INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN: 2278 – 0211 (Online)

Web Security

Katkar Anjali S.
M.E.(Pursuing) in computer science and engineering
walchand institute of technology, Sholapur, India
Kulkarni Raj B.
PhD in computer science
Assistance professor in Walchand Institute of technology,solapur, Maharastra, India

Abstract: *The growth in web applications has reached to a large extends, less trusted user and more vulnerable attacks. Code reviews, penetration testing, and intrusion detection systems are just a few ways that organizations are using to control growing attacks and by applying SSL, firewall, vulnerability scanner, periodic assessment, anti-virus, skilled web developers will not solve the web application security problems. So security mechanism has developed to provide solution for the growing problem of web application vulnerabilities.*

The research areas of this paper focused on the commonly reported security vulnerability in the web applications. Un-validated Input, Improper Error Handling, Parameter Modification and Directory Traversal have been the most popular web vulnerabilities. Further, the research includes methods for identifying the vulnerabilities and then providing security techniques to protect web application from those vulnerabilities.

Securing the websites against the web vulnerabilities is challenge. The result shows the security mechanisms for the web applicationvulnerabilities. So the study of web vulnerabilities, identifying the vulnerable attacks and providing security for the same.

Key words: *Security, Vulnerability detection and Web applications.*

1.Introduction

Security is the main problem for web application as all types of user access the website and may try to harm the web services. Different types of securing techniques are used to save the website from the attacks or vulnerability, is referred as the web security.

The most popular vulnerability to web application areUn-validated Input, Improper Error Handling, Parameter Modification and Directory Traversal.The main objective of this paper is to point out the possible vulnerabilities in a content serving web application and propose suitable security techniques to protect the site from the attack and provide significant help to the developer of a web application. That is, help in reducing the potential security risk of running the web application.

Also we will assess the level of security expertise needed to gain benefit from these security technique.We developed a Blog website and demonstrate both secured and insecure version of the website. We demonstrate the attacks through Black box testing of each vulnerability.Our scope, however, is limited to security technique to vulnerability. Any performance issues are out of the scope of this paper.

2.**Literature Review**

According to Damjanovic, V., Djuric, D., In their paper "Functional Programming Way to Interact with Software Attacks and Vulnerabilities" proposed functional programming approach to detect and interact with the software attacks and vulnerabilities. Also explore Attack Tree, which provides methodology for analyzing the security. With software attacks and vulnerabilities of the security layer of the Wireless Application Protocol, and built on top of Magic Potion specification.

Vieira, M.; Antunes, N.; Madeira, H. in their article "Using web security scanners to detect vulnerabilities in web services" detailed studied on various available scanners in the market to scan the web application vulnerabilities and also compare their performance which will be suitable to apply on web services.

Johari, R.;Sharma, P., In the article "A Survey on Web Application Vulnerabilities (SQLIA, XSS) Exploitation and Security Engine for SQL Injection", main objective of this paper is only on the study of various types of Structured Query Language Injection attacks and Cross Site Scripting(CSS or XSS) vulnerabilities and their detection and security mechanisms. They proposed to future detail study on Structured Query Language Injection attacks.

According to Fonseca J., Vieira, M.; Madeira, H. "Testing and Comparing Web Vulnerability Scanning Tools for SQL Injection and XSS Attacks". On web application automatic vulnerability scanner are used to identify vulnerabilities present in the websites. Main focused of the paper is on study of XSS and SQL injection vulnerabilities, methods to detect and apply benchmark automatic scanners to detect software fault injection techniques.

After the review of various researches on web vulnerabilities and security, focused mainly on the survey, scanner, different tools, various tester and detectors of vulnerabilities but not emphases on the prevention techniques to protect against vulnerabilities. The objective of this paper is focused not only on the study of web application vulnerabilities such as Un-validated Input, Improper Error Handling, Parameter modification and directory traversal. But also the methods on how to find out the vulnerability flaws and provide security techniques to protect the web applications.

This research paper is useful for web application developers, testers , system administrators responsible for maintaining web applications, security professionals and for academics All those how need to secure their website.

The scope of this paper is limited to study the various vulnerabilities and the technic of detecting the vulnerability in web application and providing the protection according to their approach to web application. Thus, we will not test the performance of security on the web application. When possible, however, we will provide the security to help better understand their approach.

The paper is organized as follows. Section II discusses security vulnerabilities found in web applications and the methods for identifying vulnerabilities of web application and security technique for web application vulnerability. In section IIIrepresents the result analysis of the objective of research paper. In section IV we will draw our conclusions of the study of web vulnerabilities and security technique.

3.Vulnearabilities Found In Web Application

In this section we will discuss the various vulnerabilities found in websites even though these vulnerabilities have been commonly known. Web servers, application servers, and web application are affected to following types of vulnerabilities:

3.1.Un-validated Input

If web application do not check whether input from the user is appropriate for the requests. Ifattackers try to pass malicious information to the web application which bypass the website's security mechanisms.

