BAB IV

ANALISIS, INTERPRETASI DAN IMPLIKASI PENELITIAN

4.1. Analisis Hasil Penetration Testing

Data yang telah didapat akan diolah dan dijadikan nilai (*value*) dari hasil analisis, pada proses *penetration testing* ini adalah menemukan beberapa kelemahan pada web portal tersebut. Oleh karena itu, Penulis mendapatkan hasil yang bisa dijadikan acuan untuk menjawab *reasearch question*, yaitu :

1. Identifikasi faktor-faktor yang diperlukan dalam mendukung pembangunan keamanan web portal Pemerintah
2. Membangun web portal Pemerintah terhadap ancaman web portal saat ini

Hasil analisis data yang diperoleh dari penelitian ini, akan dibandingkan dengan parameter keamanan informasi dan ancaman pada keamanan web portal saat ini, yang sudah dipaparkan pada tinjauan studi. Selain itu, hasil penelitian ini juga digunakan untuk menentukan kebenaran dari hipotesis yang telah ditentukan sebelumnya.

Disini, Penulis akan menguraikan kelemahan yang terdapat pada objek penelitian, terkait penulisan pada tesis ini. Tetapi hal ini terkait *cofidentiality* terhadap pada data yang telah didapat, serta kelemahan yang ada pada sistem web portal Pemerintah Pusat, Namun untuk kepentingan pembuktian, bahwa pada web portal tersebut teridentifikasi serangan ataupun terdapat celah keamanan, penulis akan memperlihatkan informasi tersebut. Keperluan pembuktian dalam sidang Tesis nanti, penulis akan memberikan laporan lengkap kepada dewan penguji. Perlu diketahui juga, bahwasanya seluruh aktifitas yang dilakukan oleh seorang *penetration testing* untuk mengetahui kelemahan yang terdapat pada web portal tersebut secara *online penetration* akan tercatat oleh sebuah server dan masuk dalam log server tersebut. Namun pada dasar kegiatan *penetration testing* ini tidak membahayakan web portal yang akan diuji, karena seorang *penetration testing* tidak memasang ataupun menginstal sebuah aplikasi yang sifatnya *malware, spyware, adware* ataupun sejenisnya pada web portal tersebut.

4.2. Faktor–faktor yang diperlukan dalam Proses Pengujian Keamanan Web Portal Pemerintah

Adapun faktor-faktor yang diperlukan dalam proses pengujian keamanan web portal Pemerintah, guna mencapai sebuah tujuan yang maksimal. Dalam sisi teknis, kita menggunakan berbagai macam pengujian dengan cara *black box testing* maupun *white box testing*. Tetapi tidak luput juga dalam menimbang resiko yang kita pilih dalam pengujian tersebut untuk mendapatkan hasil yang optimal dan tujuan yang tepat.

4.2.1. Metodologi Fuzzing Teknologi

Metodologi yang digunakan untuk mencari *bugs* atau kesalahan suatu program/aplikasi. *Fuzzing* akan sangat berguna bagi *developer* untuk dapat memperbaiki *bugs* yang ditemukan. Namun bagi seorang *hacker, bugs* merupakan hal menarik yang dapat digunakan untuk berbagai hal, salah satunya adalah untuk mendapatkan akses ke suatu sistem. Berbagai macam celah *security,*seperti : *bugs, stack overflow, format string, heap overflow, input validation attack, XSS*. Tak hanya itu metode ini digunakan juga oleh *hacker/cracker/security professional* untuk menemukan berbagai macam lubang keamanan (*security hole*) pada suatu aplikasi. *fuzzing* juga tidak hanya terbatas pada aplikasi sistem (*client*/*server*), namun juga pada aplikasi-aplikasi web yang sering disebut sebagai *web fuzzing*.

4.2.2. Websecurify

Websecurify merupakan sebuah alat pengujian pada keamanan web, yang dapat digunakan untuk mengindetifikasi kelemahan web yang terintegrasi pada web browser serta menggunakan metodologi *fuzzing* teknologi. w*ebsecurify* ini dikembangkan secara terus menerus oleh para *penetration tester* maupun peneliti keamanan pada web. Tidak seperti produk aplikasi *penetration tester* lain, semua fitur w*ebsecurify* dirancang untuk mudah digunakan dan untuk membantu proses penetrasi pengujian dari awal sampai akhir, dalam setiap proses selama tes secara manual otomatis, semi-otomatis atau penetrasi penuh. Termasuk *scanning* dan mesin analisisnya mampu secara otomatis mendeteksi berbagai jenis kerentanan

aplikasi web, sambil Anda melanjutkan dengan uji penetrasi. Daftar kelemahan yang secara otomatis terdeteksi, meliputi :

- *SQL Injection*
- *Local dan Remote File Include*
- *Cross-site Scripting*
- *Cross-site Request Forgery*
- *Information Disclosure Problems*
- *Session Security Problem*
- Termasuk semua kategori ancaman web pada OWASP Top 10

4.2.3. Scanning

Scanning merupakan tahap awal untuk mengumpulkan informasi (*information gathering*) yang akan dijadikan target, dalam hal ini web portal Pemerintah. Proses *scanning* inilah, seluruh web portal itu dicari dan ditemukan *bugs* serta celah keamanan (*hole security*) untuk sebagai pintu masuk bagi sebuah *cracker* ataupun *hacker*. Ibarat sebuah rumah yang akan di jadikan target perampokan oleh Maling, maka tahap awal dari maling tersebut ialah mencari sebuah pintu yang dapat dibuka dan belum di kunci dengan benar. Begitu pula seorang *hacker* ataupun *cracker* ketika ingin memasuki suatu sistem tanpa hak akses untuk memasukinya, maka *hacker* maupun *cracker* tersebut akan mencari dan mengumpulkan informasi sebanyak-banyaknya untuk bisa disusupi melalui celah keamanan yang masih terbuka. Istilah ini biasa disebut *open port*, karena seorang Penyerang selalu memanfaatkan celah keamanan tersebut pada port dari sistem yang terbuka.

Oleh sebab itu, semakin informasi dalam sistem yang kita publikasi tersebut dapat kita sembunyikan, maka kemungkinan kecil kita membuka kesempatan Penyerang untuk dengan mudah menyusupi sistem kita untuk mendapatkan informasi yang sensitif maupun *private*. Berikut adalah gambar hasil *scanning* pada sebuah web portal Pemerintah menggunakan *websecurify*, sebagai berikut:

SQL Injection

SQL Injection (SQLI) is a code injection technique that exploits a security vulnerability occurring in the database layer of a web application. The vulnerability is present when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and thereby unexpectedly executed.

solution: Sanitize all user-supplied data before using it as part of database queries.

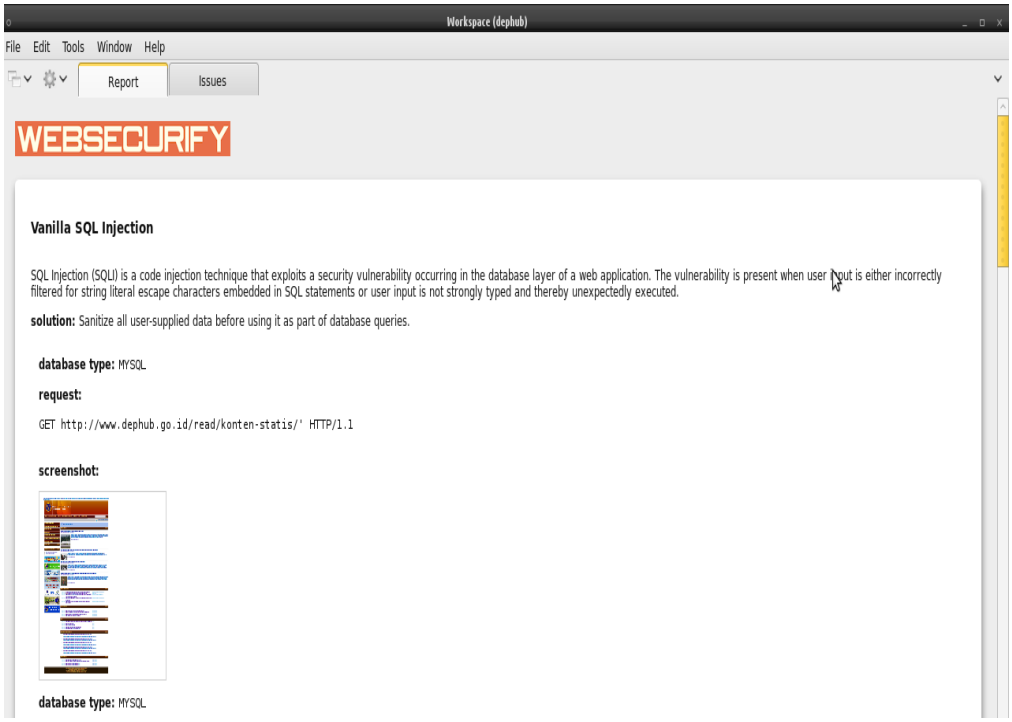
database type: MYSQL

request:

POST /v70/index.php/layanan-perijinan?lang= HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Host: www.jakarta.go.id
Content-Length: 100

id=214&sectionid=
%22&task=category&filter_order=Abc123&filter_order_Dir=Abc123&limitstart=0&limit=25

Gambar IV.1 Tampilan Output dari Websecurify



Gambar IV.2 Aplikasi Websecurify

Penjelasan :

1. Jenis Ancaman

Jenis ancaman yang terdeteksi pada web potal tersebut. Pada umumnya tak hanya serangan *SQL Injection* saja, tetapi tergantung pada kelemahan sistem web portal itu. Serangan yang terdeteksi bisa juga *cross site scripting,, remote file include* dan lain sebagainya .

2. Solution

Pada tools *websecurify* ini juga memberikan solusi pada setiap jenis ancaman yang teridentifikasi pada sebuah web portal tersebut, setelah melakukan *scaning* atau *spidering*.

3. Database Type

Pada umumnya, jika web portal tersebut terdeteksi ancaman maupun serangan *SQL Injection,* maka *websecurify* ini memberikan informasi tipe atau jenis dari *database* yang digunakan oleh web portal tersebut, misalnya : mysql, oracle dan ms sql.

4. Request

Request ini merupakan jenis serangan yang diluncurkan pada web portal tersebut, untuk mengetahui atau menemukan kelemahan dari web portal itu.

4.2.4. Enumeration

Tahapan *enumeration* ini merupakan sebagai penambah kelengkapan pada proses pengujian. Dimana pada tahapan *enumeration*, jenis serangan lebih spesifik pada model serangan *Injection Flaw. Injection Flaw* ini sepertihalnya S*QL Injection, URL Injection, Cookies Injection, Cross site scripting* dan *Xpath Injection. Enumeration* umumnya adalah urutan ke tiga (3) dari tahapan *hacking,* dimana sebuah *hacker* maupun *cracker* menggali informasi yang lebih spesifik lagi mengenai latar belakan informasi yang dijadikan target tersebut. Jadi , untuk menembus suatu sistem tidak dapat hanya melalui satu tahapan saja, melainkan beberapa tahapan yang memang terorganisir dengan rapi.

4.2.5. WebCruiser

WebCruiser Web Vulnerability Scanner, adalah sebuah alat uji penetrasi web yang efektif dan ampuh dalam audit web portal. WebCruiser ini dapat memeriksa beberapa kelemahan pada web portal sebagai alat penaksiran (*assesment tools*) seperti S*QL Injection, URL Injection, Cookies Injection, Cross site scripting* dan *Xpath Injection.* WebCruiser ini juga dilengkapi dengan PoC (*Proof of Concept*), dimana kita bisa lebih spesifik untuk tipe penyerangan terhadap web portal target sepertihalnya serangan *Cross-site Scripting, SQL Injection* dan lainnya.

