Measurement of Security System Performance on Websites of Personnel Information Systems in Government Using Common Vulnerability Scoring System

Ferlan Gisma Putra[1], Benfano Soewito[2]
[1,2] Computer Science Department, BINUS Graduate Program, Master of Computer Science, Bina Nusantara University
e-mail: ferlan.putra@binus.ac.id[1], bsoewito@binus.edu[2]

Abstrak

Perkembangan komputer semakin pesat terutama sebagai media komunikasi data. Salah satu bentuk nyata dari evolusi teknologi adalah berkembangnya media informasi online seperti website yang dapat diakses di seluruh dunia selama terhubung dengan jaringan internet tanpa dibatasi oleh ruang dan waktu. Kerentanan keamanan sistem jaringan komputer adalah kelemahan dalam sistem yang dapat dimanfaatkan oleh satu atau lebih penyerang untuk melakukan serangan yang dapat membahayakan kerahasiaan, integritas, atau ketersediaan suatu sistem. Sehingga diperlukan penerapan keamanan yang lebih baik, pada proyek ini dilakukan analisis keamanan website dengan metode scanning dan perhitungan metrik keamanan dengan pengukuran pada sistem informasi Common Vulnerability Scoring System (CVSS) pada website Sistem informasi kepegawaian di lingkungan Pemerintah , melalui metode Scanning Vulnerability Assessments untuk menganalisa keamanan pada website. Hasil yang diperoleh dalam perhitungan metrik keamanan menggunakan perhitungan skor dasar menunjukkan nilai yang tinggi untuk tingkat keparahan paling berbahaya dalam pencurian data di situs web pemerintah..

Kata Kunci: *CVSS; metrik keamanan; keamanan situs web; pemindaian; Sistem Skor Kerentanan Umum; Sistem Informasi Kepegawaian di Pemerintah*

Abstract

The development of computers is growing rapidly, especially as a data communication medium. One of the tangible forms of technological evolution is the development of online information media such as websites that can be accessed throughout the world as long as they are connected to the internet network without being limited by space and time. A computer network system security vulnerability is a weakness in a system that can be exploited by one or more attackers to carry out attacks that can compromise the confidentiality, integrity or availability of a system. So it is necessary to implement a better security, in this project a website security analysis was carried out with scanning methods and calculation of security metrics with measurements on the Common Vulnerability Scoring System (CVSS) information system on the website Personnel information system in the Government, through the Scanning Vulnerability Assessments method to analyze security on the website. The results obtained in the calculation of security metrics using the base score calculation show a high value for the most dangerous severity level in data theft on government websites.

Keywords : *CVSS; security metric; website security; scanning; Common Vulnerability Scoring System; Personnel Information System in Goverment*

INTRODUCTION

A website is a collection of pages that display a wide range of text information, data, images, animations, sounds, videos and a combination of all, provided through the internet so that it can be accessed throughout the world while connected to the internet without limited space and time (Suryayusra, 2014). A website page is a document written in Hyper Text Markup Language (HTML) format, which is accessed through a protocol that conveys various information from the server to be displayed to users through a browser or often called HTTP.

Currently the Website is one of the information services that are widely accessed by internet users in the world. As one of the dining information services need to be built a website that is able to handle requests from many users well. Web server contains web pages, which contain information or documents that want to be disseminated or needed by users.

Cyber security is now increasingly important, because now the use of computers and the use of computer networks is increasing, so is the number of cyber attacks that are increasing.

There are various types of cyber attacks that have occurred to date, the types of cyber attacks that are commonly used by cyber attackers lately include Malware, Phishing, DDoS (distributed denial-of-service), MitM (man-in-the-middle).) attack and Zero-day attack

This government website is a means of information for government personnel who have the function to receive, send, store, process and present information data about personnel in the government, in order to support the implementation of human resource development. Keeping the Personnel Information System website in the Government from irresponsible parties, researchers feel the need to conduct an analysis on the government's website so that the vulnerabilities contained on the website can be identified and analyze the impact that can be caused by these vulnerabilities.

