo! at www.yahoo.com to read a page, Yahoo! is providing a machine (probably a cluster of very large machines), for use on the Internet, to service your request. Yahoo! is providing a server. Your machine, on the other hand, is probably providing no services to anyone else on the Internet(fig.1). Therefore, it is a user machine, also known as a client. It is possible and common for a machine to be both a server and a client, but for our purposes here you can think of most machines as one or the other.A server machine may provide one or more services on the Internet. For example, a server machine might have software running on it that allows it to act as a Web server, an e-mail server and an FTP server. Clients that come to a server machine do so with a specific intent, so clients direct their requests to a specific software server running on the overall server machine. For example, if you are running a Web browser on our machine, it will most likely want to

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

talk to the Web server on the server machine. Telnet application will want to talk to the Telnet server, your e-mail application will talk to the e-mail server, and so on.Every machine on the Internet has a unique IP address(fig.2). A server has a static IP address that does not change very often. A home machine that is dialing up through a modem often has an IP address that is assigned by the ISP when the machine dials in. That IP address is unique for that session -- it may be different the next time the machine dials in. This way, an ISP only needs one IP address for each modem it supports, rather than for each customer.

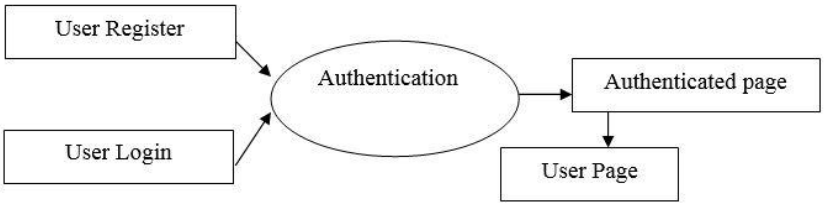

Fig.2. Basic Authentication

Once a client has connected to a service on a particular port, it accesses the service using a specific protocol. The protocol is the pre-defined way that someone who wants to use a service talks with that service. The "someone" could be a person, but more often it is a computer program like a Web browser. Protocols are often text, and simply describe how the client and server will have their conversation.Most servers add some level of security to the serving process. For example, if you have ever gone to a Web page and had the browser pop up a dialog box asking for your name and password, you have encountered a password-protected page. The server lets the owner of the page maintain a list of names and passwords for those people who are allowed to access the page; the server lets only those people who know the proper password see the page. More advanced servers add further security to allow an encrypted connection between server and browser, so that sensitive information like credit card numbers can be sent on the Internet.

IV. SYSTEM ORGANIZATION

The main focus of the framework is to be secure. Several techniques have been used to prevent attacks like SQL injection, Cross-Site Scripting and Cross-Site Request Forgery. The framework also takes care of authenticating users. Aims at to be secure, fast and easy to use. It uses the Model-View-Control architecture with XSLT for the View. Although it was designed to use MySQL as the database, other database applications can be used as well with only little effort.The controller and model are both optional.A typical Banshee root directory consists mainly of directories. Below, you find a list of typical Banshee directories and their purpose.

- Controllers: contains the controller PHP scripts.
- Database: contains database operation scripts and a MySQL database dump used to initialize the MySQL database.
- Extra: all extra files needed for the website.
- Libraries: contains all the phpSecured libraries and database drivers.
- Logfiles: contains phpSecured logfiles and can also be used to store the webserver logfiles.
- Models: contains the model PHP scripts.
- Public: the webroot directory. Contains all the files which can be requested directly via a browser, like images, javascripts and CSS files.
- Settings: contains configurations files for phpSecured framework.
- Templates: contains template files (PHP scripts and XSLT sheets), which can be used for new pages.
- Views: contains XSLT sheets, which are used as the view.

A. *Multi-language Implementation*

Methodology Types:Create a couple of files that will contain the text for each of the languages that will be supported by the website. Make a directory named “directory”. In this directory create 3 files: lang.de.php, lang.en.php, and lang.es.php. In our main file (index.php) we will include a file (common.php) containing a piece of

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

code that gets the requested language. The content of the languages are entered by language professionals. Framework an usage:By determine the value of $lang, we use switch() to compare its value with some different values, and execute a different piece of code depending on which value it equals to. After the value of the $lang_file is determined, the script will include the necessary language file. As we can see I have used sessions to register the value of $lang. This way users can navigate through the whole site and see the content in the chosen language (lang=[language here] does not need to be passed in every URL). Additionally, I have used cookies to store the selected language in user's computer for 30 days. When the visitor will come back he will see the site in the language that he previously selected.

