SYSTEM MONITORING WEBSITE WITH ISSAF METHOD IN COMMUNICATION DEPARTMENT AND INFORMATICS OF TANGERANG DISTRICT

Jajang Ruhiyat[1], Angga Setiyadi[2]

[1,2] Universitas Komputer Indonesia
Jl. Dipatiukur No. 112-116, Bandung 40132
E-mail : jajangruhiyatif@gmail.com[1], angga.setyadi@email.unikom.ac.id[2]

ABSTRACT

Department of communication and Informatics Tangerang Regency is a government organization that manages information, financial data, and data management for each department involved. In performing the information management, there are concerns that allowing such information could fall to third parties. Thus the security of web applications is something that should be noted. given the large number of government organizations that use the system to make it easier to manage the data they have. Based on the number of illegal activities such as hacking to the Government-run organization, the existence of concerns against security systems they manage. This has resulted in such systems must be continually observed for each safety contained in it. Therefore testing against security systems need to be done in order to avoid the losses that might occur in the future. Testing against the security system using ISSAF methodology with the scope of the web application. The results of security testing on this system will be a table listing tests along with the vulnerability based on domain tested. And application of monitoring system based on method of ISSAF.

Keywords : ISSAF, OISSG, security assessment, system monitoring, penetration

1. INTRODUCTION

Department of communication and Informatics Tangerang (DISKOMINFO) stand since February 2014. A Government Organization that manages the operations of the communications and information generally use platform based website. With the website DISKOMINFO, the flow of communication, data management can be done online easily. As for the main function of the website at manage Office Communications and Informatics Tangerang Regency is as an online data management for each Department and as a provider of information services to the public government official about the activities conducted local government, became a benchmark of how active or whether the activities of the Government, and make it easier for people to get to know the figure of the leader of the Tangerang Regency using this website as a medium of information. But behind it all, the presence of a vulnerability found in the system/application in the manage Office Communications and Informatics Tangerang Regency. This can compromise the data and information that are open or not open.

Based on the results of the interview on October 2, 2017 together Mr. Cecep khaerudin one of the officers in the field of telematics service of communication and Informatics Tangerang Regency, he confirmed that earlier in the year 2016 there have been some attacks that resulted in the website's performance declined. And it takes about one month for the website to be recovered, in the process of maintenance is done at the end of may until mid-June 2016, he reiterates that there is some security gaps in the form of sql-injection, ddos XSS, it is known after the discovery of artifacts are the remains of the assault contained in the system database and high traffic contained on the portal site of the Department of communication and Informatics Tangerang Regency. A result of this attack a few admin account and the user loses the privilege (privilege) and portal sites must be closed for a while. Based on this Communication and Informatics Department party Tangerang Regency decided to add a security in the form of validation against a website that is hit in the year 2016 and several other websites, this is done in order to avoid the continuation of attacks that have already happened before. But despite the presence of a security that is already applied to the system in the service of communication and Informatics Tangerang Regency is not closing the possibility that there is still a gap – security gaps in the system that they manage, things like this It is still possible for an attacker to exploit loopholes to get illegal access to DISKOMINFO system into the Tangerang Regency.

Based on the results of the research can be elaborated that, needs to be done on the website

of the Communications Office of selftest and Informatics Tangerang Regency that will produce results in the form of a gap – cheklist security gaps are still present on the system. And also the implementation of monitoring systems based on the method of Information Systems Security Assessment Framework (ISSAF). ISSAF issued by Open Systems Security Information Group (OSSIG) is a structured framework that categorizes information system security assessment based on the domain search results and details of special testing or evaluation criteria for each domain.

Based on the problems experienced by the Department of Informatics and Komunikas Tangerang Regency is the need for a form of report of the test results, i.e. in the form of a security gap ceklist gap – which will be used for documentation in order for monitoring and increase security on the website DISKOMINFO Tangerang Regency.

1.1 Research Phase

Penetration method of Information System Security Assessment Framework (ISSAF) strung together to evaluate a network, the system to be tested. There are three phases in this method and there are nine steps in the assessment phase. The following are the stages of penetration test method based on the ISSAF can be seen in Figure 1 [1].

