*International Journal of Social Science & Interdisciplinary Research*_____ ISSN 2277-3630
IJSSIR, Vol. 4 (7), JULY (2015), pp. 212-222
Online available at indianresearchjournals.com

VULNERABILITY ASSESSMENT AND PENETRATION TESTING

HEMANT KUMAR PANDEY*; AROUSHI SHARMA**

*STUDENT (MAIT , GGSIPU)

**STUDENT (MAIT , GGSIPU)

ABSTRACT

Computer system threats come in many different forms. Some of the most common threats today are software attacks, theft of intellectual property, identity theft, theft of equipment or information, sabotage, and information extortion. Most people have experienced software attacks of some sort. Viruses, worms, phishing attacks, and trojan horses are a few common examples of software attacks. The theft of intellectual property has also been an extensive issue for many businesses in the IT field. Intellectual property is the ownership of property usually consisting of some form of protection. Theft of software is probably the most common in IT businesses today. Identity theft is the attempt to act as someone else usually to obtain that person's personal information or to take advantage of their access to vital information

Information security, sometimes shortened to **InfoSec**, is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. In this paper, we did focus a common security problems faced by many of the business organizations as well as government websites which sometimes lead to a big mishap in the modern virtual cyber world. We'll focus on the vulnerabilities faced by the applications developed in popular languages such as PHP, Asp.net etc and the ways through which they can be tackled a secured. The vulnerabilities discussed in this paper are Brute Force, Command Execution, Cross Site Scripting, Insecure Captcha and SQl Injection with the solutions taken to make the applications immune to these vulnerable attacks by taking idea from source code of Damn Vulnerable Web Application (**DVWA**).

KEYWORDS- Information Security, Vulnerabilities, DVWA.

References

OWASP Top 10 Web Application Vulnerabilities.http:// www.applicure.com/blog/owasp-top-10-2010

MITRE. Common vulnerabilities and exposures. http:// cve.mitre.org/cve/, 2007

OWASP testing guide.

Vulnerable applications testing- http://resources.infosecinstitute.com/vulnerable-applications/

SQL Injection details- https://pentestlab.wordpress.com/2012/09/18/sql-injection-exploitation-dvwa/

IEEE, (2010), "The Institute of Electrical and Electronics Engineers", Available at: http://www.ieee.org/ [Accessed 25 July 2010]

O. Hallaraker and G. Vigna. Detecting malicious JavaScript code in Mozilla. In Proc. IEEE Conf. on Engineering of Complex Computer Systems, 2005.

Z. Su and G. Wassermann. The essence of command injection attacks in Web applications. In Proc. POPL, 2006.

D. Yu, A. Chander, N. Islam, and I. Serikov. JavaScript instrumentation for browser security. In POPL, 2007.