

Pencegahan Serangan Cross Site Scripting dengan Teknik Metacharacter pada Sistem e-Grocery

Rino Firmansyah^{*1}, Wahyu Sindu Prasetya²

^{1,2}Jurusan Teknik Informatika; STMIK Pontianak. Jl. Merdeka No.372 Pontianak, 0561-735555
e-mail: ^{*1}d3rino@gmail.com, ²Wahyusinduprasetya@stmikpontianak.ac.id

Abstrak

E-Grocery adalah istilah industri untuk berbelanja online, dimana customer memilih dan membayar langsung secara online. E-Grocery merupakan revolusi belanja dimana biasanya setiap hari kita harus memaksakan diri untuk belanja di pasar tradisional sekarang dapat berbelanja di rumah hanya dengan sekali klik. Internet menyediakan konsumen dengan media baru untuk memperoleh informasi yang berguna dan untuk membeli barang, informasi, dan jasa. Cross Site Scripting atau yang lebih dikenal dengan sebutan XSS merupakan salah satu metode yang digunakan para attacker untuk menyuntikan kode HTM atau Javascript kedalam sebuah halaman web yang vulnirable terhadap XSS. Cross Site Scripting sering kali diabaikan dalam pembangunan situs web, seiring dengan pemakaian aplikasi web dinamis. Kerawanan yang timbul justru mengancam hubungan pengguna dan pemilik situs web. Metode serangan XSS yang digunakan juga berkembang seiring dengan pengembangan protokol aplikasi web, bahasa yang digunakan juga berkembang. Karenanya tidak ada jaminan serangan XSS tidak mengalami perkembangan.

Kata kunci XSS, e-Grocery, Metacharakter, Aneka Mart, Toko Online

Abstract

E-Grocery is an industry term for online shopping, where customers choose and pay directly online. E-Grocery is a shopping revolution where usually every day we have to force ourselves to shop in traditional markets, now we can shop at home with just one click. The internet provides consumers with new media to obtain useful information and to buy goods, information and services. Cross Site Scripting or better known as XSS is one of the methods used by attackers to inject HTM or Javascript code into a vulnirable web page against XSS. Cross Site Scripting is often overlooked in the construction of websites, along with the use of dynamic web applications. The vulnerabilities that arise actually threaten the relationship of users and website owners. The XSS attack method used also developed along with the development of web application protocols, the languages used also developed. Therefore there is no guarantee that XSS attacks will not develop.

Keywords XSS, e-Grocery, Metacharakter, Aneka Mart, Online Shop

1. PENDAHULUAN

Internet adalah lingkungan yang kompleks dan dinamis baik dari segi topologi dan teknologi baru. Kurangnya pengetahuan dan pemahaman tentang perangkat lunak dan rekayasa keamanan menyebabkan kerentanan terhadap keamanan, misalnya dengan pemrograman yang tidak pantas, karena dikerjakan dengan cepat permintaan dari klien sehingga mengorbankan keamanan web. Beberapa solusi mungkin efektif hari ini, tetapi dengan adanya perubahan teknologi, risiko dan tantangan baru muncul. Selain itu, solusi yang berbeda harus

dikombinasikan efektif terhadap berbagai jenis serangan dan keamanan sistem harus terus-menerus dipantau. Ada empat atribut utama keamanan komputer, yaitu atribut kerahasiaan, integritas, privasi, dan ketersediaan. Layanan web telah banyak digunakan dalam bidang sistem aplikasi terdistribusikan [1].

E-Grocery adalah istilah industri untuk berbelanja online, dimana *customer* memilih dan membayar langsung secara online. Metode pemilihan dan pengiriman mungkin berbeda, tetapi konsep inti dari *E-Grocery* selalu sama untuk menawarkan pelanggan berbagai pilihan produk yang dapat dibeli secara online dan kemudian dikirim/diantar langsung kepada pelanggan. *E-Grocery* ini jelas sangat membantu bagi pihak-pihak tertentu, contoh : ibu-ibu rumah tangga tidak perlu lagi ke super market untung berbelanja keperluan sehari-hari, cuma duduk didepan komputer dan pesan, maka pesanan akan di antar sampai ke rumah. *E-Grocery* merupakan revolusi belanja dimana biasanya setiap hari kita harus memaksakan diri untuk belanja di pasar tradisional sekarang dapat berbelanja di rumah hanya dengan sekali klik. Internet menyediakan konsumen dengan media baru untuk memperoleh informasi yang berguna dan untuk membeli barang, informasi, dan jasa. Oleh karena itu, teknologi dan ketersediaan Internet menghasilkan generasi baru peluang untuk ide dalam e-bisnis [2].

E-Grocery adalah istilah untuk industri *Grocery Online*, dimana Konsumen dapat melakukan pemesanan, memilih dan membayar belanja mereka secara online. *E-Grocery* biasanya menawarkan makanan segar yang tahan lama dan proses pengirimannya juga berbeda. Selain sayuran ada juga *E-Grocery* yang menawarkan kebutuhan rumah tangga lainnya seperti bedak, atau kebutuhan bayi. Barang yang dijual di *E-Grocery* tidak lah begitu berbeda jauh dengan yang biasa di jual di supermarket atau department store di kota-kota. Ada *E-Grocery* yang menawarkan pengiriman secara langsung atau dapat dipesan terlebih dahulu yang akan dikirimkan sesuai keinginan konsumen [3].

