WEBSITE VULNERABILITY ANALYSIS USING NIST SP 800-115 AND OWASP METHOD IN DISKOMINFO, BANDUNG DISTRICT

Rubenson Christian Silaban[1], Erick Wijaya[2]

[1,2] Universitas Komputer Indonesia
Jl. Dipatiukur No. 112-116, Bandung 40132
E-mail : rubenson.cristian@gmail.com[1], Eric.wijaya@email.unikom.ac.id[2]

ABSTRACT

Currently the development of technology information has spread to remote part of the country. Both the city and the village has a division that apply the information system to community using website and the one who responsible at Bandung District is Dinas Komunikasi Dan Informasi (DISKOMINFO). Bandung District DISKOMINFO is one of Government branch who mainly focus to Communication, Information, and Technology, E-Government service, and Statistic and Encryption service. But, because the used of website for information service by government to community, there is a problem of exploitation to one of government website that result in loss and disruption of information services of DISKOMINFO Bandung District. Therefore, analysis and testing to website vulnerability using NIST SP800-115 method and OWASP. The result of this analysis and testing will be apply in application reporting that we hope will helped DISKOMINFO Bandung District to manage the website who have the vulnerability.

Keyword: NIST SP 800-115, OWASP Risk Rating Methology, Penetration Testing, website vulnerability, reporting

1. INTRODUCTION

The Office of Communication, Informatics and Statistics of Bandung District is an agency responsible for information processing in the district of Bandung. The website is also a very important need in government agencies, especially the Bandung District Office of Communication, Information and Statistics. With the availability of the website, governance, flow, communication and transactions between the community and the government can be done easily.
But with the increasing number of website facilities provided to support the Diskominfo Bandung District work program in serving the community, the threat of cyber crime is also one of the problems that must be addressed carefully. Based on data obtained from the Indonesia Security Incident Response Team on the Internet and Infrastructure / Coordination Center (Id-SIRTII / CC) which is an agency established to supervise the security of internet protocol-based telecommunications networks. It is known from the data processed by the Directorate of Cyber Crime Indonesia that Cyber Crime cases that occurred in Indonesia in 2016 were 2880 cases [1]. The impact of cyber crime affecting the economic sector based on data from Symantec Norton during 2015 to February 2016 in Indonesia caused a total loss of Rp 194.6 billion [2]. Therefore, countermeasures against Cyber Crime need to be addressed carefully.
Based on interviews with parties from the Bandung District Office of Communication, Information and Statistics, the Information Security section of the ICT section, he asserted that Cyber Attack had already taken place on the Bandung district Government website. This exploitation happened twice in 2017 with the type of exploitation in the form of a web deface, allegedly this attack was carried out by individuals to exploit and display the skills possessed by attackers in attacking websites that are vulnerable to exploitation, so the need for vulnerability analysis on websites managed by the Office of Communication, Informatics and Statistics District of Bandung, with the aim of being able to find out the vulnerabilities contained in the website, so as to reduce the attack on the website managed by Diskominfo Bandung District and. The National Institute of Standards and Technology (NIST) is a non-regulatory body and part of the United States technology administration and trade department. The mission of this organization is to create and encourage measurement, standards and technology to increase productivity, support trade and quality of life. The four main areas of the organization are modern biotechnology, nanotechnology, information technology and manufacturing. NIST issued several series of publications aimed at these four fields and one of them that led to the field of information technology was NIST SP 800-115 Techincal Guide to Information Security Testing and Assessment, a methodology devoted to assisting organizations in planning information security tests [3]

Based on the problems that occur in the Bandung District Office of Communication and Information, a research was carried out with the title "Website

Vulnerability Analysis Using NIST SP 800-115 and OWASP Methods in Diskominfo Bandung District " in hopes of helping to overcome attacks on websites managed by the Office of Communication, Informatics and Bandung District Statistics.

2. CONTENTS OF RESARCH

At this stage there will be a discussion about the problems found, the results of the analysis, a general description of the system and the processes that will be carried out in this study.

2.1 Problem Analysis

As is known in the discussion before in the introduction, there has been a case of attack on the government website which is supervised by Diskominfo, Bandung District. This exploitation occurs on the domain website rsud.cicalengka.bandungkab.go.id with the type of exploitation received in the form of a deface. With the attack on one of the website domains supervised by Diskominfo Bandung District, the domains of other government websites that are still under the supervision of Bandung District Diskominfo have the potential to be affected by the same exploitation.This can be known because there are still several website domains under the supervision of Diskominfo Bandung District which have not been tested for vulnerability.