Hasil dari *enumeration* ini dengan menggunakan WebCruiser, sebagai berikut :

www.indonesia.go.id Scan Report

Made By M. Sholeh

Created By WebCruiser - Web Vulnerability Scanner

2010-12-13

Vulnerability Result

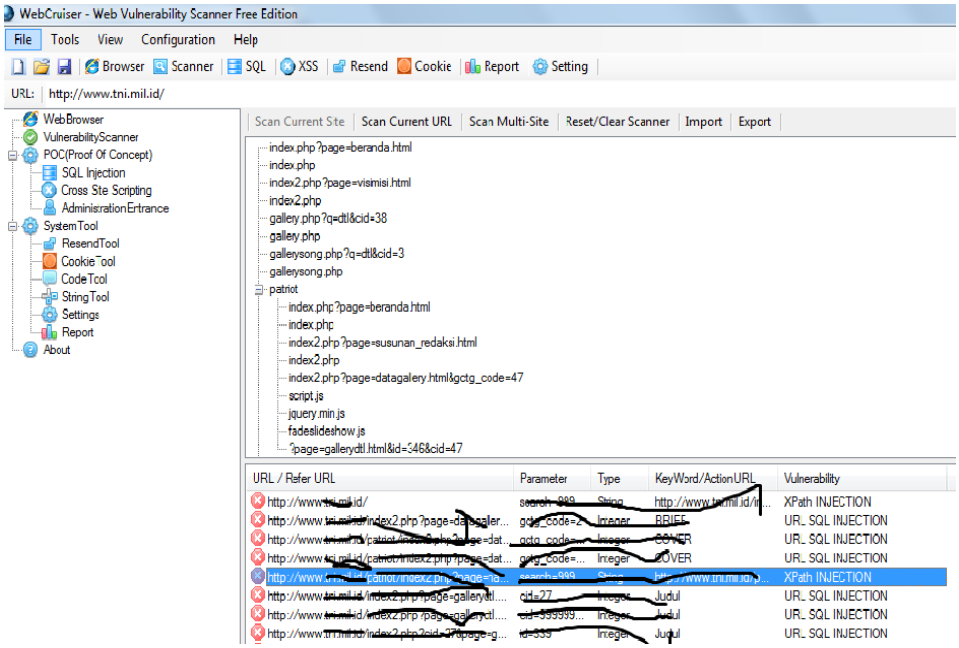
No.	1
ReferURL	
Parameter	
Type	
KWordActionURL	
Vulnerability	COOKIE SQL INJECTION

No.	2
ReferURL	
Parameter	
Type	
KWordActionURL	
Vulnerability	COOKIE SQL INJECTION

No.	3
ReferURL	
Parameter	
Type	
KWordActionURL	
Vulnerability	URL SQL INJECTION

Gambar IV.3. Hasil scanning vulenerbility dan enumeration terhadap web portal

Tabel diatas menjelaskan bahwa, terdeteksi kelemahan pada web portal tersebut. Sehingga bisa berpotensi serangan *SQL injection* pada web tersebut dan diberitahukan pula alamat URL yang berpotensi pada serangan tersebut.



Gambar IV.4. Aplikasi WebCruiser

Penjelasan :

1. Refer URL

Refer URL merupakan sebuah penaksiran serangan *injection*, yang terjadi pada kelemahan URL tersebut.

2. Parameter

Parameter disini adalah menunjukan sebuah *input* parameter, kemungkinan dapat menunjukan sebuah kelemahan pada alamat URL tersebut yang terdapat komponen dari web portal.

3. Type

Type ini menunjukan t*ype data* dari field pada *database* yang dimiliki oleh web portal tersebut, teridentifikasi serangan *injection*.

4. KeyWord/ActionURL

KeyWord/ActionURL ini merupakan sebuah kata kunci yang mungkin serta dapat menimbulkan serangan injection pada web portal tersebut.

5. Vulnerbility

Vulnerability ini memberikan informasi, bahwa web portal tersebut terdapat serangan jenis *injection flaw*, dimana serangan itu bisa *SQL Injection*, *Cookies Injection*, ataupun X*path Injection.*

4.3. Analisa Hasil Keamanan Web Portal Pemerintah berdasarkan Parameter CIA

Proses selanjutnya dalam menetukan tingkat keamanan sistem informasi adalah membandingkan hasil yang didapat dalam proses *penetration testing* ini dengan kriteria keamanan sistem informasi berdasarkan parameter keamanan yaitu *Confidentiality*, *Availability*, dan *Integrity* (CIA). Penulis membagi hasil *penetration testing* menjadi 3 bagian, jika diakitkan dengan parameter CIA, selain itu sebagaimana telah ditetapkan pada *sub-sub system* tentang persyaratan amannya sebuah sistem informasi.

Tabel IV.1. Hasik Analisa Kelemahan terhadap Keamanan Web Portal Pemerintah

No	Nama Kementerian/Badan/ Lembaga	Alamat URL	Jenis Kelemahan/Serangan	Parameter CIA
1	Badan Pengawas Obat dan Makanan	Http://www.pom.go.id	SQL Injection, Cross-site Scripting, Information Disclosure	Confidentiality, Integrity
2	DKI Jakarta	Http://prov.jakarta.go.id	SQL Injection, Cross-site Scripting, Information Disclosure	Confidentiality, Integrity
3	Mahkamah Agung	Http://www.mahkamahagung.go.id	SQL Injection, Cross-site	Confidentiality,

			Scripting, Information Disclosure	Integrity
4	Perpustakaan Nasional Republik Indonesia	Http://www.pnri.go.id	SQL Injection, information discloser, Information Disclosure	Confidentiality
5	Kementerian Lingkungan Hidup	Http://www.menlh.go.id	Reflected Cross-site Scripting, Information Disclosure	Integrity, Confidentiality
6	Komisi Pemilihan Umum	Http://www.kpu.go.id	Information Disclosure	Confidentiality
7	Kementerian Kehutanan	Http://www.dephut.go.id	Reflected Cross-site Scripting, Information Disclosure	Integrity, Confidentiality
8	Badan Pemeriksa Keuangan	Http://www.bpk.go.id	Information Disclosure	Confidentiality
9	Lembaga Administrasi Negara	Http://www.lan.go.id	Information Disclosure	Confidentiality
10	Badan Meteorologi dan Geofisika	Http://www.bmkg.go.id	Information Disclosure	Confidentiality
11	Lembaga Pengembangan Antariksa Nasional	Http://www.lapan.go.id	Reflected Cross-site Scripting, Information Disclosure	Integrity, Confidentiality
12	Sekretariat Negara	Http://www.setneg.go.id	Information Disclosure	Confidentiality
13	Sistem Administrasi Badan Hukum	Http://www.sisminbakum.go.id	SQL Injection, Reflected Cross-site Scripting Information Disclosure	Confidentiality, Integrity
14	Tentara Nasional Indonesia	Http://www.tni.mil.id	Injection Flaw, Reflected Cross-site Scripting, Information Disclosure	Confidentiality, Integrity
15	Komisi Penyiaran Indonesia	Http://www.kpi.go.id	SQL Injection, Cross-site Scripting, Information Disclosure	Confidentiality, Integrity
16	Kementerian Aparatur Negara	Http://www.menpan.go.id	SQL Injection, Information Disclosure	Confidentiality

17	Kementerian Politik dan Keamanan	Http://www.polkam.go.id	SQL Injection, Information Disclosure	Confidentiality
18	Polisi Republik Indonesia	Http://www.polri.go.id	SQL Injection, Cross-site Scripting, Information Disclosure	Confidentiality, Integrity
19	Kejaksaan	Http://www.kejaksaan.go.id	SQL Injection, Information Disclosure	Confidentiality
20	Kementerian Perindustrian	Http://www.kemenperin.go.id	SQL Injection, Cross-site Scripting, Information Disclosure	Confidentiality, Integrity
21	Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah	Http://www.lkpp.go.id	SQL Injection, Cross-site Scripting, Information Disclosure	Confidentiality, Integrity
22	Kementerian Pemuda dan Olahraga	Http://www.kemenpora.go.id	SQL Injection, Information Disclosure	Confidentiality
23	Kementerian Pertahanan	Http://www.kemhan.go.id	SQL Injection, Information Disclosure	Confidentiality
24	Kementerian Kelautan dan Perikanan	Http://www.kkp.go.id	Information Disclosure	Confidentiality
25	Kementerian Agama	Http://www.kemenag.go.id	Information Disclosure	Confidentiality
26	Kementerian Sosial	Http://www.depsos.go.id	SQL Injection, Reflected Cross-site Scripting, Information disclosure	Confidentiality, Integrity
27	Kementerian Ekonomi	Http://www.ekon.go.id	Information Disclosure	Confidentiality
28	Badan Tenaga Nuklir Nasional	Http://www.batan.go.id	SQL Injection, Cross-site Scripting, Information Disclosure	Confidentiality, Integrity
29	Badan Pengawas Pasar Modal	Http://www.bapepam.go.id	SQL Injection, Cross-site Scripting	Confidentiality, Integrity
30	Bakosurtanal	Http://www.bakosurtanal.go.id	SQL Injection, Cross-site	Confidentiality,

			Scripting, Information Disclosure	Integrity
31	Arsip Nasional Republik Indonesia	Http://www.anri.go.id	Cross-site Scripting, Information Disclosure	Integrity, Confidentiality
32	Badan Pengawas Tenaga Nuklir	Http://www.bapeten.go.id	SQL Injection, Reflcted Cross-site Scripting, Cross-site Scripting, Information Disclosure	Confidentiality, Integrity
33	Badan Pertanahan Nasional	Http://www.bpn.go.id	SQL Injection, Information Disclosure	Confidentiality
34	Badan Pengawas Keuangan dan Pembangunan	Http://www.bpkp.go.id	SQL Injection, Reflected Cross-site Scripting, Information Disclosure	Confidentiality, Integrity
35	Badan Pembinaa Hukum Nasional	Http://www.bphn.go.id	SQL Injection, Information Disclosure	Confidentiality
36	Badan Koordinasi Penanaman Modal	Http://www.bkpm.go.id	SQL Injection, Cross-site Scripting, Information Disclosure	Confidentiality, Integrity
37	Badan Kepegawaian Negara	Http://www.bkn.go.id	SQL Injection, Information Disclosure	Confidentiality
38	Bank Indonesia	Http://www.bi.go.id	Information Disclosure	Confidentiality
39	Beacukai	Http://www.beacukai.go.id	SQL Injection, Cross-site Scripting, Information Disclosure	Confidentiality, Integrity
40	Badan Perencanaan Nasional	Http://www.bappenas.go.id	SQL Injection, Information Disclosure	Confidentiality
41	Komisi Pengawan Persaingan Usaha	Http://www.kppu.go.id	SQL Injection, Reflected Cross-site Scripting, Information Disclosure	Confidentiality, Integrity
42	Lembaga Pertahanan	Http://www.lemhannas.go.id	Cross-site	Confidentia

	Nasional		Scripting, Information Disclosure	lity, Integrity
43	Lembaga Sandi Negara	Http://www.lemsaneg.go.id	SQL Injection, Information disclosure	Confidentia lity
44	Lembaga Penelitian Indonesia	Http://www.lipi.go.id	SQL Injection, Cross-site Scripting, Information Disclosure	Confidentia lity, Integrity
45	Kementerian Pemberdayaan Perempuan	Http://www.menegpp.go.id	SQL Injection, Cross-site Scripting, Information Disclosure	Confidentia lity, Integrity
46	Kementerian Koordinator Bidang Kesejahteraan Rakyat	Http://www.menkokesra.go.id	SQL Injection, Information Disclosure	Confidentia lity
47	Mahkamah Konstitusi	Http://www.mahkamahkonstitusi.go.id	SQL Injection, Information Disclosure	Confidentia lity
48	Majelis Permusyawaratan Indonesia	Http://www.mpr.goid	SQL Injection, Information Disclosure	Confidentia lity
49	Dinas Tenaga Kerja dan Transmigrasi	Http://www.nakertrans.go.id	SQL Injection, Cross-site Scripting, Information Disclosure	Confidentia lity, Integrity
50	Pos dan Telekomunikasi	Http://www.postel.go.id	SQL Injection, Cross-site Scripting, Information Disclosure	Confidentia lity, Integrity
51	Kementerian Pekerjaan Umum	Http://www.pu.go.id	SQL Injection, Cross-site Scripting, Information Disclosure	Confidentia lity, Integrity
52	Sekretariat Kabinet	Http://www.setgab.go.id	SQL Injection, Cross-site Scripting, Information Disclosure	Confidentia lity, Integrity
53	Kementerian Riset dan Teknologi	Http://www.ristek.go.id	SQL Injection, Cross-site Scripting, Information	Confidentia lity, Integrity

