ANALISIS KERENTANAN *WEBSITE* MENGGUNAKAN METODE NIST SP 800-115 DAN OWASP DI DISKOMINFO KABUPATEN BANDUNG

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]

ABSTRAK

Saat ini perkembangan teknologi di bidang informasi telah merambat ke pelosok bagian di tanah air, baik di desa, kecamatan, kabupaten dan kota sudah mulai memiliki divisi yang menerapkan sistem penyebaran informasi kepada masyarakat dengan menggunakan *website* dan salah satu pihak yang bertanggung jawab di dalam pelayanan penyebaran informasi di Kabupaten Bandung adalah Diskominfo. Diskominfo Kabupaten Bandung merupakan salah satu perangkat kerja daerah yang dimiliki Pemerintah Kabupaten Bandung yang berfokus pada layanan informasi TIK, layanan E-*Government* dan layanan statistik dan persandian. Namun demikian dengan digunakannya *website* sebagai media pelayanan informasi masyarakat oleh pemerintah, telah terjadi kasus eksploitasi terhadap salah satu *website* yang dikelola oleh pihak Diskominfo Kabupaten Bandung yang menimbulkan kerugian dan terganggunya pelayanan informasi yang disediakan pihak Diskominfo Kabupaten Bandung. Maka dari itu di lakukan analisis dan pengujian pada kerentanan *website* menggunakan Metode NIST SP 800-115 dan OWASP. Hasil dari analisis dan pengujian ini akan diterapkan dalam sebuah aplikasi *reporting* yang diharapkan dapat membatu pihak Diskominfo Kabupaten Bandung untuk mengelola website yang memiliki kerentanan..
Kata kunci : NIST SP 800-115, *OWASP Risk Rating Methodology*, uji penetrasi, kerentanan *website*, *Reporting*.

1. PENDAHULUAN

Dinas Komunikasi, Informatika dan Statistika Kabupaten Bandung merupakan sebuah instansi yang bertanggung jawab atas pengolahan informasi di lingkungan kabupaten Bandung. *Website* pun merupakan kebutuhan yang sangat penting di instansi pemerintah khususnya Dinas Komunikasi, Informatika dan Statistika Kabupaten Bandung. Dengan di tersedianya *website* Pemerintahan alur Komunikasi dan transaksi antara masyarakat dan pemerintah dapat dilakukan dengan mudah.

Namun dengan semakin banyaknya fasilitas *website* yang disediakan untuk mendukung program kerja Diskominfo Kabupaten Bandung dalam melayani masyarakat, Ancaman akan kejahatan dunia maya pun menjadi salah-satu masalah yang harus dihadapi secara seksama. Berdasarkan data yang di dapat dari *Indonesia Security Incident Response Team on Internet and Infrastructure/Coordination Center* (*Id-SIRTII/CC*) yang merupakan badan yang dibentuk untuk melakukan pengawasan keamanan jaringan telekomunikasi berbasis protokol internet. Diketahui dari data yang diolah oleh Direktorat *Cyber Crime* Indonesia kasus *Cyber Crime* yang terjadi di Indonesia pada tahun 2016 adalah 2880 kasus [1]. Dampak kejahatan di dunia maya yang mempengaruhi sektor ekonomi berdasarkan data dari Norton *Symantec* selama tahun 2015 sampai dengan Februari 2016 di Indonesia menimbulkan total kerugian Rp 194.6 miliar [2]. Oleh karena itu penanggulangan terhadap Cyber Crime perlu ditanggulangi secara seksama.

Berdasarkan hasil wawancara dengan pihak dari Dinas Komunikasi, Informatika dan Statistika Kabupaten Bandung, bidang TIK bagian Keamanan Informasi, beliau menegaskan bahwa sudah pernah terjadi Cyber *Attack* yang di lakukan terhadap website Pemerintahan Kabupaten Bandung. Eksploitasi ini

