

Identifying susceptibilities in webpage using open source security tool Vega

| | | |
|--|--|--|
| Juita Tushar Raut | Dr.Vikram Patil | Dr.Yogeshkumar Sharma |
| Research Scholar | Research co-guide | Research guide |
| Shri JJT University, Rajasthan, India | Shri JJT University, Rajasthan, India | Shri JJT University, Rajasthan, India |
| Computer Science & Applications | Computer Science & Applications | Computer Science & Applications |
| patiljuita@gmail.com | vikrams.patil@gmail.com | dr.yogeshkumar@yahoo.in |

Abstract: Now a day's web-based systems are very popular. Because it plays a noteworthy role in to making a person's life easier. Their presence in a person's life in various areas like education, banking, social media, organizations, online services, and many more. These systems may have some instinctive security weaknesses due to the language they use. Many security tools are available for scanning vulnerabilities within the web applications, some of them are paid, and others are open source. In this study, the author chooses Vega tool to scan the web page to find the vulnerabilities in the web before goes wrong with the whole website. After that results will be analyzed towards the relevant results.

Keywords: website, vulnerability, Vega tool.

I.INTRODUCTION:-Social networking has become an everyday a part of many folks lives as evidenced by the large user communication. Platforms provided by social networking to simplify communication and shared between users, demonstrating real-world relationship. Such type of an application provide amenities to people permitting to their desires both proficiently and cost excellently. But only efficiency and proficiently is not enough. Such type of an application should be locked and consistent too. Over the past ten years, a number of different technologies have targeted application development on the web. A web application includes a script on a web server that interacts with databases or other resources of dynamic content. Such technologies was developed by using different types of languages like PHP, Active Server Pages (ASP), Perl, Common Gateway Interface, Java Server pages, ASP.NET, VBScript and many more. So most of the time languages are itself expose to the attacker in terms of HTTP methods. So it makes easy to an attacker to gain access within an application. In this study, only the client-side address of an application was used. Web applications are usually smaller than regular desktop applications and can have rich graphical interactive interfaces. The whole website was developed within ASP.NET. But only a single web page was going to scan in this implementation.

1.1 Vega scanning tool:-It is available in open source web scanner and used to test the security of web appliances. It find many common types of vulnerabilities like SQL injection, Cross-Site Scripting (XSS), Local File Inclusion, and other type of vulnerabilities. It supports multi-platform also written in java and GUI based. It has some special features which adds it qualities like intercepting proxy, proxy scanner and automatic in nature.

II.Related Work:- The Vega tool has crawling capacity that automatically log into websites when provided with user identifications. Such type of tool can easily figure out the weakness within web pages or application before an attacker finds that and try to attack into it.

V. Okanovic, T. Mateljan, described the designing of a replacement web appliance framework. The target of the online application framework should be flexibility of rapid and quality development of a dynamic web appliance. Then examines several existing open source java web context and defines their positive and negative structures. Then the approach participates and smears the positive appearances of the analyzed web framework.

Muhammet BAYKARA, now a day's popularity of web application increases day by day. But such type of application were developed using various types programming languages. Such languages are exploitable by an attackers using different types of methods. To protect and maintain qualities of application it requires to identify the vulnerabilities that are already existed in the application. To figure out such kind of vulnerabilities from a website, there are so many security tools are available in free and commercial. In this article, author analyzed both types of tools paid and free on application and evaluated results that which tool is best for whom.

Korra Manasa and L. Venkateswara Reddy, illustrated the web application is useful for entire human's life like online education, social media, organizations and many more. But such communication isn't secure so it requires security scanner which gives intimation to the web developer about the alerts happens inside the application and then take care of it. In this study, Vega tool is used to figure out the vulnerabilities from an offline web application before it hosting on online. Mainly focused on students who faced such kind of problems during such kind of education including conferences, workshops, online events etc.

III. Implementation:-Implementing a web application using various frameworks and different technologies aren't big challenge to providing security is a very major challenge. Developing web application which will rise the users to browse their need in the correct way. In this study, implementation was performed to figure out the vulnerability whether present or not in the website. Most of the time, many developers doesn't care of security of web application and some of non-technical persons aren't aware about such kind of security. With the help of such kind of study, non-technical or developers be take care of this while developing application. So they can protect their websites from unwanted attacks. In this section, Vega scanner was examined against web page before going to host whole website online. Such test was made on the <http://localhost:1999/contact.aspx>.

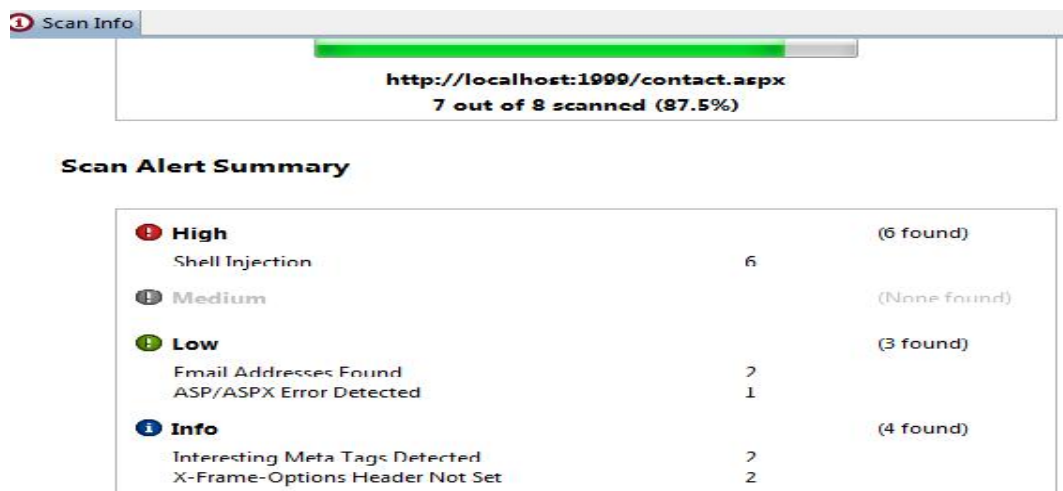


Figure. 1 Running scanning using Vega tool

After applying Vega tool on this web page it takes one and half hour to complete the scanning of vulnerability. In single web page it finds total 13 alerts with levels of severity like high, low and information level.