			Disclosure	
54	Republik Indonesia	Http://www.indonesia.go.id	SQL Injection, Information Disclosure	Confidentiality
55	Kementerian Imigrasi	Http://www.imigrasi.go.id	SQL Injection, Information Disclosure	Confidentiality
56	Energi dan Sumber Daya Mineral	Http://www.esdm.go.id	SQL Injection, Information Disclosure	Confidentiality
57	Dewan Perwakilan Rakyat	Http://www.dpr.go.id	SQL Injection, Cross-site Scripting, Information Disclosure	Confidentiality, Integrity
58	Dewan Perwakilan Daerah	Http://www.dpd.go.id	Cross-site Scripting, Information Disclosure	Confidentiality, Integrity
59	Kementerian Pendidikan Nasional	Http://www.kemdiknas.go.id	SQL Injection, Cross-site Scripting, Information Disclosure	Confidentiality, Integrity
60	Direktorat Jenderal HAKI	Http://www.dgip.go.id	SQL Injection, Information Disclosure	Confidentiality
61	Kementerian Pertanian	Http://www.deptan.go.id	SQL Injection, Cross-site Scripting, Information Disclosure	Confidentiality, Integrity
62	Kementerian Luar Negeri	Http://www.deplu.go.id	SQL Injection, Information Disclosure	Confidentiality
63	Kementerian Koperasi dan Usaha Kecil dan Menengah	Http://www.depkop.go.id	SQL Injection, Information, Disclosure	Confidentiality
64	Kementerian Komunkasi dan Informatika	Http://www.depkominfo.go.id	SQL Injection, Cross-site Scripting, Information Disclosure	Confidentiality, Integrity
65	Kementerian Keuangan	Http://www.depkeu.go.id	Cross-site Scripting, Information Disclosure	Integrity
66	Kementerian Kesehatan	Http://www.depkes.go.id	SQL Injection,	Confidentia

			Information Disclosure	lity
67	Kementerian Perhubungan	Http://www.dephub.go.id	SQL Injection, Cross-site Scripting, Information Disclosure	Confidentia lity, Integrity
68	Badan Umum dan Logistik	Http://www.bulog.co.id	Cross-site Sctipting, Information Disclosure	Confidentia lity, Integrity
69	Kementerian Dalam Negeri	Http://www.depdagri.go.id	Cross-site Scripting, Information Disclosure	Confidentia lity, Integrity
70	Kementerian Budaya dan Pariwisata	Http://www.budpar.go.id	SQL Injection, Information Disclosure	Confidentia lity
71	Badan Standar Nasional	Http://www.bsn.go.id	SQL Injection, Information Disclosure	Confidentia lity
72	Badan Pusat Statistik	Http://www.bps.go.id	SQL Injection, Cross-site Scripting, Information Disclosure	Confidentia lity, Integrity
73	Badan Pengkajian dan Pengembangan Teknologi	Http://www.bppt.go.id	SQL Injection, Information Disclosure	Confidentia lity
74	Kementerian Hukum dan Hak Asasi Manusia	Http://www.kemhumkam.go.id	SQL Injection, Information Dis	Confidentia lity
75	Sistem E-Pengadaan Pemerintah Kemkominfo	Http://sepp.depkominfo.go.id	SQL Injection, Put Method, Delete Method, Information Disclosure	Confidentia lity, Integrity
77	Komisi Perlindungan Anak Indonesia	Http://www.kpai.go.id	Information Disclosure	Confidentia lity
78	Pajak	Http://www.pajak.go.id	Reflected Cross-site Scripting, Information Disclosure	Confidentia lity, Integrity
79	Badan Koordinasi Keluarga Berencana Nasional	http://www.bkkbn.go.id	Information Disclosure	Confidentia lity
80	Perbendaharaan	http://www.perbendaharaan.go.id81	Reflected Cross-site Scripting, Information	Confidentia lity, Integrity

			Disclosure	
81	Indonesia National Single Window	Http://www.insw.go.id	SQL Injection, Information Disclosure	Confidentiality
82	Badan Nasional Penanggulan Bencana	Http://www.bnpb.go.id	SQL Injection, Information	Confidentiality
83	Kementerian Perumahan Rakyat	Http://www.kemenpera.go.id	Reflected Cross-site Scripting, Information Disclosure	Confidentiality, Integrity

4.3.1. Confidentiality (Kerahasiaan)

Merupakan sebuah konsep dalam keamanan informasi, bahwa setiap informasi harus terjaga kerahasiannya jangan sampai rahasia informasi tersebut bocor atau diketahui oleh orang yang tidak berhak. Dalam hal ini dalam keamanan informasi pada web portal adalah : sebuah informasi pada sistem yang sensitif, seperti ketika web portal tersebut bisa disusupi oleh orang yang tidak berhak dan merubah serta mengakses sistem tersebut. Sepertihalnya serangan *SQL Injection* pada suatu itu menyebabkan kerahasiaan suatu sistem aplikasi web sudah tidak lagi terjaga kerahasiaannya.

4.3.2. *Integrity* (Keutuhan)

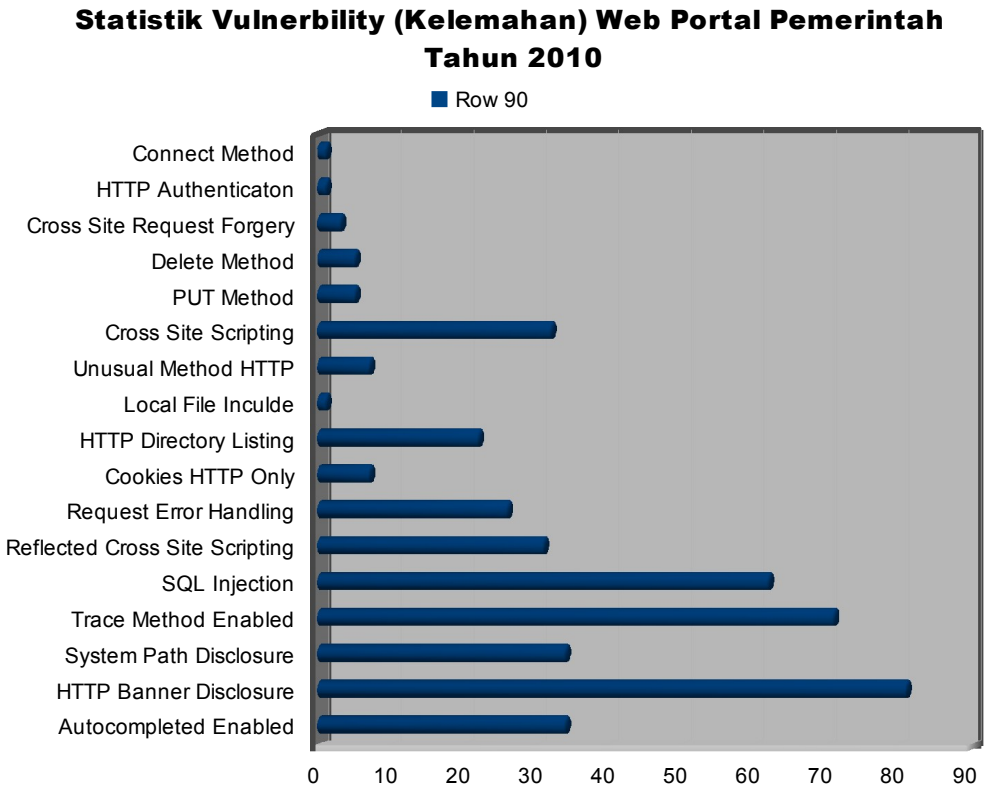
Keutuhan (*integrity*) pada suatu inforamasi adalah sangat penting dan harus dijaga dengan sebenar-benarnya. Karena ketika informasi tersebut berkurang maka nilai informasi dan keutuhannya sudah tidak lagi sempurna. Serangan yang sering terjadi pada sebuah web yang menyerang keutuhan (*integrity*) tersebut adalah *cross-site scripting*, *reflected cross-site scripting.*

4.3.3. *Availability* (Ketersediaan)

Ketersediaan dari informasi pada web portal pemerintah adalah amat sangat penting, terlebih dalam web portal tersebut ada layanan informasi yang sifatnya harus selalu ada dan penting untuk diakses oleh orang lain yang memerlukannya. Namun serangan pada *availability* suatu web amat sangat maju dan berkembang, sepertihalnya serangan *web defacement,* yang menyerang secara keseluruhan tampilan depan halaman web secara penuh.

4.4. Statistik Ancaman pada Kelemahan (*Vulnerability*) Keamanan Informasi terhadap Web Portal Pemerintah Pusat Tahun 2010

Hasil analisis menggunakan perhitungan sederhana, yang digabungkan dari beberapa audit keamanan web portal pemerintah sebanyak 83 yang terdiri dari web portal kementerian, lembaga dan badan yang berada dibawah naungan pemerintah. Dengan menggunakan *tools* yang sudah di jelaskan diatas, ada beberapa kelemahan yang terdapat pada web portal pemerintah saat ini, yaitu digambarkan dengan grafik berikut ini :



Gambar IV.5. Statistik Kelemahan Web Portal Pemerintah 2010

Penjelasan :

1. ***Reflected Cross Site Scripting***, ***Cross-site Scripting*** (XSS) adalah jenis kerentanan keamanan aplikasi web yang memungkinkan kode injeksi oleh pengguna web jahat ke halaman web yang dilihat oleh pengguna lain. Sebuah kerentanan XSS dimanfaatkan dapat digunakan oleh penyerang

untuk memotong kontrol akses, mencuri data, sering pada serangan phishing dan melancarkan serangan ditargetkan menggunakan browser exploits.

2. ***Error Handling***, Server gagal untuk memenuhi permintaan serangan. Server baik adalah sadar bahwa telah mengalami kesalahan atau jika tidak mampu menangani permintaan. manual penyelidikan lebih lanjut diperlukan.
3. ***System Path Disclosure,*** Berbagai sistem jalur diungkapkan dalam kode sumber aplikasi klien atau file lainnya. Informasi ini dapat digunakan oleh penyerang untuk membuat tebakan tentang lingkungan aplikasi dan segala kelemahan warisan yang mungkin datang dengan itu.
4. ***Method Trace Enable,*** Metode TRACE digunakan untuk debug koneksi web server dan memungkinkan klien untuk melihat apa yang diterima di ujung lain dari rantai permintaan. Diaktifkan secara default pada beberapa server web, penyerang remote dapat pelecehan HTTP TRACE fungsi, yaitu Cross-site Scripting (XSS). Biasanya fungsi ini tidak dapat secara mudah dieksploitasi dalam skenario dunia nyata.
5. ***HTTP Directory Listing,*** *Directory listing* memungkinkan penyerang untuk mendapatkan pemahaman yang lebih baik tentang server dan struktur aplikasi. Dalam beberapa situasi listing directroy dapat mengungkapkan sumber daya yang tidak seharusnya diketahui.
6. ***Autocompleted Enable,*** *Autocomplete* selalu harus dinonaktifkan ('off' autocomplete =), terutama dalam bentuk yang proses data sensitif, seperti formulir dengan field password, karena penyerang, jika dapat mengakses cache browser, dengan mudah dapat memperoleh informasi cache dalam teks-jelas.
7. ***HTTP Banner Disclosure***, Aplikasi ini mengungkapkan jenis dan versi. Informasi ini dapat digunakan oleh penyerang untuk membuat tebakan tentang lingkungan aplikasi dan segala kelemahanya.
8. ***SQL Injection (SQLI)*** , teknik injeksi kode yang mengeksploitasi kerentanan keamanan yang terjadi di lapisan basis data sebuah aplikasi

web. kerentanan ini hadir ketika masukan pengguna baik salah disaring untuk lolos karakter string literal tertanam dalam pernyataan SQL atau masukan pengguna tidak *strongly typed* dan dengan demikian tak terduga dieksekusi.