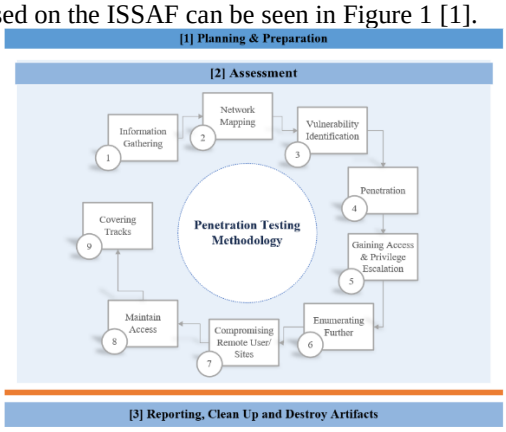


Figure 1. Penetration Testing Methodology

2. Content of Research

At this stage will discuss issues that will be analyzed, a general overview of the system, each stage of the process and the results of the research..

2.1 The type of vulnerability

Some of the attacks had a significant impact on a web application that can be detrimental to the owner of the website. The type of attack that includes :

a. SQL Injection

SQL Injection is a technique for exploiting a web page that uses the database such as MySQL (database) by giving the code into the SQL query. There are 3 different types of SQL Injection attacks using methods including the following :

- Error Based SQL Injection

Error Based SQL Injection exploits in doing into a web page that uses the database only displays error messages if the exploits successfully conducted, these error messages provide a variety of information such as the version of the database used, which can be exploited by the attacker.

- Union Based SQL Injection

The Union Based SQL Injection is a method of SQL Injection by using a UNION query command and combined it with some other queries such as SELECT commands to generate the desired information by the attacker.

- Blind SQL Injection

Blind SQL Injection attack using this type of method, it will not display the error message on the web page or not also display data or information is desirable, because the attack using Blind SQL Injection only produce condition True or False from a SQL query that is placed on a web page that is the target.

Based on the type of SQL Injection vulnerabilities each have a different impact – different, but in the end it always had the same result on the type of the vulnerability of SQL Injection is a technique for exploiting a web page that uses the database such as MySQL (the database) by giving the code into the SQL query. There are 3 different types of SQL Injection attacks using methods including the following: SQL Injection. Because of the existence of this vulnerability secret about the structure of the database or the data therein could be threatened, because an attacker could easily use this vulnerability to be able to get information about the database.

b. XSS (Cross Site Scripting)

XSS is one type of web attacks conducted by leveraging weaknesses and errors lies in the writing of scripting in a web application that allows a person to inject HTML tag or a Client Side Script on the web application due the variables not disanitasi properly. This XSS attacks from an attacker will try to get a right of access in the form of session cookies by having direct interaction with the victim (victim) with a variety of approaches such as social engineering. Because without any interaction with the victim, it is impossible for an attacker to be able to get a right of access to be used to infiltrate into the system.

c. DOS (Denial of service)

DOS (Denial of service) is a method to prevent the user to obtain the services provided by the server, with the hope that this method can be lethal

and menyibukan server by flooding the service on the server.

2.2 Proof of Concept Exploit

Proof of Concept Exploit or often called (PoC) is a type of attack on a computer system or network. This is done only to prove that all that can be done, and this generally does not cause any harm, but it shows how a hacker can exploit vulnerabilities in software or hardware may be [2].

2.3 Common Weakness Enumeration (CWE)

Common weakness enumeration is targeted for developers and security practitioners, is the official list of software weakness types that are used to:

1 Serve as a common language for describing software security weaknesses in terms of architecture, design, or code.
2 Serve as standards that became a benchmark of tools targeting software security weaknesses in the system.
3 Provides one standard base for identification of weaknesses, mitigation and prevention [3].

2.4 Nikto

Nikto is a free tools (opensource) which is in use for scanning a web application by using the CLI (command line interfaces) karna nikto developed using the programming language perl. Despite the absence of the user interface on the nikto but inside there are 6700 potential vulnerabilities file/program for testing. With the feature of auto scanning done nikto to find vulnerabilities automatically [4].

2.5 Web Application Security Assessment

The security of a web application is the security of all kompone – components that are used by the web application, the web server that is running the web application and modules – modules on the web server. All traffic on the point to the web server through the http/https protocol, which the traffic there is a trusted and some are not blocked by the firewall. Web servers are often targeted for attack targets [5].

a. Purpose
   To create a web application and web servers as secure as possible from attacks and shut down some information not in need, which will be difficult for attacker to be able to get the information.
b. Objective
   To get access to the remote machine by bypassing the firewall and the master jaringa. Collect what information from the network and servers.
c. Expected Result
   In General, any company or organization placing a firewall for security usually on port 80 to your webserver.
d. Pre-requisite
   Basik knowledge of the HTTP Protocol.

