Jurnal Teknovasi
Volume 02, Nomor 2, 2015, 1 –7
ISSN : 2355-701X

ANALISIS CELAH KEAMANAN *WEBSITE* INSTANSI PEMERINTAHAN DI SUMATERA UTARA

Lipantri Mashur Gultom[1]* & Mawaddah Harahap[2]
[1,2]Program Studi Teknik Komputer, Politeknik LP3I Medan
Telp. 061-7322634 Fax. 061-7322649
*E-mail : lipantri@gmail.com

ABSTRAK

Keamanan *website* merupakan satu hal penting dalam perancangan sebuah *website*. Namun masih banyak *developer website* yang kurang teliti dalam meningkatkan keamanan *website* mereka. Seharusnya para *developer website* harus menerapkan keamanan *website* yang baik di awal perancangan *website* mereka, karena mungkin suatu saat *website* yang telah mereka bangun akan menjadi target pengerusakan oleh hacker. Selain itu *developer website* juga harus sering mengikuti tren serangan terbaru agar mereka dapat mempertahankan dan memperbaiki *website* mereka dari hal-hal yang tidak diinginkan. Ada beberapa masalah pada celah keamanan diantaranya : *cross-site scripting, information leakage, authentication and authorization, Session management, SQL injection, CSRF* dan lain – lain. Pada penelitian ini dianalisis beberapa celah keamanan pada beberapa *website* instansi pemerintahan di sumatera utara yang diambil dari domain *.go.id, karena biasanya *website* ini sangat rentan dari *cybercrime*. Dari hasil analisis ini akan dirancang sebuah model penanganan dari setiap celah keamanan pada setiap *website*. Tujuan jangka panjang dari penelitian ini adalah menghasilkan model penanganan yang baik dari setiap celah keamanan pada *website* berdasarkan tingkat kerentanan sebuah *website*. Sedangkan tujuan khusus dari penelitian ini menganalisis beberapa celah keamanan yang terdapat pada *website* dan tingkat kerentanan setiap *website*. Metode penelitian yang dilakukan ialah Model Black Box dengan tiga tahapan yaitu *Post-attack phase, Attack phase dan Pre-attack phase*. Dari hasil pengujian 64 alamat *website* diperoleh 3 alamat *website* yang memiliki celah keamanan yang terbanyak yaitu : www.binjaikota.go.id (kota binjai), www.taputkab.go.id (kabupaten tapanuli utara) dan www.dairikab.go.id (kabupaten dairi). Selain itu dari 64 alamat webiste yang diuji menunjukkan 48% dengan tingkat celah keamanan yang tinggi dan 52% dengan tingkat celah keamanan yang menengah. Hasil akhir dari pengujian ini telah dimodelkan kedalam bentuk *use case* diagram untuk mempermudah penelitian-penelitian selanjutnya.

Kata kunci : celah keamanan, *website, cybercrime*

PENDAHULUAN

Perkembangan *website* di Indonesia sekarang ini sangat pesat, hal ini terjadi karena semakin bertambahnya jumlah pengguna layanan internet dari tahun ke tahun. Beberapa *website* yang sering diakses oleh pengguna diantaranya *search engine, e-commerce, social networking, forum, portal* berita dan lain – lain. Akan tetapi dibalik kemudahan layanan yang disediakan oleh setiap *website* tersebut ternyata terdapat beberapa masalah pada celah keamanan diantaranya : cross-site scripting, *information leakage, authentication and authorization, Session management*, SQL *injection*, CSRF dan lain–lain. Dengan memanfaatkan celah kemanan ini seseorang dapat melakukan *hacking* pada *website* tersebut.

Pada penelitian ini dianalisis beberapa celah keamanan pada beberapa *website* instansi pemerintahan di sumatera utara yang diambil dari domain *.go.id, karena biasanya *website* ini sangat rentan dari *cybercrime*. Beberapa celah keamanan yang diuji diambil dari hasil survey

Jurnal Teknovasi
Volume 02, Nomor 2, 2015, 1 –7
ISSN : 2355-701X

Application Vulnerability Trends Report : 2014. Dari hasil analisis ini akan dirancang sebuah model penanganan dari setiap celah keamanan pada setiap *website*.