RELATED WORKS

Previous Research

From the previous research conducted by Peter, Sasha and Karen (2006), entitled, “Common vulnerability scoring system”. The purpose of this research is to test and determine the level of vulnerability by identifying gaps that can become hacker attacks so that it can provide a score based on the level of vulnerability of an object of research and can determine the potential impact of the vulnerability. As well as the data security aspect becomes a very important aspect although in practice it is often forgotten, just because of the pursuit of performance. This security is needed to fulfill the Confidentially, Integrity and Availability aspects of an information system. Using penetration testing, a proactive, approved and authorized effort to safely evaluate the security of information technology infrastructure.

Common Vulnerability Scoring System

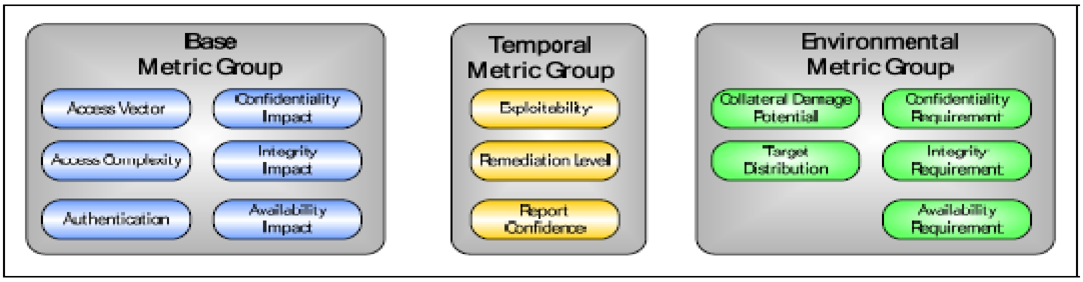


Figure 1. Metric CVSS

CVSS is a quantitative metric and uses a simple formula that returns values as vulnerability severity (Atefeh and Mohammad, 2015). CVSS consists of three metric groups, namely:

1. Base metric, representing the intrinsic and fundamental characteristics of a vulnerability that is constant throughout the user's time and environment.

2. Temporal metric, representing vulnerability characteristics that change over time but not among user environments.
3. Enviromental metric, representing vulnerability characteristics relevant and unique to a particular user environment

Acunetix

Acunnetix web vulnerability scanner is software developed to scan vulnerabilities on a website. The advantage of Acunetix Website Application Scanner is that it can provide solutions to the weaknesses found and manage the traceability of each vulnerability.

Personnel Information System in Government

The Personnel Information System in Government is a computer-based system that has the function to receive, send, store, process and present information data about personnel in the government, both which can be accessed online or manually, accurately, quality, and timely to support the implementation of coaching. clean, transparent, accountable and humane human resources, so that they are used as a means of support as a medium for storing personnel data that is accurate, precise and accessible and available at any time. This Personnel Information System was built to also function as a supporting tool in determining policies and making decisions in the field of HR development within the Government.

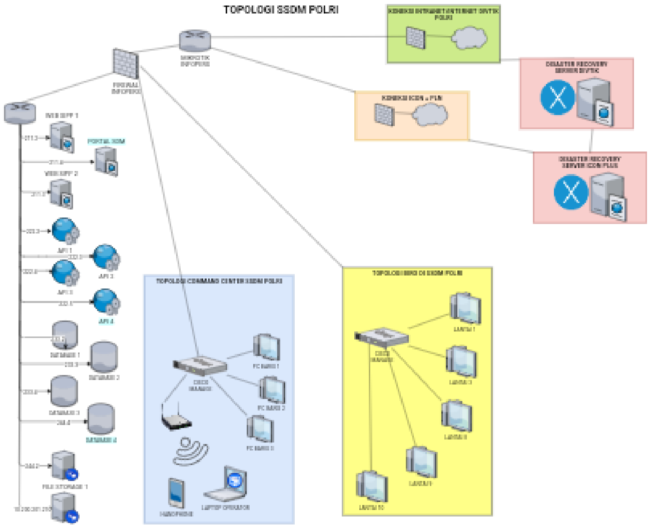


Figure 2. Topology of Personnel Information Systems in Government

METHOD RESEARCH

Framework of Thought

This research is motivated by the desire to detect vulnerabilities that exist in the website security system in the Government. Activities that must be carried out to detect this vulnerability are to establish procedures and methods for compiling research materials, research implementation plans, a number of test measuring instruments, and data collection methods. After determining the various activities, the work steps that must be carried out include:

1. Set the address of the domain to be scanned.
2. Selecting a tool for scanning using the Acunetix Web Vulnerability Scanner tool, which is a software that serves to test the vulnerability of a website and is able to quickly check web server and website weaknesses and provide advice on what to do if weaknesses are found on the website. How to use acunetix by downloading the application at the website address https://www.acunetix.com/, after downloading you can register by visiting the acunetix application and logging into the acunetix account then specify the target website

to be scanned, where is the web address to be scanned , the next stage is create scan with limitations on personnel search and personnel database in the government and the results of the scan will display the page of scan results in real time carried out by acunetix in the form of scan information such as, acunetix thread level, activity, duration, target information and latest alerts.

3. Measure the vulnerability of government websites with CVSS base metrics.
4. Based on points b and c an analysis of the Government's website security system is then carried out to show the various vulnerabilities that exist on the website.
5. Evaluate the results of the security analysis of the government's website, to explain what vulnerabilities exist, and the level of these vulnerability categories on the website.
6. Provide conclusions and recommendations.

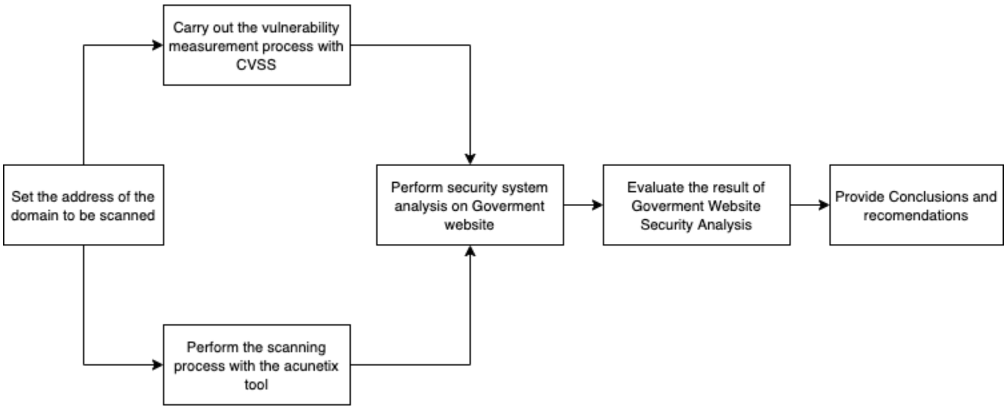

Carry out the vulnerability measurement process with CVSS
Set the address of the domain to be scanned
Perform security system analysis on Goverment website
Evaluate the result of Goverment Website Security Analysis
Provide Conclusions and recomendations
Perform the scanning process with the acunetix tool

Figure 3. Frame of mind

Theory & Method

Calculation of CVSS

The way CVSS works can start from assigning values to Base Metrics, where the basic equation is calculated with a score ranging from 0 to 10, and creating a vector, in this case a text string that contains the values as set for each metric, and is used to communicate exactly how the score for each vulnerability is obtained.