terjadi 2 kali di tahun 2017 dengan tipe eksploitasi berupa *web deface*, diduga penyerangan ini dilakukan individual untuk melakukan eksploitasi dan menampilkan *skill* yang dimiliki para penyerang dalam menyerang website yang rentan akan eksploitasi, sehingga dibutuhkannya analisis kerentanan pada website yang dikelola oleh Dinas Komunikasi, Informatika dan Statistika Kabupaten Bandung, dengan tujuan agar dapat mengetahui kerentanan yang terdapat pada *website* tersebut, sehingga dapat mengurangi penyerangan terhadap website yang dikelola Diskominfo Kabupaten Bandung dan. National Institute of *Standards* and Technology (NIST) merupakan badan non-regulator dan bagian ari administrasi teknologi dan departemen perdagangan Amerika Serikat. Misi dari organisasi ini adalah untuk membuat dan mendorong pengukuran , standar dan teknologi untuk meningkatkan produktivitas, mendukung perdagangan dan kualitas hidup. Empat bidang

utama organisasi ini adalah bioteknologi, nanoteknologi, teknologi informasi dan manufakturing moderen. NIST mengeluarkan beberapa seri publikasi yang ditujukan ke keempat bidang tersebut dan salah satunya yang menjurus ke dalam bidang teknologi informasi adalah NIST SP 800-115 *Techincal Guide to Information Security Testing and Assessment*, metodologi yang dikhususkan untuk membatu organisasi dalam melakukan perencanaan tes keamanan informasi [3].

Berdasarkan masalah yang terjadi di Dinas Komunikasi Dan Informatika Kabupaten Bandung maka dilakukan penelitian dengan judul "Analisis Kerentanan *Website* Menggunakan Metode NIST SP 800-115 dan OWASP di Diskominfo Kabupaten Bandung" dengan harapan dapat membatu membantu menanggulangi penyerangan terhadap website yang dikelola oleh Dinas Komunikasi, Informatika dan Statistika Kabupaten Bandung.

2. ISI PENELITIAN

Pada tahapan ini akan dilakukan pembahasan mengenai masalah yang ditemukan, hasil analisis, gambaran umum sistem dan proses-proses yang akan dilakukan di dalam penelitian ini .

2.1 Analisis Masalah

Seperti yang telah diketahui pada pembahasan sebelum dalam pendahuluan, telah terjadi kasus penyerangan terhadap website pemerintahan yang diawasi oleh Diskominfo Kabupaten Bandung. Eksploitasi ini terjadi pada domain *website* rsud.cicalengka.bandungkab.go.id dengan tipe eksploitasi yang diterima berupa *deface*.

Dengan terjadinya penyerangan pada salah satu domain website yang diawasi oleh Diskominfo Kabupaten Bandung, maka domain *website* pemerintahan lainya yang masih berada di dalam pengawasan Diskominfo Kabupaten Bandung memiliki potensi untuk terkena eksploitasi yang sama. Hal

ini dapat diketahui karena masih terdapat beberapa domain website di bawah pengawasan Diskominfo Kabupaten Bandung yang belum di uji kerentanannya.

Selain itu pihak Diskominfo Kabupaten Bandung belum memiliki panduan dalam menangani website yang terkena eksploitasi. Sehingga dibutuhkan panduan yang dapat digunakan apabila terjadi eksploitasi pada *website* pemerintahan lainya. Salah satu solusi yang dapat dilakukan adalah dengan melakukan *Security Assessment dan Penetration Testing* untuk menguji apakah website pemerintahan memiliki kerentanan dan dapat di eksploitasi. Dengan demikian setelah diketahui bahwa website yang diuji memiliki kerentanan dan dapat di eksploitasi, maka pihak Diskominfo Kabupaten Bandung dapat melakukan perbaikan guna menutup kerentanan yang ditemui.

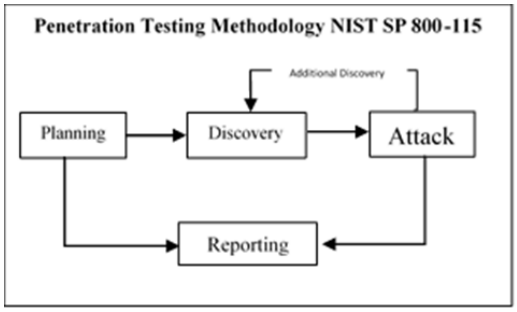
Berikut ada domain yang akan diuji di dalam penelitian ini

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

Gambar 1. Domain yang diuji

2.2 Analisis Metode

Pada penelitian ini Analisis Metode dilakukan analisis terhadap metode yang akan digunakan di dalam penelitian ini. Metode yang digunakan untuk *Security Assessment* dan *Penetration Testing* mengacu pada dokumen yang dikeluarkan oleh *National Institute of Standar and Technology (NIST)* dengan kode dokumen NIST SP 800-115. Dokumen NIST SP 800-115 menyediakan metode yang dapat digunakan untuk melakukan *Penetration Testing* beserta *tools-tools* pendukung yang dapat digunakan untuk melalukan *Security Assessment*.