Penelitian ini menggunakan konsep ethical hacking karena berhubungan erat dengan beberapa materi *cybercrimes* yang diatur dalam UU ITE, antara lain: 1. konten ilegal, yang terdiri dari, antara lain: kesusilaan, perjudian, penghinaan/pencemaran nama baik, pengancaman dan pemerasan (Pasal 27, Pasal 28, dan Pasal 29 UU ITE); 2. akses ilegal (Pasal 30); 3. intersepsi ilegal (Pasal 31); 4. gangguan terhadap data (data interference, Pasal 32 UU ITE); 5. gangguan terhadap sistem *(system interference*, Pasal 33 UU ITE); 6. penyalahgunaan alat dan perangkat (*misuse of device,* Pasal 34 UU ITE).

Adapun yang menjadi rumusan masalah dalam penelitian ini, yaitu : Seberapa berapa besar tingkat kerentanan sebuah *website* jika dilakukan pengujian pada beberapa jenis celah keamanan dan bagaimana menghasilkan model penanganan yang baik dari setiap celah keamanan pada *website*. Manfaat dari penelitian ini adalah memberikan kontribusi dalam meningkatkan keamanan dan penanganan kepada pengelola *website* sehingga dapat mengoptimalkan siklus hidup, pemeliharaan dan pengujian *website*.

METODE PENELITIAN

Tahapan–Tahapan Penelitian

Penelitian ini menggunakan model black box dengan tiga tahapan dalam uji penetrasi *website*, yaitu :

1) *Pre-attack phase* : mengumpulkan informasi dengan footprinting dari *website* yang akan di uji. *Website* yang akan diuji diambil dari domain *.go.id yang merupakan *website* resmi pemerintahan daerah yang berada di sumatera utara.
2) *Attack phase* : mencoba melakukan serangan dari informasi yang didapat dari tahapan sebelumnya, misalnya menembus sistem, mendapatkan hak akses ke dalam sistem, mengekspolitasi data yang sensitif dan menanamkan kode yang berbahaya. Pada tahap ini celah keamanan yang akan diuji berdasarkan laporan dari *Application Vulnerability Trends Report* : 2014.
3) *Post-attack phase* : menghasilkan analisis dari semua serangan berdasarkan celah keamanan yang telah di uji pada tahap kedua sehingga akan ditemukan tingkat kerentanan *website* berdasarkan serangan yang telah dilakukan. Hasil akhir analisis berupa model penanganan celah keamanan yang akan direkomendasikan kepengelola *website*.

Kegiatan penelitian dilakukan di laboratorium komputer Politeknik LP3I Medan, Jl. Sisingamangaraja No. 24/275 Simp. Limun Medan–Sumatera Utara.

Peubah Penelitian

Peubah yang diamati dalam penelitian ini yaitu, beberapa alamat *website* resmi pemerintahan daerah di sumatera utara dengan domain *go.id, beberapa celah keamanan yang diuji berdasarkan laporan dari *Application Vulnerability Trends Report* : 2014 dan tingkat kerentanan dari setiap celah kemanan yang ada.

Teknik Pengumpulan Dan Analisis Data

Teknik pengumpulan data yang digunakan sebagai berikut :

1) Observasi : melakukan pengamatan dan analisis beberapa celah keamanan dan tingkat kerentanan *website* dengan menggunakan Arachni Web Application Security Scanner
2) Kepustakaan : mencari data yang berhubungan dengan variabel yang diamati berupa buku, jurnal, surat kabar, artikel, majalah dan sebagainya.

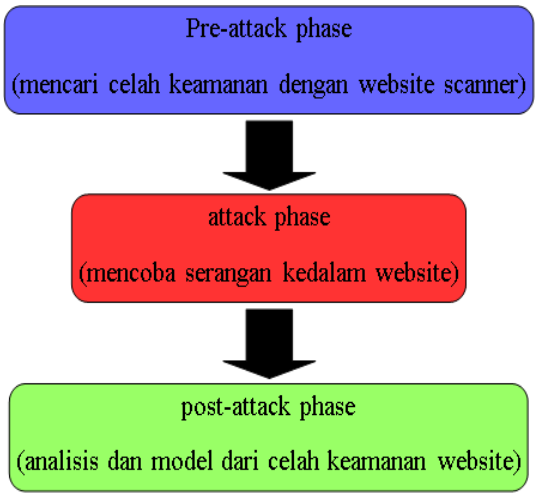
Proses analisis data yang dilakukan yaitu menghitung presentase dan mengklasifikasikan beberapa celah keamanan sesuai dengan tingkat kerentanan yang ditimbulkan serta disajikan dalam

Jurnal Teknovasi
Volume 02, Nomor 2, 2015, 1 –7
ISSN : 2355-701X

bentuk tabel, diagram dan grafik. Dari hasil analisis ini dirancang sebuah model penanganan dari setiap celah keamanan dan tingkat kerentanan yang ada dalam bentuk UML.