V. RESULTS AND DISCUSSIONS

We analyzed, one by one, each vulnerability injected that was not successfully attacked, in order to understand the reason why the attack was not successful. In five situations, belonging to the edit_authors.php file of the MyReferences web application the vulnerability was injected by removing an intval PHP function. By removing this function it is expected that the variable could be attacked injecting string values, such as "or 1 ¼ 1". However, the affected variables are used inside strings formatted with the %d format which also filters non-numeric variables. Therefore, this string formatting gives another level of protection preventing the attack to succeed through the supposedly vulnerable variable. In these situations, when the tool injects one vulnerability (by removing the code responsible for the sanitation of the variable) it leaves the other pieces of code still preventing the variable from being exploited which is described in table 1. Recall that only a single vulnerability is injected at a time (even when multiple vulnerabilities can be injected in the same file). The reason is that we have no field study data supporting the realistic injection of more than one vulnerability at the same time.

Web apps	Files attacked	Vuln. injected	Total attacks	Successful attacks	Attacks detected by the IDS	IDS false positives
TikiWiki	tiki-editpage.php	3	84	34	34	49
	tiki-index.php	1	7	6	6	1
	tiki-login.php	3	21	0	0	21
	Total	7	112	40	40 (100%)	71 (99%)
phpBB	search.php	3	42	42	42	0
	login.php	1	21	21	21	0
	viewforum.php	1	7	7	7	0
	viewtopic.php	5	84	84	84	0
	posting.php	4	112	112	112	0
	Total	14	266	266	266 (100%)	0 (0%)
MyRefs	edit_paper.php	27	525	61	61	294
	edit_authors.php	6	196	46	41	28
	Total	33	721	107	102 (95%)	322 (52%)
	Grand total	**54**	**1099**	**413**	**408 (99%)**	**393 (57%)**

Table.1 Evaluation Results of the IDS

VI. CONCLUSION AND FUTURE WORK

All the security modules are describes the workflow logics to avoid attacks in web application. It solves most of the basic attacks like SQL injection through password field, safe session management etc., Even though the security

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

framework helps to prevent several attacks, hackers or attackers find new types of attacks in daily life. To handle those things every programmer must update his/her knowledge regularly. The developmental framework is efficient till next versions of attacks logs and outcomes. The php security frameworks have to be updated based on new attacks and preventions. The multiple language implementations help worldwide clients to understand web contents quickly and easily. But the problem is every update of the web content needs to update in all language files. Simulation results showed that the proposed algorithm performs better with the total transmission energy metric than the maximum number of hops metric. The proposed algorithm provides energy efficient path for data transmission and maximizes the lifetime of entire network.As the performance of the proposed algorithm is analyzed between two metrics in future with some modifications in design considerations the performance of the proposed algorithm can be compared with other energy efficient algorithm. We have used very small network of 5 nodes, as number of nodes increases the complexity will increase. We can increase the number of nodes and analyze the performance.

REFERENCES

1. Jose Fonseca, Marco Vieira, and Henrique Madeira," Evaluation of Web Security Mechanisms Using Vulnerability & Attack Injection", IEEE Transactions On Dependable And Secure Computing, Vol. 11, No. 5,October 2014
2. Jose Fonseca, Nuno Seixas, Marco Vieira, and Henrique Madeira," Analysis of Field Data on Web Security Vulnerabilities", IEEE Transactions On Dependable And Secure Computing, Vol. 11, No. 2, March/April 2014
3. Nuno Antunes, Marco Vieira," Assessing and Comparing Vulnerability Detection Tools for Web Services: Benchmarking Approach and Examples", IEEE Transactions On Services Computing, Vol. 8, No. 2, March/April 2015
4. Samuel Marchal, Jérôme François, Radu State, and Thomas Engel," PhishStorm: Detecting Phishing With Streaming Analytics", IEEE Transactions On Network And Service Management, Vol. 11, No. 4, December 2014
5. Yi Xie, S. Tang, Y. Xiang and J. Hu," Resisting Web Proxy-based HTTP Attacks by Temporal and Spatial Locality Behavior", IEEE Transactions On Parallel And Distributed Systems, Vol. 6, No. 1, January 2007
6. Li Qian, Jiahua Wan, Lu Chen, Xiuming Chen," Complete Web Security Testing Methods and Recommendations", 2013 International Conference on Computer Sciences and Applications
7. Jean Arlat, Member, Yves Crouzet, Jean-Claude Laprie, and David Powell," Fault Injection and Dependability Evaluation of Fault-Tolerant Systems", IEEE Transactions On Computers, Vol. 42, No. 8, August 1993
8. Anna Thankachan, R. Ramakrishnan, M.Kalaiarasi," A Survey and Vital Analysis of Various State of the Art Solutions for Web Application Security", ICICES2014 - S.A.Engineering College, Chennai, Tamil Nadu, India
9. LaShanda Dukes, Xiaohong Yuan, Francis Akowuah," A Case Study on Web Application Security Testing with Tools and Manual Testing", IEEE Transactions On Parallel And Distributed Systems, Vol. 6, No. 1, January 2007
10. Hatoon Matbouli, Qigang Gao," An Overview on Web Security Threats and Impact to E-Commerce Success", IEEE Transactions On Parallel And Distributed Systems, Vol. 8, No. 1, January 2012