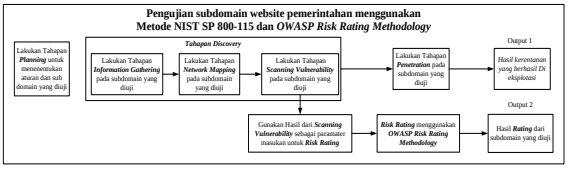
Gambar 2. Metode NIST SP 800-115

Selanjutnya setelah dilakukan *Penetration testing* maka akan dilakukan *Risk Ranting* menggunakan data yang didapat dari tahap Security Assessment sebelumnya untuk melihat risiko dari website yang memiliki kerentanan menggunakan *OWASP Risk Rating Methodology*.

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

Gambar 3. Overvall Risk Severity OWASP

Risk Rating ini dibutuhkan agar pihak Diskominfo Kabupaten Bandung dapat menentukan prioritas dalam melakukan perbaikan terhadap website yang memiliki kerentanan. Berikut merupakan gambar dari analisis metode yang akan dilakukan dalam pengujian subdomain yang akan diuji



Gambar 4. Analisis Metode Penelitian

2.2 Analisis Pengujian Penetrasi

Seperti yang telah dijelaskan sebelumnya, metode *penetration testing* yang disediakan di dalam NIST SP 800-115 terdiri dari 4 tahap yaitu *Planning*, *Discovery*, *Attack* dan *Report*. Setiap tahapan di dalam metode ini dimaksudkan untuk membantu penguji dalam melakukan pengujian terhadap domain website. Berikut langkah-langkah yang dilakukan dalam pengujian berdasarkan Metode NIST SP 800-115

1) Planning

Pada fase *planning* akan dilakukan pembicaraan dengan pihak dari Diskominfo Kabupaten Bandung. Pembicaraan ini dilakukan untuk menentukan proses yang akan dilakukan di dalam penelitian ini. Kesepakatan yang berhasil dihasilkan pada tahap ini adalah sebagai berikut.

1. Identifikasi Kontak peneliti dan petugas Diskominfo Kabupaten Bandung.
2. Konfirmasi ruang lingkup penelitian, pendekatan dan penjelasan metode NIST SP 800-115 yang digunakan dalam pengujian kerentanan website.
3. Persetujuan pengujian kasus spesifik.
4. Penyerahan hasil penelitian kepada pihak Dikominfo Kabupaten Bandung yang akan digunakan untuk perbaikan aplikasi website .
5. Melakukan permintaan data dalam bentuk domain yang di kelola oleh Diskominfo Kabupaten Bandung
6.

Dengan demikian tahapan *planning* telah selesai dilaksanakan dan dapat masuk ke tahap selanjutnya.

2) Discovery

Fase ini dapat dilakukan setelah tahapan *planning* telah selesai dilaksanakan. Dalam tahap Discovery akan dilakukan pencarian informasi dan kerentanan pada website yang diuji. Kedua tahapan ini adalah tahapan *Information Gathering* dan *Vulnerability Scanning.*

2. *Information Gathering*

Dalam fase Information *Gathering* akan dilakukan pencarian informasi terkait data masukan yaitu domain website yang diduga memiliki kerentanan. *Tools* yang digunakan dalam fase ini adalah *Whois* Domain dan Nmap *(Network Mapping). Tools* ini dapat digunakan di dalam platform Windows maupun *Linux*. *Whois* domain digunakan dalam *Information Gathering* untuk menemukan informasi terkait dengan domain yang diuji seperti nama pemesan domain, perusahaan penyedia domain, dan kapan domain tersebut dibuat. Berikut merupakan tabel hasil pencarian menggunakan Whois Domain pada subdomain *website* rsudcicalengka.bandungkab.go.id :

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

Gambar 5. ***Hasil Whois Domain***

Pada gambar 4.hasil Whois Domain bandungkab.go.id dapat diketahui bahwa saat dilakukan pencarian pada Whois domain untuk sub domain rsudcicalengka.bandungkab.go.id data yang dihasilkan mengarah pada domain utama yaitu domain *website* dengan nama domain Bandungkab.go.i, hal ini terjadi karena sub domain diskop.bandungkab.go.id masih satu kesatuan dengan domain Bandungkab.go.id sehingga domain muncul dalam hasil Whois adalah domain Bandungkab.go.id.

