Mencegah Exploit URL Pada Model Business to Customer Pada Toko Citra Ponsel Ketapang

Doni Muliawan[*1], Ria Risti Astanti[2]
[1,2]Jurusan Teknik Informatika; STMIK Pontianak. Jl. Merdeka No.372 Pontianak, 0561-735555
Email: [*1]muliawandoni@gmail.com, [2]RiaRisti@stmikpontianak.ac.id

Abstrak

Keamanan website merupakan satu hal penting dalam perancangan sebuah website. Namun masih banyak developer website yang kurang teliti dalam meningkatkan keamanan website mereka. Celah keamanan (vulnerability) pada dunia komputer adalah suatu kelemahan program/infrastruktur yang memungkinkan terjadinya exploitasi sistem. Penelitian bertujuan membangun sistem pencegahan Exploit URL dengan merapkan algoritma base64. Base64 adalah istilah umum untuk sejumlah skema pengkodean serupa yang mengkodekan data biner dan menerjemahkannya ke dalam representasi basis 64. Skema pengkodean Base64 biasanya digunakan ketika ada kebutuhan untuk menyandikan data biner yang perlu disimpan dan ditransfer melalui media yang dirancang untuk menangani data tekstual. Metode perancangan menggunakan Rapid Application Development (RAD) yang merupakan sebuah strategi pengembangan sistem yang menekankan kecepatan melalui keterlibatan pengguna. Pengumpulan data menggunakan teknik wawancara yang melibat pemakaian recorder untuk perekaman dan melakukan observasi terhadap operasional dan proses bisnis. Pemodelan berorientasi objek yaitu Unified Modelling Language (UML). Pada tahapan pengembangan sistem Exploit URL Pada Model Business to Customer langsung melibat pihak manajemen toko untuk dirumuskan kebutuhan dari pemilik bisnis sebagai penyedia produk. Pemilihan model perangkat lunak yang cocok untuk digunakan dalam sebuah organisasi sangat penting untuk keberhasilan proyek. Hasil penelitian ini adalah sebuah sistem B2C yang menerapkan algoritma base64 dalam mencehah Exploit URL.

Kata kunci*—Algoritma Base64, B2C, Exploit URL*

Abstract

Website security is one important thing in designing a website. But there are still many website developers who are not careful in increasing the security of their websites. The vulnerability in the computer world is a weakness of the program / infrastructure that allows system exploitation. The research aims to build a prevention system for URL exploitation by applying the base64 algorithm. Base64 is a general term for a number of similar coding schemes that encode binary data and translate it into base 64 representations. The Base64 coding scheme is usually used when there is a need to encode binary data that needs to be stored and transferred through media designed to handle textual data. The design method uses Rapid Application Development (RAD), which is a system development strategy that emphasizes speed through user involvement. Data collection uses interview techniques that involve the use of recorders for recording and observing operational and business processes. Object-oriented modeling namely Unified Modeling Language (UML). In the development phase of the URL Exploit system the Business to Customer Model directly involves the store management to formulate the needs of business owners as product providers. The choice of a suitable software model for use in an

organization is very important for the success of the project. The results of this study are a B2C system that applies the base64 algorithm to prevent URL exploits.

Keywords*—Base64 algorithm, B2C, exploit URL*

1. PENDAHULUAN

Keamanan website merupakan satu hal penting dalam perancangan sebuah website. Namun masih banyak developer website yang kurang teliti dalam meningkatkan keamanan website mereka[1]. Celah keamanan (*vulnerability*) pada dunia komputer adalah suatu kelemahan program/infrastruktur yang memungkinkan terjadinya exploitasi sistem[2]. Kerentanan (*vulnerability*) ini terjadi akibat kesalahan dalam merancang, membuat atau mengimplementasikan sebuah sistem. *Vulnerability* akan digunakan oleh *hacker* sebagai jalan untuk masuk kedalam sistem secara ilegal. Hacker biasanya akan membuat *Exploit* yang desesuaikan dengan *vulnerability* yang telah ditemukannya[3]. *Vulnerability/bug* terjadi ketika *developer* melakukan kesalahan logika koding atau menerapkan validasi yang tidak sempurna sehingga aplikasi yang dibuatnya mempunyai celah yang memungkinkan user atau metode dari luar sistem bisa dimasukan kedalam program nya. *Exploit* adalah sebuah kode yang menyerang keamanan komputer secara spesifik. *Exploit* banyak digunakan untuk penentrasi baik secara legal ataupun ilegal untuk mencari kelemahan (*Vulnerability*) pada komputer tujuan[4].

URL (*Uniform Resource Locator*) menunjukan alamat dari sebuah homepage atau menunjukan sumber daya Internet, yaitu alamat suatu dokumen atau program yang ingin ditampilkan atau digunakan[5]. URL dapat menjadi salah satu aspek yang menjadi kelemahan pada suatu website, karena pada URL terdapat berbagai informasi yang berisikan protocol, alamat server dan path file yang dapat digunakan untuk melakukan aksi SQL Injection. URL website juga dapat digunakan untuk memberikan berbagai macam perintah terhadap basis data yang terdapat pada server website tersebut. Oleh karena itu URL website sering digunakan sebagai media untuk melakukan tindakan kejahatan terhadap suatu website.

Sebelum diterapkannya kriptografi pada URL website, basis data dapat diakses dengan mudah menggunakan SQL injection[6]. Menyamarkan URL merupakan salah satu cara yang diterapkan untuk meningkatkan keamanan dari celah kerentanan. Konsep B2C menawarkan banyak kelebihan baik bagi pelaku bisnis maupun bagi konsumen, seperti kemudahan dalam melakukan transaksi karena pelaku bisnis dan konsumen tidak perlu berada pada tempat dan waktu yang sama[7]. Oleh karena itu, banyak pelaku bisnis yang tertarik untuk menerapkan konsep B2C dalam e-commerce. Di dalam transaksi B2C, transaksi online dibuat antara bisnis dengan konsumen. Transaksi ini meliputi transaksi penjualan dengan pembeli-pembeli individu. Business berbasis B2C mampu memberi kemudahan dalam aksebilitas Sistem *Business-to-consumer* (B2C) dalam penyampaiannya berfungsi sebagai sistem basisdata dan sarana transaksi melalui internet yang memanfaatkan teknologi web serta serta dapat meningkatan jumlah pengunjung dan omset bagi pelaku usaha kecil[8].