9. ***PUT Method,*** memungkinkan klien untuk meng-upload file baru pada web server. Seorang penyerang bisa memanfaatkannya dengan meng-upload file berbahaya (misalnya: file asp yang mengeksekusi perintah dengan cmd.exe memohon), atau dengan hanya menggunakan server korban sebagai file repositori.
10. ***Delete Method,*** memungkinkan klien untuk menghapus file pada web server. Seorang penyerang dapat memanfaatkan sebagai cara yang sangat sederhana dan langsung ke deface situs web atau untuk me-mount serangan DoS.
11. ***Connect Method,*** digunakan oleh klien dan proxy untuk berhasil masuk pada jalur koneksi HTTPS tanpa proxy untuk melihat data.
12. ***Local File Include*** (LFI), adalah kerentanan yang memungkinkan penyerang untuk mengambil atau mengeksekusi file server-side. Kerentanan muncul dengan memungkinkan input pengguna yang disediakan unsanitized, yang biasanya berisi karakter khusus, untuk diteruskan ke fungsi yang jalan proses.
13. ***'HTTPOnly',*** adalah sebuah bendera tambahan termasuk dalam header respon HTTP *Set-Cookie* yang menentukan bahwa cookie tidak dapat diakses oleh kode *client-side* seperti JavaScript, Flash, dll Akibatnya, bahkan jika *Cross-site Scripting* (XSS) ada cacat, dan pengguna sengaja mengakses sumber daya yang mengeksploitasi cacat ini, browser tidak akan mengungkapkan cookie untuk pihak ketiga dan karenanya sesi pengguna akan dilindungi dari dibajak.
14. ***Cross-site Request Forgery*** (CSRF), adalah jenis berbahaya mengeksploitasi dimana perintah yang tidak sah yang dikirimkan dari pengguna bahwa kepercayaan dari web site. Tidak seperti *Cross-site Scripting* (XSS), yang mengeksploitasi kepercayaan pengguna memiliki

untuk situs tertentu, kepercayaan CSRF mengeksploitasi bahwa situs telah di browser pengguna.

Hasil statistik diatas adalah diambil dari hasil audit *scanning* pada web portal Pemerintah sebanyak 83 web portal Pemerintah yang terdiri dari Kementerian, Lembaga dan Badan di dibawah naungan Pemerintah Pusat, antara lain :

Tabel IV.2. Nama Instansi Pemerintah yang telah diaudit Keamanan Web Portalnya

No	Nama Kementerian/Badan/Lembaga	Alamat URL
1	Badan Pengawas Obat dan Makanan	Http://www.pom.go.id
2	DKI Jakarta	Http://prov.jakarta.go.id
3	Mahkamah Agung	Http://www.mahkamahagung.go.id
4	Perpustakaan Nasional Republik Indonesia	Http://www.pnri.go.id
5	Kementerian Lingkungan Hidup	Http://www.menlh.go.id
6	Komisi Pemilihan Umum	Http://www.kpu.go.id
7	Kementerian Kehutanan	Http://www.dephut.go.id
8	Badan Pemeriksa Keuangan	Http://www.bpk.go.id
9	Lembaga Administrasi Negara	Http://www.lan.go.id
10	Badan Meteorologi dan Geofisika	Http://www.bmkg.go.id
11	Lembaga Pengembangan Antariksa Nasional	Http://www.lapan.go.id
12	Sekretariat Negara	Http://www.setneg.go.id
13	Sistem Administrasi Badan Hukum	Http://www.sisminbakum.go.id
14	Tentara Nasional Indonesia	Http://www.tni.mil.id
15	Komisi Penyiaran Indonesia	Http://www.kpi.go.id
16	Kementerian Aparatur Negara	Http://www.menpan.go.id
17	Kementerian Politik dan Keamanan	Http://www.polkam.go.id
18	Polisi Republik Indonesia	Http://www.polri.go.id
19	Kejaksaan	Http://www.kejaksaan.go.id
20	Kementerian Perindustrian	Http://www.kemenperin.go.id
21	Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah	Http://www.lkpp.go.id
22	Kementerian Pemuda dan Olahraga	Http://www.kemenpora.go.id
23	Kementerian Pertahanan	Http://www.kemhan.go.id
24	Kementerian Kelautan dan Perikanan	Http://www.kkp.go.id

25	Kementerian Agama	Http://www.kemenag.go.id
26	Kementerian Sosial	Http://www.depsos.go.id
27	Kementerian Ekonomi	Http://www.ekon.go.id
28	Badan Tenaga Nuklir Nasional	Http://www.batan.go.id
29	Badan Pengawas Pasar Modal	Http://www.bapepam.go.id
30	Bakosurtanal	Http://www.bakosurtanal.go.id
31	Arsip Nasional Republik Indonesia	Http://www.anri.go.id
32	Badan Pengawas Tenaga Nuklir	Http://www.bapeten.go.id
33	Badan Pertanahan Nasional	Http://www.bpn.go.id
34	Badan Pengawas Keuangan dan Pembangunan	Http://www.bpkp.go.id
35	Badan Pembinaa Hukum Nasional	Http://www.bphn.go.id
36	Badan Koordinasi Penanaman Modal	Http://www.bkpm.go.id
37	Badan Kepegawaian Negara	Http://www.bkn.go.id
38	Bank Indonesia	Http://www.bi.go.id
39	Beacukai	Http://www.beacukai.go.id
40	Badan Perencanaan Nasional	Http://www.bappenas.go.id
41	Komisi Pengawan Persaingan Usaha	Http://www.kppu.go.id
42	Lembaga Pertahanan Nasional	Http://www.lemhannas.go.id
43	Lembaga Sandi Negara	Http://www.lemsaneg.go.id
44	Lembaga Penelitian Indonesia	Http://www.lipi.go.id
45	Kementerian Pemberdayaan Perempuan	Http://www.menegpp.go.id
46	Kementerian Koordinator Bidang Kesejahteraan Rakyat	Http://www.menkokesra.go.id
47	Mahkamah Konstitusi	Http://www.mahkamahkonstitusi.go.id
48	Majelis Permusyawaratan Indonesia	Http://www.mpr.goid
49	Dinas Tenaga Kerja dan Transmigrasi	Http://www.nakertrans.go.id
50	Pos dan Telekomunikasi	Http://www.postel.go.id
51	Kementerian Pekerjaan Umum	Http://www.pu.go.id
52	Sekretariat Kabinet	Http://www.setgab.go.id
53	Kementerian Riset dan Teknologi	Http://www.ristek.go.id
54	Republik Indonesia	Http://www.indonesia.go.id
55	Kementerian Imigrasi	Http://www.imigrasi.go.id
56	Energi dan Sumber Daya Mineral	Http://www.esdm.go.id
57	Dewan Perwakilan Rakyat	Http://www.dpr.go.id
58	Dewan Perwakilan Daerah	Http://www.dpd.go.id
59	Kementerian Pendidikan Nasional	Http://www.kemdiknas.go.id
60	Direktorat Jenderal HAKI	Http://www.dgip.go.id

61	Kementerian Pertanian	Http://www.deptan.go.id
62	Kementerian Luar Negeri	Http://www.deplu.go.id
63	Kementerian Koperasi dan Usaha Kecil dan Menengah	Http://www.depkop.go.id
64	Kementerian Komunkasi dan Informatika	Http://www.depkominfo.go.id
65	Kementerian Keuangan	Http://www.depkeu.go.id
66	Kementerian Kesehatan	Http://www.depkes.go.id
67	Kementerian Perhubungan	Http://www.dephub.go.id
68	Badan Umum dan Logistik	Http://www.bulog.co.id
69	Kementerian Dalam Negeri	Http://www.depdagri.go.id
70	Kementerian Budaya dan Pariwisata	Http://www.budpar.go.id
71	Badan Standar Nasional	Http://www.bsn.go.id
72	Badan Pusat Statistik	Http://www.bps.go.id
73	Badan Pengkajian dan Pengembangan Teknologi	Http://www.bppt.go.id
74	Kementerian Hukum dan Hak Asasi Manusia	Http://www.kemhumkam.go.id
75	Sistem E-Pengadaan Pemerintah Kemkominfo	Http://sepp.depkominfo.go.id
77	Komisi Perlindungan Anak Indonesia	Http://www.kpai.go.id
78	Pajak	Http://www.pajak.go.id
79	Badan Koordinasi Keluarga Berencana Nasional	http://www.bkkbn.go.id
80	Perbendaharaan	http://www.perbendaharaan.go.id81
	Indonesia National Single Window	Http://www.insw.go.id
81	Badan Nasional Penanggulan Bencana	Http://www.bnpb.go.id
82	Kementerian Perumahan Rakyat	Http://www.kemenpera.go.id
83	Kementerian Pedesaan Tertinggal	Http://www.kemenegpdt.go.id

4.5. Analisa Kajian Model Keamanan Web Portal Pemerintah

Kajian terhadap analisis model keamanan web portal ini, Penulis telah melakukan analisa tersebut menggunakan sebuah pendekatan *attack model* berdasarkan dari *Building Security in Maturity Model* (BSIMM). Dimana dari hasil tersebut dapat berkesimpulan dengan pendekatan beberapa teknologi, salah satunya adalah *Web Application Firewall.* Mungkin dengan mengadopsi teknologi tersebut dapat memberikan hasil yang lebih baik dari model sebelumnya.

4.6. Membangun Rancangan Model Keamanan Web Portal Pemerintah

Model merupakan representasi atau deskripsi yang menerangkan suatu objek, sistem ataupun konsep yang akan diimplementasikan pada dunia nyatanya. Disini penulis mencoba untuk merancang suatu model dari sebuah keamanan web portal untuk Pemerintah guna menjaga keamanan informasi suatu web portal penyelenggara Pemerintah.

4.6.1. BSIMM (*Building Security in Maturity Model*)

BSIMM (*Building Security in Maturity Model*) dirancang untuk membantu kita memahami, mengukur, dan membangun inisiatif rencana ketika kita akan membangun sebuah perangkat lunak yang aman.. BSIMM (*Building Security In Maturity Model*) diciptakan sebagai panduan, dengan mengamati dan menganalisa data dalam dunia nyata. Dalam hal ini Penulis mengadopsi domain *Intellegence Attack Model* bagian dari BSIMM (*Building Security In Maturity Model*). BSIMM ini juga mempunyai beberapa domain yang bisa kita jadikan acuan model seperti *Governance*, *Intellegence*, *SSDL Touchpoint*, dan *Deployment*. tersebut. Tetapi Penulis telah mengambil *Attack Model* bagian dari model *Intellegence.* Untuk attack model itu sendiri juga mempunyai beberapa panduan, pada tabel dibawah ini :

Tabel IV.3. Building Security In Maturity Model, Intelligence : Attack Model

KECERDASAN: MODEL SERANGAN **Ancaman pemodelan, kasus-kasus, klasifikasi data, pola serangan dan teknologi yang spesifik**			
Urutan	Obyektif	Aktifitas	Level
AM1.1	Memahami dasar serangan	Membangun dan menganalisa daftar jumlah kemungkinan serangan	1
AM1.2	Prioritaskan aplikasi dengan data yang dikonsumsi / manipulasi	Buat skema klasifikasi data dan inventarisasi	
AM1.3	Memahami "siapa" penyerang	Identifikasi potensi serangan	
AM1.4	Memahami latar belakang dari	Mengumpulkan dan	

	organisasi	mempublikasikan cerita serangan	
AM2.1	Menyediakan sumber daya untuk menguji keamanan	Membangun pola serangan dan kasus penyalahgunaan terkait dengan serangan yang berpotensial	2
AM2.2	Memahami teknologi serangan didorong	Membuat pola teknologi serangan tertentu	
AM2.3	Serangan saat ini / kelemahan pada lingkungan sistem tersebut	Kumpulkan tipe/pola serangan	
AM2.4	Perspektif komunikasi dalam penyerangan	Membangun forum internal untuk membahas serangan (Teknologi / Standart / Kebutuhan)	
AM3.1	Lakukan skenario serangan	Memiliki tim untuk mengembangkan metode serangan baru	3
AM3.2	Tester dan audit	Membuat dan menggunakan otomatisasi untuk melakukan apa yang akan dilakukan penyerang (*Prevention Attack*)	

Dari hasil tabel diatas dapat disimpulkan ada beberapa level yang harus dilalui untuk mendapatkan sebuah model keamanan informasi tersebut, seperti gambar berikut :

Gambar IV.6. Alur Level Attack Model BSIMM

Ket :

Level 1 Kategori Serangan (penyerangan, serangan yang mungkin terjadi, dan

kronologis serangan) yang tertuju pada basis data atau asset dari aplikasi tersebut. Mengidentifikasi potensial serangan yang terjadi, baik serangan potensial yang menyebabkan perhatian pada organisasi serta setiap serangan fatal yang telah terjadi. Manajer harus membuat skema klasifikasi data pada serangan tersebut dan meprioritaskan keamanan sistem pada aplikasi tersebut, level ini masuk dalam tahap *assesment security* terhadap keamanan aplikasi.