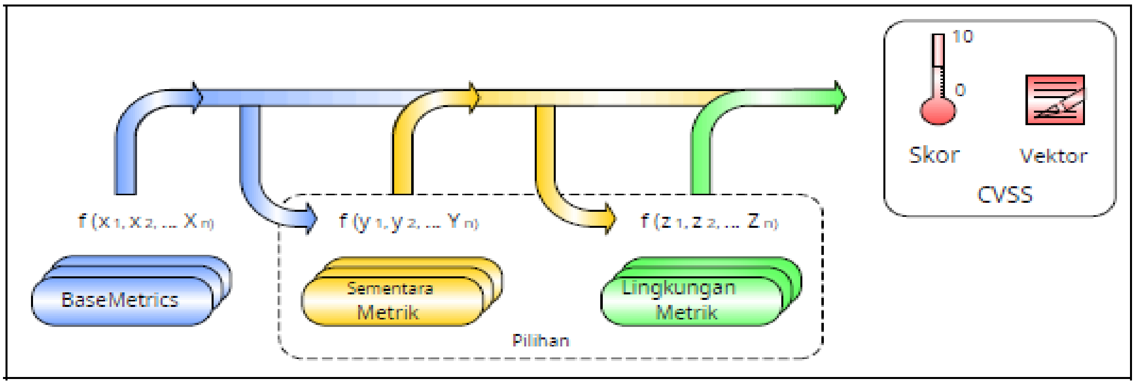


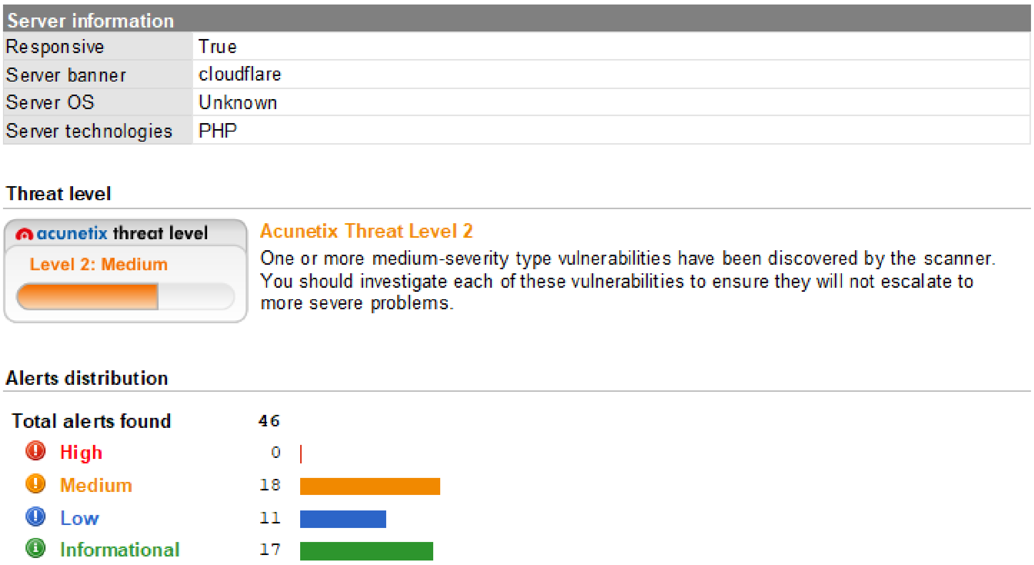
Figure 4. CVSS Calculation Flow

As illustrated in the above figure described Base Metrics can be perfected by assigning values on Temporal Metrics and Enviromental Metrics, this is useful for providing additional context for vulnerabilities by more accurately reflecting the risks posed by vulnerability to users. However, usually Base Metrics and Temporal Metrics are determined by application vendor vulnerability analysts because they have the most accurate information about vulnerability characteristics. Enviromental Metrics are determined by users because they are best able to assess the potential impact of vulnerabilities in their own environment.

CVSS metrics also produce vector strings, textual representations of the metric values used to assess vulnerabilities. This vector string is a specially formatted text string that contains each value assigned to each metric and should always be displayed with a vulnerability score.

Proposed Method

Implementation



Server information	
Responsive	True
Server banner	cloudflare
Server OS	Unknown
Server technologies	PHP

Threat level

Acunetix Threat Level 2

One or more medium-severity type vulnerabilities have been discovered by the scanner. You should investigate each of these vulnerabilities to ensure they will not escalate to more severe problems.

Alerts distribution

Total alerts found	46
High	0
Medium	18
Low	11
Informational	17

Figure 5. Scanning Results

In Figure 4 it can be seen that the scan results on the government website show that "Acunetix Threat Level 2" is categorized as moderate for the vulnerability level which places the target scan at the maximum for hacking and data theft.