Penelitian ini terhadap perbedaan dengan penelitian terdahulu yaitu pada pencegahan Exploit URL dengan merapkan algoritma base64. Base64 adalah istilah umum untuk sejumlah skema pengkodean serupa yang mengkodekan data biner dan menerjemahkannya ke dalam representasi basis 64. Skema pengkodean Base64 biasanya digunakan ketika ada kebutuhan untuk menyandikan data biner yang perlu disimpan dan ditransfer melalui media yang dirancang untuk menangani data tekstual. Ini untuk memastikan bahwa data tetap utuh tanpa modifikasi selama transportasi. Base64 umumnya digunakan dalam sejumlah aplikasi termasuk email melalui MIME.

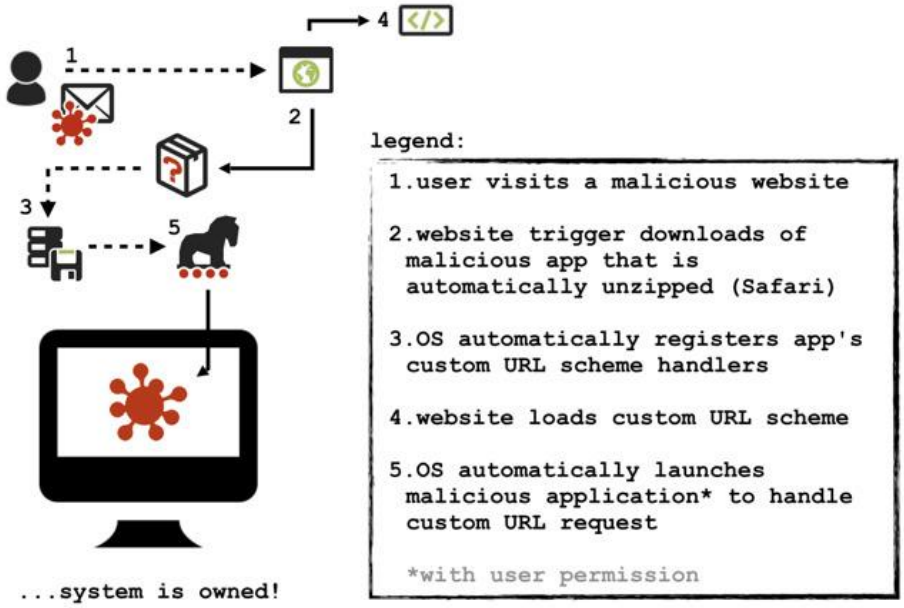
2. METODE PENELITIAN

Penelitian Mencegah Exploit URL Pada Model *Business to Customer* Pada Toko Citra Ponsel Ketapang menggunakan metode penelitiannya *Research & Development* (R&D). Metode perancangan menggunakan Rapid Application Development (RAD) yang merupakan sebuah strategi pengembangan sistem yang menekankan kecepatan melalui keterlibatan pengguna. Melibatkan pengguna pada proses desain menyebabkan kebutuhan pengguna dapat terpenuhi dengan baik dan secara otomatis kepuasan pengguna sebagai pengguna sistem semakin meningkat[9]. Pengumpulan data menggunakan teknik wawancara yang melibat pemakaian recorder untuk perekaman dan melakukan observasi terhadap operasional dan proses bisnis. Rancangan model sistem Exploit URL Pada Model *Business to Customer* digambarkan dengan pemodelan berorientasi objek yaitu *Unified Modelling Language* (UML). Pada tahapan pengembangan sistem Exploit URL Pada *Model Business to Customer* langsung melibat pihak manajemen toko untuk dirumuskan kebutuhan dari pemilik bisnis sebagai penyedia produk. Pemilihan model perangkat lunak yang cocok untuk digunakan dalam sebuah organisasi sangat penting untuk keberhasilan proyek. Pemilihan salah satu model terhadap yang lain adalah didorong oleh ukuran proyek, anggaran, ukuran team dan banyak faktor lainnya[10].

3. HASIL DAN PEMBAHASAN

Design mengindentifikasikan semua struktur sistem, prinsip komponen (sub-sistem/modul), hubungannya dan bagaimana didistribusikan. Berdasarkan pemahaman dari sistem yang berjalan, maka penuis mengusulkan untuk menggunakan website sebagai media untuk melakukan penjualan secara online. Sistem yang rancang nantinya dapat memberikan kemudahan bagi pengguna karena dibuat dengan interface yang mudah digunakan dan dapat menangani masalah pengelolaan data profil, barang yang dijul, deskripsi barang secara detil dan pemesanan secara online dimana data yang tersimpan dalam bentuk file yang terpusat dalam bentuk server dan kemudian diproses oleh komputer. Perancangan arsitektur mempresentasi framework dari sistem perangkat lunak yang dibangun. Berdasarkan pemahaman dari sistem yang berjalan, maka penuis mengusulkan untuk menggunakan E-Commerce sebagai media untuk melakukan penjualan secara online. Sistem yang rancang nantinya dapat memberikan kemudahan bagi pengguna karena dibuat dengan interface yang mudah digunakan dan dapat menangani masalah pengelolaan data profil, barang yang dijul, deskripsi barang secara detil dan pemesanan secara online dimana data yang tersimpan dalam bentuk file yang terpusat dalam bentuk server dan kemudian diproses oleh komputer.

