ANALISIS PERBANDINGAN METODE *WEB SECURITY* PTES, ISSAF DAN OWASP DI DINAS KOMUNIKASI DAN INFORMASI KOTA BANDUNG

Tio Revolino Syarif [1,] Didit Andri Jatmiko [2]

[1,2] Universitas Komputer Indonesia

Jl. Dipatiukur No. 112-116, Bandung 40132

E-mail : tio.revolino.syarif@email.unikom.ac.id [1], didit@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 Kota Bandung adalah Diskominfo. Namun demikian, dengan digunakannya *website* sebagai media pelayanan informasi masyarakat oleh pemerintah, akan sangat memungkinkan jika *website* tersebut dapat diserang oleh orang-orang yang tidak bertanggung jawab yang dapat menimbulkan kerugian dan terganggunya pelayanan informasi pemerintah ke masyarakat. Salah satu upaya pencegahan hal tersebut ialah *Penetration Testing*. *Penetration Testing*, atau bisa juga disebut *Pen Testing*, merupakan sebuah percobaan untuk menemukan kerentanan pada sistem komputer, jaringan komputer, ataupun aplikasi web, yang dimana kerentanan tersebut dapat dimanfaatkan oleh penyerang. Pada penelitian kali ini akan membandingkan tiga *Penetration Testing Framework*, yaitu PTES, ISSAF, dan OWASP. Hasil dari penelitian ini diharapkan dapat mebantu pihak DISKOMINFO kota Bandung dalam mengelola *website* dan memberikan pemahaman tentang perbedaan ke tiga *Framework* tersebut.

Kata Kunci : PTES, OWASP, ISSAF, *Penetration Testing*, kerentanan *website*, *Reporting*

1. PENDAHULUAN

Dinas Komunikasi dan Informatika Kota Bandung merupakan sebuah instansi yang bertanggung jawab atas pengolahan informasi dilingkungan kota Bandung. *Website* pun merupakan kebutuhan yang sangat penting di instansi pemerintah khususnya Dinas Komunikasi dan Informatika kota Bandung. Manfaat *Website* diantaranya, sebagai media peyampaian informasi, sebagai media interaksi, sebagai tolak ukur aktif atau tidaknya kegiatan pemerintahan, sebagai tempat masyarakat untuk meyampaikan aspirasinya, dan sebagai tempat untuk promosi.

Tetapi, dibalik banyaknya manfaat, terdapat juga ancaman-ancaman yang dapat terjadi. Berdasarkan data yang di dapat dari Direktorat *Cyber Crime* Indonesia, pada tahun 2015-2016 di Indonesia terdapat 2880 kasus *Cyber Crime* [1]. Pada bulan Mei 2017, terjadi sebuah serangan siber *Ransomware Wannacry* yang menyebabkan gangguan pada perusahaan dan rumah sakit di lebih dari 150 negara [2]. Serangan tersebut membuka mata dunia dan menjadi langkah awal untuk bekerja sama dalam keamanan siber.

Sistem Keamanan Komputer dapat dikatakan sebuah cara yang dibuat untuk mengamankan fungsi, data, performa, atau proses yang ada pada sebuah sistem komputer. Sebuah percobaan harus dilakukan untuk mengetahui apakah sebuah *website* aman atau tidak dari aksi-aksi berbahaya yang dilakukan oleh penyerang [3]. Salah satu cara untuk mengetahui apakah sistem kita aman atau tidak ialah dengan melakukan *Penetration Testing.*

Penetration Testing dapat dikatakan sebuah cara yang legal dan resmi untuk menemukan dan mengeksploitasi sistem komputer yang bertujuan untuk menjadikan sistem tersebut lebih aman [4]. Tetapi pada beberapa kasus, kerentanan yang didapat dari *Penetration Testing* justru dimanfaatkan oleh pihak yang tidak bertanggung jawab. Oleh karena itu sangat penting untuk meminta izin kepada pihak yang ingin di *Penetration Testing* [5].

Penetration Testing Execution Standard (PTES) belakangan muncul sebagai salah satu Framework untuk Penetration Testing. Walaupun Framework ini masih dalam tahap pengembangan, menyediakan sebuah metode yang sangat terstruktur untuk memotivasi komunitas yang bertujuan untuk mengidentifikasi apa itu Security Assesment.