- Identifying web server vendor and version

The first step when doing an assessment of web applications is an application on the web server to identify what is running. To detect webser, things – things that need to be done i.e. :

1. Banner grabbing
2. Use automated means to detect web server
3. Default file detection
4. Check the file extension on the server

2.6 Kali Linux

Kali Linux is a distribution based on Debian GNU/Linux distribution for the purpose of digital forensics and is used for penetration testing, which is maintained and funded by Offensive Security. Time linux was developed by the developers of Backtrack earlier Die Aharoni together developers recently named Devon Kearns of Offensive Security [6]. In general the time linux has a variety of tools that can be divided into several kasifikasi based on its function :

1. Information Gathering used to gather information from a system
2. Reverse Enginerring used to analyze a system through the identification of components and linkages between the component and then make the abstraction and design of information systems which analyzed
3. Exploitation Tools used for mengekspoitasi gaps in a system.
4. Vulnerability Assessement used to perform the search, identification, calculation against the vulnerability of a system
5. Privilege Escalation is used to perform attacks that aim to raise the level of access within a system

2.4 Issue Analisys

Based on the results of the research that has been done in previous website explain that the Office of communications and Informatics Tangerang Regency have been exposed to attacks and cause a serious impact that diakibatan the attack. Therefore it needs to be done analysis of the website that is linked to the main domain Diskominfo. The analysis is done in reference to methods of Information System Security Assessment Framework (ISSAF), as for the analysis being performed will be divided into three stages in accordance with the method of ISSAF.

1) Planning and Preparation

At this stage the researcher will conduct meetings directly with one of the officers in the service of communication and Informatics Tangerang Regency to request approval to do research in the form of penetration testing research of the system the factory was built/developed by the Tangerang Regency DISKOMINFO, researcher at the meeting with the parties on the basis of consent do DISKOMINFO perindungan law together. As for the thing – the thing that becomes the topic of conversation at the time of the meetings between researchers with the Department of communication and Informatics Tangerang Regency is:

- Identification of contacts for both parties.
- Confirmation of the scope, approach and an explanation of the method.
- Approve the testing of specific cases.
- the end result of this study will be submitted to the repair process for the system.
- Do the request in the form of data in the form of the primary domain used.
- Outlines about the vulnerability and security on system before/after maintenance is done.

2) Assessment

a. Information gathering

Researchers collect information on domains that are targets in research. The information will be collected at this stage is whois domains and subdomains. The following is information based on domain whois info that can be seen in Figure 2.

tangerangkab.go.id	
WHOIS DOMAIN	Domain ID:PANDI-DO286393
	Domain Name:TANGERANGKAB.GO.ID
	Created On:19-Aug-2007 13:35:21 UTC
	Last Updated On:23-Jul-2017 03:57:05 UTC
	Expiration Date:29-Aug-2019 23:59:59 UTC
	Status:ok
	Registrant ID:abualw-4263
	Registrant Name:Abu Alwakiel
	Registrant Organization:DISKOMINFO Kabupaten Tangerang
	Registrant Street1:Jl. Somawinata No.1
	Registrant City:Kabupaten Tangerang
	Registrant State/Province:Banten
	Registrant Postal Code:15710
	Registrant Country:ID
	Registrant Phone:+62.81285920614
	Registrant Email:isa.lpse@gmail.com
	Sponsoring Registrar ID:H4964483
	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:ID
	Sponsoring Registrar Phone:622138433507
	Sponsoring Registrar Website:domain.go.id
	Name Server:NS1.DESIBLE.NET
	Name Server:NS2.DESIBLE.NET
	Name Server:DNS1.DESIBLE.NET
	Name Server:DNS2.DESIBLE.NET
	DNSSEC:Unsigned

Figure 2. Whois domain info

Then the subdomain information obtained can be seen in Figure 3.

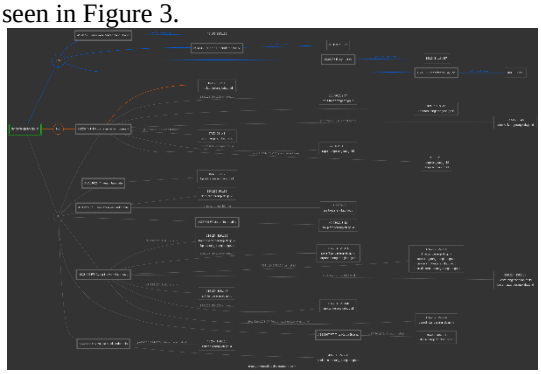


Figure 3. Subdomain

b. Network mapping

The results of testing network-mapping to one DISKOMINFO party-run domain, the results can be seen in table 1.