Penyerang dapat menyalahgunakan cara browser dan aplikasi lain menangani steam: // protokol URL untuk mengeksploitasi kerentanan. Semua browser yang mengeksekusi penangan URL eksternal secara langsung tanpa peringatan dan yang didasarkan pada Mozilla Firefox. Selain itu untuk browser seperti Internet Explorer dan Opera masih mungkin untuk menyembunyikan bagian URL yang cerdik agar tidak ditampilkan dalam pesan peringatan dengan menambahkan beberapa spasi ke dalam steam: // URL itu sendiri. Berikut ini adalah gambar 1 cara kerja Exploit URL

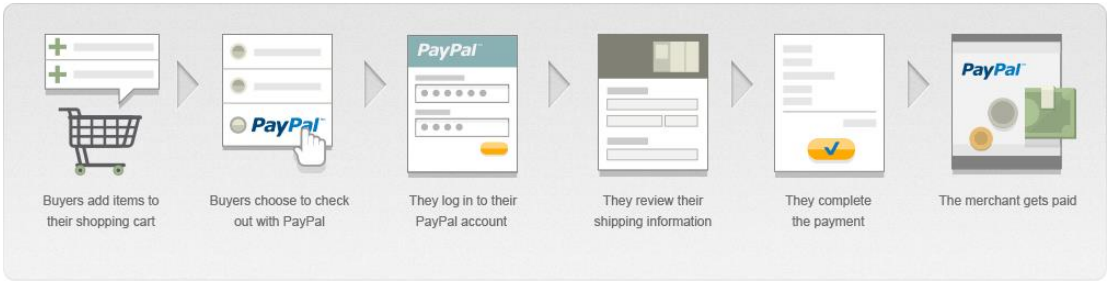


Gambar 1. Cara Kerja Exploit URL

Deskripsi arsitektur mengadopsi spesifikasi sistem, model analisis, dan interaksi subsistem yang telah didefenisikan pada tahap analisis. Arsitektur pengembangan sistem Mencegah Exploit URL Pada Model Business to Customer Pada Toko Citra Ponsel Ketapang yang diusulkan diperlihatkan pada gambar 2.

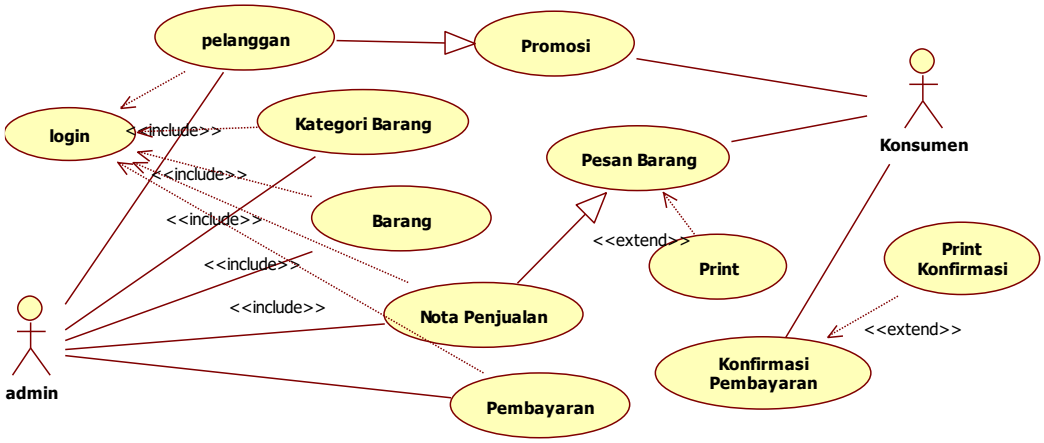
Gambar 2 Arsitektur E-Commerce Citra Ponsel Ketapang

Arsitektur E-commerce Citra Ponsel Ketapang dimulai dari pelanggan mengakses website www.citraponsel.com, kemudian pelanggan membeli barang dengan cara menambahkan item barang ke dalam keranjang belanja. Setelah belanja selesai, maka pembeli dapat memasukkan informasi penagihan ke dalam kartu kredit atau pembeli yang sudah memiliki account paypal dapat melakukan login guna melakukan pembayaran. Sebelum melakukan pembayaran, pembeli melakukan konfirmasi rincian dari transaksi dan berikutnya pembeli melihat dan mencetak konfirmasi pembayaran. Langkah terakhir adalah pembeli menerima pemberitahuan pambayaran dari email, seperti yang diperlihatkan pada gambar 3.