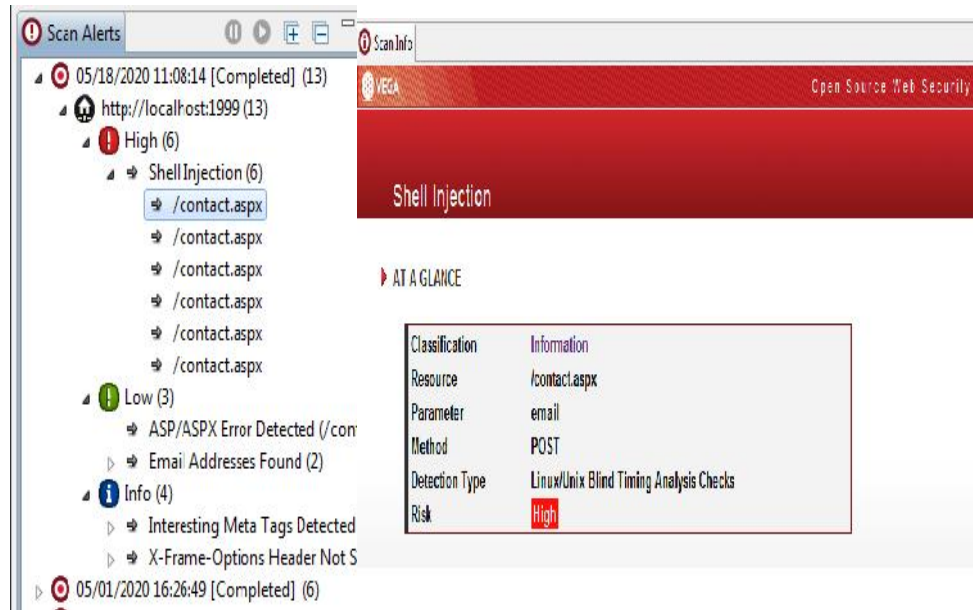


Figure. 2 Web page attacks in High, Low, and Informational

The above figure shows the types of alerts were founded within scanning. In which shell injection, Asp/ASPX error, e-mail address not found, interesting Meta tags detected and x-frame-options header not set etc. Above detected errors are known to be harmful to the application. Each alert has special features or techniques to exploit the methods of web page. In this implementation, tool detects high alert known as shell injection or command injection that executes random command on the server for spiteful purposes. Low level alerts are actually notice messages may interpretation delicate data about an application's internal working to an attacker. And finally informational errors in which clickjacking attacks was detected within application. From scanning it was cleared that POST method is expose to the vulnerable. So it helps to an attacker to get chance inside the application to harm the system.

IV.Results:-



Figure. 3 Potential attacks on web page

Above figure shows the levels of vulnerability. In which high alerts found in highest number means 46 % of total vulnerability. In high alerts, shell injection type of vulnerability. In which total six URLs of page are found to be vulnerable because of POST and GET methods. After that second alert was informational error in which four alerts were found with different types of vulnerability with 31 % of total susceptibility. And finally 23 % of total errors of low alerts were detected within application. Creating website with the use of different technologies and applications and also providing security to that particular website is big challenge. In this study, efforts are taken to scan website by using Vega tool and finds alerts and prevent from an attackers.

V.Conclusion:-This study provides the solution, to the problem faced by web developers while developing any kind of website which is useful for any small organization, educational institution, social networking, etc. Applying security tools on single web page or the whole website gives alerts about the security flaws that presents inside the application. Which protect from the damage or crash the system and developers should take precautions while developing web application. Vega tool was used to scan the vulnerability because such tool is best suitable for individual use in the system of minimum security. Vega tool also provides remedied to protect such kind of an alert found within vulnerability scanning.

References:-V. Okanovic; T. Mateljan (2011),”Designing a new web application framework”, MIPRO, 2011 proceedings of the 34th international convention; PP: 1315-1318; ISBN: 98-1-4577-0996-8; IEEE; 23-27 May-2011.

Fakhreldeen Abbas Saeed, Eltyeb E. Abed Elgabar (2014),” Assessment of Open Source Web Application Security Scanners”, ISSN: 1992-8645, Journal of Theoretical and Applied Information Technology, Vol. 61 No.2.

Mohamed Al-Ibrahim, Yousef Shams Al-Deen (2014),” The Reality of Applying Security in Web Applications in Academia”, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 5, No. 10.

Korra Manasa, L.Venkateswara Reddy (2016),” Designing a Web Application and Detecting Vulnerabilities Using Vega Vulnerabilities Scanner”, American Journal of Engineering Research (AJER) e-ISSN: 2320-0847 p-ISSN: 2320-0936 Volume-5, Issue-8, pp-227-232.

Muhammet BAYKARA (2018),” Investigation and Comparison of Web Application Vulnerabilities Test Tools”, International Journal of Computer Science and Mobile Computing, Vol.7 Issue.12, December- 2018, pg. 197-212.