Journal of Theoretical and Applied Information Technology
30th November 2019. Vol.97. No 22

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

PERFORMANCE MEASUREMENT OF THE SECURITY SYSTEM IN XYZ WEBSITE USING CALCULATION OF CVSS BASE MATRIX

[1]MOH SUKRON MUFAQIH, [2]FORD LUMBAN GAOL

1,2, Information Systems Management Department, BINUS Graduate Program-Master of Information Systems Management, Bina Nusantara University Jakarta, Indonesia 11480

E-mail: [1]mufaqih96@gmail.com, [2] ford.gaol@gmail.com

ABSTRACT

The Security vulnerability in website is one of the flaws in website that could be exploited by irresponsible party whose attack could jeopardise the website's privacy, integrity and its availability. Without a vulnerability mapping in a website could harm and risk the data's security, not to mention the effect on the SQL Injection that could led to a disturbance in information and data exchanges. This series of events will likely damage XYZ's reputation in the eyes of the people, government and user and also financial implication to the company. To overcome this issues, XYZ will need to conduct an evaluation in its website security through website vulnerability test. The purpose of this test is to scale the maturity of the website security. The method that will be used in this test is through CVSS as the tool. This measurement is done using Access Vector, Attack Complexity dan Authentication as the gauge in the prioritising the handling and mitigation of the website vulnerability. The result of XYZ website is that it has 3 high level threats, 5 medium level and the rest are low level that will not be harmful to XYZ.Institution.

Keywords: *Website, Handling, Handling, CVSS, Security*

1. INTRODUCTION

XYZ Institution is a non-ministerial Indonesian government institution that carries out governmental tasks in the field of financial and development supervision in the form of Audit, Consultation, Assistance, Evaluation, Eradication of KKN and Supervision Education and Training in accordance with applicable regulations.

The results of financial and development oversight are reported to the President as the head of government as a material consideration for setting policies in running the government and fulfilling its accountability obligations. The results of XYZ Institution supervision are also needed by other government organizers including provincial and district / city governments in achieving and improving the performance of the agencies they lead. The XYZ Institute is always committed to providing the best service and data protection information to their service users, implementing good corporate governance practices, improving the welfare of employees and their families and increasing social care for the general public and the environment around the XYZ institutions through the Social Responsibility program[1].

In this era of globalization, the use of information technology in all fields of activity has become fairly common and many have used it. The most commonly used information technology now is the internet. Based on statistics obtained from [2] internet usage in the world has reached 4,208,571,287 billion users of the total human population worldwide 7,634,758,428. This is a very large number, considering that more than 62% of the world's population has used the internet.

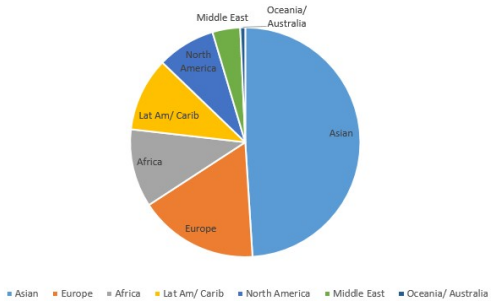

Figure 1.1 User internet in the world

The xyz.co.id website which is also one of the developments in the application of information technology in general and the internet in particular

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

at Government Agencies is one of the important factors in establishing a relationship between Government Agencies and customers.

By seeing this good opportunity, the XYZ institution as a government agency is trying to build a website as a means of providing information to everyone who accesses it. Everyone can access Government Agency information in general or specifically. This website is also useful for providing information about the services provided by Government Agencies, besides that in its indirect application the XYZ institution has adopted e-government for the government bureaucracy and is expected to be an alternative for bureaucratic reform towards better services[3].