Trends in cyber attacks that are vulnerable experienced by webiste, among others:

1. SQL Injection
   SQL injection is an attack method that injects SQL code into a website with the aim of gaining access to a database.
2. Cross site scripting (XSS)
   Cross site scripting (XSS) is done by attackers by inserting HTML code or client script code into a website. This attack will appear to have originated from the site. As a result of this attack, attackers can bypass security on the client side, obtain sensitive information, or store malicious applications.
3. Cross-site Request Forgery (CSRF)
   Cross-site Request Forgery (CSRF) is an attack method that utilizes the authentication and authorization of targets when a fake request is being sent to a web server (Ian, 2019).

Base Score

Represents the intrinsic and fundamental characteristics of vulnerabilities that are constant over time and the user environment.

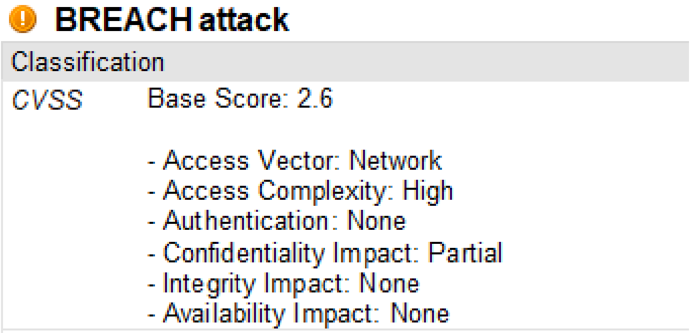
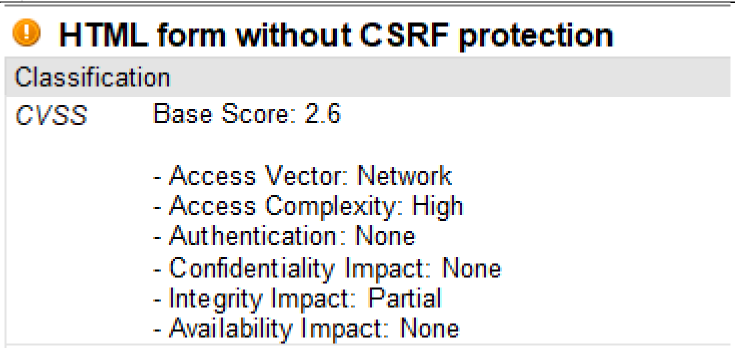
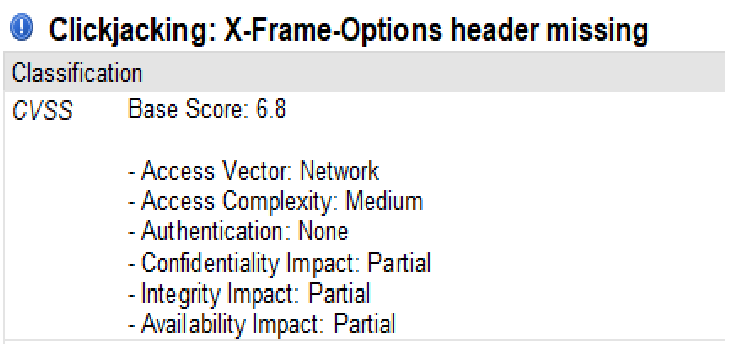
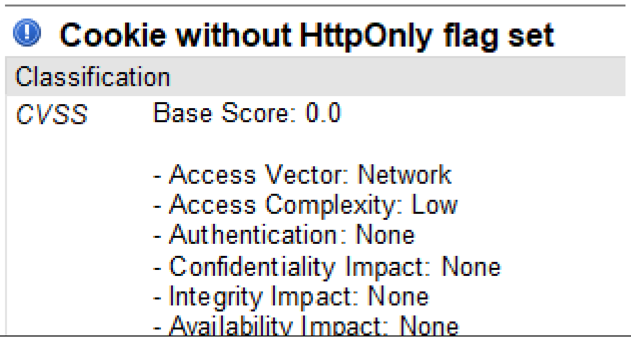
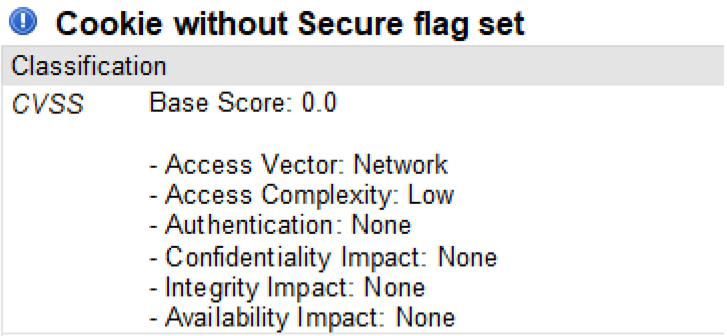
BaseScore = (0.6*Impact +0.4*Exploitability-1.5)*f(Impact)