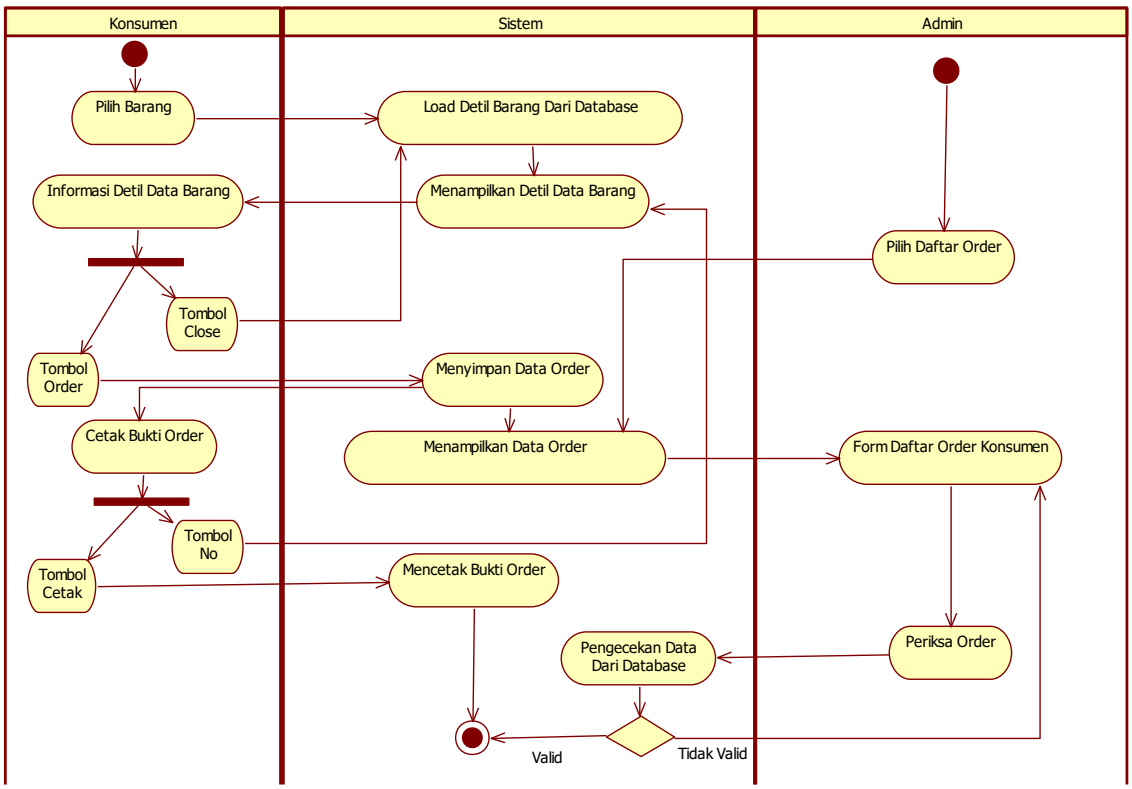
Gambar 3. Arsitektur Metode Pembayaran Dengan PayPal

Strategi dalam tahapan perancangan E-Commerce mengacu pada perancangan berbasis obyek. Startegi ini dalam istilah aslinya disebut sebagai OOD (*Object Oriented Design*) dan dianggap menjadi startegi perancanaan paling modern. Dalam penelitian ini penulis menggunakan UML (*Unified Modeling Language*). Berikut ini adalah perancangan astitektur perangkat lunak yang dimodelkan dengan usecase diagram, seperti yang diperlihatkan pada gambar 4.



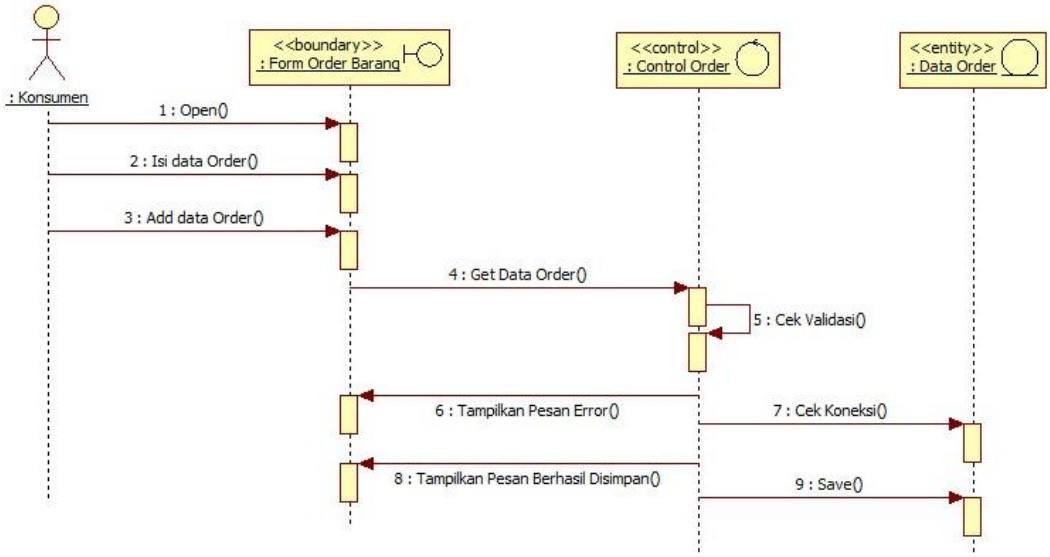
Gambar 4. Usecase Diagram Pengelolaan Konten E-commerce

Pemesanan barang dimulai dari konsumen dengan memilih barang. Sistem menampilkan data barang secara detil. Pada tampilan detil data barang, konsumen bisa melakukan proses order dengan cara mengklik tombol order. Setelah tombol order diklik maka data barang yang diorder akan masuk ke dalam database. Setelah data masuk, maka konsumen dapat mencetak bukti order dan sistem akan mencetak bukti order tersebut. Admin melakukan membuka daftar order dan sistem menampilan form daftar order. Pada form data order, admin melakukan pengecekan terhadap data dan sistem akan memvalidasinya. Apabila data sesuai maka order akan terpenuhi dan kegiatan order barang selesai**.** Model yang diusulkan diperlihatkan pada gambar 5.