Level 2 *Risk Assesment,* pada tahap ini meliputi sejauh mana penyerang dan serangan yang cukup bisa membahayakan sistem aplikasi tersebut. Para SSG (*Software Security Group*) harus mengumpulkan intelijen serangan dan memperluas pengetahuan serangannya untuk memasukkan kedua pola serangan tingkat yang lebih tinggi dan lebih rendah tingkat kasus penyalahgunaan. pola serangan harus mencakup informasi teknologi-spesifik yang relevan untuk organisasi. Para SSG (*Software Security Group*) harus mengkomunikasikan informasi penyerang kepada semua pihak yang berkepentingan

Level 3 *Penetration Testing,* Penelitian dan mengurangi pola serangan baru. SSG harus melakukan penelitian serangan pada perangkat lunak perusahaan untuk maju aktivitas penyerang. SSG (*Software Security Group*) harus memberikan pengetahuan dan otomatisasi untuk auditor dan penguji untuk memastikan kegiatan mereka merefleksikan serangan aktual dan potensial yang dilakukan perangkat lunak organisasi.

4.6.1.1. Hasil Analisa Keamanan Web Portal menggunakan Building Security In Maturity Model (BSIMM)

Penulis menjabarkan hasil analisa audit keamanan web portal Pemerintah tmenggunakan panduan dari BSIMM pada domain *attack model,* sebagai berikut :

Tabel IV.3. Tahap Level I Attack Model pada BSIMM

No	Nama Kementerian/Badan/Lembaga	Alamat URL	Jenis Kelemahan/Serangan
1	Badan Pengawas Obat dan Makanan	Http://www.pom.go.id	SQL Injection, Cross-site Scripting, Information Disclosure
2	DKI Jakarta	Http://prov.jakarta.go.id	SQL Injection, Cross-site Scripting, Information Disclosure
3	Mahkamah Agung	Http://www.mahkamahagung.go.id	SQL Injection, Cross-site Scripting, Information Disclosure
4	Perpustakaan Nasional Republik Indonesia	Http://www.pnri.go.id	SQL Injection, information discloser, Information Disclosure
5	Kementerian Lingkungan Hidup	Http://www.menlh.go.id	Reflected Cross-site Scripting, Information Disclosure
6	Komisi Pemilihan Umum	Http://www.kpu.go.id	Information Disclosure
7	Kementerian Kehutanan	Http://www.dephut.go.id	Reflected Cross-site Scripting, Information Disclosure
8	Badan Pemeriksa Keuangan	Http://www.bpk.go.id	Information Disclosure
9	Lembaga Administrasi Negara	Http://www.lan.go.id	Information Disclosure
10	Badan Meteorologi dan Geofisika	Http://www.bmkg.go.id	Information Disclosure
11	Lembaga Pengembangan Antariksa Nasional	Http://www.lapan.go.id	Reflected Cross-site Scripting, Information Disclosure
12	Sekretariat Negara	Http://www.setneg.go.id	Information Disclosure
13	Sistem Administrasi Badan	Http://www.sisminbakum.go.id	SQL Injection,

	Hukum		Reflected Cross-site Scripting Information Disclosure
14	Tentara Nasional Indonesia	Http://www.tni.mil.id	Injection Flaw, Reflected Cross-site Scripting, Information Disclosure
15	Komisi Penyiaran Indonesia	Http://www.kpi.go.id	SQL Injection, Cross-site Scripting, Information Disclosure
16	Kementerian Aparatur Negara	Http://www.menpan.go.id	SQL Injection, Information Disclosure
17	Kementerian Politik dan Keamanan	Http://www.polkam.go.id	SQL Injection, Information Disclosure
18	Polisi Republik Indonesia	Http://www.polri.go.id	SQL Injection, Cross-site Scripting, Information Disclosure
19	Kejaksaan	Http://www.kejaksaan.go.id	SQL Injection, Information Disclosure
20	Kementerian Perindustrian	Http://www.kemenperin.go.id	SQL Injection, Cross-site Scripting, Information Disclosure
21	Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah	Http://www.lkpp.go.id	SQL Injection, Cross-site Scripting, Information Disclosure
22	Kementerian Pemuda dan Olahraga	Http://www.kemenpora.go.id	SQL Injection, Information Disclosure
23	Kementerian Pertahanan	Http://www.kemhan.go.id	SQL Injection, Information Disclosure
24	Kementerian Kelautan dan Perikanan	Http://www.kkp.go.id	Information Disclosure
25	Kementerian Agama	Http://www.kemenag.go.id	Information Disclosure

26	Kementerian Sosial	Http://www.depsos.go.id	SQL Injection, Reflected Cross-site Scripting, Information disclosure
27	Kementerian Ekonomi	Http://www.ekon.go.id	Information Disclosure
28	Badan Tenaga Nuklir Nasional	Http://www.batan.go.id	SQL Injection, Cross-site Scripting, Information Disclosure
29	Badan Pengawas Pasar Modal	Http://www.bapepam.go.id	SQL Injection, Cross-site Scripting
30	Bakosurtanal	Http://www.bakosurtanal.go.id	SQL Injection, Cross-site Scripting, Information Disclosure
31	Arsip Nasional Republik Indonesia	Http://www.anri.go.id	Cross-site Scripting, Information Disclosure
32	Badan Pengawas Tenaga Nuklir	Http://www.bapeten.go.id	SQL Injection, Reflcted Cross-site Scripting, Cross-site Scripting, Information Disclosure
33	Badan Pertanahan Nasional	Http://www.bpn.go.id	SQL Injection, Information Disclosure
34	Badan Pengawas Keuangan dan Pembangunan	Http://www.bpkp.go.id	SQL Injection, Reflected Cross-site Scripting, Information Disclosure
35	Badan Pembinaa Hukum Nasional	Http://www.bphn.go.id	SQL Injection, Information Disclosure
36	Badan Koordinasi Penanaman Modal	Http://www.bkpm.go.id	SQL Injection, Cross-site Scripting, Information Disclosure
37	Badan Kepegawaian Negara	Http://www.bkn.go.id	SQL Injection, Information Disclosure
38	Bank Indonesia	Http://www.bi.go.id	Information

			Disclosure
39	Beacukai	Http://www.beacukai.go.id	SQL Injection, Cross-site Scripting, Information Disclosure
40	Badan Perencanaan Nasional	Http://www.bappenas.go.id	SQL Injection, Information Disclosure
41	Komisi Pengawan Persaingan Usaha	Http://www.kppu.go.id	SQL Injection, Reflected Cross-site Scripting, Information Disclosure
42	Lembaga Pertahanan Nasional	Http://www.lemhannas.go.id	Cross-site Scripting, Information Disclosure
43	Lembaga Sandi Negara	Http://www.lemsaneg.go.id	SQL Injection, Information disclosure
44	Lembaga Penelitian Indonesia	Http://www.lipi.go.id	SQL Injection, Cross-site Scripting, Information Disclosure
45	Kementerian Pemberdayaan Perempuan	Http://www.menegpp.go.id	SQL Injection, Cross-site Scripting, Information Disclosure
46	Kementerian Koordinator Bidang Kesejahteraan Rakyat	Http://www.menkokesra.go.id	SQL Injection, Information Disclosure
47	Mahkamah Konstitusi	Http://www.mahkamahkonstitusi.go.id	SQL Injection, Information Disclosure
48	Majelis Permusyawaratan Indonesia	Http://www.mpr.goid	SQL Injection, Information Disclosure
49	Dinas Tenaga Kerja dan Transmigrasi	Http://www.nakertrans.go.id	SQL Injection, Cross-site Scripting, Information Disclosure
50	Pos dan Telekomunikasi	Http://www.postel.go.id	SQL Injection, Cross-site Scripting, Information

			Disclosure
51	Kementerian Pekerjaan Umum	Http://www.pu.go.id	SQL Injection, Cross-site Scripting, Information Disclosure
52	Sekretariat Kabinet	Http://www.setgab.go.id	SQL Injection, Cross-site Scripting, Information Disclosure
53	Kementerian Riset dan Teknologi	Http://www.ristek.go.id	SQL Injection, Cross-site Scripting, Information Disclosure
54	Republik Indonesia	Http://www.indonesia.go.id	SQL Injection, Information Disclosure
55	Kementerian Imigrasi	Http://www.imigrasi.go.id	SQL Injection, Information Disclosure
56	Energi dan Sumber Daya Mineral	Http://www.esdm.go.id	SQL Injection, Information Disclosure
57	Dewan Perwakilan Rakyat	Http://www.dpr.go.id	SQL Injection, Cross-site Scripting, Information Disclosure
58	Dewan Perwakilan Daerah	Http://www.dpd.go.id	Cross-site Scripting, Information Disclosure
59	Kementerian Pendidikan Nasional	Http://www.kemdiknas.go.id	SQL Injection, Cross-site Scripting, Information Disclosure
60	Direktorat Jenderal HAKI	Http://www.dgip.go.id	SQL Injection, Information Disclosure
61	Kementerian Pertanian	Http://www.deptan.go.id	SQL Injection, Cross-site Scripting, Information Disclosure
62	Kementerian Luar Negeri	Http://www.deplu.go.id	SQL Injection, Information

			Disclosure
63	Kementerian Koperasi dan Usaha Kecil dan Menengah	Http://www.depkop.go.id	SQL Injection, Information, Disclosure
64	Kementerian Komunkasi dan Informatika	Http://www.depkominfo.go.id	SQL Injection, Cross-site Scripting, Information Disclosure
65	Kementerian Keuangan	Http://www.depkeu.go.id	Cross-site Scripting, Information Disclosure
66	Kementerian Kesehatan	Http://www.depkes.go.id	SQL Injection, Information Disclosure
67	Kementerian Perhubungan	Http://www.dephub.go.id	SQL Injection, Cross-site Scripting, Information Disclosure
68	Badan Umum dan Logistik	Http://www.bulog.co.id	Cross-site Sctipting, Information Disclosure
69	Kementerian Dalam Negeri	Http://www.depdagri.go.id	Cross-site Scripting, Information Disclosure
70	Kementerian Budaya dan Pariwisata	Http://www.budpar.go.id	SQL Injection, Information Disclosure
71	Badan Standar Nasional	Http://www.bsn.go.id	SQL Injection, Information Disclosure
72	Badan Pusat Statistik	Http://www.bps.go.id	SQL Injection, Cross-site Scripting, Information Disclosure
73	Badan Pengkajian dan Pengembangan Teknologi	Http://www.bppt.go.id	SQL Injection, Information Disclosure
74	Kementerian Hukum dan Hak Asasi Manusia	Http://www.kemhumkam.go.id	SQL Injection, Information Dis
75	Sistem E-Pengadaan Pemerintah Kemkominfo	Http://sepp.depkominfo.go.id	SQL Injection, Put Method, Delete Method,

			Information Disclosure
77	Komisi Perlindungan Anak Indonesia	Http://www.kpai.go.id	Information Disclosure
78	Pajak	Http://www.pajak.go.id	Reflected Cross-site Scripting, Information Disclosure
79	Badan Koordinasi Keluarga Berencana Nasional	http://www.bkkbn.go.id	Information Disclosure
80	Perbendaharaan	http://www.perbendaharaan.go.id81	Reflected Cross-site Scripting, Information Disclosure
81	Indonesia National Single Window	Http://www.insw.go.id	SQL Injection, Information Disclosure
82	Badan Nasional Penanggulan Bencana	Http://www.bnpb.go.id	SQL Injection, Information
83	Kementerian Perumahan Rakyat	Http://www.kemenpera.go.id	Reflected Cross-site Scripting, Information Disclosure

Penjelasan :

Level 1 Kategori Serangan (penyerangan, serangan yang mungkin terjadi, dan *kronologis* serangan) yang tertuju pada basis data atau asset dari aplikasi tersebut. Mengidentifikasi potensial serangan yang terjadi, baik serangan potensial yang menyebabkan perhatian pada organisasi serta setiap serangan fatal yang telah terjadi. Manajer harus membuat skema klasifikasi data pada serangan tersebut dan meprioritaskan keamanan sistem pada aplikasi tersebut, level ini masuk dalam tahap *assesment security* terhadap keamanan aplikasi.