Selanjutnya dilakukan pencarian informasi mengenai *Network Mapping* menggunakan Nmap. Berikut hasil dari Nmap untuk domain rsudcicalengka.bandungkab.go.id

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

Tabel 6. *Hasil Scanning Nmap*

2. *Vulnerabiliti Scanning*

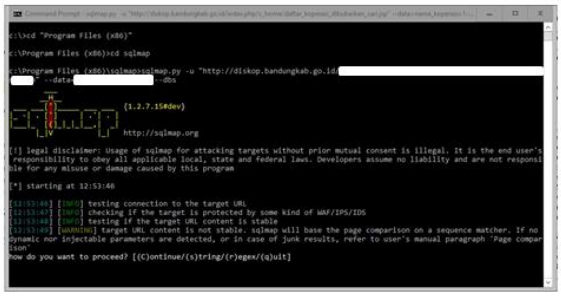
Setelah dilakukan tahapan *Information Gathering* tahapan selanjutnya *Vulnerability Scanning*, pada tahapan ini dilakukan pemindaian terhadap website yang akan diuji untuk melihat apakah website yang diuji memiliki kerentanan atau tidak, dan seberapa parah kerentanan yang dimiliki oleh website tersebut. Bila mana terdapat kerentanan maka penguji akan menggunakan kerentanan tersebut untuk melakukan langkah pengujian selanjutnya.

Berikut merupakan hasil dari pengujian menggunakan beberapa *tools vulnerability scanning*, setelah dilakukan scanning pad domain rsudcicalengka.bandungkab.go id, diketahui bahwa kerentanan yang terdapat pada subdomain tersebut tidak di eksploitasi hingga ke tingkat *deface*, namun pada salah-satu domain uji dengan nama subdomain diskop.bandungkab.go.id telah ditemukan kerentanan yang berbahaya yaitu *Sql injection.*

3) Attack

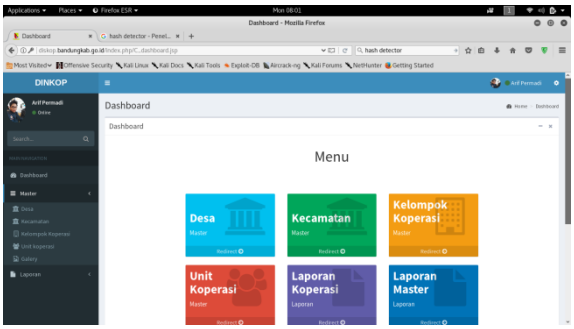
Attack merupakan salah satu tahapan dari metode NIST SP 800-115 untuk melakukan penetrasi terhadap *website* yang diuji guna melihat apakah kerentanan yang ditemukan pada tahap Discovery dapat di eksploitasi dan dapatkah penguji untuk mendapatkan hak akses *website* dari hasil uji penetrasi tersebut.

Untuk memulai *patching* pada *website* diskop.bandungkab.go.id dibutuhkan url yang memiliki kerentanan *SQL injection*. Berikut merupakan parameter kerentanan yang digunakan dalam *patching* SQL *injection* menggunakan *SQLmap*.



Gambar 7. *Patching SQLmap*

Dari hasil *patching* didapat hak akses dari subdomain diskop.bandungkab.go.id . berikut merupakan tampilan dari halaman utama diskop.bandungkab.go.id



Gambar 8. Halaman Admin

4) Report

Report merupakan tahapan laporan berdasarkan proses yang dilakukan pada bab sebelumnya. Berikut merupakan laporan dari kerentanan yang ditemukan.

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

Berdasarkan Tabel 1 *Reporting* dapat disimpulkan bahwa *website* dengan nama domain diskop.bandungkab.go.id memiliki risiko kerentanan tinggi dan diperlukan tindakan lanjut untuk menangani kerentanan tersebut.