Table 1. Network mapping

sakip.tangerangkab.go.id		
PORT	**STATUS**	**SERVICE**
21	Open	ftp
80	Open	http
1922	Open	ssh
3306	Open	MySQL
5432	Open	Postgresql
25	Filtered	smtp

c. Vulnerability identification

At this stage the examiners try to identify kerentanna in one of the domains that were tested. As for the test results can be seen in table 2.

Table 2.vulnerability identification

Sakip.tangerangkab.go.id:80		
Vulnerability Type	**Parameter**	**Method**
BlindSQL Injection	filter	POST
SQL Injection	filter	POST
	/	GET
CrossSiteScripting (XSS)	filter	POST
	Gallery()	GET
	Peraturan()	GET
ApplicationError message	Host	GET
	filter	POST
Host header attack	Host	GET

d. Penetration

At this stage the researcher will conduct security testing system based on data obtained from the results of the analysis. testing ditahap is divided into two SQL injection vulnerability testing by using the filter parameter, payload "' SQLinjection" as the input ditahap SQLinjection testing. And cross site scripting (XSS) with the

parameters that are contained in the event onclick i.e. gallery (), payload "alert (' XSS PoC ')". Testing for SQL injection vulnerabilities can be seen in Figure 4.

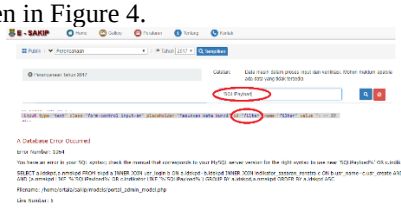


Figure 4. Sql injection

Then test against cross site scripting vulnerability can be seen in Figure 5.

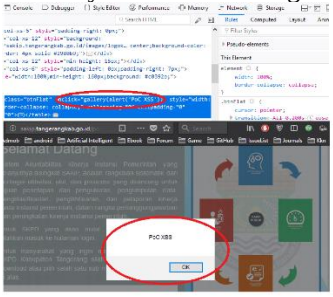


Figure 5. Cross site scripting

e. Gaining access & privilege escalation

At this stage it is a process that allows testers to get an account is not valid. As for the process to get that account will be split into two parts with the proof of concept (PoC) SQL injection and cross site scripting (XSS). For testing against SQL injection PoC can be seen in Figure 6.

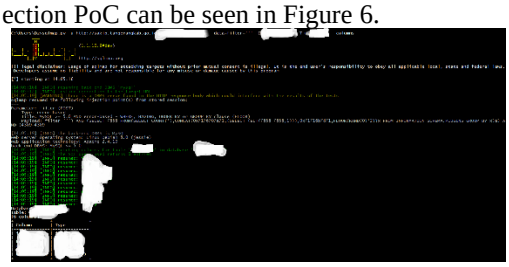


Figure 6. PoC SQL injection

And testing the PoC XSS can be seen in Figure 7.

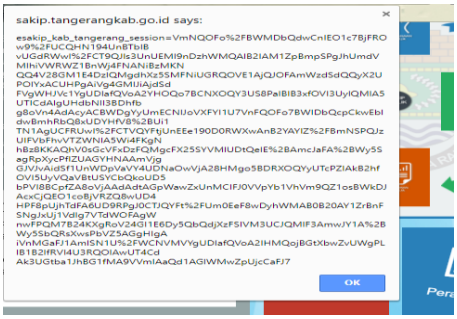


Figure 7. PoC XSS

f. Enumerating further

At this stage the testers will store data in the form of session cookies, the user dump & pass. Data results dump can be seen in Figure 8.

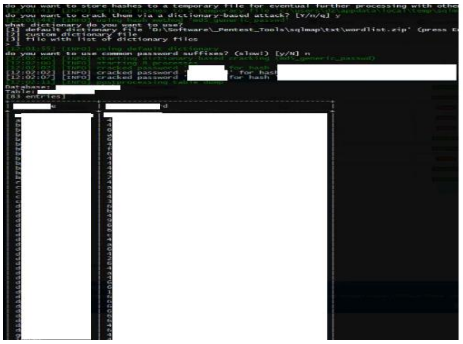


Figure 8. Dump process

g. Compromise remote user/sites

Exploitable relationship connections between the remote user and enterprise users (researchers). Based on the data already obtained make it possible for researchers to enter into the system being tested. Display intrusion into the system can be seen in Figure 9.