In addition the Diskominfo District of Bandung does not yet have a guide in handling websites that are affected by exploitation. So we need guidance that can be used if there is exploitation on other government websites. One solution that can be done is to do Security Assessment and Penetration Testing to test whether government websites have vulnerabilities and can be exploited. Thus, after it is known that the website tested has vulnerability and can be exploited, the Diskominfo Bandung District can make improvements to cover the vulnerabilities encountered. Here is the domain that will be tested in this study

No	Domain	Keterangan	Riwayat Eksploitasi
1	http://diskop.bandungkab.go.id	*Website* Dinas Koperasi Kabupaten Bandung	Belum pernah terjadi eksploitasi
2	http://Diskominfo.bandungkab.go.id	*Website* resmi Diskominfo	Belum pernah terjadi eksploitasi
3	http://rsudcicalengka.bandungkab.go.id	*Website* rumah sakit daerah Cicalengka	Terjadi Eksploitasi *Deface*
4	http://kecamatancicalengka.bandungkab.go.id	*Website* Resmi Kecamatan Cicalengka	Belum pernah terjadi eksploitasi
5	http://kesehatan.bandungkab.go.id	*Website* Resmi Dinas Kesehatan Kabupaten bandung	Belum pernah terjadi eksploitasi

Figure 1. Tested domain

2.2 Method Analysis

In this study Analysis Method was carried out an analysis of the method to be used in this study. The method used for Security Assessment and Penetration Testing refers to documents issued by the National Institute of Standards and Technology (NIST) with the NIST SP 800-115 document code. NIST SP 800-115 document provides a method that can be used to perform Penetration Testing along with supporting tools that can be used to carry out Security Assessment.

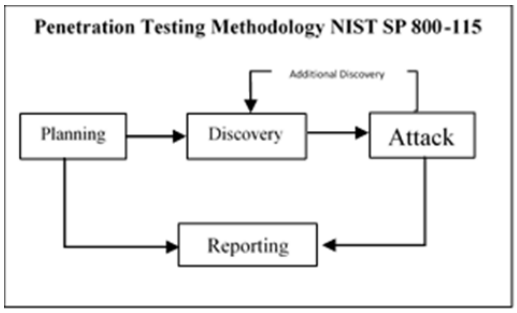


Figure 2. NIST SP 800-115 Method

Furthermore, after Penetration testing is carried out, Risk Branch will use the data obtained from the previous Security Assessment stage to see the risks of websites that have vulnerabilities using the OWASP Risk Rating Methodology.

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

Figure 3. Overvall Risk Severity OWASP

Risk Rating is needed so that the Bandung Regency Diskominfo can determine priorities in making improvements to websites that have vulnerabilities. The following is a picture of the analysis method that will be carried out in testing the subdomain to be tested

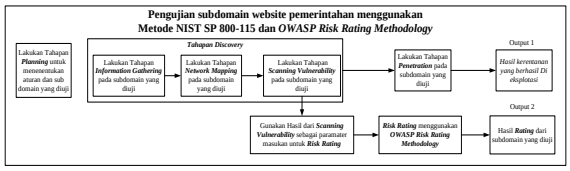


Figure 4. Analysis of Research Methods

2.2 Penetration Testing Analysis

As previously explained, the penetration testing method provided in NIST SP 800-115 consists of 4 stages, namely Planning, Discovery, Attack and Report. Each stage in this method is intended to assist testers in testing the website domain. Following are the steps taken in testing based on the NIST SP 800-115 Method.

1) Planning

In the planning phase there will be talks with parties from the Bandung District Diskominfo. This discussion was conducted to determine the process to be carried out in this study. The agreements that are successfully generated at this stage are as follows.

1. Identify Contacts of the Bandung District researchers and Diskominfo officers.
2. Confirm the scope of the research, approach and explanation of the NIST SP 800-115 method used in testing website vulnerabilities.
3. Approval of testing specific cases.
4. Submission of research results to the Bandung Regency Dikominfo which will be used to improve website applications.
5. Requesting data in the form of domains managed by Diskominfo Bandung Regency
6. Thus the planning stage has been completed and can enter the next stage.

2) Discovery

This phase can be done after the planning phase has been completed. In the Discovery phase information search and vulnerability will be conducted on the website being tested. These two stages are the Information Gathering and Vulnerability Scanning stages.