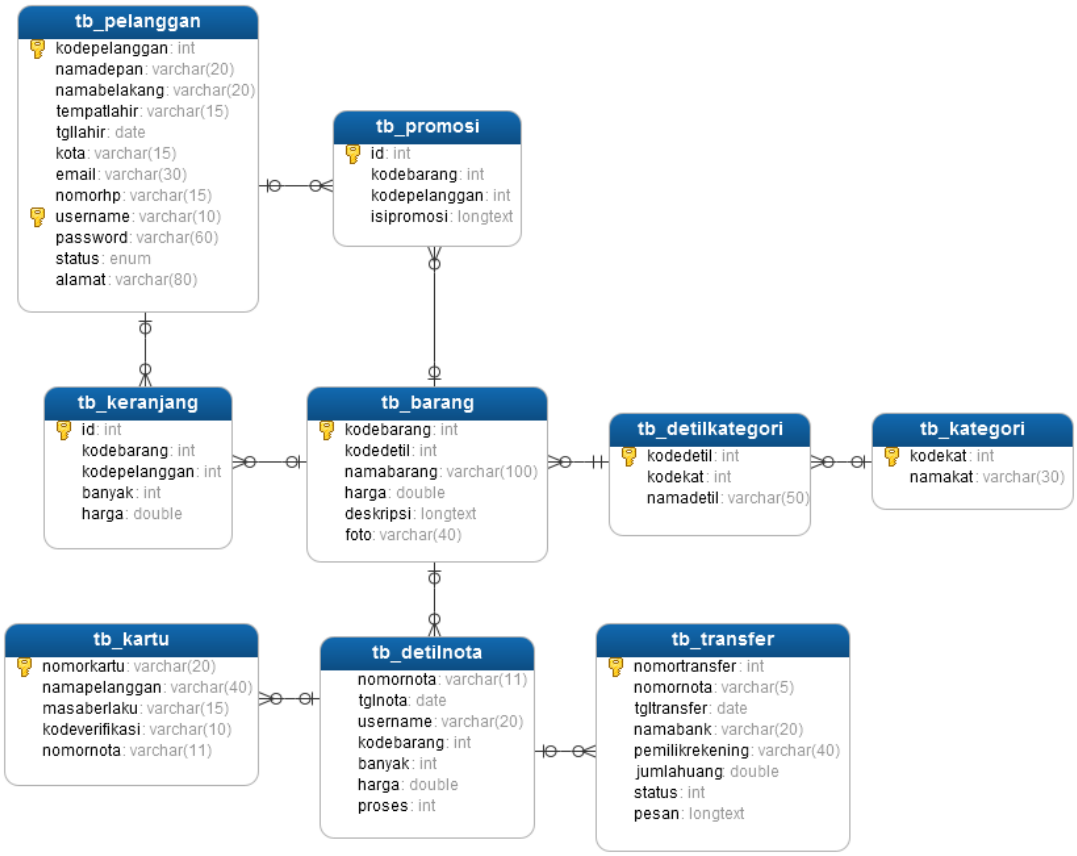
Gambar 5. Activity Diagram Pemesanan Barang

Konsumen berinteraksi dengan form pemesanan barang dengan memilih data barang pada form order barang. Data yang telah diorder akan masuk ke dalam sistem dan sistem akan memasukkan data tersebut ke dalam entity data order. Sistem akan melakukan update order barang dengan cara mengakses database. Model yang diusulkan diperlihatkan pada gambar 6.



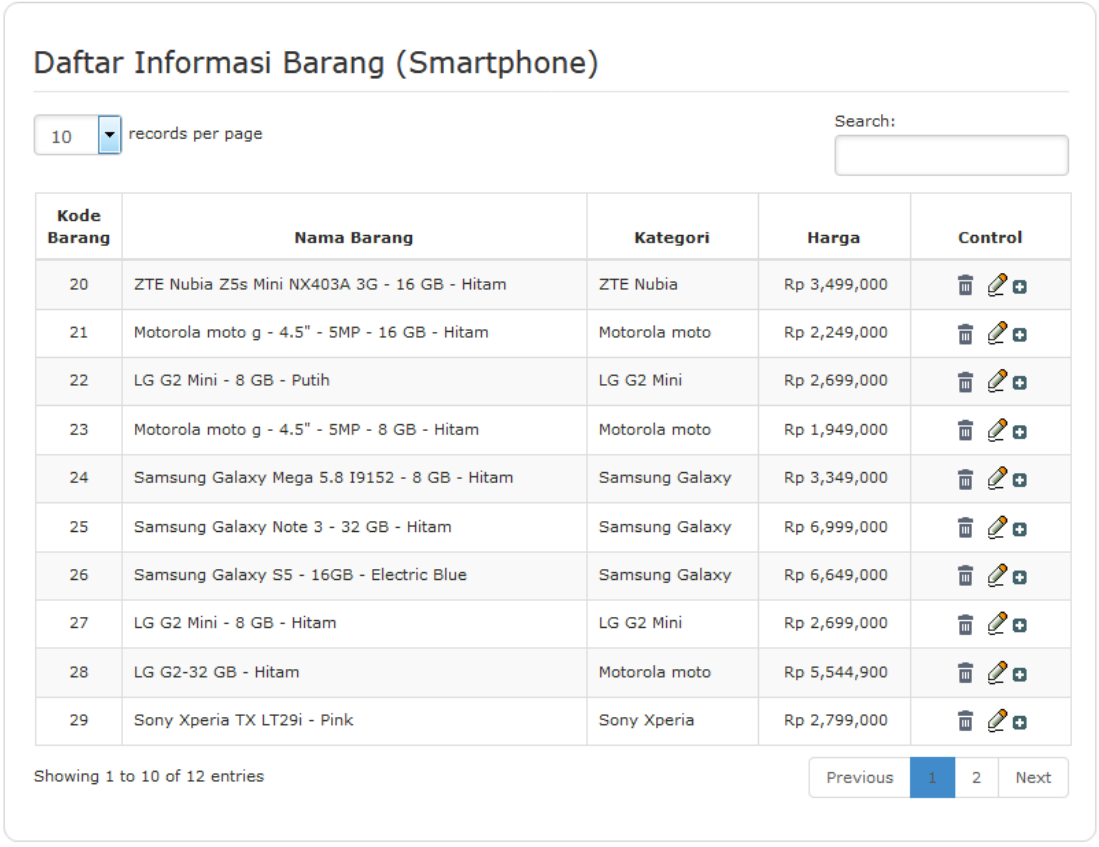
Gambar 6. Sequence Diagram Pemesanan Barang

Sistem Mencegah Exploit URL Pada Model *Business to Customer* Pada Toko Citra Ponsel Ketapang adalah sebuah sistem yang dapat dipergunakan untuk menjual barang dan melakukan transkasi penjualan secara online ke pelanggan dan dilengkapi dengan teknik keamanan pada URL. Tidak semua tabel database yang ada pada web ini memiliki keterkaitan dengan tabel yang lainnya. Maka dari itu dalam pembuatan diagram hubungan entitas penulis hanya menampilkan tabel yang memiliki keterkaitan dengan tabel yang lainnya. Adapun relasi-relasi yang ada dalam diagram tersebut dapat dilihat pada gambar 7.