3.1.1.Detection:

All user input that provided to the web applications requested, must be check against its proper format that exactly what input must be allowed. Ensure that all parameters are validated before they are used.

3.1.2.Security:

- The input parameters to the web application should be validated against specification such as use of data type, length of all fields,
- Also whether null, duplicates are allowed, parameter is required or not, numeric range.
- Check for the legal values and patterns.
- Run the inputs against a library and get to confirm that the information is valid.

3.2 Improper Error Handling

Attacker intentionally inputting errors to web application request to occur error message which may receive clues on flaws about the web application security.

3.2.1.Detection:

Error handling must be focused on each part of web application.Simple trial and error testing can determine how your site responds to various kinds of input errors.

3.2.2.Security:

- The web application should inform the user with proper error message.
- Restrict error messages on sensitive data as user id, password, credit card number etc.
- Do not provide specific information about the internal details or directory in error messages.
- Provide the user with diagnostic information (e.g., validation errors), instead of developer level debug information.

3.3.Parameter Modification

Parameter modification refers to web application how theattacker's do not fill the form but rather passes the parameters from URL itself, bypassing the form validations.

3.3.4.Detection:

In this vulnerability, ensure that application must not allow parameter values, query string or form GET parameters to the URL. These are handled through dynamic parameter detection.

3.3.5.Security:

- Do not allow user to provide the input parameter in the URL of the web application.
- Do not trust on the values of HTTP request to identify that the request originated from a page that is generated by Web application which creates vulnerabilities.

3.4.Directory Traversal

Directory Traversal attack is said when the attackers access files/directory or execute commands from restricted directories of web server. In this type of vulnerability attacker uses HTTP request to bypass Web server and Web application security.

3.4.1.Detection:

The best way to check whether web applications are vulnerable to Directory Traversal attacks is by using a Web Vulnerability Scanner.

3.4.2.Security:

- Do not allow attackers to access files from root directory by using the address bar of web browser.
- Administrators can maintain access control list.
- Install latest version of web server software.
- Web applications should filter and validate all inputs i.e. only safe inputs are passed to the Web server.

4.Result Analysis

4.1.Un-validated Input

Any input web applications accept must be checked against a format that specifies exactly what input will be allowed. In application we provide both the client and server side validation. (Fig1)

Figure 1: Un-validated Input

4.2.Parameter Modification

In this vulnerability, attacker tries to pass parameter in the URL of web application such as "http://...../LoginPage.aspx?username=abc&password=abc1234"

Which do not allow attacker to login and redirect the attacker to custom error page. (Fig2 and Fig 3)

