Measuring Severity of Attributes That Create Vulnerabilities in Websites and Software Applications Using Two Way Assessment Technique

Swati Narang, Amity Institute of Information Technology, Amity University, Noida, India
P.K. Kapur, Amity Centre for Interdisciplinary Research, Amity University, Noida, India
D. Damodaran, Center for Reliability, Government of India, Delhi, India

ABSTRACT

Inadequacies and faults that are the reason of vulnerabilities are hazardous for the websites. The authors’ chief intention is to trim down those assailon websites by restraining the attributes accountable for these assails. This article categorizes those cases/attributes into 10 categories and arranges them in priority according to their severity. These attributes influence which contributes to losses in terms of monetary as well as humanity. By prioritizing these attributes, web designers as well as users will check twice on these aspects before entering confidential information into the website. The opinion of different web designers and experts of different companies was captured to prioritize these attributes using an analytical hierarchical process and two way assessment methods so that the loss should be minimized. Research confirms that total severity measure aids the severities of these attribute’s contribution towards vulnerabilities. The findings of the two way assessment technique show that there is only one such attribute which happens to be extremely severe in comparison to other attributes and needs imperative consideration while designing websites and also by users before entering their confidential credentials on a website to curtail the losses caused by black hat guys.

KEYWORDS

Assessment Techniques, Multi-Criterion Decision Making Techniques, Security Threats, Severity Measure, Two-Fold Approach, Vulnerability Management, Website Designing

INTRODUCTION

Software vulnerability is a defect, which permits an attacker to seize into system’s information safety system. Risk on protection or safety of confidential information saved in the software is named to be software vulnerability. The menace associated with the exploitability of those vulnerabilities can be a reason or possibility of momentous loss. Some vulnerabilities have little risk attached to them while there are few vulnerabilities which have high risks attached to their exploitability, these vulnerabilities are known as exploitable vulnerabilities. If these vulnerabilities get discovered by hackers or black hat guys, it can cause great financial, potential losses which can further lead to loss of lives too. Basically, the vulnerability exploitation is the combination of three fundamentals: system’s incompetency or flaw, how attacker reacts to the flaw and the potential of an attacker i.e. he must be having a tool or

DOI: 10.4018/JCIT.2019040103

Copyright © 2019, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
technique that is tied to any of the limitation of our system. Here we are considering vulnerability to be a point in our website where attack can occur rapidly.

Vulnerability management is basically associated with identifying, classifying, remediating, and mitigating the security flaws of the software. There are some vulnerabilities which are not associated with software used, this concept of vulnerability can be associated with the hardware on which the software is installed and even the operating system of that hardware. In our context our focus is on security defects which occur in websites.

Web applications and websites need protection against the attacks due to security holes or vulnerabilities present in them. Users save their credentials into these applications and expect it from the servers to keep them protected but hacking can occur. Chances of data being misused by the hackers are very high. A successful approach to information confidentiality must, as the definition says, be practical, shielding and self-protective. While heading to our work, it is aimed at igniting the state of mind towards protection, hopefully injecting the reader with a healthy dose of paranoia.

In particular, this paper focuses on ten most widespread and major web safety snags to be aware of so that web developers can avoid them while designing the websites and webpages. Reason behind the selection of two way assessment for this prioritization is the independence of attributes.

This paper presents a study of the causes of these vulnerabilities. Below section represents the problems or the impact which occurs due to scanning of websites for vulnerabilities. This section also informs us about some precautions to ensure safety of information of users of website. Section succeeding the same gives a brief history and use of two way assessment technique and the meaning and importance of TESM. Further the next section describes 10 factors which lead to vulnerabilities in websites, we will compute the weight of each factor and also TESM of current case by methodology given in the next section. Subsequent section gives results of the methodology and calculations done. References are mentioned in consequent sections. Final section displays all calculations in tabular form.

**IMPACT OF VULNERABILITY SCAN ON WEBSITES**

Black hat guys or unsavoury people commonly known as hackers have an eye on our information. We can see in the past that educational websites, government sites or personal blogs(almost all types of websites) are the victims of the harms caused by these hackers who exploit vulnerabilities. As we know there are enormous number of websites which are flooded with lots of vulnerabilities, the chances that bad guy will break through the code for his favour increases with each passing day of software release. Best way to save our self is to try to Hack Yourself First. This will enable us to know loop holes of our websites. Hack Yourself First can only be done by the scanners of websites as there are thousands of transfigurations which can’t be scanned manually. But scanning has its side effects too which can impact our profits. These impacts can also be trivial. Sometimes the scanning causes aperture to attacks while on other times the websites are itself faulty but our main concern here is not to find who is at fault but rather to find ways so that we remain the driver of our website not the bad guy. Precautions are taken for risk reduction due to the harms caused by scanner.

Here we are going to investigate the root cause of the risks. Years of battlefield testing is the only way to accomplish this investigation correctly. Scanner guys themselves are not sure of how much the scanning is harming the website. Their business model doesn’t give them access to know the measurable impact. So the web developers fear of the negative gust which causes vulnerabilities. Users as well as developers should know the following to ensure security:

- First, the sensitive hyperlinks and forms should be known well and not clicked;
- Second, sometimes website executes meta characters in place of executable code which is signalling the presence of vulnerabilities. Badly designed vulnerability tests cause harm to the executable code and even browser’s configuration;
Semantic Approach to Web-Based Discovery of Unknowns to Enhance Intelligence Gathering
Natalia Danilova and David Stuples (2017). *Ontologies and Big Data Considerations for Effective Intelligence* (pp. 196-213).
www.igi-global.com/chapter/semantic-approach-to-web-based-discovery-of-unknowns-to-enhance-intelligence-gathering/177394?camid=4v1a