1. Information Gathering

In the Information Gathering phase, an information search will be conducted regarding the input data, namely the website domain that is suspected of having a vulnerability. The tools used in this phase are Whois Domain and Nmap (Network Mapping). This tool can be used on Windows and Linux platforms. Domain Whois is used in Information Gathering to find information related to the domain that is tested such as the name of the domain ordering, domain provider company, and when the domain was created. The following is a table of search results using the Whois Domain on the rsudcicalengka.bandungkab.go.id website subdomain:

bandungkab.go.id
Domain ID:PANDI-DO51853
Domain Name:BANDUNGKAB.GO.ID
Created On:14-Nov-2006 13:23:29 UTC
Last Updated On:08-Jan-2018 07:57:22 UTC
Expiration Date:31-Jan-2019 23:59:59 UTC
Status:ok
Registrant ID:elly7
Registrant Name:Elly Agustini
Registrant Organization:Kantor Pengolahan Data Elektronik
Registrant Street1:Jl. Raya Soreang Km. 17 Soreang Bandung
Registrant City:Kabupaten Bandung
Registrant State/Province:Jawa Barat
Registrant Postal Code:40911
Registrant Country:IDE
Sponsoring Registrar Organization:Kementerian Komunikasi dan Informatika
Sponsoring Registrar Street1:Jl. Medan Merdeka Barat No. 9
Sponsoring Registrar City:Jakarta Pusat
Sponsoring Registrar State/Province:Jakarta
Sponsoring Registrar Postal Code:10110
Sponsoring Registrar Country:IDE
Sponsoring Registrar Phone:622138433507
Sponsoring Registrar Website:domain.go.id
Name Server:DNS1.MASTERWEBNET.COM
Name Server:DNS2.MASTERWEBNET.COM
Name Server:DNS3.MASTERWEBNET.COM
Name Server:DNS4.MASTERWEBNET.COM

Figure 5. ***Result Whois Domain***

In Figure 4. Whois results Bandungkab.go.id Domain can be seen that when the domain Whois domain search for sub domain rsudcicalengka.bandungkab.go.id generated data leads to the main domain that is the website domain with the Bandungkab.go.i domain name, this happens because the sub domain of diskop.bandungkab.go.id is still united with the Bandungkab.go.id domain so that the domain appears in the Whois results is the Bandungkab.go.id domain.

Next is searching for information about Network Mapping using Nmap. Here are the results from Nmap for the rsudcicalengka.bandungkab.go.id domain

rsudcicalengka.bandungkab.go.id		
PORT	***STATUS***	***SERVICE***
21	Open	Ftp
53	Open	Domain
80	Open	Http
110	Open	Pop3
143	Open	Imap
443	Open	Ssl/http
587	Open	Smtp
993	Open	Ssl/imap
995	Open	Ssl/ipo3
3306	Open	MySQL

Figure 6. ***Scanning Nmap Result***

2. Vulnerability Scanning

After the Information Gathering stage is carried out, the next step is Vulnerability Scanning. At this stage, a website is being scanned for testing to see whether the website tested has a vulnerability or not, and how severe the vulnerability is. If there is a vulnerability, the tester will use the vulnerability to carry out the next test step.

The following are the results of testing using several vulnerability scanning tools, after scanning the domain rsudcicalengka.bandungkab.go id, it is known that the vulnerabilities contained in the subdomain are not exploited to the level of deface, but in one test domain with a discrete subdomain name .bandungkab.go.id has found a dangerous vulnerability, namely Sql injection.

3) Attack

Attack is one of the stages of the NIST SP 800-115 method to penetrate websites tested to see if the vulnerabilities found in the Discovery stage can be exploited and testers can get website access rights from the results of the penetration test. To start patching on the diskop.bandungkab.go.id website, a url that has SQL injection vulnerability is needed. The following are the vulnerability

parameters used in patching SQL injection using SQLmap.

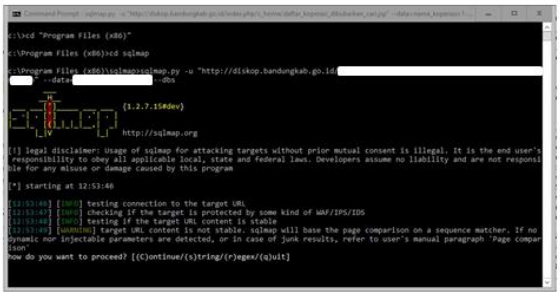


Figure 7. *Patching SQLmap*

From the results of patching obtained access rights from the diskop.bandungkab.go.id subdomain. the following is a view of the main page of diskop.bandungkab.go.id