Rancangan Penelitian

Rancangan penelitian yang direncanakan digambarkan dalam bentuk diagram blok seperti gambar berikut :



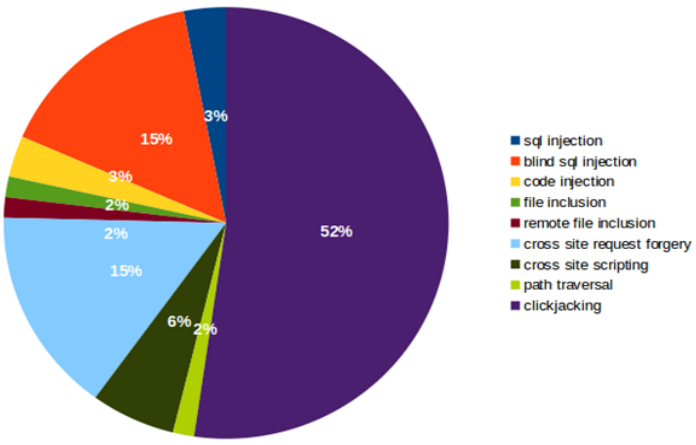
Gambar 1. Rancangan Penelitian

HASIL DAN PEMBAHASAN

Pada sub bab ini dipaparkan hasil penelitian dari tahapan pre-attack phase dari 64 alamat *website* yang aktif dengan kategori domain *.go.id. Berikut ini alamat *website* dengan jumlah celah keamanan yang terbanyak yaitu :

1) www.binjaikota.go.id (kota binjai) dengan 5 celah keamanan
2) www.taputkab.go.id (kabupaten tapanuli utara) dengan 3 celah keamanan
3) www.dairikab.go.id (kabupaten dairi) dengan 2 celah keamanan

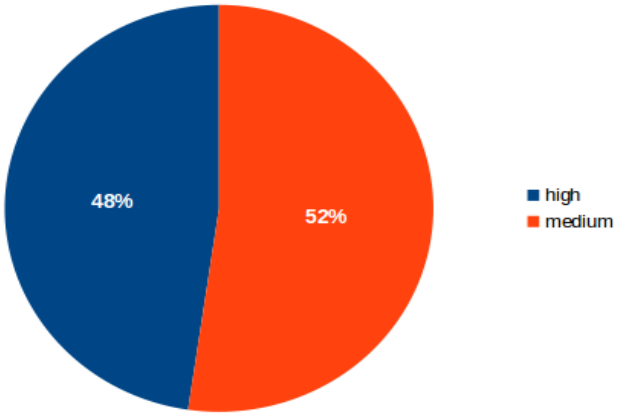
pada alamat *website* tersebut juga memiliki celah keamanan dengan tingkat yang tinggi. Berikut ini ditampilkan perbandingan jenis celah keamanan dari 64 alamat *website* dapat dilihat pada gambar 2.



Gambar 2. Perbandingan Jenis Celah Keamanan

Jurnal Teknovasi
Volume 02, Nomor 2, 2015, 1 –7
ISSN : 2355-701X

Serta perbandingan tingkat celah keamanan dari 64 alamat *website* dapat dilihat pada gambar 3.