2.3 Perangkat Keras

Pada bagian Analisis Perangkat Keras akan dijelaskan minimal kebutuhan perangkat keras yang dibutuhkan untuk dapat membangun sistem didalam penelitian ini

Tabel 2. Spesifikasi Perangkat Keras

NO	Nama Perangkat	Spesifikasi
1	RAM	4 GB
2	Harddiks	125 GB
3	Proccesor	Core i3
4	Monitor	LCD
5	Maouse dan Keyboard	Standar

2.4 Perangkat Lunak

Pada bagian Analisis Perangkat Lunak akan dijelaskan kebutuhan minimal dari perangkat lunak agar dapat membangun sistem dan melakukan penelitian penelitian ini.

Tabel 3. Spesifikasi Perangkat Lunak

NO	Nama Perangkat	Spesifikasi
1	Sistem Operasi	Windows 10 dan 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 Implementasi Metode

Tahap Implementasi Metode merupakan tahapan di mana dilakukan pembahasan mengenai tercapainya implementasi Metode di dalam aplikasi *Report* Kerentanan *Website* pemerintah di Diskominfo Kabupaten Bandung yang dibangun dalam penelitian ini. Berikut implementasi metode *NIST SP 800-115* dan OWASP *Risk Rating Methodology*

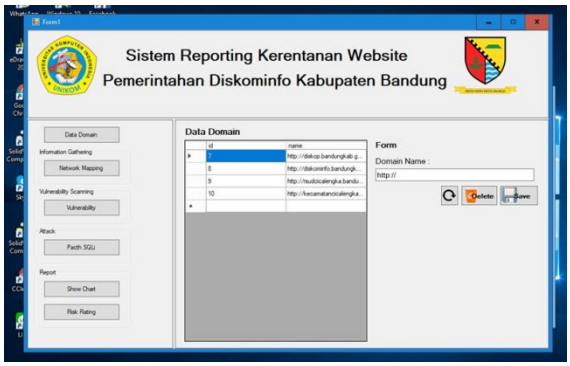
Tabel 4. Implementasi Metode

No	Metode	Tahap	Keterangan
1	*NIST SP 800-115*	*Planning*	Tidak diimplementasikan
		Discovery	Diimplementasikan
		Attack	Diimplementasikan
		Report	Diimplementasikan
2	*OWASP Riks Rating Methodology*	*Risk Rating*	Diimplementasikan

2.6 Implementasi Antarmuka

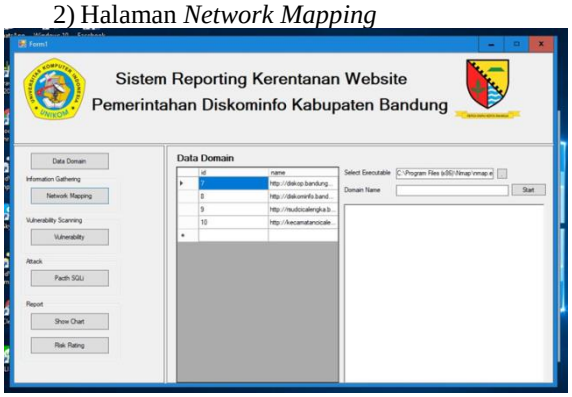
Implementasi antarmuka di lakukan dengan setiap bagian halaman program yang dibuat dalam bentuk program sesuai dengan bahasa pemograman yang digunakan. Berikut ini adalah implementasi antarmuka dari aplikasi *Report* Kerentanan *Website* pemerintah di Diskominfo Kabupaten Bandung.