Information Systems Security Assessment Framework (ISSAF) merupakan sebuah *framework* terstruktur dari *Open Information System Security Grop* yang mengelompokkan penilaian informasi keamanan sistem kedalam beberapa domain dan menilai detail secara spesifik atau kriteria pengujian setiap domain [6].

Open Web Application Security Project (OWASP) adalah sebuah komunitas yang bebas dan terbuka di seluruh dunia terfokus pada peningkatan keamanan perangkat lunak aplikasi. Misi OWASP adalah untuk membuat aplikasi keamanan "terlihat", sehingga orang-orang dan organisasi dapat membuat keputusan tentang risiko keamanan aplikasi. Hasil

yang dilakukan dari pengujian OWASP ini akan dipetakan menggunakan parameter penilaian Risk Rating. Risk Rating adalah parameter penilaian yang digunakan untuk mengukur tingkat suatu resiko. Pada metodologi ini resiko (risk) adalah hasil kali kemungkinan (Likelihood) dengan dampak (impact). Hasil dari pengujian tersebut akan dijadikan parameter penilaian seberapa tinggi tingkat keamanan suatu web.

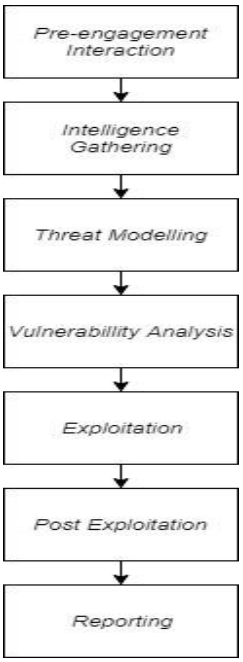
Berdasarkan masalah yang terjadi, maka dilakukan penelitian ini yang diharapkan dapat membantu pihak DISKOMINFO Kota Bandung, dalam menjaga keamanan website, dan menentukan *Framework* apa yang tepat untuk digunakan.

2. LANDASAN TEORI

Pada tahapan ini akan dilakukan pembahasan tentang teori-teori yang digunakan dalam penelitian.

2.1. PTES (Penetration Testing Execution Standard)

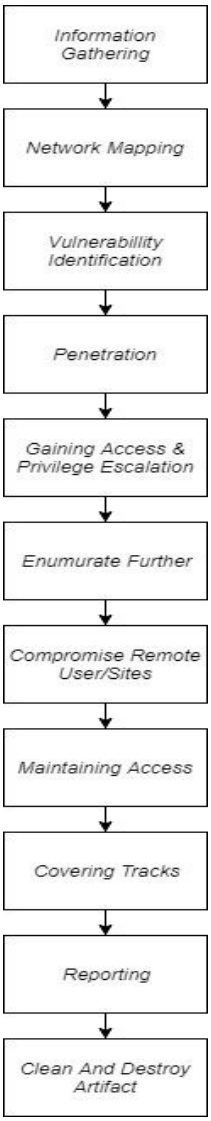
Penetration Testing Execution Standard (PTES) merupakan sebuah standar baru yang di desain bisnis dan penyedia servis keamanan dengan menggunakan Bahasa yang umum dengan cakupan dalam melakukan penetration testing. PTES dimulai pada awal tahun 2009 dan berawal dari pertemuan antara anggota pendiri disaat membicarakan tentang kepentingan atau kelemahan dalam penetration testing yang ada sekarang [7].Fase PTES didesain untuk menjelaskan sebuah *Penetration Testing* dan memastika *client* bahwa sebuah usaha level standarisasi akan diperluas pada *Penetration Testing* oleh semua orang yang melakukan tipe *assestment* ini[8] . 7 langkah dalam melakukan penetration testing execution:



Gambar 1. Tahap-Tahap PTES

2.2. ISSAF (Information System Security Assesment Framework)

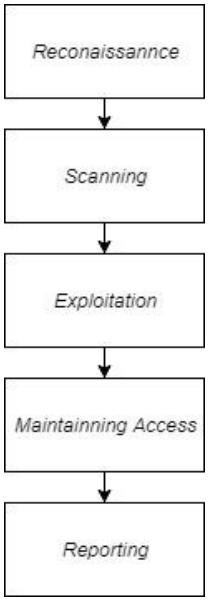
ISSAF adalah suatu kerangka terstruktur yang mengkategorikan penilaian keamanan sistem informasi kedalam berbagai domain dan rincian evaluasi yang spesifik atau kriteria pengujian untuk setiap domainnya [9]. Hal ini bertujuan untuk menyediakan masukan terhadap penilaian keamanan berdasarkan skenario sebenarnya. Kecukupan penggunaan ISSAF untuk memenuhi syarat penilaian keamanan pada sebuah Organisasi dan bisa digunakan sebagai referensi untuk memenuhi keamanan informasi lainnya. ISSAF mencakup aspek penting dalam memproses keamanan, penilaian, dan membantu untuk mendapatkan gambaran lengkap tentang kerentanan yang mungkin ada. Berikut tahapan – tahapan pada ISSAF (Information System Security Assesment Framework):



Gambar 2 Tahap-Tahap ISSAF

2.3. OWASP (Open Web Application Security Project)

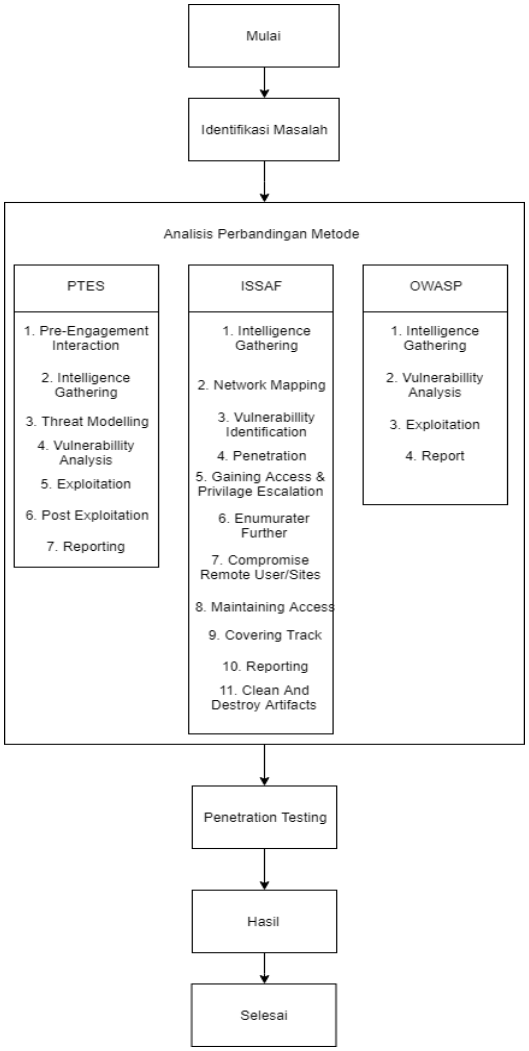
Open Web Application Security Project (OWASP) adalah sebuah komunitas yang bebas dan terbuka yang berdedikasi untuk memungkinkan organisasi untuk mengembangkan, membeli, dan menjaga aplikasi yang dapat dipercaya, semua *tools*, dokumen, forum yang digunakan OWASP bersifat gratis dan terbuka untuk siapa saja yang tertarik untuk memperbaiki keamanan aplikasi [10]. Berikut merupakan tahapan dari framework OWASP (Open Web Application Security Project):



Gambar 3 Tahap-Tahap OWASP

3. METODE PENELITIAN

Metodologi penelitian yang digunakan ialah metode penelitian kualitatif, yaitu penelitian tentang riset yang bersifat deskriptif dan cenderung menggunakan analisis. Berikut merupakan alur penelitian yang dilakukan pada penelitian kali ini:



Gambar 4 Alur Penelitian

1. Identifikasi Masalah

Pada tahap ini, peneliti bekerja sama dengan pihak diskominfo untuk mengidentifikasi masalah – masalah yang terdapat pada website DISKOMINFO Kota Bandung.

2. Analisis Perbandingan Metode

Peneliti melakukan perbandingan antara ketiga metode yang digunakan.