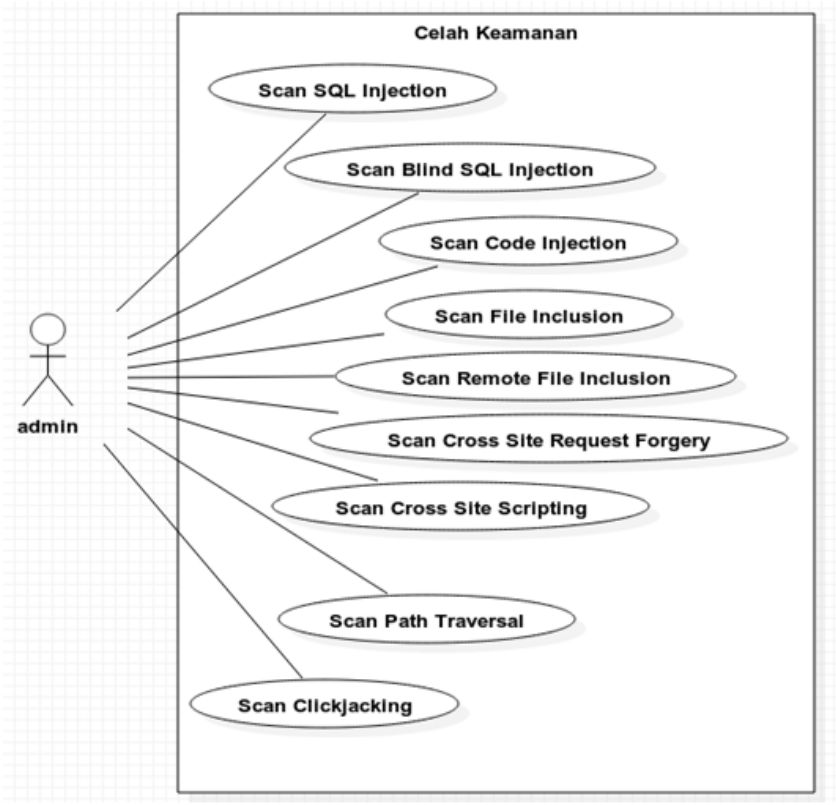


Gambar 3. Perbandingan Tingkat Celah Keamanan

Selanjutnya pada tahapan attack phase dipaparkan beberapa URL dari seluruh alamat *website* yang memiliki celah keamanan sesuai dengan jenis celah keamanannya.

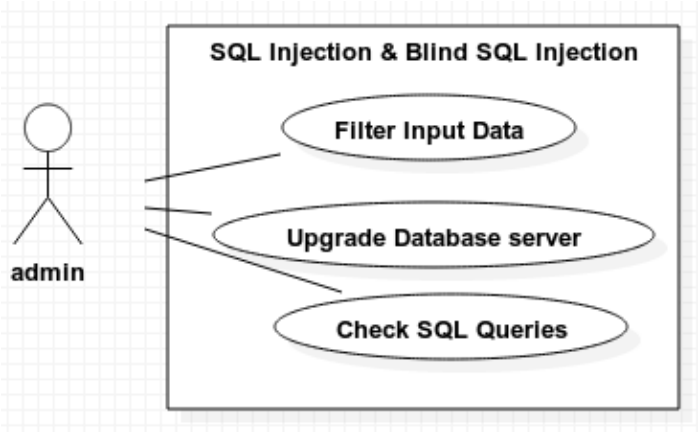
Pada sub bab ini dipaparkan beberapa model penanganan terhadap URL yang memiliki celah keamanan dalam bentuk *use case* diagram.

1. *Use case* Diagram : Celah Keamanan (gambar 4)



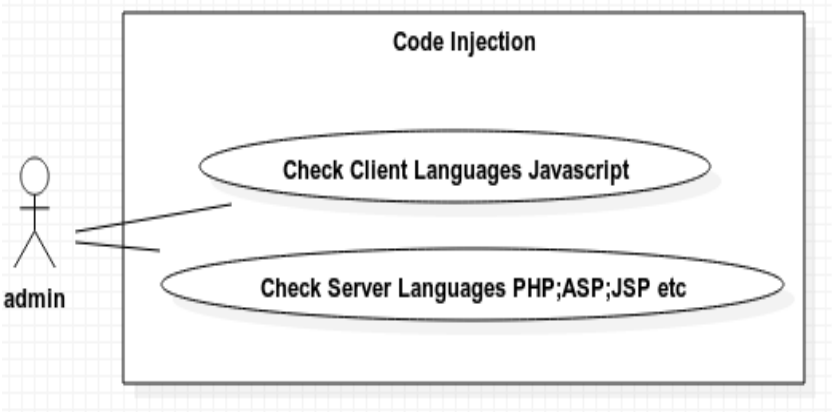
Gambar 4. *use case* diagram : celah keamanan

2. *Use case* Diagram : SQL *Injection & Blind SQL Injection* (gambar 5)