Tabel IV.4. Hasil pada Tahap Level II Attack Model pada BSIMM

No	Nama Kementerian/Badan/ Lembaga	Alamat URL	Jenis Kelemahan/Serangan	Parameter CIA
1	Badan Pengawas Obat dan Makanan	Http://www.pom.go.id	SQL Injection, Cross-site Scripting, Information Disclosure	Confidentiality, Integrity
2	DKI Jakarta	Http://prov.jakarta.go.id	SQL Injection, Cross-site Scripting, Information Disclosure	Confidentiality, Integrity
3	Mahkamah Agung	Http://www.mahkamahagung.go.id	SQL Injection, Cross-site Scripting, Information Disclosure	Confidentiality, Integrity
4	Perpustakaan Nasional Republik Indonesia	Http://www.pnri.go.id	SQL Injection, information discloser, Information Disclosure	Confidentiality
5	Kementerian Lingkungan Hidup	Http://www.menlh.go.id	Reflected Cross-site Scripting, Information Disclosure	Integrity, Confidentiality
6	Komisi Pemilihan Umum	Http://www.kpu.go.id	Information Disclosure	Confidentiality
7	Kementerian Kehutanan	Http://www.dephut.go.id	Reflected Cross-site Scripting, Information Disclosure	Integrity, Confidentiality
8	Badan Pemeriksa Keuangan	Http://www.bpk.go.id	Information Disclosure	Confidentiality
9	Lembaga Administrasi Negara	Http://www.lan.go.id	Information Disclosure	Confidentiality
10	Badan Meteorologi dan Geofisika	Http://www.bmkg.go.id	Information Disclosure	Confidentiality
11	Lembaga Pengembangan Antariksa Nasional	Http://www.lapan.go.id	Reflected Cross-site Scripting, Information Disclosure	Integrity, Confidentiality
12	Sekretariat Negara	Http://www.setneg.go.id	Information Disclosure	Confidentiality
13	Sistem Administrasi Badan	Http://www.sisminbakum.go.	SQL Injection,	Confidentia

	Hukum	id	Reflected Cross-site Scripting Information Disclosure	lity, Integrity
14	Tentara Nasional Indonesia	Http://www.tni.mil.id	Injection Flaw, Reflected Cross-site Scripting, Information Disclosure	Confidentia lity, Integrity
15	Komisi Penyiaran Indonesia	Http://www.kpi.go.id	SQL Injection, Cross-site Scripting, Information Disclosure	Confidentia lity, Integrity
16	Kementerian Aparatur Negara	Http://www.menpan.go.id	SQL Injection, Information Disclosure	Confidentia lity
17	Kementerian Politik dan Keamanan	Http://www.polkam.go.id	SQL Injection, Information Disclosure	Confidentia lity
18	Polisi Republik Indonesia	Http://www.polri.go.id	SQL Injection, Cross-site Scripting, Information Disclosure	Confidentia lity, Integrity
19	Kejaksaan	Http://www.kejaksaan.go.id	SQL Injection, Information Disclosure	Confidentia lity
20	Kementerian Perindustrian	Http://www.kemenperin.go.id	SQL Injection, Cross-site Scripting, Information Disclosure	Confidentia lity, Integrity
21	Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah	Http://www.lkpp.go.id	SQL Injection, Cross-site Scripting, Information Disclosure	Confidentia lity, Integrity
22	Kementerian Pemuda dan Olahraga	Http://www.kemenpora.go.id	SQL Injection, Information Disclosure	Confidentia lity
23	Kementerian Pertahanan	Http://www.kemhan.go.id	SQL Injection, Information Disclosure	Confidentia lity
24	Kementerian Kelautan dan Perikanan	Http://www.kkp.go.id	Information Disclosure	Confidentia lity
25	Kementerian Agama	Http://www.kemenag.go.id	Information Disclosure	Confidentia lity

26	Kementerian Sosial	Http://www.depsos.go.id	SQL Injection, Reflected Cross-site Scripting, Information disclosure	Confidentiality, Integrity
27	Kementerian Ekonomi	Http://www.ekon.go.id	Information Disclosure	Confidentiality
28	Badan Tenaga Nuklir Nasional	Http://www.batan.go.id	SQL Injection, Cross-site Scripting, Information Disclosure	Confidentiality, Integrity
29	Badan Pengawas Pasar Modal	Http://www.bapepam.go.id	SQL Injection, Cross-site Scripting	Confidentiality, Integrity
30	Bakosurtanal	Http://www.bakosurtanal.go.id	SQL Injection, Cross-site Scripting, Information Disclosure	Confidentiality, Integrity
31	Arsip Nasional Republik Indonesia	Http://www.anri.go.id	Cross-site Scripting, Information Disclosure	Integrity, Confidentiality
32	Badan Pengawas Tenaga Nuklir	Http://www.bapeten.go.id	SQL Injection, Reflcted Cross-site Scripting, Cross-site Scripting, Information Disclosure	Confidentiality, Integrity
33	Badan Pertanahan Nasional	Http://www.bpn.go.id	SQL Injection, Information Disclosure	Confidentiality
34	Badan Pengawas Keuangan dan Pembangunan	Http://www.bpkp.go.id	SQL Injection, Reflected Cross-site Scripting, Information Disclosure	Confidentiality, Integrity
35	Badan Pembinaa Hukum Nasional	Http://www.bphn.go.id	SQL Injection, Information Disclosure	Confidentiality
36	Badan Koordinasi Penanaman Modal	Http://www.bkpm.go.id	SQL Injection, Cross-site Scripting, Information Disclosure	Confidentiality, Integrity
37	Badan Kepegawaian Negara	Http://www.bkn.go.id	SQL Injection, Information	Confidentiality

			Disclosure	
38	Bank Indonesia	Http://www.bi.go.id	Information Disclosure	Confidentiality
39	Beacukai	Http://www.beacukai.go.id	SQL Injection, Cross-site Scripting, Information Disclosure	Confidentiality, Integrity
40	Badan Perencanaan Nasional	Http://www.bappenas.go.id	SQL Injection, Information Disclosure	Confidentiality
41	Komisi Pengawan Persaingan Usaha	Http://www.kppu.go.id	SQL Injection, Reflected Cross-site Scripting, Information Disclosure	Confidentiality, Integrity
42	Lembaga Pertahanan Nasional	Http://www.lemhannas.go.id	Cross-site Scripting, Information Disclosure	Confidentiality, Integrity
43	Lembaga Sandi Negara	Http://www.lemsaneg.go.id	SQL Injection, Information disclosure	Confidentiality
44	Lembaga Penelitian Indonesia	Http://www.lipi.go.id	SQL Injection, Cross-site Scripting, Information Disclosure	Confidentiality, Integrity
45	Kementerian Pemberdayaan Perempuan	Http://www.menegpp.go.id	SQL Injection, Cross-site Scripting, Information Disclosure	Confidentiality, Integrity
46	Kementerian Koordinator Bidang Kesejahteraan Rakyat	Http://www.menkokesra.go.id	SQL Injection, Information Disclosure	Confidentiality
47	Mahkamah Konstitusi	Http://www.mahkamahkonstitusi.go.id	SQL Injection, Information Disclosure	Confidentiality
48	Majelis Permusyawaratan Indonesia	Http://www.mpr.goid	SQL Injection, Information Disclosure	Confidentiality
49	Dinas Tenaga Kerja dan Transmigrasi	Http://www.nakertrans.go.id	SQL Injection, Cross-site Scripting, Information Disclosure	Confidentiality, Integrity
50	Pos dan Telekomunikasi	Http://www.postel.go.id	SQL Injection,	Confidentia

			Cross-site Scripting, Information Disclosure	lity, Integrity
51	Kementerian Pekerjaan Umum	Http://www.pu.go.id	SQL Injection, Cross-site Scripting, Information Disclosure	Confidentia lity, Integrity
52	Sekretariat Kabinet	Http://www.setgab.go.id	SQL Injection, Cross-site Scripting, Information Disclosure	Confidentia lity, Integrity
53	Kementerian Riset dan Teknologi	Http://www.ristek.go.id	SQL Injection, Cross-site Scripting, Information Disclosure	Confidentia lity, Integrity
54	Republik Indonesia	Http://www.indonesia.go.id	SQL Injection, Information Disclosure	Confidentia lity
55	Kementerian Imigrasi	Http://www.imigrasi.go.id	SQL Injection, Information Disclosure	Confidentia lity
56	Energi dan Sumber Daya Mineral	Http://www.esdm.go.id	SQL Injection, Information Disclosure	Confidentia lity
57	Dewan Perwakilan Rakyat	Http://www.dpr.go.id	SQL Injection, Cross-site Scripting, Information Disclosure	Confidentia lity, Integrity
58	Dewan Perwakilan Daerah	Http://www.dpd.go.id	Cross-site Scripting, Information Disclosure	Confidentia lity, Integrity
59	Kementerian Pendidikan Nasional	Http://www.kemdiknas.go.id	SQL Injection, Cross-site Scripting, Information Disclosure	Confidentia lity, Integrity
60	Direktorat Jenderal HAKI	Http://www.dgip.go.id	SQL Injection, Information Disclosure	Confidentia lity
61	Kementerian Pertanian	Http://www.deptan.go.id	SQL Injection, Cross-site Scripting, Information	Confidentia lity, Integrity

			Disclosure	
62	Kementerian Luar Negeri	Http://www.deplu.go.id	SQL Injection, Information Disclosure	Confidentiality
63	Kementerian Koperasi dan Usaha Kecil dan Menengah	Http://www.depkop.go.id	SQL Injection, Information, Disclosure	Confidentiality
64	Kementerian Komunkasi dan Informatika	Http://www.depkominfo.go.id	SQL Injection, Cross-site Scripting, Information Disclosure	Confidentiality, Integrity
65	Kementerian Keuangan	Http://www.depkeu.go.id	Cross-site Scripting, Information Disclosure	Integrity
66	Kementerian Kesehatan	Http://www.depkes.go.id	SQL Injection, Information Disclosure	Confidentiality
67	Kementerian Perhubungan	Http://www.dephub.go.id	SQL Injection, Cross-site Scripting, Information Disclosure	Confidentiality, Integrity
68	Badan Umum dan Logistik	Http://www.bulog.co.id	Cross-site Sctipting, Information Disclosure	Confidentiality, Integrity
69	Kementerian Dalam Negeri	Http://www.depdagri.go.id	Cross-site Scripting, Information Disclosure	Confidentiality, Integrity
70	Kementerian Budaya dan Pariwisata	Http://www.budpar.go.id	SQL Injection, Information Disclosure	Confidentiality
71	Badan Standar Nasional	Http://www.bsn.go.id	SQL Injection, Information Disclosure	Confidentiality
72	Badan Pusat Statistik	Http://www.bps.go.id	SQL Injection, Cross-site Scripting, Information Disclosure	Confidentiality, Integrity
73	Badan Pengkajian dan Pengembangan Teknologi	Http://www.bppt.go.id	SQL Injection, Information Disclosure	Confidentiality
74	Kementerian Hukum dan Hak Asasi Manusia	Http://www.kemhumkam.go.id	SQL Injection, Information Dis	Confidentiality