Aneka Mart adalah salah satu perusahaan dagang yang melakukan kegiatan bisnis penjualan bahan kebutuhan pangan rumah tangga. Sampai dengan saat ini, dalam menjalankan aktivitas penjualan, Aneka Mart masih melakukannya secara konvensional yaitu melayani Konsumen yang datang secara langsung ke tempat usaha. Penjualan dengan jumlah yang banyak mengharuskan Aneka Mart untuk mengantarkan barang tersebut ke tempat Konsumen. Pemesanan melalui nota pesanan yang berisikan data barang secara detil sering juga diberikan oleh Konsumen kepada karyawan untuk mempermudah dalam pengelolaan data pesanan Konsumen. Kesibukan karyawan dalam melayani Konsumen yang datang secara langsung dan juga kesibukan karyawan dalam memberikan informasi kepada Konsumen membuat pesanan Konsumen menjadi terlambat untuk dipenuhi.

Cross Site Scripting atau yang lebih dikenal dengan sebutan XSS merupakan salah satu metode yang digunakan para *attacker* untuk menyuntikan kode HTM atau *Javascript* kedalam sebuah halaman web yang *vulnerable* terhadap XSS. [7]. Metode serangan XSS yang digunakan berkembang seiring dengan pengembangan protokol aplikasi web, bahasa yang digunakan juga berkembang. Karenanya tidak ada jaminan serangan XSS tidak mengalami perkembangan [5].

Keamanan aplikasi yang tidak baik mengakibatkan data penting dan kerahasiaan pengguna menjadi terancam. Hal ini tentu saja merugikan bagi pihak pengguna maupun penyelenggara. *Cross Site Scripting* merupakan jenis serangan *injection* terhadap situs dengan mengandalkan kelemahan dari target atau pengguna internet. Penyerang akan memanfaatkan kelemahan pengguna melalui ajakan atau bujukan untuk mengikuti arahan menuju suatu kondisi tertentu yang telah diminati oleh usaha untuk pencurian data, kerahasiaan atau perintah tertentu melalui *code scripting* oleh penyerang [8]. XSS (*Cross Site Script*) adalah jenis serangan injeksi *code* (*Code Injection Attack*), suatu jenis serangan web dimana penyerang berusaha untuk menyisipkan *script* yang berisikan kode jahat terhadap suatu website untuk menjalankan suatu perintah. Serangan XSS biasanya digunakan untuk mencuri *cookie*, penyebaran *malware*, *session hijacking/pembajakan session*, dan pemblokiran tujuan/*malicious redirects* [4]. Teknologi *dynamic web page* kini telah menjadi bagian yang tidak terpisahkan dari kehidupan dunia maya. Teknologi ini membawa perubahan yang signifikan dalam proses pembangunan sistem penyedia

layanan dalam jaringan internet. Efek yang diharapkan tentu saja peningkatan dari segi ekonomi. Namun dibalik keuntungan-keuntungan tersebut, teknologi ini memiliki permasalahan dari segi keamanan [7].

2. METODE PENELITIAN

Bentuk penelitian berbentuk studi kasus. Studi kasus merupakan strategi penelitian yang berusaha memahami kedinamisan dalam konteks tunggal yang dalam hal ini mengacu pada variabel tunggal pada Aneka Mart Tebas serta objek penelitian berupa Pencegahan Serangan *Cross Site Scripting (XSS)* Dengan Teknik Metacharacter Pada Sistem *E-Grocery*.

Metode penelitian yang digunakan adalah metode penelitian dan pengembangan atau yang lebih dikenal dengan *Research and Development*. Metode penelitian dan pengembangan adalah “metode yang digunakan untuk menghasilkan produk tertentu dan menguji keefektifan produk tersebut”. Metode jenis ini memerlukan waktu yang cukup lama agar menghasilkan produk yang terbaik. Namun, karena waktu yang tidak memungkinkan jika melalui semua tahapan yang ada dalam metode penelitian dan pengembangan tersebut, dalam penelitian ini hanya melakukan tahap awal dari metode penelitian dan pengembangan [6].

Metode pengumpulan data merupakan bagian paling penting dalam sebuah penelitian. Ketersediaan data akan sangat menentukan dalam proses pengolahan dan analisa selanjutnya. Karenanya, dalam pengumpulan data harus dilakukan dengan teknik yang dapat menjamin bahwa data diperoleh itu adalah benar, akurat dan bisa dipertanggungjawabkan sehingga hasil pengolahan dan analisa data tidak bias. Adapun jenis data yang digunakan dalam penelitian ini adalah Data Primer dan Data Sekunder. Data Primer Merupakan data yang diperoleh secara langsung dari objek yang diteliti. Sumber primer adalah sumber data yang langsung memberikan data kepada pengumpul data. Data primer yang diperoleh dengan cara observasi dan wawancara dengan pihak Aneka Mart Tebas. Data sekunder Pengertian dari data sekunder merupakan data yang berhubungan secara langsung dengan penelitian yang dilaksanakan dan bersumber dari Aneka Mart Tebas data lain yang diperlukan hasil *searching* di internet mengenai artikel-artikel, jurnal, dan adanya hasil dari penelitian sebelumnya yang dapat digunakan oleh peneliti sebagai bahan perbandingan dengan penelitian yang dilakukan.