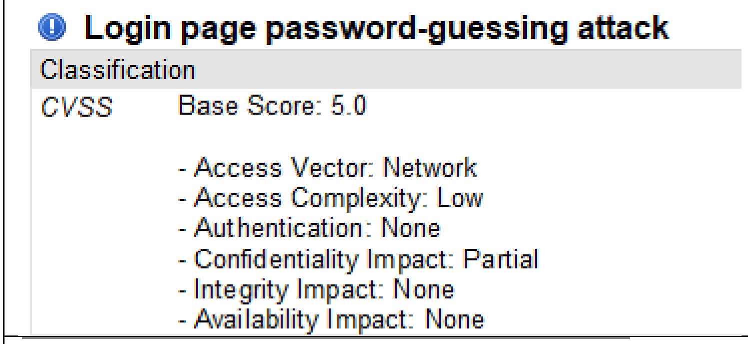
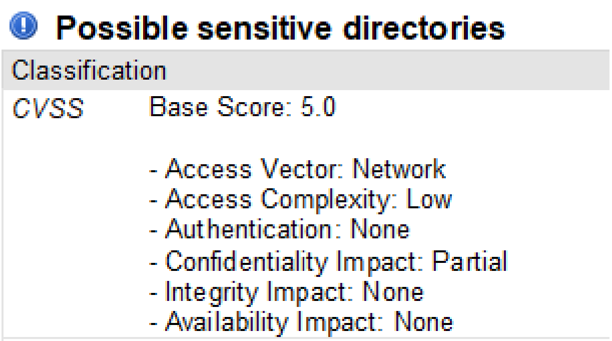
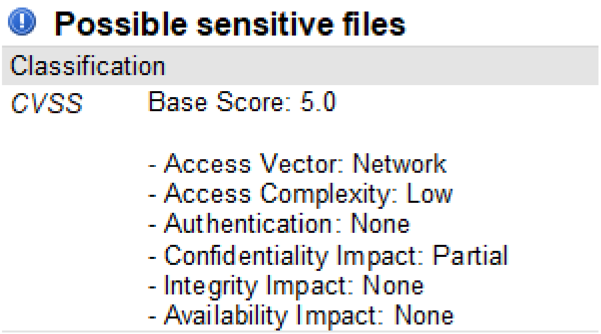
*Impact = 10.41 * (1 - (1 - ConfImpact) * (1 - IntegImpact) * (1 - AvailImpact))*

*Exploitability = 20 * AccessComplexity * Authentication * AccessVector*

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

Table 1. Base Score

Vulnerability	*Score*	Category
 BREACH attack Classification *CVSS* Base Score: 2.6 - Access Vector: Network - Access Complexity: High - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None	2.6	Low
 HTML form without CSRF protection Classification *CVSS* Base Score: 2.6 - Access Vector: Network - Access Complexity: High - Authentication: None - Confidentiality Impact: None - Integrity Impact: Partial - Availability Impact: None	2.6	Low
 Clickjacking: X-Frame-Options header missing Classification *CVSS* Base Score: 6.8 - Access Vector: Network - Access Complexity: Medium - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: Partial - Availability Impact: Partial	6.8	Medium
 Cookie without HttpOnly flag set Classification *CVSS* Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None	0.0	Low
 Cookie without Secure flag set Classification *CVSS* Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None	0.0	Low