75	Sistem E-Pengadaan Pemerintah Kemkominfo	Http://sepp.depkominfo.go.id	SQL Injection, Put Method, Delete Method, Information Disclosure	Confidentiality, Integrity
77	Komisi Perlindungan Anak Indonesia	Http://www.kpai.go.id	Information Disclosure	Confidentiality
78	Pajak	Http://www.pajak.go.id	Reflected Cross-site Scripting, Information Disclosure	Confidentiality, Integrity
79	Badan Koordinasi Keluarga Berencana Nasional	http://www.bkkbn.go.id	Information Disclosure	Confidentiality
80	Perbendaharaan	http://www.perbendaharaan.go.id81	Reflected Cross-site Scripting, Information Disclosure	Confidentiality, Integrity
81	Indonesia National Single Window	Http://www.insw.go.id	SQL Injection, Information Disclosure	Confidentiality
82	Badan Nasional Penanggulan Bencana	Http://www.bnpb.go.id	SQL Injection, Information	Confidentiality
83	Kementerian Perumahan Rakyat	Http://www.kemenpera.go.id	Reflected Cross-site Scripting, Information Disclosure	Confidentiality, Integrity

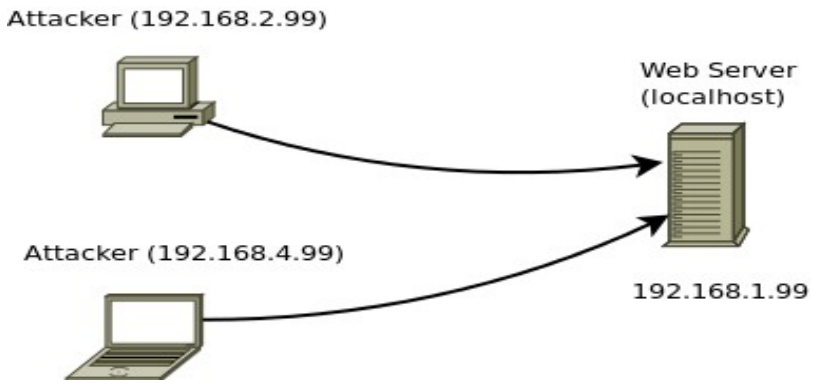
Penjelasan :

Level 2 *Risk Assesment,* pada tahap ini meliputi sejauh mana penyerang dan serangan yang cukup bisa membahayakan sistem aplikasi tersebut. Para SSG harus mengumpulkan intelijen serangan dan memperluas pengetahuan serangannya untuk memasukkan kedua pola serangan tingkat yang lebih tinggi dan lebih rendah tingkat kasus penyalahgunaan. pola serangan harus mencakup informasi teknologi-spesifik yang relevan untuk organisasi. Para SSG (*Software Security Group*) harus mengkomunikasikan informasi penyerang kepada semua pihak yang berkepentingan

Tabel IV.5. Tahap Level III Attack Model pada BSIMM

No	Nama Server	Alamat URL	Jenis Kelemahan/Serangan	Parameter CIA
1	Localhost	http://192.168.1.99	SQL Injection, Cross-site Scripting, Information Disclosure	Confidentiality, Integrity

Dengan ilustrasi serangan (*tester*) dan *penetration / audit* sebagai berikut :



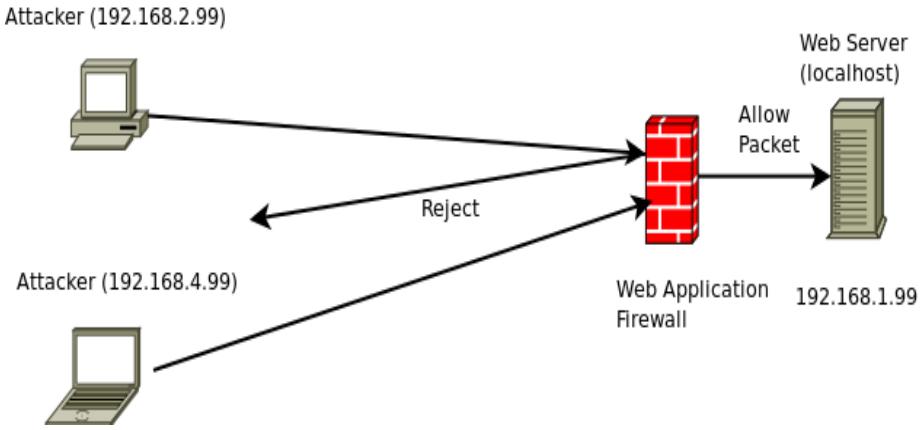
Gambar IV.7. Pengujian / Audit Web Aplikasi

Penjelasan :

Level 3 *Penetration Testing,* Penelitian dan mengurangi pola serangan baru. SSG harus melakukan penelitian serangan pada perangkat lunak perusahaan untuk maju aktivitas penyerang. SSG (*Software Security Group*) harus memberikan pengetahuan dan otomatisasi untuk auditor dan penguji untuk memastikan kegiatan mereka merefleksikan serangan aktual dan potensial yang dilakukan perangkat lunak organisasi.

Tabel IV.6. Hasil Penetration Testing pada Server Internal

No	Nama Server	Alamat URL	Jenis Kelemahan/Serangan	Parameter CIA
1	PL-Server	http://192.168.1.99	-	-



Gambar IV.8. Simulasi Penetration Testing

4.6.2. Web Application Firewall

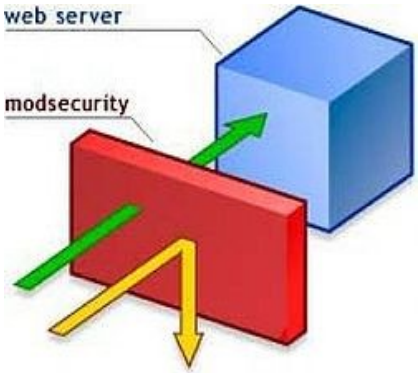
Sebuah aplikasi W*eb Applications Firewall* (WAF) adalah suatu *tools* tambahan modul yang terintegrasi dengan *web server apache*, dimana berfungsi sebagai *filtering* atau penyaringan dengan menerapkan aturan komunikasi HTTP. Secara umum, aturan-aturan ini mencakup serangan umum seperti *Cross-site Scripting* (XSS) dan *SQL Injection*. Dengan menyesuaikan aturan ke aplikasi *web server apache*, banyak serangan yang dapat diidentifikasi dan diblokir. Dalam pemggunaan web aplikasi *firewall* ini Penulis menggunakan *Mod Security* sebagai ujicoba dalam penelitian. Perlu diketahui *web application firewall* banyak sekali ragam jenis dan kebutuhannya, kebetulan Peneliti menggunakan *web application firewall* berbasis *open source* yaitu mod security. Berikut beberapa produk dari *web application firewall* tersebut :

- Applicure - DotDefender
- Radware AppWall

- Armorlogic - Profense
- Barracuda Networks - Application Firewall
- Bee-Ware - iSentry
- BinarySec - Application Firewall
- BugSec - WebSniper
- Cisco - ACE Web Application Firewall
- Citrix - Application Firewall
- eEye Digital Security - SecureIIS
- F5 - Application Security Manager
- Forum Systems - Xwall, Sentry
- mWEbscurity - webApp.secure
- Phion / Visonys - Airlock
- Privacyware - ThreatSentry IIS Web Application Firewall
- Protegrity - Defiance TMS - Web Application Firewall
- Xtradyne - Application Firewalls

4.6.2.1. ModSecurity

ModSecurity adalah sebuah *web server Apache* modul yang menyediakan web aplikasi *firewall* berbentuk modul aplikasi. *ModSecurity* dalam Bahasa ekstrimnya yaitu fleksibel dan kuat, bahkan medapat julukan sebgai '*Swiss Army Knife firewall Web Application*. " Meskipun hal ini memang benar, aplikasi ini tidak berbuat banyak dan memerlukan aturan untuk memberitahu apa yang harus dilakukan pada aturan web aplikasi firewall ini. ModSecurity telah mengembangkan *Core Role Set* (CRS) yang menyediakan perlindungan penting terhadap serangan di sebagian setiap arsitektur web. Dimana gambaran dari *ModSecurity* itu adalah :

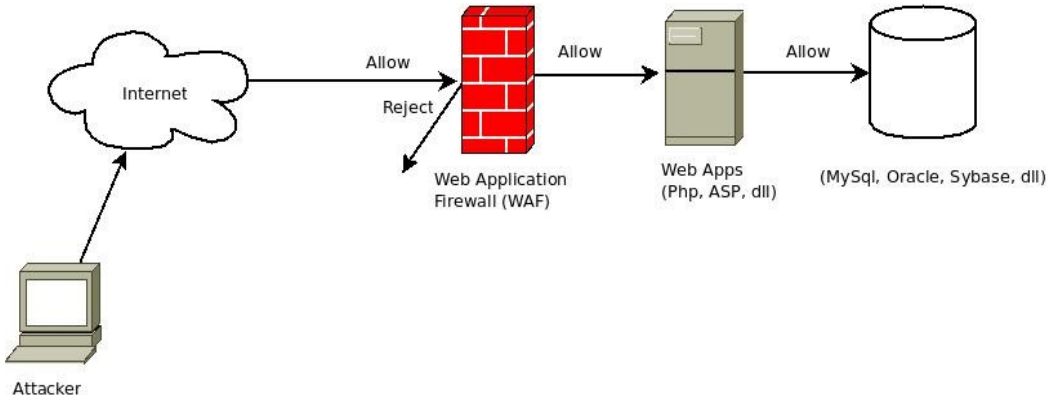


Gambar IV.9. Ilustrasi menggunakan Web Application Firewall

CRS didasarkan pada aturan umum yang berfokus pada identifikasi serangan muatan dalam rangka memberikan perlindungan dari awal dan kerentanan yang tidak diketahui sering ditemukan dalam aplikasi web, yang di sebagian besar kasus *customize* kode.

4.7. Interpretasi

Berdasarkan hasil penelitian menggunakan salah satu model dari BSIMM (*Building Security In Maturity Model*), Peneliti menyimpulkan bahwa model yang cocok untuk web portal pemerintah adalah menggunakan sebuah *web application firewall* sebagai standart keamanan pada web portal Pemerintah untuk menjaga *Confidentiality, Availability, dan Integrity* atas serangan pada kelemahan web portal tersebut, dengan ilustrasi gambar sebagai berikut :



Gambar IV.10. Model Keamanan Web Portal Pemerintah

Sekian sudah interpretasi dari hasil penelitian ini dalam rangka kajian model keamanan web portal pemerintah. Mudah – mudahan kedepannya bisa dikembangkan penelitian ini.

4.8. Implikasi Penelitian

Implikasi dari penelitian ini, ada beberapa hal yang bisa dikembangkan dari penelitian tersebut. Begitu banyak yang harus dikembangkan dalam penelitian serta di perluas aspeknya, takhanya pada sisi teknis semata melainkan organisasi dan sistem pun harus di kembangkan.