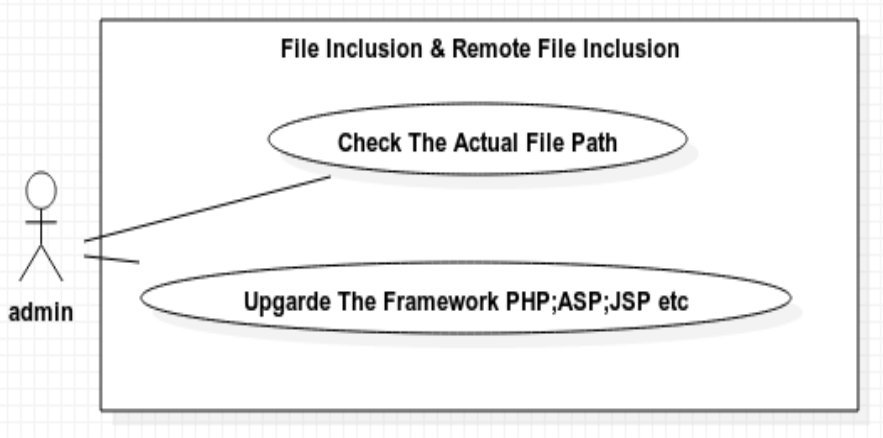
Gambar 5. *use case* diagram : SQL *injection & Blind SQL injection*

3. *Use case* Diagram : *Code Injection* (gambar 6)



Gambar 6. *use case* diagram : *code injection*

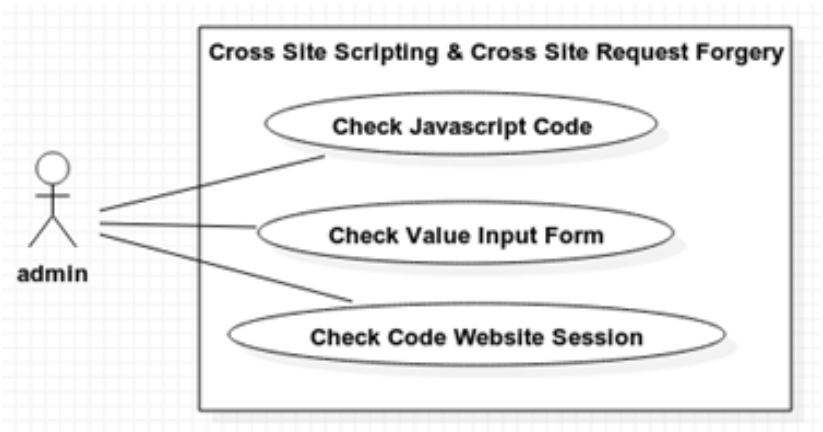
4. *Use case* Diagram : *File Inclusion & Remote File Inclusion* (gambar 7)



Gambar 7. *use case* diagram : *file inclusion & remote file inclusion*

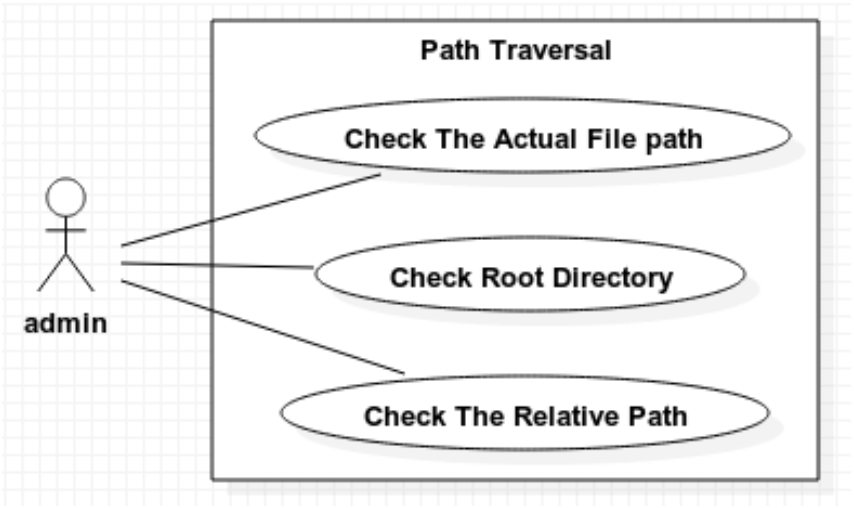
Jurnal Teknovasi
Volume 02, Nomor 2, 2015, 1 –7
ISSN : 2355-701X

5. *Use case* Diagram : *Cross Site Scripting & Cross Site Request Forgery* (gambar 8)