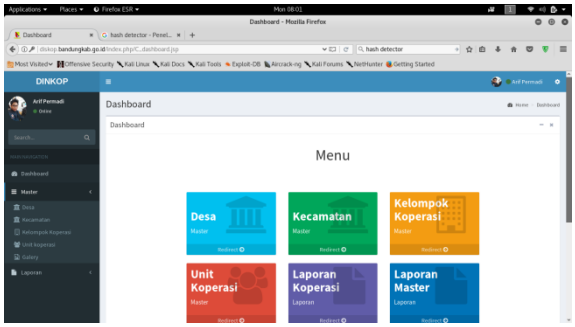


Figure 8. Admin Page

1) Report

Report is a report stage based on the process carried out in the previous chapter. Following are reports of vulnerabilities found

Tabel 1. *Reporting*

NO	Domain	*SQL injection*
1	diskop.badungkab.go.id	YA
2.	diskominfo.bandungkab.go.id	TIDAK
3.	rsudcicalengka.bandungkab.go.id	TIDAK
4.	kecamatan.cicalengka.bandungkab.go.id	TIDAK
5	kesehatan.bandungkab.go.id	TIDAK

Based on Table 1, Reporting can be concluded that a website with the domain name diskop.bandungkab.go.id has a high risk of vulnerability and further action is needed to deal with the vulnerability.

2.3 Hardware

In the Hardware Analysis section will be explained at least the hardware requirements needed to be able to build the system in this study

Table 2. Hardware Specifications

NO	Device Name	Spesifications
1	RAM	4 GB
2	Harddiks	125 GB
3	Proccesor	Core i3
4	Monitor	LCD
5	Maouse and Keyboard	Standar

2.4 Softwatre

In the Software Analysis section will be explained the minimal requirements of the software in order to be able to build the system and conduct research research.

Table 3.Software Spesifications

NO	Device name	Spesification
1	Operating system	Windows 10 and Kali Linux
2	Builder Application	Visual Studio 2016
3	Database	Xampp
4	Tools information gathering	Whois, Zenmap
5	Tools Vulnerability Scanning	Acunetix vulnerability Scanner Vega, Sniper

2.5 Method Implementation

Implementation Phase The method is the stage where a discussion is carried out on the implementation of the Method in the Government Website Vulnerability Report application at Diskominfo Bandung District which was built in this study. Following is the implementation of the NIST SP 800-115 method and the OWASP Risk Rating Methodology

Tabel 4. Method Implementation

No	Method	step	Information
1	*NIST SP 800-115*	*Planning*	Not implemented
		Discovery	Implemented
		Attack	Implemented
		Report	Implemented
2	*OWASP Riks Rating Methodology*	*Risk Rating*	Implemented

2.6 Interface Implementation

Interface implementation is done with each part of the program page created in the form of a program in accordance with the programming language used. The following is the implementation of the interface from the Government Website Vulnerability Report application at Diskominfo, Bandung District.