1) Implementasi Halaman Tambah Domain



Gambar 9. Halaman tambah domain

2) Halaman *Network Mapping*



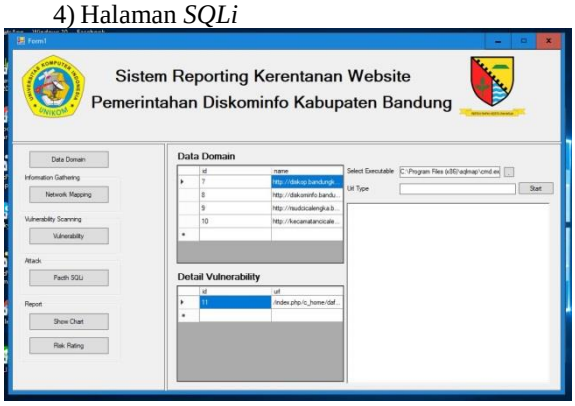
Gambar 10. Halaman *Network Mapping*

3) Halaman *Vulnerability*



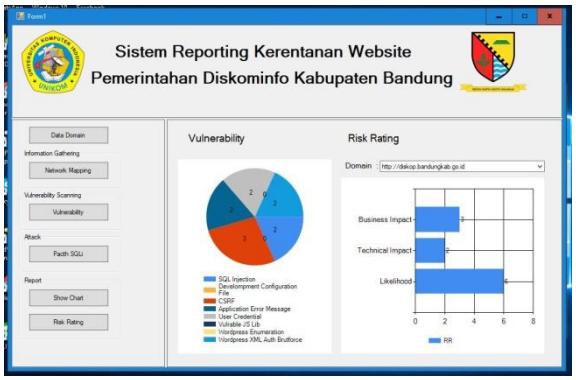
Gambar 11. Halaman *Vulnerability*

4) Halaman *SQLi*



Gambar 12. Halaman *Sqli*

5) Halaman Grafik



Gambar 12. Halaman *Grafik*

6) Halaman *Risk Rating*



Gambar 12. Halaman *Risk Rating*

3. PENUTUP

Berikut merupakan bagian akhir dari penelitian yang berisikan kesimpulan serta saran yang didapat.

3.1 Kesimpulan

Berdasarkan hasil analisis dan pengujian dapat disimpulkan bawa keamanan *website* yang dikelola oleh Diskominfo Kabupaten Bandung rentan terhadap kerentanan *SQL Injection* dan dapat dengan mudah di eksploitasi oleh pihak yang tidak bertanggung jawab. Sehingga diperlukan antisipasi untuk menanggulangi kerentanan tersebut. Kemudian setelah dibangunnya aplikasi *Report* Kerentanan *Website* pemerintah di Diskominfo Kabupaten Bandung sebagai sarana yang membantu pihak Diskominfo untuk menampilkan laporan kerentanan maka dapat disimpulkan bahwa :

1) Setelah dilakukan Analisis terhadap kerentanan yang ditemukan dalam *website* yang dikelola oleh Diskominfo Kabupaten Bandung berupa kerentanan *SQL injection* pada http://diskop.bandungkab.go.id yang sangat berbahaya dan jika berhasil dieksploitasi data berisiko tercurinya hak akses *website*.
2) Setelah dilakukan Pengujian *Security Assessment* pada *website* yang dikelola oleh Diskominfo kabupaten Bandung terhadap kerentanan yang telah dianalisis sebelumnya maka didapatkan data eksploitasi berupa hak akses pada subdomain diskop.bandungkab.go.id, hal ini sangat mengkhawatirkan dan diperlukan tindakan lebih lanjut untuk menutup cela kerentanan tersebut
3) Setelah dibangun aplikasi *Report* Kerentanan *Website* pemerintah di Diskominfo Kabupaten Bandung, pihak Diskominfo dapat melakukan pengujian sederhana dan mengetahui informasi kerentanan *website* dalam bentuk grafik.

3.2 Saran

Aplikasi *Report* Kerentanan *Website* pemerintah di Diskominfo Kabupaten Bandung bukanlah sebuah sistem yang sempurna. Untuk dapat mendapatkan hasil yang memuaskan, perlu dilakukan pengembangan terhadap sistem yang dibangun. Untuk pengembangan aplikasi *Report* Kerentanan *Website* pemerintah di Diskominfo Kabupaten Bandung, terdapat beberapa hal yang harus diperhatikan yaitu :

1) Perlu ditambahkan *Tools* pendukung tambahan yang kompatibel dengan OS Windows, karena aplikasi *Report* Kerentanan *Website pemerintah di Diskominfo Kabupaten Bandung merupakan aplikasi yang berjalan dalam platform OS Windows.*
2) Ditambahkannya fitur yang dapat membaca hasil *Scanning Vulnerabily*, sehingga pengguna dapat langsung memasukan data kerentanan tanpa harus memasukan datanya secara manual.
3) Dapat dilakukan pengembangan aplikasi serupa untuk platform OS *linux*, agar dapat mempermudah pengguna yang menggunakan OS ini, karena fitur yang disediakan oleh OS kali *linux* sangat lengkap.

DAFTAR PUSTAKA

[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].