Gambar 7. Diagram Hubungan Entitas

Hasil akhir dari fase pengkodean adalah platform, hardware dan software yang digunakan, serta daftar batasan implementasi, dan rencana pengujian. Fase pengkodean merupakan fase pembuatan website e-commerce yang sesungguhnya dari seorang programmer. Dalam pengimplementasian sistem yang dibuat, penulis akan menggunakan aplikasi berbasis web, sebagai bahasa pemograman yang akan digunakan PHP dan sistem database yang dipakai adalah MYSQL. Rancangan form input data barang dipergunakan admin untuk mengisikan data barang secara detil dan daftar untuk melihat data barang yang sudah diinputkan. Berikut ini adalah rancangan form daftar barang yang diusulkan diperlihatkan pada gambar 8.



Daftar Informasi Barang (Smartphone)

10 records per page

Search:

Kode Barang	Nama Barang	Kategori	Harga	Control
20	ZTE Nubia Z5s Mini NX403A 3G - 16 GB - Hitam	ZTE Nubia	Rp 3,499,000	
21	Motorola moto g - 4.5" - 5MP - 16 GB - Hitam	Motorola moto	Rp 2,249,000	
22	LG G2 Mini - 8 GB - Putih	LG G2 Mini	Rp 2,699,000	
23	Motorola moto g - 4.5" - 5MP - 8 GB - Hitam	Motorola moto	Rp 1,949,000	
24	Samsung Galaxy Mega 5.8 I9152 - 8 GB - Hitam	Samsung Galaxy	Rp 3,349,000	
25	Samsung Galaxy Note 3 - 32 GB - Hitam	Samsung Galaxy	Rp 6,999,000	
26	Samsung Galaxy S5 - 16GB - Electric Blue	Samsung Galaxy	Rp 6,649,000	
27	LG G2 Mini - 8 GB - Hitam	LG G2 Mini	Rp 2,699,000	
28	LG G2-32 GB - Hitam	Motorola moto	Rp 5,544,900	
29	Sony Xperia TX LT29i - Pink	Sony Xperia	Rp 2,799,000	

Showing 1 to 10 of 12 entries

Previous 1 2 Next

Gambar 8. Rancangan Form Daftar Data Barang

Rancangan form detil pesanan dipergunakan admin untuk mengontrol pesanan pelanggan yang belum diproses. Pelanggan dapat memesan barang secara online melalui fitur yang sudah disediakan. Setiap pesanan barang akan masuk ke halaman admin untuk dikalakukan pengecekan. Berikut ini adalah rancangan form detil pesanan yang diusulkan diperlihatkan pada gambar 9.

Daftar Pesanan Konsumen / Pelanggan

10 records per page

Search:

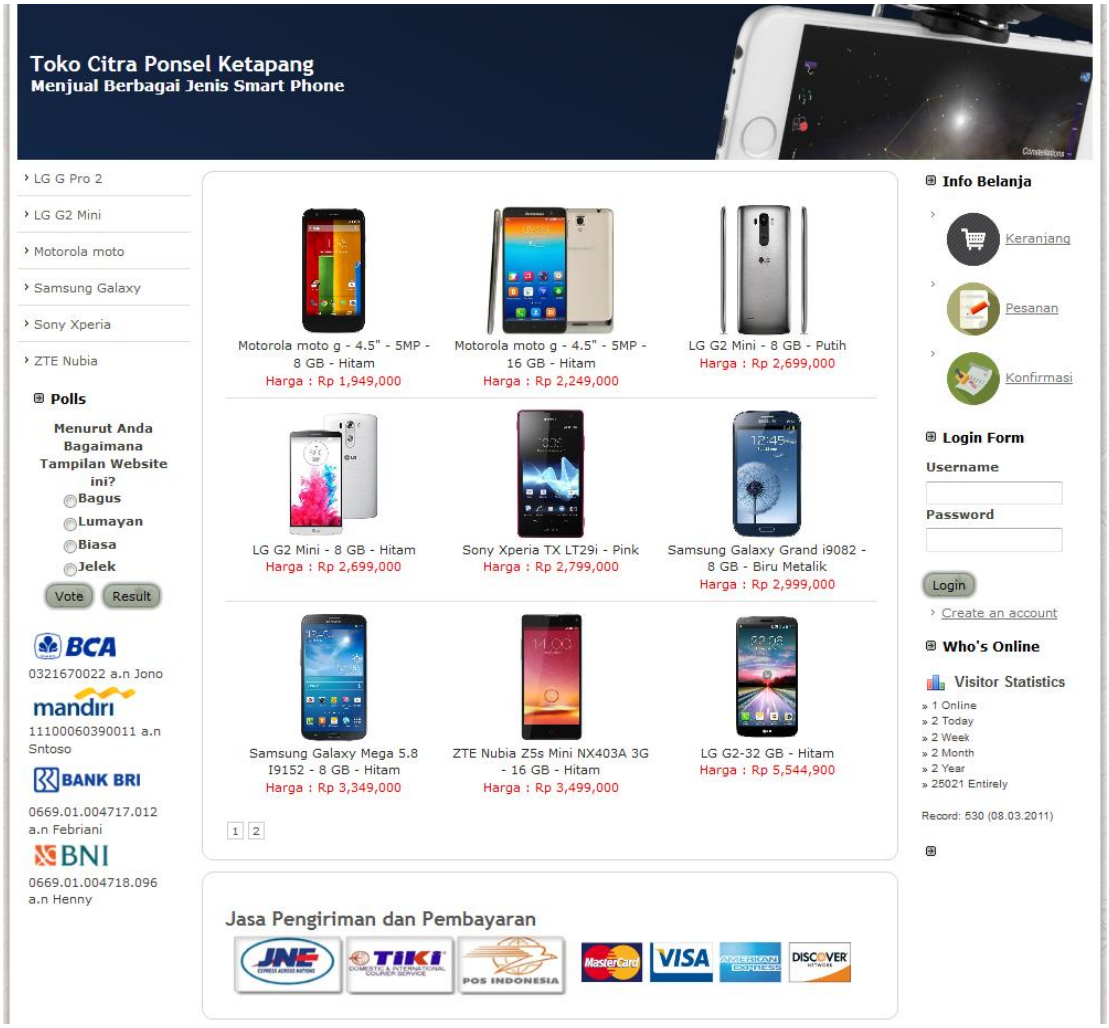
Nomor Nota	Tanggal Nota	Nama Barang	Banyak	Harga	Nama Pelanggan	Kota	Control
00007	2018-08-18	LG G2 Mini - 8 GB - Hitam	1	2699000	Nunung Herlina	Pontianak	
00003	2018-08-18	LG G2 Mini - 8 GB - Putih	1	2699000	Frediansyah -	Pontianak	
00002	2018-08-18	Motorola moto g - 4.5" - 5MP - 16 GB - Hitam	1	2249000	Yahya Kurnia	Pontianak	
00004	2018-08-18	Motorola moto g - 4.5" - 5MP - 8 GB - Hitam	1	1949000	Ernawati -	Pontianak	