3. Penetration Testing

Dalam tahap ini peneliti akan melakukan uji kerentanan pada website yang telah ditentukan. Pemeriksaan mengenai kerentanan dilakukan dengan menggunakan tools yang akan disesuaikan.

4. Hasil

Dalam tahap ini, penguji mendapatkan hasil dari perbandingan ke tiga metode dan mendapatkan hasil dari *Penetration Testing*

4. HASIL DAN PEMBAHASAN

- **PTES (Penetration Testing Execution Standard)**

1. Pre-Engagement Interaction

Pada fase Pre-Engagement Interaction akan dilakukan pembicaraan dengan pihak dari Diskominfo Kota 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
2. Konfirmasi ruang lingkup penelitian, pendekatan dan penjelasan metode yang akan digunakan dalam pengujian kerentanan pada diskominfo.bandung.go.id
3. Melakukan permintaan data dalam bentuk domain yang di kelola oleh Diskominfo Kota Bandung

2. Intelligence Gathering

Pada tahap ini akan dilakukan pencarian informasi tentang domain diskominfo.bandung.go.id, berikut merupakan hasil dari pencarian tersebut dengan menggunakan Whois Domain dan Zenmap :

Gambar 5 Whois diskominfo.bandung.go.id

Berikut merupakan tabel hasil whois domain diskominfo.bandung.go.id

Tabel 1 Whois diskominfo.bandung.go.id

Diskominfo.bandung.go.id	
Domain ID	PANDI-DO282184
Domain Name	BANDUNG.GO.ID
Created On	10-May-2000
Expiration Date	31-Jan-2020
Status	OK

Selanjutnya akan dilakukan pencarian informasi mengenai *Network Mapping* dengan menggunakan Zenmap untuk domain diskominfo.bandung.go.id. Berikut hasil Zenmap untuk domain diskominfo.bandung.go.id:

Tabel 2 Zenmap diskominfo.bandung.go.id

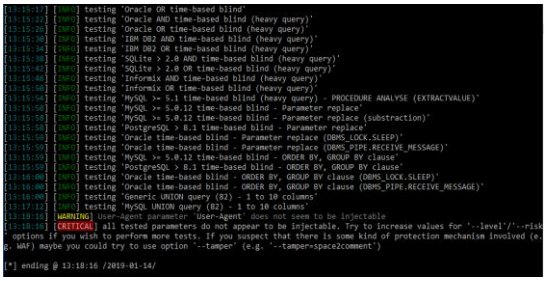
diskominfo.bandung.go.id		
Port	***Status***	***Services***
80	Open	http
443	Open	https

3. Vulnerabillity Analysis

Berikut merupakan hasil Vulnerabillity Analysis dengan menggunakan *tools vulnerability scanning* Accunetix,, yaitu *Application Error Message (CWE-209), Error Message On Page (CWE-200), Vulnerable Javascript Library (CWE-16). Application Error Message (CWE-209)*

4. Exploitation

Exploitation merupakan salah satu tahapan pada *Framework Penetration Execution Standard* (PTES) dimana pada tahapan ini penguji akan melakukan penetrasi terhadap website yang diuji guna melihat apakah domain **diskominfo.bandung.go.id** memiliki celah kemanan. Berikut hasil dari *exploitation* dengan menggunakan sqlmap:

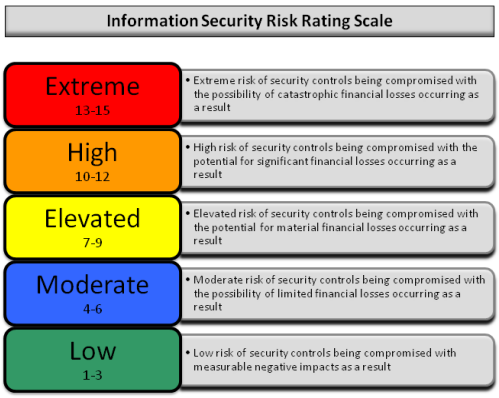


Gambar 6 Sqlmap diskominfo.bandung.go.id

Berdasarkan Gambar 6, domain diskominfo.bandung.go.id tidak memiliki celah SQL Injection.