 Login page password-guessing attack Classification CVSS Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None	5.0	Medium
 Possible sensitive directories Classification CVSS Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None	5.0	Medium
 Possible sensitive files Classification CVSS Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None	5.0	Medium

RESULT AND DISCUSSION

The results of the analysis of the CVSS method can determine treatment based on the potential impact caused by vulnerabilities and vulnerabilities in government websites. From the above findings, it can be said that the assessment and vulnerability status includes:

Table 2. Scanning Result

No	Vulnerability	*Score*	Category
1.	Breach Attack	2.6	Low
2.	HTML Form Without CSRF Protection	2.6	Low
3.	Clickjacking: X-Frame Option Header Missing	6.8	Medium
4.	Cookie Without HttpOnly Flag Set	0.0	Low
5.	Cookie Without Secure Flag Set	0.0	Low
6.	Login Page Password-Guessing Attack	5.0	Medium
7.	Possible Sensitive Directories	5.0	Medium
8.	Possible Sensitive File	5.0	Medium

CONCLUSION

Based on the results of the study, the following conclusions can be drawn, namely, The results of the analysis of this study explain that the government's website has 8 security holes. According to the results shown from the CVSS calculation, it shows that the government website has a risk level that is not too high in impact. It is recommended to make improvements to improve website security

REFERENCES

Ahad, D. S., Akbar, M., & Ulfa, M. ANALISIS KERENTANAN TERHADAP ANCAMAN SERANGAN PADA WEBSITE PDAM TIRTA MUSI PALEMBANG.

Celebic, G., & Rendulic, D. Basic Concepts of Information and Communication Technology, 2011. *Zagreb, Croatia: Open Society for Idea Exchange* (ODRAZI).

Chew, E., Swanson, M. M., Stine, K. M., Bartol, N., Brown, A., & Robinson, W. (2008). Performance measurement guide for information security.

Collier, Z. A., DiMase, D., Walters, S., Tehranipoor, M. M., Lambert, J. H., & Linkov, I. (2014). Cybersecurity standards: Managing risk and creating resilience. *Computer*, 47(9), 70-76.

Collier, Z. A., Panwar, M., Ganin, A. A., Kott, A., & Linkov, I. (2016). Security metrics in industrial control systems. *In Cyber-security of SCADA and other industrial control systems* (pp. 167-185). Springer, Cham.

Halim, D. (2020). *Inilah Analisa Pakar Digital Forensik Bahwa Database Anggota Polri Telah Diretas,* [Electronic Version]. Available: *https://nasional.kontan.co.id/news/inilah-analisa-pakar-digital-forensik-bahwa-database-anggota-polri-telah-diretas?page=2* [2021, Juni 18].

Horváth, A., Erdősi, P. M., & Kiss, F. (2016). The common vulnerability scoring system (cvss) generations–usefulness and deficiencies.

Ian, M. (2019). *What is Cross-site Request Forgery?.* [Electronic Version]. Available: https://www.acunetix.com/blog/articles/cross-site-request-forgery/ [14 Februari 2019].

INDONESIA, K. N. R. (2015). Peraturan Kepala Kepolisian Negara Republik Indonesia No. 5 Tahun 2015 Tentang Sistem Informasi Personil Kepolisian Negara Republik Indonesia.

Indonesia, R. (2002). Undang-Undang Republik Indonesia Nomor 2 Tahun 2002 Tentang Kepolisian Negara Republik Indonesia. Lembaran Negara RI Tahun.

Ismail, R., & Zainab, A. N. (2013). Information systems security in special and public libraries: an assessment of status. *arXiv preprint arXiv*:1301.5386.

Joseph, A. E. (2006). Cybercrime definition. *Computer Crime Research Center*. *Retrieved April*, 20, 2012.

Joshi, C., & Singh, U. K. (2016). Performance evaluation of web application security scanners for more effective defense. *International Journal of Scientific and Research Publications* (IJSRP), 6(6), 660-667.