1) Add Domain Page

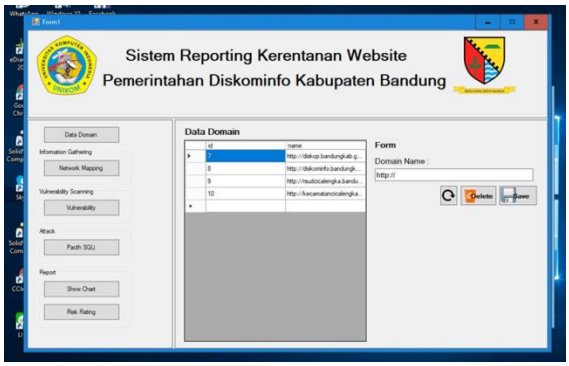


Figure 9. add domain page

2) Network Mapping page

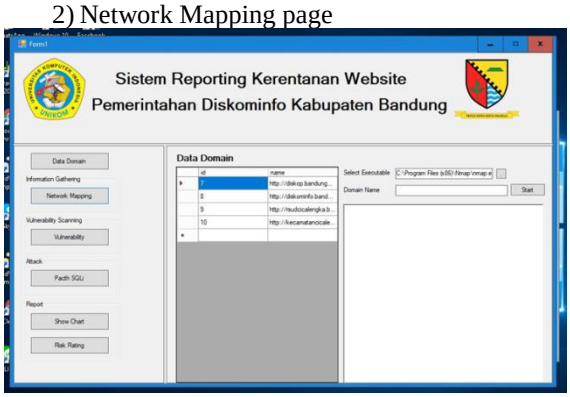


Figure 10. Network Mapping page

3) Vulnerability page



Figure 11.Vulnerability page

4) SQLi page

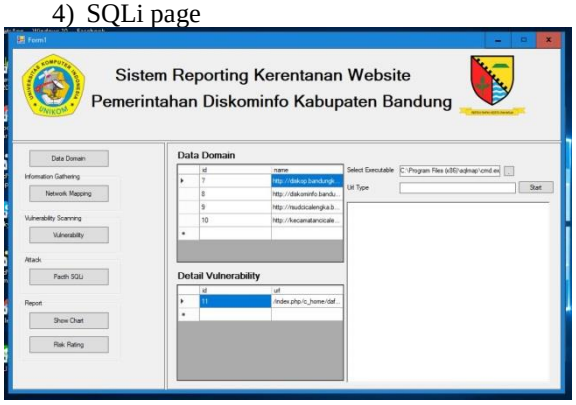


Figure 12. *Sqli page*

5) Chart Page

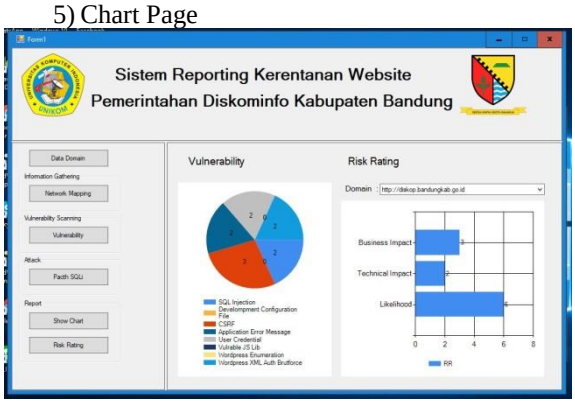


Figure 12. Chart page

6) Risk Rating page



Figure 12. Risk Rating Page

3. CLOSING

The following is the final part of the study which contains the conclusions and suggestions obtained.

3.1 Conculsion

Based on the results of the analysis and testing it can be concluded that the website security managed by Bandung Regency Diskominfo is vulnerable to SQL Injection vulnerabilities and can be easily exploited by irresponsible parties. So that anticipation is needed to overcome this vulnerability. Then after the application of the Government Website Vulnerability Report application in Diskominfo Bandung Regency was built as a means to help Diskominfo to display vulnerability reports, it can be concluded that:

1) After doing an analysis of the vulnerabilities found in the website managed by Diskominfo Bandung regency in the form of SQL injection vulnerability in http://diskop.bandungkab.go.id which is very dangerous and if successfully exploited the data is at risk of website access rights..
2) After a Security Assessment Test on a website managed by Diskominfo Bandung regency against vulnerabilities that have been analyzed previously, the exploitation data is obtained in the form of access rights on diskop.bandungkab.go.id subdomain, this is

very worrying and further action is needed to close the vulnerability.

3) After the Government Website Vulnerability Report application was built in Diskominfo Bandung Regency, Diskominfo can do a simple test and find out website vulnerability information in graphical form..

3.2 Suggestion

Application of Vulnerability Report The government website at Diskominfo Bandung Regency is not a perfect system. In the order to get satisfactory results, it is necessary to develop a system that is built. For the development of the Government Website Vulnerability Report application in Diskominfo Bandung Regency, there are several things that must be considered, namely:

1) Need to add additional support tools that are compatible with Windows OS, because the Government Website Vulnerability Report application in Diskominfo Regency Bandung is an application that runs on the OS Window platform.

2) Added a feature that can read the results of Scanning Vulnerability, so that users can directly enter data vulnerabilities without having to enter the data manually.

3) A similar application can be developed for the Linux OS platform, so that it can make it easier for users who use this OS, because the features provided by OS Linux are very complete.

BIBLIOGRAPHY

[1] H. Djanggih, "The Effectiveness of Law Enforcement on Child Protection for Cybercrime Victims in Indonesia," *IOP Conf. Series: Journal of Physics: Conf. Series 1028 (2018) 012192* , 2018.

[2] M. J. Islami, "TANTANGAN DALAM IMPLEMENTASI STRATEGI KEAMANAN SIBER NASIONAL INDONESIA DITINJAU DARI PENILAIAN GLOBAL CYBERSECURITY INDEX," no. Puslitbang Aptika dan IKP, Badan Litbang SDM, Kemenkominfo , 2017.

[3] "NIST," The National Institute of Standards and Technology (NIST), [Online]. Available: https://www.nist.gov/about-nist. [Diakses 18 Maret 2018].

[4] "Tupoksi Diskominfo," [Online]. Available: http://www.bandungkab.go.id/category/dinas-komunikasi-informatika-dan-statistik-. [Diakses 1 mei 2018].