Figure 9. Login access

h. Maintain access

By using something like the backdoor, to still be able to get into the system that's been exploitable.

i. Covering tracks

remove all traces in a way to hide files, delete log, avoid checking the integrity and antivirus.

3) Reporting, clean-up and destroy artefacts

a Reporting

After completing all the tests that are in scope, wrote a report that describes the results of the test and complete a presentation already in being prepared with recommendations and solutions. As for things – things that became the topic of the report include:

- Management Summary

  Based on the research that has been conducted from the early stages to the final stages, there are two vulnerabilities that are very fatal berletak on four websites from seven websites that have been tested. The vulnerability is SQLInjection and Cross Site Scripting. number of in scope the domain has been approved at the time of the interview process there are 35 parties managed domain service of communication and Informatics Tangerang Regency.

Based on the results of a test of penetration was done starting from the analysis stage up to implementation, then the conclusions of this research are as follows.

a Deliver reports in the form of vulnerability – the vulnerability based on a managed domain Service-party communication and Informatics Tangerang Regency.

b This report can be a reference point against the vulnerabilities of the system that occurred in the Department of communication and Informatics Tangerang Regency.

Based on the testing that's been researched there is a vulnerability in the form of cross site scripting vulnerability id with CWE-79 and SQLi vulnerabilities with id CWE-89, and this is very worrying for the data contained therein. The vulnerability ID is taken from the website cwe.mitre.org which is one of the site's provider of common weakness enumeration, the site serves as a reference point against the vulnerabilities that are examined.

Based on the results of the research, the advice given to avoid XSS vulnerability researchers that have id CWE-79 that is by paying attention to all the potential areas of input (input) that are on the system such as: parameters, variables, cookies, request header, the components of the URL, file, filename and all sorts of external data that is associated with the system.

Berdasrkan research results, the advice given to avoid vulnerability researcher SQLi which has id CWE-89 is to do whitelist input (input) against a given, and blacklist all kinds of input (input) which allows can changing the standard of entries has been given.

- Scope Of The Project

  The scope of the project is the report regarding the scope taken researchers. The scope itself is actually already taken investigators based on consent of the parties and in the test. As for the scope taken researchers is a web application. And scope the domain based on data already provided by the Office of communications and Informatics Tangerang Regency.

- Vulnerability Scan Reports

  Vulnerability scan reports are reports based on process analysis on phase two methods ISSAF coupled with implementation has been done. Because testing vulnerabilities based on the results of the scan are very important for the Parties reported to the DISKOMINFO. Here is the report in the form of a table that contains domains and accompanied by the value of the vulnerability that there is/is not in a domain that was tested in the study, the value of the vulnerability is taken from there cwe.mitre.org. the site is one of the recommendations of the assessment of the vulnerabilities contained in modules ISSAF. As for the table reports the vulnerability can be seen in table 4.

Table 4. Vulnerability scann report

CommonWeaknessEnumeration	**CWE 79**	**CWE 89**
Domain	xss	sqli
lpse.tangerangkab.go.id:443	✓	✓
mail.dinkes.tangerangkab.go.id:80	x	✓
sakip.tangerangkab.go.id:80	✓	x
Sikda.dinkes.tangerangkab.go.id:80	x	x
Sitt.dinkes.tangerangkab.go.id:80	✓	✓
Bpkad.tangerangkab.go.id:80	x	x
koperasi.tangerangkab.go.id	x	x
Sipinter.tangerangkab.go.id:80	x	✓

- Exploit Report

  Exploit report is a section where researchers reported each stage is done successfully or not based on a diguanakan tools for research in progress. The following is an exploit report based on the domain – the domain that already finished researched. The shape of the exploit report can be seen in Figure 10.

Domain	**sakip.tangeragkab.go.id:80**		
Tahapan	**Source**	**Tools**	**Status**
Information gathering	Domain Info	whois	✓
	Subdomain info	dnsdumpster	✓
Network Mapping	Port Mapping	zenmap	✓
Vulnerability Identification	Web Scanner Vulnerability	acunetix	✓
		vega	✓
		nikto	✓
Penetration	Cross Site Scripting	Browser (Chrome,Firefox)	x
	Sql Injection		x
Gaining Access & Privilege Escalation	Cross Site Scripting	Burpsuite	x
	Sql Injection	Sqlmap	x
Enumerating Further	Cross Site Scripting	Burpsuite	x
Compromising Remote User/Sites	Sql Injection	Sqlmap	x
Maintain Access	Backdoor	php rootkit	x
Covering Tracks	Backdoor	php rootkit	x

Figure 10. Exploit Report

b Clean-up and destroy artefacts

All information that is created is stored on/test system should be deleted from the system, if it can not be done with the remote system then it should at notify the Government of Tangerang Diskominfo, so that IT staff can directly delete such information After the report on the receipt of such parties.