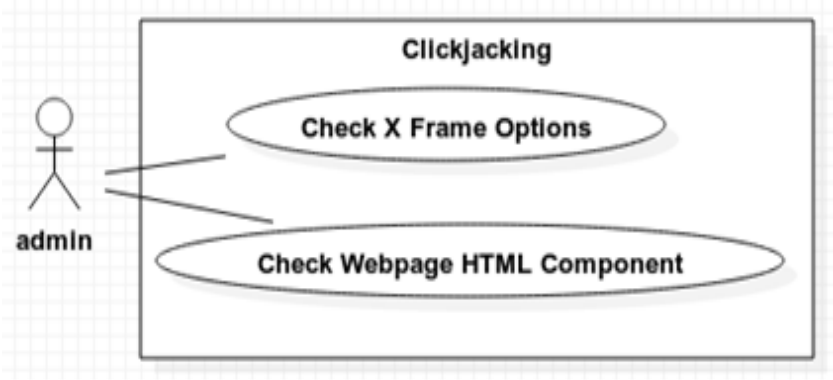
Gambar 8. *use case* diagram : *cross site scripting & cross site request forgery*

6. *Use case* Diagram : *Path Traversal* (gambar 9)



Gambar 9. *use case* diagram : *path traversal*

7. *Use case* Diagram : *Clickjacking* (gambar 10)



Gambar 10. *use case* diagram : *clickjacking*

Dari keseluruhan gambar *use case* diagram tersebut, terdapat komponen actor yaitu admin. Admin merupakan pengelola *website* yang bertanggung jawab dalam menjaga keamanan *website*. Dalam menjaga keamanan *website* tersebut seorang admin harus dapat memantau secara priodik kemungkinan terjadinya penyusupan, pengerusakan dan tindakan–tindakan ilegal lainnya. Oleh karena itu admin dapat menggunakan model *use case* diagram tersebut dalam menjalankan aktifitas pemantauan terhadap *website*nya. Seluruh *use case* diagram tersebut dibagi menjadi beberapa bagian sesuai dengan jenis celah kemanan yang didapat. Selain itu admin juga dapat menentukan tindakan pencegahan terhadap kemungkinan serangan yang akan terjadi dan tindakan perbaikan jika seandainya *website* telah dirusak oleh orang lain.

KESIMPULAN

Website pemerintahan di provinsi sumatera utara memiliki beberapa celah keamanan seperti SQL injection, Blind SQL Injection, Code Injection, File Inclusion, Remote File Inclusion, Cross Site Request Forgery, Cross Site Scripting, Path Traversal dan Clickjacking. Dari hasil penelitian terdapat beberapa *website* yang memiliki celah keamanan yang terbanyak yaitu : www.binjaikota.go.id, www.taputkab.go.id, www.dairikab.go.id dengan tingkat celah keamanan yang tinggi. Hasil pembahasan dapat dirancang beberapa model penanganan dalam bentuk *use case* diagram. Dimana model ini dapat digunakan oleh pengelola *website* untuk melakukan kegiatan pencegahan dan perbaikan dari setiap celah keamanan yang ditemukan.

DAFTAR PUSTAKA

Application Vulnerability Trends Report : 2014. http://www.cenzic.com/downloads/Cenzic_Vulnerability_Report_2014.pdf. Diakses 1 april 2014.

Choy Men Lin. Ethical Hacking. http://uwcisa.uwaterloo.ca/Biblio2/Topic/Choy_Men_Lin_Ethical_Hacking_Final_Report.pdf. Diakses 1 april 2014.

Fuady, M.E. (2005). "*Cybercrime": Fenomena Kejahatan melalui Internet di Indonesia* . *Mediator*,Vol 6, No 2 (2005).

Kesuma, M. C., (2014). *Pencari Celah Keamanan pada Aplikasi Web. Publikasi Jurusan Teknik Informatika,* Fakultas Teknologi Informasi, Institut Teknologi Sepuluh Nopember. Diakses 1 april 2014.

Rodriguez, C., (2012). *The Growing Hacking Threat to Websites* : An Ongoing Commitment to Web Application Security. A Frost & Sullivan White Paper.

Scambray, J., (2011). *Hacking Exposed Web Applications* : Web Application Security Secrets And Solutions Third Edition. McGrawHil.

Shema, M., (2012). *Hacking Web Apps Detecting and Preventing Web Application Security Problems*. Elsevier, Inc.

Utami, E., (2010). *Perbandingan Sistem Keamanan Pengembangan Aplikasi Website Web 2.0 Menggunakan Framework Ruby On Rails Dan Cakephp*. Jurnal DASI Bulan Juni.

Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.