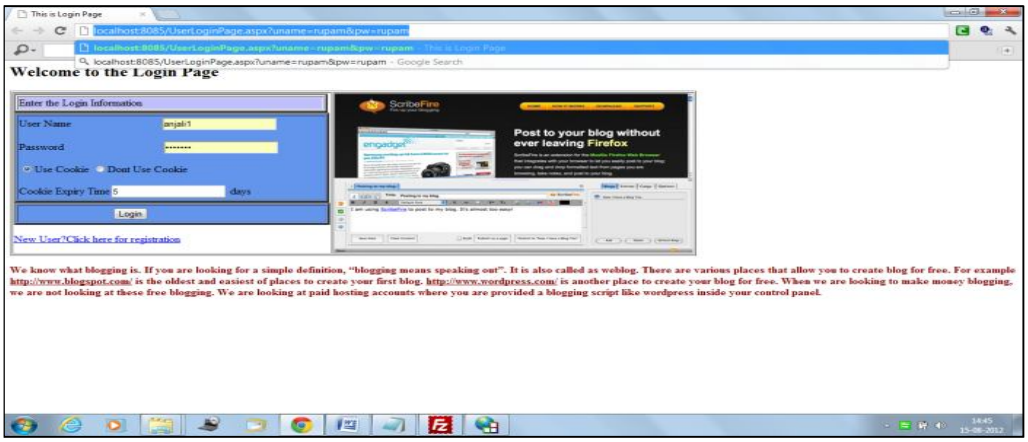

Figure 2: Parameter Modification

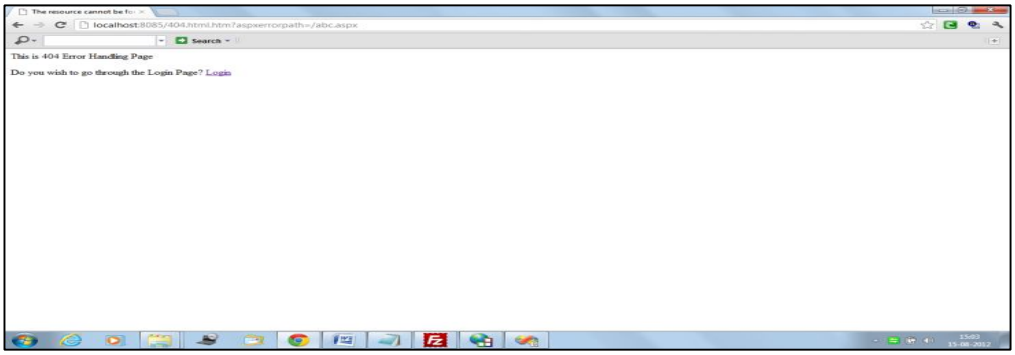

Figure 3: Parameter Modification (Custom Error page is displayed)

4.3.Improper Error Handling:

When errors occur, the site should respond with a specific designed result and do not provide clue or unnecessary internal details to the user. So if attacker pass the non-existent URL, instead of displaying browser error message such as "File Not Exist" information it will redirect to custom error page.

(Fig 4 and Fig 5)

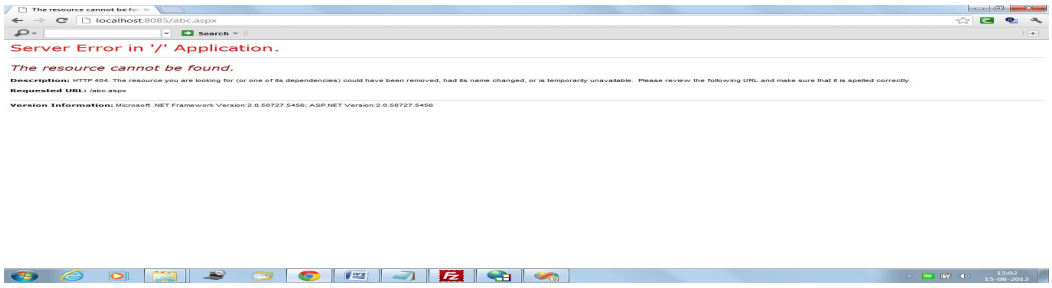

Figure 4: Improper Error Handling

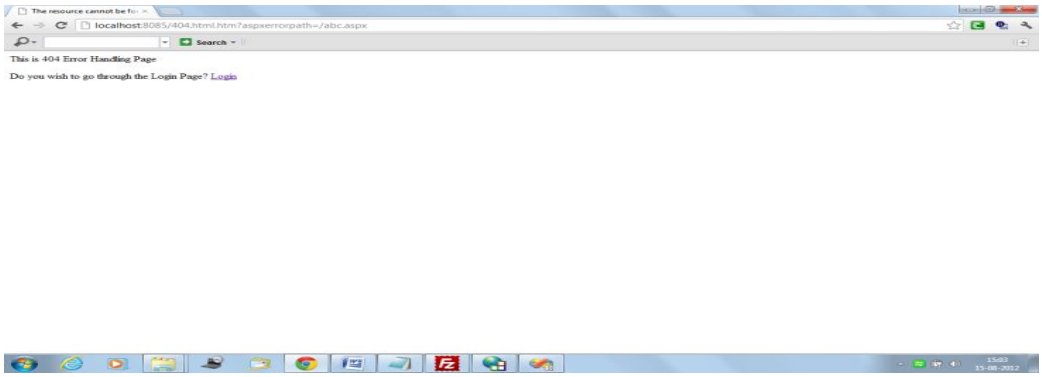

Figure 5: Improper Error Handling (Custom Error page is displayed)

4.4.Directory Traversal

Web application must restrict the access to files and directories of root directory.If hackers try to pass the URL ashttp://...../BlogArticles, (For Example “Blog Articles” is name of root directory) it will not enlist the files or directory of root directory. Which donot allow viewing or executingcommands offiles from root directory. (Fig 6)