Juhad, H. A., Isnanto, R. R., & Widianto, E. D. (2016). Analisis Keamanan pada Aplikasi Her-registrasi Online Mahasiswa Universitas Diponegoro. *Jurnal Teknologi dan Sistem Komputer*, 4(3), 479-484.

Khazaei, A., Ghasemzadeh, M., & Derhami, V. (2016). An automatic method for CVSS score prediction using vulnerabilities description*. Journal of Intelligent & Fuzzy Systems*, 30(1), 89-96.

Kiran, K. V. D., Sruthi, P., Neema, P. S., Vani, G. M., & Sahu, R. (2014). *Risk Assessment in Online Banking System. International Journal of Computer Trends and Technology IJCTT*, 9(6), 279-85.

Mell, P., Romanosky, S., & Scarfone, K. (2006). *Common vulnerability scoring system, (ARTICLE)*

Mell, P., Scarfone, K., & Romanosky, S. (2006). Common vulnerability scoring system. *IEEE Security & Privacy*, 4(6), 85-89.

Mell, P., Scarfone, K., & Romanosky, S. (2007, June). A complete guide to the common vulnerability scoring system version 2.0. In *Published by FIRST-forum of incident response and security teams* (Vol. 1, p. 23).

Mell, P., Scarfone, K., & Romanosky, S. (2007). The common vulnerabi-lity scoring system (CVSS) and its applicability to federal agency sys-tems, NIST IR 7435. *USA: Department of Commerce*.

Mulya, B. W. R., & Tarigan, A. (2018). Pemeringkatan Risiko Keamanan Sistem Jaringan Komputer Politeknik Kota Malang Menggunakan Cvss Dan Fmea. *ILKOM Jurnal Ilmiah*, 10(2), 190-200.

National Research Council. (1999). *Realizing the potential of C4I: Fundamental challenges*. National Academies Press.

Pitoyo A. (2013). *Disusupi Peretas, Situs polri.go.id Tumbang Semalama*n, [Electronic Version]. Available: https://www.merdeka.com/peristiwa/disusupi-peretas-situs-polrigoid-tumbang semalaman.html [2013, Mei 17]

Rezaei, H. (2012). The application of information technology and its relationship with organizational intelligence. *Procedia Technology*, 1, 94-97.

Robby, P. (2013). Analisis Web Vulnerability pada Portal Pemerintahan Kota Palembang Menggunakan Acunetix Vulnerability (Doctoral dissertation, UNIVERSITAS BINA DARMA).

Sima, V., Gheorghe, I. G., Subić, J., & Nancu, D. (2020). Influences of the industry 4.0 revolution on the human capital development and consumer behavior: A systematic review. *Sustainability*, 12(10), 4035.

Singh, U. K., Joshi, C., & Gaud, N. (2016). Information security assessment by quantifying risk level of network vulnerabilities. *International Journal of Computer Applications*, 156(2), 37-44.

Violeta S., dkk. (2020). Influences of the Industry 4.0 Revolution on the Human Capital Development and Consumer Behavior: A Systematic Review. *Sustainability* 2020, 12, 4035.

Wirtz, R., & Heisel, M. (2019, May). CVSS-based Estimation and Prioritization for Security Risks. In *ENASE* (pp. 297-306).

Yang, F., & Gu, S. (2021). Industry 4.0, a revolution that requires technology and national strategies. *Complex & Intelligent Systems*, 7(3), 1311-1325.

Zen, B. P., Gultom, R. A., & Reksoprodjo, A. H. (2020). ANALISIS SECURITY ASSESSMENT MENGGUNAKAN METODE PENETRATION TESTING DALAM MENJAGA KAPABILITAS KEAMANAN TEKNOLOGI INFORMASI PERTAHANAN NEGARA. *Teknologi Penginderaan*, 2(1).

Zieja, M., Zieja, M., & Stachurski, A. (2018). An outline of the method for predicting IT vulnerabilities. In *MATEC Web of Conferences* (Vol. 210, p. 02010). EDP Sciences