On its use the application of the XYZ Institution website has been attacked. For example, websites exposed to DDOS (Distributed Denial of Service and SQL Injection, host header attacks and Bruteforce Attack. Implementation of the website has various risks. For example, users who access the website can be infected with trojans, viruses, malware, or websites affected by DDOS (Distributed Denial of Service), cracking and hacking activities, SQL Injection, etc. By looking at the many risks posed in the application of the website, it is necessary to risk management of information systems on the website, by looking at the vulnerability and the results arising from the attack harming the XYZ institutions risk management is required by measuring the CVSS information system on the website.

It is necessary to implement a better security, by analyzing the website security using the Scanning vulnerability assessment method using the acunetix application to analyze security on a website [4].

After that, the calculation of CVSS (Common Vulnerability Scoring System) base metrics. The main reason for implementing CVSS is because CVSS is a free and open industry standard for assessing the latest level of computer system security vulnerabilities. CVSS seeks to establish severity scores for vulnerabilities, allowing respondents to prioritize responses and resources according to threats[6].

The results of the CVSS base metrics calculation using the base score formula show the measurement values to assess a vulnerability to the system. Which in 2014 - CVSS article has updated its version to CVSS 3.0. CVSS will assess vulnerability from score 0.0 - 10.0 which is divided into 4 aspects [5].

2. STYLE OF PAPER

The analysis here is an advanced stage where a process is carried out to understand the nature of the identified vulnerabilities and determine the level of vulnerability. This analysis provides a basis for knowing what risks can be caused and their impacts and decisions about how to handle them.Calculation

BaseScore = (0.6*Impact +0.4*Exploitability-1.5)*f(Impact)

Impact = 10.41 * (1 - (1 - ConfImpact) * (1 - IntegImpact) * (1 - AvailImpact))

Exploitability = 20 * AccessComplexity * Authentication * AccessVector

f(Impact) = 0 if Impact=0; 1.176 otherwise

2.1 Access Vector

Access vector (AV) menunjukkan bagaimana kerentanan dapat dieksploitasi.

Value	Description	Score
Local (L)	Attackers must have physical access to vulnerable systems (eg firewire attacks) or local accounts (eg attacks using registered accounts).	0.395
Adjacent Network (A)	Attackers must have access to the broadcast domain (eg ARP spoofing, bluetooth attacks).	0.646
Network (N)	Vulnerable user interfaces working at	1.0

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

	layer 3 or above the OSI Network. This type of vulnerability is often described as being remotely exploited (eg remote buffer overflow in network services)	

2.2 Attack Complexity

The attack complexity (AC) metric illustrates how easy or difficult it is to exploit the vulnerabilities found.

Value	Description	Score
High (H)	There are special conditions, such as requirements for social engineering methods that will be noticed by knowledgeable people.	0.35
Medium (M)	There are several additional requirements for this level, such as an attack limit, or a requirement that a vulnerable system be run with an unusual non-default configuration.	0.61
Low (L)	There are no special conditions for exploiting vulnerabilities, such as when a system is available to users without access restrictions, or vulnerable configurations are everywhere.	0.71

2.3 Authentication

(Au) describes the number of times an attacker must authenticate to a target to exploit it.

Value	Description	Score
Multiple (M)	Vulnerability exploits require an attacker to authenticate two or more times, even if the same credentials are used every time.	0.45
Single (S)	Attackers must authenticate once to exploit vulnerabilities.	0.56
None (N)	There is no requirement	0.704

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

	for an attacker to authenticate.	

Impact Metrics

4.4 Confidentiality

Confidentiality (C) metrics explain the impact on the confidentiality of data processed by the system.

Value	Description	Score
None (N)	There is no impact on system confidentiality.	0.0
Partial (P)	There is a lot of information disclosure, but the scope of the damage is limited so not all data is available.	0.275
Complete (C)	There is total disclosure of information, providing access to all / all data on the system. Or, access to only a limited amount of information is obtained, but the information disclosed presents a direct and serious impact.	0.660

4.4 Integrity

Integrity (I) metric describes the impact on the integrity of the system being exploited.