5. Reporting

Pada tahap ini juga peneliti akan memberikan sebuah *Risk Rating* kepada domain **diskominfo.bandung.go.id.** Tingkatan *Risk Rating* ini mengacu kepada *Risk Rating* yang telah diberikan oleh *framework Penetration Testing Execution Standard (PTES).* Berikut merupakan gambaran *Risk Rating* tersebut.



Gambar 7 Risk Rating Scale

Berdasarkan penelitian yang telah dilakukan, maka Skor Resiko untuk website **diskominfo.bandung.go.id** untuk saat ini ialah 6, hal ini mengacu kepada adanya kemungkinan bahwa adanya kelemahan pada kontrol keamanan yang dapat menyebabkan kerugian finansial yang terbatas.

- **ISSAF (Information System Security Assesment Framework)**

1. Information Gathering

Pada tahap ini akan dilakukan pencarian informasi tentang website yang akan diteliti, berikut merupakan hasil dari pencarian tersebut dengan menggunakan *Whois Domain:*

```
Domain ID:PANDI-DO282184
Domain Name:BANDUNG.GO.ID
Created On:10-May-2000 13:35:10 UTC
Last Updated On:07-Jan-2018 06:27:20 UTC
Expiration Date:31-Jan-2020 23:59:59 UTC
Status:ok
==========================================================
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
Sponsoring Registrar Contact Email: hostmaster@pandi.id

Name Server:DNS1.BANDUNG.GO.ID
Name Server:DNS2.BANDUNG.GO.ID
Name Server:NS3.BANDUNG.GO.ID
Name Server:DNS4.BANDUNG.GO.ID
Name Server:NS1.BANDUNG.GO.ID
Name Server:DNS3.BANDUNG.GO.ID
DNSSEC:Unsigned
```

Gambar 8 Whois diskominfo.bandung.go.id

Berikut merupakan tabel hasil whois domain diskominfo.bandung.go.id

Tabel 3 Whois diskominfo.bandung.go.id

Diskominfo.bandung.go.id	
Domain ID	PANDI-DO282184
Domain Name	BANDUNG.GO.ID
Created On	10-May-2000
Expiration Date	31-Jan-2020
Status	OK

2. Network Mapping

Network mapping akan dilakukan dengan bantuan tool Zenmap, berikut merupakan hasil dari penelusuran *Port – Port* dengan menggunakan Zenmap:

Tabel 4 Zenmap diskominfo.bandung.go.id

diskominfo.bandung.go.id		
Port	***Status***	***Services***
80	Open	http
443	Open	https

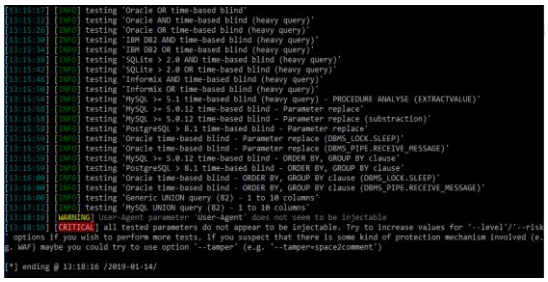
3. Vulnerability Identification

Setelah dilakukan tahapan *Information Gathering*, tahapan selanjutnya ialah *Vulnerability Identification*, pada tahapan ini akan dilakukan pemindaian terhadap *website* untuk dilihat apakah website tersebut memiliki sebuah kerentanan atau tidak, dan seberapa parah kerentanan yang dimiliki oleh website tersebut,. Jika terdapat kerentanan maka penguji akan menggunakan kerentanan tersebut untuk melakukan langkah pengujian yang selanjutnya. Berikut merupakan hasil Vulnerabillity Analysis dengan menggunakan *tools vulnerability scanning* Accunetix,, yaitu *Application Error Message (CWE-209), Error Message On Page (CWE-200), Vulnerable Javascript Library (CWE-16). Application Error Message (CWE-209).*

4. Penetration

Penetration merupakan salah satu tahapan pada *Information System Security Assesment Framework* (ISSAF) dimana pada tahapan ini penguji akan melakukan penetrasi terhadap website yang diuji.