Showing 1 to 4 of 4 entries

Previous 1 Next

Gambar 9. Rancangan Form Detil Pesanan

Rancangan halaman utama ini adalah gambaran dari bentuk E-Commerce secara umum. Dimana pada rancangan ini dibagi menjadi beberapa bagian yaitu bagian header, bagian footer, bagian menu atas, bagian menu kiri dan bagian tengah. Berikut ini adalah rancangan halaman utama yang diusulkan diperlihatkan pada gambar 10.



Gambar 10. Rancangan Form Halaman Utama

Rancangan form detil barang dapat dipergunakan oleh konsumen untuk melihat informasi barang secara detil. Pada form ini juga konsumen dapat melakukan pembelian terhadap barang. Berikut ini adalah rancangan form detil barang seperti yang ditunjukkan pada gambar 11.

Gambar 11. Rancangan Informasi Detil Barang

Rancangan form keranjang belanja dipergunakan untuk menampung data belanja sementara ketika komsumen melakukan pemilihan terhadap barang. Setelah konsumen melakukan proses terhadap keranjang belanja, maka data barang yang ada dikeranjang belanja berubah menjadi data pesanan barang sah milik konsumen. Berikut ini adalah gambar 12 keranjang belanja konsumen.

Gambar 12 keranjang belanja konsumen

URL menunjukan alamat dari sebuah homepage atau menunjukan sumber daya Internet, yaitu alamat suatu dokumen atau program yang ingin ditampilkan atau digunakan. URL dapat menjadi salah satu aspek yang menjadi kelemahan pada suatu website, karena pada URL terdapat berbagai informasi yang berisikan protocol, alamat server dan path file yang dapat digunakan untuk melakukan aksi SQL Injection. Salah satu cara yang dapat digunakan untuk mengamankan suatu website dari serangan SQL injection adalah dengan ilmu kriptografi. Ilmu kriptografi dapat menyamarkan URL website menjadi kode atau sandi yang tidak dapat dibaca oleh sembarang orang, sehingga dapat mencegah serangan SQL injection pada suatu website. Penerapan keamanan URL website dari serangan SQL injection ini menggunakan metode kriptografi dengan algoritma base64.

```
function fixtags($text){
    $text = htmlspecialchars($text);
    $text = preg_replace("/=/", "=\"\"", $text);
    $text = preg_replace("/&quot;/", "&quot;\"", $text);
    $tags = "/&lt;(\/|)(\w*)(\ |)(\w*)([\\\=]*)(?|(\")\"&quot;\"|)(?|(.*)?&quot;(\")|)([\
    ]?)(\/|)&gt;/i";
    $replacement = "<$1$2$3$4$5$6$7$8$9$10>";
    $text = preg_replace($tags, $replacement, $text);
    $text = preg_replace("/=\"\"/", "=", $text);
return $text;
}
```

Berfungsi filtering atau penyararingan karakter inputan

```
function encrypt_par( $s ) {
    $cryptKey='d8578edf8458ce06fbc5bb76a58c54';
    $qEncoded=base64_encode( mcrypt_encrypt( MCRYPT_RIJNDAEL_256, md5( $cryptKey ), $s,
    MCRYPT_MODE_CBC, md5( md5( $cryptKey ) ) ) );
    return( $qEncoded );
}
```

Algoritman Bas64 untuk melakukan enkripsi dari suatu nilai variabel

```
function decrypt_par($s) {
    $cryptKey='d8578edf8458ce06fbc5bb76a58c54';
    $qDecoded=rtrim( mcrypt_decrypt( MCRYPT_RIJNDAEL_256, md5( $cryptKey ),
    base64_decode($s),MCRYPT_MODE_CBC, md5( md5( $cryptKey ) ) ), "\0");
    return( $qDecoded );
}
```

Algoritma dekripsi suatu nilai parameter URL

```
<a href='./?pages=viewproduk&id=".encrypt_par($id)."'>$row['namaproduk']</a>'
```

Kode ini berfungsi untuk melakukan enkripsi terhadap nilai variabel id saat posisi kursur berada pada link nama produk. Berikut ini contoh bentuk enkripsi URL saat klik mouse pada suatu linl.
?pages=viewproduk&id=C1Xji9mKWGa5eZfnAJ7W4NhUdwtPLog6goxmVnoRrIg=

```
$id=$_GET["id"];
$ganti = str_replace(" ", "+", $id);
$xpar=decrypt_par($ganti);
```

Nilai varameter yang ditampilkan pada URL akan ditangkap dengan perintah GET dan kemudian disimpan pada variabel id untuk selanjut di dekripsi sehingga menjadi bentuk asli.