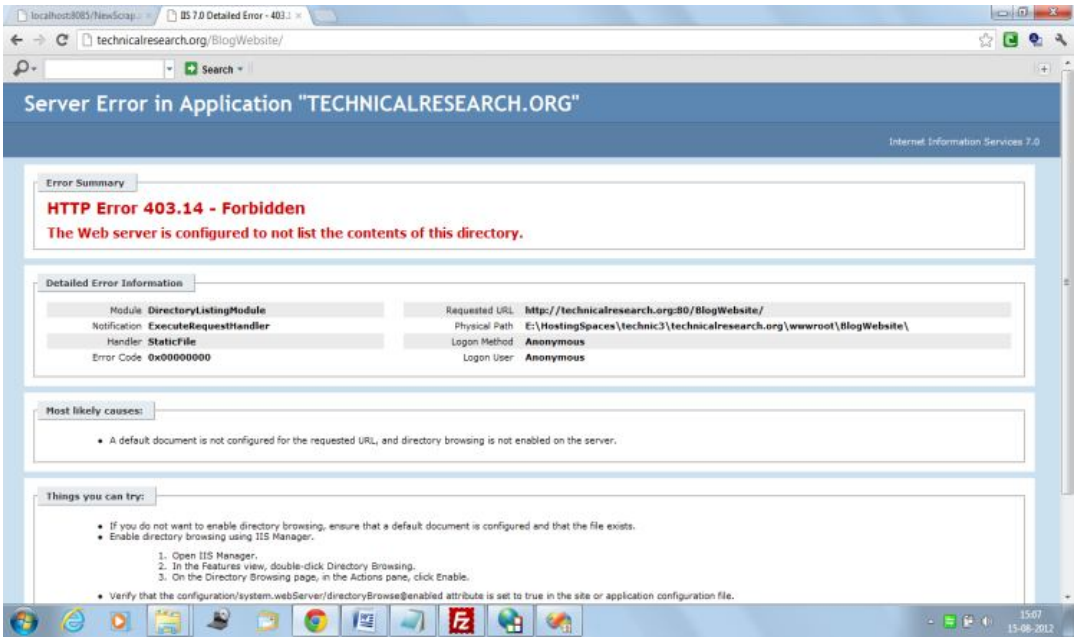

Figure 6: Directory Traversal

5.Conclusion

The internet and web becoming vulnerable as the advanced in technologies and skills are implemented for wrong reasons by attacking in advance and complex technique .So the solution has to provide for the various types of web vulnerabilities. These issues are popular irrespective types of websites it is.

Hence we presented a technique for web vulnerabilities through live secured and insecure websiteand prove that simple configuration and code library changes can ensure secured website. We studied web vulnerabilities like un-validated input, Improper Error Handling, Parameter Modification and Directory Traversal, methods for identify those vulnerabilities and successfully implemented security mechanism to all those vulnerabilities to provide protection.

The work can be further improved by studying,identifying and providing security mechanism to various vulnerabilities like Broken Access Control, Broken Authentication

and Sessions Management, Insecure Configuration Management, Cookie Modification, SQL injection, Cross Site Scripting, Buffer Overflow, Daniel of Service and providing solution for the same.

6.Reference

1. Top 10 web vulnerabilities part 1
   http://www.computerworlduk.com/how-to/infrastructure/424/the-top-10-web-vulnerabilities-and-what-to-do-about-them/?intcmp=in_article;related
2. Top 10 web vulnerabilities part 2
   http://www.computerworlduk.com/how-to/infrastructure/424/the-top-10-web-vulnerabilities-and-what-to-do-about-them/?pn=2
3. Functional Programming Way to Interact with Software Attacks and Vulnerabilities Software Testing, Verification, and Validation Workshops (ICSTW), 2010 Third International Conference on Date of Conference: 6-10 April 2010 Author(s): Damjanovic, V., Djuric, D.Knowledge-based Inf. Syst., Salzburg Res., Salzburg, Austria
4. A Survey on Web Application Vulnerabilities (SQLIA, XSS) Exploitation and Security Engine for SQL Injection Communication Systems and Network Technologies (CSNT), 2012 International Conference on Date of Conference: 11-13 May 2012 Author(s): Johari, R.;Sharma, P. USIT, GGSIP Univ., Delhi, India
5. Security vulnerabilities in modern web browser architecture MIPRO, 2010 Proceedings of the 33rd International Convention Date of Conference: 24-28 May 2010 Author(s): Silic, Marin;Krolo, Jakov ; Delac, Goran Faculty of Electrical Engineering and Computing, University of Zagreb, Unska 3, 10000, Croatia
6. Testing and Comparing Web Vulnerability Scanning Tools for SQL Injection and XSS Attacks Dependable Computing, 2007.PRDC 2007. 13th Pacific Rim International Symposium on Date of Conference: 17-19 Dec. 2007
   Author(s): Fonseca, J. CISUC - Polytechnic Inst. of Guardia, Guardia
   Vieira, M. ; Madeira, H.
7. Using web security scanners to detect vulnerabilities in web services Dependable Systems& Networks, 2009. DSN '09. IEEE/IFIP International Conference on Date of Conference: June 29 2009-July 2 2009 Author(s): Vieira, M.;Antunes, N. ; Madeira, H. Dept. of Inf. Eng., Univ. of Coimbra, Coimbra, Portugal
8. OPEN WEB APPLICATION SECURITY PROJECT; OWASP Top 10-2010 PDF

9. A Web Security Solution Based On XML Technology TengLv; Ping Yan; Communication Technology, 2006.ICCT '06. International Conference on Digital Object Identifier: 10.1109/ICCT.2006.341975 Publication Year: 2006 , Page(s): 1 – 4