Dalam tahap ini penguji akan menguji apakah website ini terdapat kerentanan kepada SQL Injection dengan menggunakan tool yaitu *SQLmap.* Berikut merupakan screenshot hasil dari pengujian menggunakan *SQLmap:*



Gambar 9 SQLmap diskominfo.bandung.go.id

Berdasarkan dari Gambar 9, dapat dilihat bahwa website diskominfo.bandung.go.id tidak memiliki kerentanan SQL Injection.

5. Reporting

- **Management Summary**

Berdasarkan penelitian yang telah dilakukan dari tahap awal hingga tahap akhir, terdapat beberapa kerentanan yang terdapat pada domain **diskominfo.bandung.go.id.** Kerentanan tersebut ialah *Application Error Message, Error Message On Page, Vulnerable Javascript Library (CWE-16).*

- **Scope Of The Project**

Scope of the project merupakan laporan mengenai ruang lingkup yang diambil peneliti. Ruang lingkup ini sendiri sebenarnya sudah diambil peneliti berdasarkan persetujuan dari peneliti dan pihak yang di uji. Adapun ruang lingkup yang diambil peneliti adalah web aplikasi.

- **Vulnerabillity Scan Report**

Vulnerability scan reports merupakan tahap laporan berdasarkan proses analisis pada fase ke dua metode ISSAF ditambah dengan implementasi yang telah dilakukan. Berikut ini adalah laporan berupa table

Tabel 5 Vulnerabillity Scan Report

No	Common Weakness Enumeration	*CWE-209*	*CWE-444*	*CWE-260*
	Domain			
1	Diskominfo.bandung.go.id	✓	✓	✓

- **OWASP (Open Web Application Security Project)**

1. Reconaissance

Pada tahap ini akan dilakukan pencarian informasi tentang website yang akan diteliti, berikut merupakan hasil dari pencarian tersebut dengan menggunakan *Whois Domain* dan *Zenmap :*

Gambar 10 Whois diskominfo.bandung.go.id

Berikut merupakan tabel hasil whois domain diskominfo.bandung.go.id

Tabel 6 Whois diskominfo.bandung.go.id

Diskominfo.bandung.go.id	
Domain ID	PANDI-DO282184
Domain Name	BANDUNG.GO.ID
Created On	10-May-2000
Expiration Date	31-Jan-2020
Status	OK

Selanjutnya akan dilakukan pencarian informasi mengenai *Network Mapping*. Berikut hasil Zenmap untuk domain diskominfo.bandung.go.id:

Tabel 7 Zenmap diskominfo.bandung.go.id

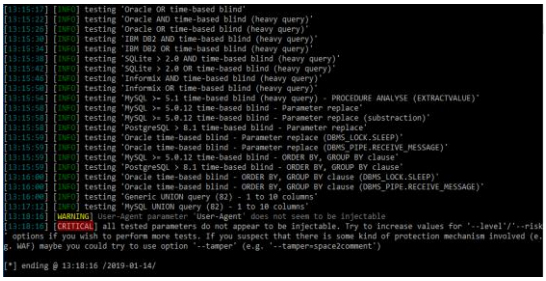
diskominfo.bandung.go.id		
Port	***Status***	***Services***
80	Open	http
443	Open	https

2. Scanning

Tahapan selanjutnya ialah *Scanning*, pada tahapan ini akan dilakukan pemindaian terhadap *website* untuk dilihat apakah website tersebut memiliki sebuah kerentanan atau tidak, dan seberapa parah kerentanan yang dimiliki oleh website tersebut, Berikut merupakan hasil scanning dengan menggunakan *tools vulnerability scanning* Accunetix,, yaitu *Application Error Message (CWE-209), Error Message On Page (CWE-200), Vulnerable Javascript Library (CWE-16). Application Error Message (CWE-209).*

3. Exploitation

Exploitation merupakan salah satu tahapan pada *Open Web Application Security Project (OWASP)* dimana pada tahapan ini penguji akan melakukan penetrasi terhadap website yang diuji. Berikut merupakan screenshot hasil dari pengujian menggunakan *SQLmap:*



Gambar 11 SQLmap diskominfo.bandung.go.id

Berdasarkan dari Gambar 11, dapat dilihat bahwa website **diskominfo.bandung.go.id** tidak memiliki kerentanan SQL Injection.