Based on the research that has been done, the researchers will report all sorts of artefacts that are embedded during the pengujain on the system

takes place. As for the form of the report concerning the artefacts will be shown on table 5

Table 5. Artefacts

Domain	Type	Name
sitt.dinkes.tangerangkab.go.id	user/pass	4****/4****
sakip.tangerankab.go.id	user/pass	4****/4****

2.6 Analysis Hardware

The hardware specifications used in the construction of the monitoring system:

Table 6. Hardware Requirements Analysis System Development

Hardware	Spec
Processor	Intel Core i3
RAM	2 GB
Harddisk	160 GB

2.7 Needs Analysis Software

The following is the analysis of the needs of the software of the system to be built. Specifications for the developer of software used in building educational games is a proverb :

Table 7. Needs Analysis Software

Software	Spec
Operating System	Windows / linux
Python	The Python interpreter is used as the programming language used. In this study using python 2.7
perl	Used as interpreters for the bundle of opensource nikto.
Hackertarget api	Used for A P I in the process of information gathering
Nikto	Used to process the identification of vulnerabilities

2.8 Perancangan Struktur Menu

In the design of the menu structure using an automated process for researchers every process contained therein. Just before the process required input in the form of the domain that will be tested.

1. Domain input stage can be seen in Figure 11.

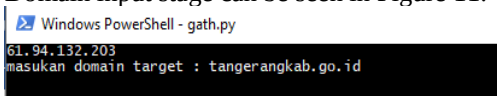


Figure 11.input domain

2. Domain whois scanning stage can dililhat in Figure 12.



Figure 12.whois test

3. Tahap tracert dapat dilihat pada gambar 13.



Figure 13. tracert

4. Tahap DNSLookup dapat dilihat pada gambar 14.



Figure 14.DNS Lookup

5. Open port phase can be seen in Figure 15.

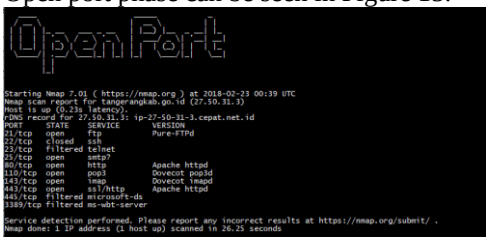


Figure 15. Open port

6. Open port phase can be seen in Figure 15.



Figure 16. Vulnerability identification test

3. CLOSING

3.1 Conclusion

Based on the results of the analysis and testing of web security can be concluded that the application on the website DISKOMINFO Tangerang Regency is vulnerable to an attack that be bad for the system they manage. This looks at the vulnerability of SQL injection and Cross Site Scripting, which allows for an attacker to take over DISKOMINFO party-run system.

3.1 Suggestions

The following are suggestions – advice given researchers based on research on the website DISKOMINFO Kab. Tangerang.

1. Do penetration testing against the website DISKOMINFO then gives reports the results of the analysis and implementation has been done on this phase of the assessment method ISSAF.
2. Provide recommendations for tackling common weakness enumeration value based (CWE), in order to menganggulangi a vulnerability found in the system DISKOMINFO.

BIBLIOGRAPHY

[1] OISSG, “Penetration Testing Metodology”, p 136, 04 September 2005, 2005..

[2] ”Definition of: PoC exploit”,[Online]. Available:https://www.pcmag.com/encyclopedia/term/58148/poc-exploit. [Accessed 05 February 2018].

[3]”CommonWeaknessEnumeration”,[Online].Available:https://cwe.mitre.org/about/index.html.[Accessed 15 Februari 2018]

[4]“Nikto”,[Online].Available:https://cirt.net/Nikt2. [Accessed 16 October 2017]

[5]OISSG, ”Web Application Security Assessment”,p 719, 04 September 2005, 2005.

[6]Angga Setyadi, Implementasi Modul Network MITM Pada Websploit sebagai Monitoring Aktifitas Pengguna dalam Mengakses Internet, Bandung: Prosiding Seminar Nasional Komputer dan Informatika (SENASKI) , 2017.