4.8.1. Aspek Sistem

Aspek sistem merupakan bagian dari satu entititas yang terkait dengan entitas lain untuk membangun sebuah sistem dengan tujuan yang sama. Terkait dalam penelitian ini yang konsen terhadap keamanan informasi fokus terhadap keamanan web portal Pemerintah saat ini. Beberapa aspek sistem yang harus diperhatikan yaitu :

a. *People* (Pengguna)

People (*User*) sangat krusial dalam sebuah sistem TI khususnya keamanan sistem informasi. Kenapa ? Karena tergantung pada dua aspek yaitu teknis dan non teknis . Seorang user sangat rentan terhadap ancaman sebuah keamanan

informasi. Salah satunya serangan *social engineering, mis configuration* pada sebuah server aplikasi sehingga dengan mudah di terobos keamanan suatu sistem informasi. Pengguna harus selalu meng*improve* kemampuannya dalam pengetahuan Sistem Informasi khususnya keamanan informasi dengan cara *Training IT Security.,*

b. *Process* (Proses)

Proses disini juga merupakan andil besar terhadap kelangsungan aspek pada sistem tersebut, karena proses ini yang menentukan berhasilnya suatu sistem tersebut. Sesempurna apapun sistem tersebut jika pada pada proses ini tidak dijalankan dengan benar secara SOP (*Standart Operating Procedure*) yang telah ditetapkan oleh perusahaan, maka akan gagal sistem tersebut . Karena proses ini terkait sekali dengan disiplin pada user (pengguna) sebagai contoh, seorang staf harus mengupdate / patching suatu sistem pada server yang telah di tentukan jadwalnya, tapi karena proses / SOP itu tidak dijalankan oleh staf tersebut maka akan terjadi sesuatu yang berakibat fatal terhadap pada sistem tersebut. Jadi, pada proses ini amat sangat dibutuhkan SOP sesuai dengan ruang lingkup pada sebuah sistem informasi terkait pada keamanan informasi tersebut.

c. *Technology* (Teknologi)

Teknologi merupakan salahsatu yang amat terpenting setelah ***People*** , dan ***Process***. Tetapi teknologi secanggih apapun dan semahal apapun, jika tidak dikelola dan dikonfigurasi dengan baik sesuai kebutuhan maka hasilnya akan sia-sia juga. Oleh karena itu untuk teknologi peneliti menekankan pada sisi *requirement* (kebutuhan) sesuai organisasi. Dimana harus memenuhi kebutuhan yang salahsatunya : *manageable, implementable, customizeable, interoperability* serta *qualitative*. Disini peneliti mengadopsi sebuah teknologi Open Source dalam implementasi keamanan web portal, yaitu :

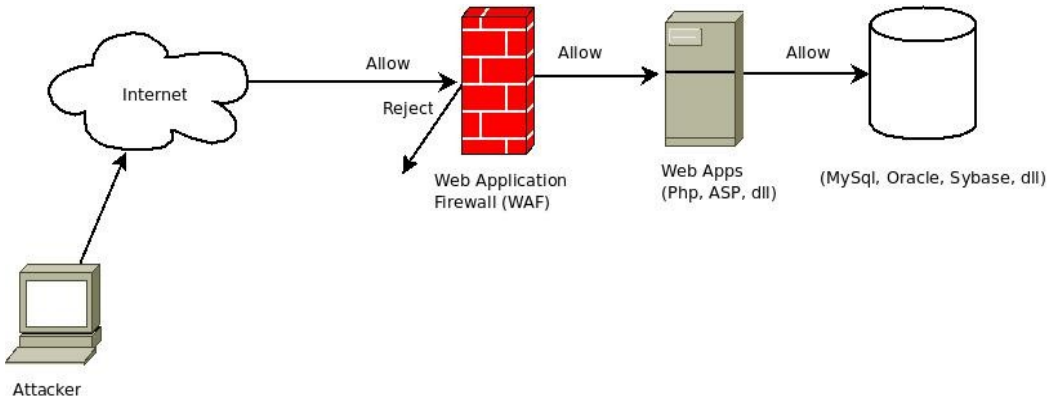
a. Sistem Operasi : Linux Ubuntu 10.4

b. Web Server : Apache web server

c. Web Application Firewall : Mod Security

d. Database : MySQL

Spesifikasi teknologi diatas, bisa diilustrasikan dengan topologi berikut :



Gambar IV.11. Ilustrasi Model Keamanan Web Portal Pemerintah

4.8.1.1. Organisasi / Lembaga

Beberapa pendukung non teknis untuk membangun sebuah keamanan informasi untuk skala *enterprise* pada suatu negara, oleh karenanya peneliti memberi masukan untuk hal tersebut agar terjadi suatu kesinambungan dalam proses keamanan informasi khususnya di Indonesia, antara lain :

a. CoEIS (*Centre of Excellence for Information Security*)

Merupakan sebuah organanisasi yang terdiri dari berbagai elemen, mulai dari institusi Pemerintah, Swasta, Pendidikan . Dimana tugas pokoknya adalah menmbuat sebuah riset tentang keamanan informasi, boleh dikatakan CoEIS ini sebuah wadah organisasi yang cukup besar, karena ada kolaborasi dari seluruh lapisan masyarakat. Sebagaimana telah di jelaskan pada landasan teori.

b. CSIRCC (Computer Security Incident Response Coordinating Centre)

Merupakan badan dibawah naungan Pemerintah yang bertanggungjawab secara terpusat untuk meresponse kejadian insiden keamanan informasi dalam pada instansi Pemerintah.

c. CERT (Computer Emergency Response Team)

Merupakan sebuah organisasi yang berperan sebagai tanggap darurat yang berkaitan dengan insiden keamanan informasi di beberapa lapisan instansi swasta, pendidikan maupun Pemerintah.

d. Centrelized Services Collocation Server Web Portal Government

Merupakan layanan collocation hosting web yang diperuntukan kepada instansi Pemerintah yang mempunyai sistem informasi berbasis web, dengan alasan untuk layanan web hosting terpusat untuk Pemerintah ini adalah agar terjaganya keamanan, stabilitas pada layanan web portal pada Pemerintah.

4.8.2. Aspek Manajerial

Pada umumnya aspek manegerial ini amat sangat dibutuhkan untuk me*manage* sebuah kebijakan, peraturan ataupun *standart operating procedure* yang berlaku pada setiap organisasi maupun lembaga. Pada dasarnya aspek manajerial ini terbagai menjadi dua yaitu teknis maupun non teknis. Pada sisi teknis, mengatur sebuah kebijakan-kebijakan yang sifatnya teknis pada suatu organisasi. Sedangkan non teknis lebih fokus terhadap perkembangan perusahaan pada sisi sumber daya manusia (*human resources*). Pada penelitian ini, untuk aspek manajerial pada sisi teknis harus mempunyai standart keamanan yang mengacu pada beberapa standar, yaitu :

- *ISO/IEC 27001:2005*

  Suatu standar sistem manajemen keamanan informasi (ISMS, information security management system) yang diterbitkan oleh ISO dan IEC pada Oktober 2005. Standar yang berasal dari BS 7799-2 ini ditujukan untuk digunakan bersama dengan ISO/IEC 27002, yang memberikan daftar tujuan pengendalian keamanan dan merekomendasikan suatu rangkaian pengendalian keamanan spesifik. Organisasi yang mengimplementasikan ISMS sesuai dengan pedoman praktek terbaik pada ISO/IEC 27002 kemungkinan juga akan memenuhi persyaratan pada ISO/IEC 27001 walaupun sertifikasinya tetap opsional dan terlepas satu sama lain, kecuali

jika diminta oleh para pemangku kepentingan organisasi [WIK11].

Sedangkan untuk aspek teknis, bisa mengacu pada :

1. ISMS (*Information Security Management System*)

Istilah yang muncul terutama dari ISO/IEC 27002 yang merujuk pada suatu sistem manajemen yang berhubungan dengan keamanan informasi. Konsep utama ISMS untuk suatu organisasi adalah untuk merancang, menerapkan, dan memelihara suatu rangkaian terpadu proses dan sistem untuk secara efektif mengelola keamanan informasi dan menjamin kerahasiaan, integritas, serta ketersediaan aset-aset informasi serta meminimalkan risiko keamanan informasi.

Standar ISMS yang paling terkenal adalah ISO/IEC 27001 dan ISO/IEC 27002 serta standar-standar terkait yang diterbitkan bersama oleh ISO dan IEC. Information Security Forum juga menerbitkan suatu ISMS lain yang disebut *Standard of Good Practice* (SOGP) yang lebih berdasarkan praktik dari pengalaman mereka. Kerangka manajemen teknologi informasi (TI) lain seperti COBIT dan ITIL juga menyentuh masalah-masalah keamanan walaupun lebih terarah pada kerangka tata kelola TI secara umum.

Information Security Management Maturity Model (dikenal dengan ISM-cubed atau ISMS) adalah suatu bentuk lain dari ISMS yang disusun berdasarkan standar-standar lain seperti ISO 20000, ISO 9001, CMM, ISO/IEC 27001, serta konsep-konsep umum tata kelola dan keamanan informasi. ISM3 dapat digunakan sebagai dasar bagi ISMS yang sesuai dengan ISO 9001. ISM3 berbasis pada proses dan mencakup metrik proses sedangkan ISO/IEC 27001 berbasis pada kontrol [WIK11].

2. ITSM (*Information Technology Service Management*)

Suatu metode pengelolaan sistem teknologi informasi (TI) yang secara filosofis terpusat pada perspektif konsumen layanan TI terhadap bisnis perusahaan. ITSM merupakan kebalikan dari pendekatan manajemen TI dan interaksi bisnis yang terpusat pada teknologi. Istilah ITSM tidak

berasal dari suatu organisasi, pengarang, atau pemasok tertentu dan awal penggunaan frase inipun tidak jelas kapan dimulainya.

ITSM berfokus pada proses dan karenanya terkait dan memiliki minat yang sama dengan kerangka kerja dan metodologi gerakan perbaikan proses (seperti TQM, Six Sigma, Business Process Management, dan CMMI). Disiplin ini tidak memedulikan detil penggunaan produk suatu pemasok tertentu atau detil teknis suatu sistem yang dikelola, melainkan berfokus pada upaya penyediaan kerangka kerja untuk menstrukturkan aktivitas yang terkait dengan TI dan interaksi antara personil teknis TI dengan pengguna teknologi informasi.

ITSM umumnya menangani masalah operasional manajemen teknologi informasi (kadang disebut operations architecture, arsitektur operasi) dan bukan pada pengembangan teknologinya sendiri. Contohnya, proses pembuatan perangkat lunak komputer untuk dijual bukanlah fokus dari disiplin ini, melainkan sistem komputer yang digunakan oleh bagian pemasaran dan pengembangan bisnis di perusahaan perangkat lunak-lah yang merupakan fokus perhatiannya. Banyak pula perusahaan non-teknologi, seperti pada industri keuangan, ritel, dan pariwisata, yang memiliki sistem TI yang berperan penting, walaupun tidak terpapar langsung kepada konsumennya [WIK11].

4.8.3. Penelitian Selanjutnya

Cloud Computing (Komputasi Awan) merupakan gabungan pemanfaatan teknologi komputer ('komputasi') dan pengembangan berbasis Internet ('awan'). Awan (cloud) adalah metefora dari internet, sebagaimana awan yang sering digambarkan di diagram jaringan komputer. Sebagaimana awan dalam diagram jaringan komputer tersebut, awan (*cloud*) dalam Cloud Computing juga merupakan abstraksi dari infrastruktur kompleks yang disembunyikannya. Ia adalah suatu metoda komputasi di mana kapabilitas terkait teknologi informasi

disajikan sebagai suatu layanan (*as a service*), sehingga pengguna dapat mengaksesnya lewat Internet ("di dalam awan") tanpa mengetahui apa yang ada didalamnya, ahli dengannya, atau memiliki kendali terhadap infrastruktur teknologi yang membantunya. Menurut sebuah makalah tahun 2008 yang dipublikasi *IEEE Internet Computing* "*Cloud Computing* adalah suatu paradigma di mana informasi secara permanen tersimpan di server di internet dan tersimpan secara sementara di komputer pengguna (client) termasuk di dalamnya adalah desktop, komputer tablet, notebook, komputer tembok, handheld, sensor-sensor, monitor dan lain-lain.

Komputasi awan adalah suatu konsep umum yang mencakup *SaaS*, Web 2.0, dan tren teknologi terbaru lain yang dikenal luas, dengan tema umum berupa ketergantungan terhadap Internet untuk memberikan kebutuhan komputasi pengguna. Sebagai contoh, *Google Apps* menyediakan aplikasi bisnis umum secara dari yang diakses melalui suatu penjelajah web dengan perangkat lunak dan data yang tersimpan di server.

Seiring dalam penyelenggaraan teknologi informasi terhadap pemerintah, peneliti akan mencoba melakukan penelitian pada *cloud computing security* [WIK11].