Value	Description	Score
None (N)	There is no impact on system integrity.	0.0
Partial (P)	Modification of some data or system files is possible, but the scope of the modification is limited.	0.275
Complete (C)	There is total integrity lost; an attacker can modify any file or information on the target system.	0.660

4.5 Availability

The availability (A) metric describes the impact on the availability of the target system. Attacks that use network bandwidth, processor cycles, memory or other resources affect system availability.

Value	Description	Score
None (N)	There is no impact on system availability.	0.0
Partial (P)	There is a decrease in performance or loss of some functions.	0.275
Complete (C)	There is a total loss of availability of the resources that were attacked.	0.660

3. TABLES AND FIGURES

The analysis here is an advanced stage where a process is carried out to understand the nature of the identified vulnerabilities and determine the level of vulnerability. This analysis provides a basis for knowing what risks can be caused and their impacts and decisions about how to handle them. In this case the determination of the base score matrix uses the CVSS calculator tool as a scoring determinant of a vulnerability on the website.

Journal of Theoretical and Applied Information Technology
30th November 2019. Vol.97. No 22

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3.1 Blind SQL Injection

Figure 3.1 Blind SQL Injection matrix

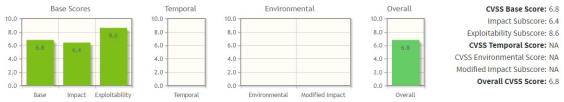

Figure 3.2 Scoring SQL Injection

3.2 Cross Site Scripting

Figure 3.3 Matriks Blind Cross Site Scripting matrix

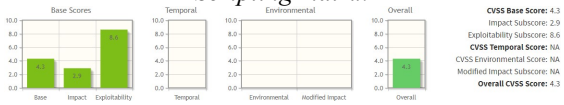

Figure 3.4 Matriks Blind Cross Site Scripting

3.3 SQL Injection

Figure 3.5 SQL Injection Matrix

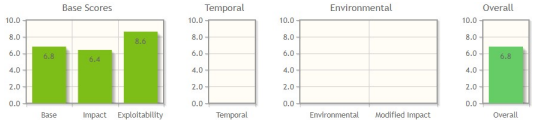

Figure 3.6 Scoring SQL Injection

3.4 Application error message

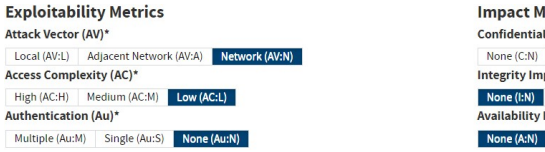

Figure 3.7 Application error message

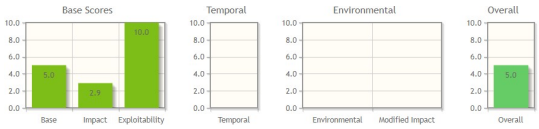

Figure 3.8 Scoring Application Error Message

3.5 HTML form without CSRF protection

Figure 3.9 Matriks HTML form without CSRF protection

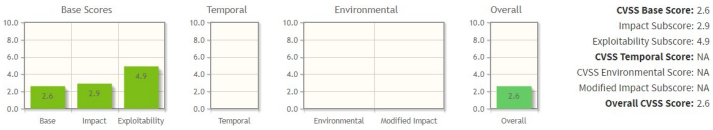

Figure 3.10 Scoring HTML form without CSRF protection

3.6 Multiple Vulnerabilities Fixed in PHP Versions 5.5.12 and 5.4.28

Figure 3.11 Matriks Multiple vulnerabilities fixed in php versions 5.5.12 and 5.4.28

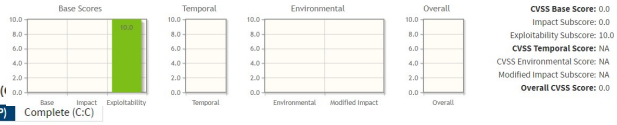

Figure 3.12 Scoring Multiple vulnerabilities fixed in php versions 5.5.12 and 5.4.28