4. KESIMPULAN

Keamanan website merupakan satu hal penting dalam perancangan sebuah website. Namun masih banyak developer website yang kurang teliti dalam meningkatkan keamanan website mereka. Celah keamanan (vulnerability) pada dunia komputer adalah suatu kelemahan program/infrastruktur yang memungkinkan terjadinya exploitasi sistem. Penelitian bertujuan membangun sistem pencegahan Exploit URL dengan merapkan algoritma base64. Base64 adalah istilah umum untuk sejumlah skema pengkodean serupa yang mengkodekan data biner dan menerjemahkannya ke dalam representasi basis 64. Skema pengkodean Base64 biasanya digunakan ketika ada kebutuhan untuk menyandikan data biner yang perlu disimpan dan ditransfer melalui media yang dirancang untuk menangani data tekstual. Metode perancangan menggunakan Rapid Application Development (RAD) yang merupakan sebuah strategi pengembangan sistem yang menekankan kecepatan melalui keterlibatan pengguna. Pengumpulan data menggunakan teknik wawancara yang melibat pemakaian recorder untuk perekaman dan melakukan observasi terhadap operasional dan proses bisnis. Pemodelan berorientasi objek yaitu Unified Modelling Language (UML). Pada tahapan pengembangan sistem Exploit URL Pada Model Business to Customer langsung melibat pihak manajemen toko untuk dirumuskan kebutuhan dari pemilik bisnis sebagai penyedia produk. Pemilihan model perangkat lunak yang cocok untuk digunakan dalam sebuah organisasi sangat penting untuk keberhasilan proyek. Hasil penelitian ini adalah sebuah sistem B2C yang menerapkan algoritma base64 dalam mencehah

Exploit URL. Penelitian ini belum mendapatkan hasil yang maksimal karena penelitian ini hanya fokus pada keamanan explot URL dengan menerapkan algoritma base64.

5. SARAN

Pengembangan sistem Exploit URL Pada Model Business to Customer telah berjalan sesuai dengan algoritma yang diterapkan. Hasil rancangan sistem tetap saja meninggalkan kelemahan terutama bagi para hacker profesional. Perlu dilakukan pengembangan lebih lanjut dan tidak hanya fokus pada exploit URL tapi harus memperhatikan celah keamanan lainnya seperti keamanan database. Penerapan algoritma perlu dipertimbang untuk menggunakan gabungan dari dua atau lebih algoritma agar dapat menghasilkan tingkat keamanan yang sangat baik.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Sekolah Tinggi Manajemen Informatika dan Komputer (STMIK) Pontianak yang telah memberikan dukungan dalam rangka penyelesaian terhadap penelitian ini. Terima kasih kepada para teman-teman dan keluarga yang telah memberikan masukan dan dukungan dalam menyelesaikan tulisan ini. Kepada para reviewer saya juga mengucapkan banyak terima kasih atas bimbingan dan arahannya sehingga tulisan ini dapat sesuai seperti apa yang diharapkan. Semoga tulisan ini dapat memberikan manfaat bagi banyak orang, saat ini maupun yang akan datang..

DAFTAR PUSTAKA

[1] Gultom, L. M., & Harahap, M. (2018). Analisis Celah Keamanan Website Instansi Pemerintahan di Sumatera Utara. Jurnal Teknovasi: Jurnal Teknik dan Inovasi, 2(2), 1-7.

[2] Maharani, M. Z., Andrian, H. R., & Ismail, S. J. I. (2017). Analisis Keamanan Website Menggunakan Metode Scanning Dan Perhitungan Security Metriks. eProceedings of Applied Science, 3(3).

[3] Suartana, I., Indriyani, T., & Mardiyanto, B. (2016). Analisis Dan Implementasi Honeypot Dalam Mendeteksi Serangan Distributed Denial-Of-Services (DDOS) Pada Jaringan Wireless. INTEGER: Journal of Information Technology, 1(2).

[4] Purwanto, T. D., & Wijaya, A. (2017). EVALUASI APLIKASI EXPLOID WIFI DI TINGKAT AVAILABILITY DAN VULNERABILITY. Simetris: Jurnal Teknik Mesin, Elektro dan Ilmu Komputer, 8(2), 801-806.

[5] Gat. (2018). Mencegah Exploit URL Website Sensitek STMIK Pontianak Dengan Algoritma Blowfish. Voice of Informatics, 7(2), 55-66.

[6] Gunadhi, E., & Nugraha, A. P. (2016). PENERAPAN KRIPTOGRAFI BASE64 UNTUK KEAMANAN URL (UNIFORM RESOURCE LOCATOR) WEBSITE DARI SERANGAN SQL INJECTION. Jurnal Algoritma, 13(1), pp. 491-498.

[7] Gat. (2018). Adopsi Model Business to Consumer (B2C) Dalam Menghasilkan Sistem Mobile Marketplace. Cogito Smart Journal, 4(1), 200-212.

[8] Muslihudin, M., & Listiarini, M. (2017). Perancangan Aplikasi Business Berbasis Business to Consumer (B2C) Pada Wisata Kuliner Khas Lampung. Jurnal Keuangan dan Bisnis, 15(1), 54-69.

[9] J. L. Whitten, L. D. Bentley, & K. C. Dittman, Systems Analysis and Design Methods: Sixth Edition, New York: McGraw-Hill/Irwin, 2004.

[10] A. I. Khan, R. J. Qurashi, & U. A. Khan, ”A comprehensive study of commonly practiced heavy and light weight software methodologies”, IJCSI International Journal of Computer Science Issues, vol. 8, no. 2, p. 144-450, July 2011.