4. Reporting

Di dalam fase *Reporting*, OWASP (*Open Web Application Security Project)* memiliki sebuah metode yaitu *OWASP Risk Rating Methodolgy.* OWASP Risk Rating Methodology merupakan metode yang digunakan untuk menentukan klasifikasi risiko pada website..

Likelihood and Impact Levels	
0 to <3	LOW
3 to <6	MEDIUM
6 to 9	HIGH

Gambar 12 Likelihood dan Impact Level

Setelah dilakukan perhitungan, domain diskominfo.bandung.go.id memiliki score *Likelihood* sebesar 5, sehingga memiliki rating *Medium*. Sedangkan score *Impact sebesar 4*, dan juga memiliki rating *Medium.* Setelah itu tentukan klasifikasi risiko berdasarkan rumus dari OWASP Risk Rating Methodology dan disesuaikan dengan gambar 13

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

Gambar 13 Overall Risk Severity

Berdasarkan gambar 13 dapat diketahui bahwa subdomain **Diskominfo.bandung.go.id** memiliki tingkat resiko **Medium.**

5. KESIMPULAN

Berdasarkan hasil penelitian ini, menurut penulis bahwa *Framework* yang tepat untuk digunakan pada DISKOMINFO kota Bandung ialah *Framework Penetration Testing Execution Standard (PTES)* dan *Open Web Application Security Project (OWASP),* dikarenakan penilaian pada *framework* ini menggunakan level-level yang dapat dimengerti oleh user yang bukan hanya orang yang berpengalaman dengan *Penetration Testing*, tetapi dapat juga dimengerti oleh *user* yang juga tidak memiliki pengalaman di bidang *Penetration Testing*. Sedangkan *framework Information System Security Assesment Framework (ISSAF)* hanya dapat dimengerti oleh *user* yang berpengalaman pada bidang *Penetration Testing*, dikarenakan *reporting* pada *framework* ini tidak memiliki level-level seperti pada kedua *framework* yang lain. Saran yang dapat peneliti berikan adalah:

- Memberikan format laporan mengenai kerentanan - kerentanan berdasarkan ketiga Framework, Penetration Testing Execution Standard (PTES), Information System Security Assesment Framework (ISSAF), dan Open Web Applicatin Security Project (OWASP) yang bisa

digunakan untuk penelitian dimasa yang akan datang

- Menjaga Website dengan menggunakan acuan dari hasil laporan yang telah dilakukan dan berharap dapat mencegah kerentanan yang akan datang.

6. 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) 021292, 2018*

[2] M. J. Islami, TANTANGAN DALAM IMPLEMENTASI STRATEGI KEAMANAN SIBER NASIONAL INDONESIA DITINJAU DARI PENILAIAN GLOBAS CYBERSECURITY INDEX, Puslitbang Aptika dan IKP, Badan Litbang SDM, Kemenkominfo,2017

[3] E.B.Setiawan, A Setiyadi, Web Vulnerabillity Analysis and Implementation, *IOP Conf. Series: Materials Science and Engineering 407 (2018) 012081, 2018*

[4] Patrick Engebretson, The Basic of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy, Elsevier, 2010

[5] Vibhurushi Chotaliya, Fiyona Mistry, New Era of Web Security By Implementing of Penetration Testing, International Journal of Trend in Scientific Research and Development, 2018

[6] Shorunke Muyiwa Musaddiq. Penetration Testing in WI-FI network. *International Journal of Computer Science Engineering,Vol 4 issues 4*, pp.115

[7] The Penetration Execution Standard, *Penetration Execution Standard-The FAQ, http://www.pentest-standard.org/index.php/FAQ,* 26 Februari 2018 19.45

[8] D. Kennedy, J. O'Gorman, D. Kearns, M. Aharoni, "METASPLOIT The Penetration Tester's Guide", No Starch Press, pp. 2, 2011

[9] Jajang Ruhiyat, Angga Setiyadi, Sistem Monitoring Website Dengan Metode ISSAF Di Dinas Komunikasi dan Informatika Kabupaten Tangerang, Unikom, 2018

[10] OWASP, "OWASP Top 10 – 2013 : The ten most Critical Web Application Security Risk", OWASP, pp.2