3.7 Same Site Scripting

Figure 3.13 Matriks Same site scripting

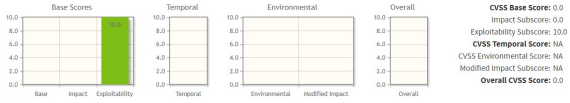

Figure 3.14 Scoring Same site scripting

3.8 User Credencial are Sent in Clear Text

Figure 3.15 User Credencial are sent in clear text

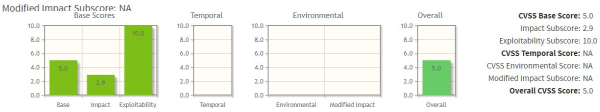

Figure 3.16 User Credencial are sent in clear text score

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4. EQUATIONS

The results of the analysis of this study describe that the XYZ institute's website has several security holes, among others:

- Blind SQL Injection
- Cross Site Scripting
- SQL Injection
- Application Error Message
- HTML Form Without CSRF Protection
- Multiple Vulnerabilities Fixed In PHP Versions 5.5.12 and 5.4.28
- Same Site Scripting
- User Credencial Are Sent In Clear Text

The results of the analysis of the CVSS method can rank the handling based on the potential impacts caused by vulnerabilities and website vulnerabilities that exist in XYZ institutions. From the findings above, it can be concluded that Scoring and the status of vulnerability levels include:

Vulnerability	Status	Scoring
Blind SQL Injection	High	6.8
Cross Site Scripting	High	4.4
SQL Injection	High	6.8
Application Error Message	Medium	5.0
HTML Form Without CSRF Protection	Medium	2.6
Multiple Vulnerabilities Fixed In PHP Versions 5.5.12 and 5.4.28	Medium	0.0
Same Site Scripting	Medium	0.0
User Credencial Are Sent In Clear Text	Medium	5.0

Based on the findings of the vulnerability above, it can be suggested that the handling that must be done by XYZ institutions is :

- Blind SQL Injection
  Program scripts must filter meta characters from user input.
- Cross Site Scripting
  The script on the website is recommended for filtering metacharacter from user input. The two most important countermeasures to prevent cross-site scripting attacks are input constraints (limiting input characters, validation of input types, length, format, and range) and encoding output (encoding or encoding output).
- SQL Injection
  Program scripts must filter meta characters from user input.
- Application error message
  Review the source code for the affected script.
- HTML form without CSRF protection
  Improve the firewall and use SSL (Secure Socket Layer) or implement other CSRF precautions if needed.
- Multiple vulnerabilities fixed in php versions 5.5.12 and 5.4.28
  Upgrade to the latest version PHP
- Same site scriping
  It is recommended that non-FQ localhost entries be removed from the server name configuration for domains that host websites that depend on HTTP status management.
- User Credencial are sent in clear text
  Because user credentials are considered sensitive information, they must always be transferred to the server via an encrypted connection (HTTPS).

REFRENCES:

[1] Falih Suaedi dan Bintoro Wardiyanto.2010.Revitalisasi Administrasi Negara, Reformasi Birokrasi dan E-Governance.Yogyakarta: Graha Ilmu

[2] First.org. (2019, February 18). Common Vulnerability Scoring System SIG. Retrieved from www.first.org/cvss: www.first.org/cvss/

[3] Hidayat, B. (2015). PENGUKURAN KINERJA DENGAN BALANCED SCORECARD PADA KOPERASI. media.neliti.com, 1.

[4] internetworldstats.com. (2018, June 30). word stats. Retrieved from INTERNET USAGE STATISTICS: https://www.internetworldstats.com/stats.htm

[5] ISACA. (2012). COBIT 5 for Information Security . Washington DC: ISACA.

[6] M. Khan, “Security Metrics Based Network Risk Asessment,” Thesis , 2013.