Adapun metode pengumpulan data yang harus dilakukan oleh peneliti dalam melakukan penelitian ini yaitu dengan melakukan Wawancara untuk mendapatkan informasi dengan memberikan pertanyaan secara langsung atau lisan, menggunakan teknik wawancara semi terstruktur dimana untuk mengetahui gambaran umum Toko dan prosedur yang berjalan pada Aneka Mart Tebas. Observasi dengan meninjau secara langsung ke Aneka Mart Tebas yang ada. Dokumentasi sumber-sumber berupa data, catatan, maupun laporan yang berhubungan dengan Aneka Mart Tebas untuk mendapatkan kelengkapan informasi yang mendukung penelitian sesuai permasalahan dan topik yang dibahas.

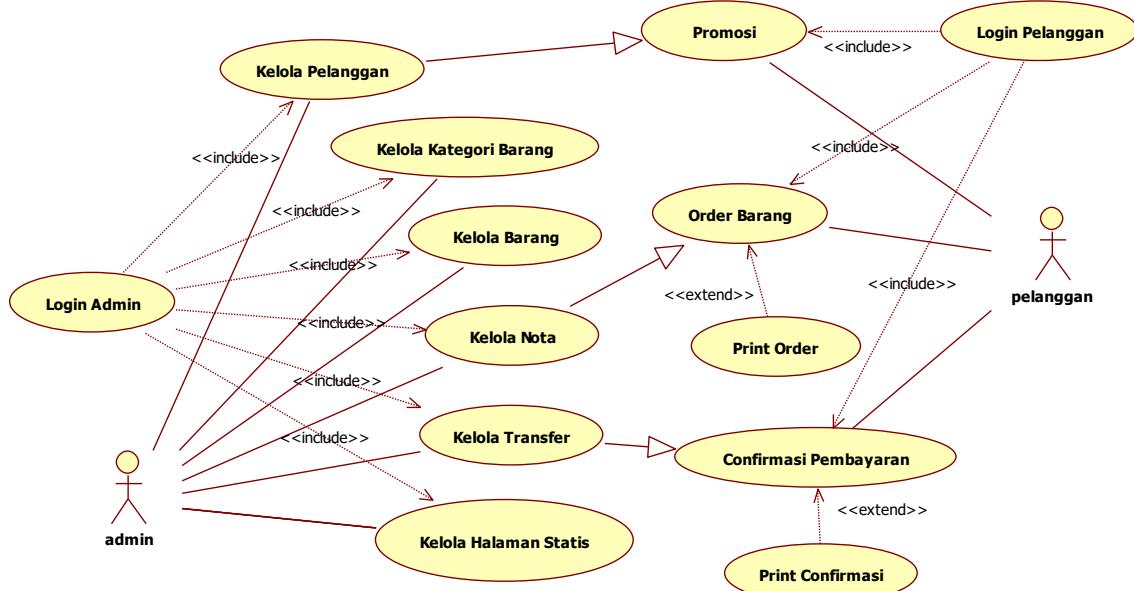
3. HASIL DAN PEMBAHASAN

Tahapan Pemodelan (*Modeling*) Proses ini berfokus pada perancangan struktur data, arsitektur dari program yang akan dibuat, user interface dan detail (algoritma) prosedural. Pada proses modelling akan menghasilkan software requirement dimana akan menerjemahkan syarat kebutuhan ke sebuah perancangan program yang dapat diperkirakan sebelum dibuat coding. Untuk mempermudah dalam pemahaman model arsitektur dari sistem yang dikembangkan, maka disajikan model dari arsitektur sistem informasi E-grocery berbasis web. Seperti dalam arsitektur tradisional, fokusnya adalah benar pada pengguna dan kebutuhan pengguna.

Hal ini memerlukan perhatian khusus pada konten web, rencana bisnis, kegunaan, desain interaksi, informasi dan desain arsitektur web. Model arsitektur ini mendeskripsikan rancangan dari perangkat lunak disisi web server dan komputer *client*. Web *server* menggunakan apache,

script PHP dan *database* MySQL. Secara umum pengguna dari website ini adalah pengelola E-grocery, perusahaan dan konsumen.

Use case diagram menjelaskan manfaat sistem jika dilihat menurut pandangan orang yang berada di luar sistem atau *actor*. Diagram ini menunjukkan fungsionalitas suatu sistem atau kelas dari bagaimana sistem berinteraksi dengan dunia luar. Perancangan proses yang terjadi dalam sistem website Toko Aneka Mart Tebas dengan *Use Case Diagram* sebagai berikut.

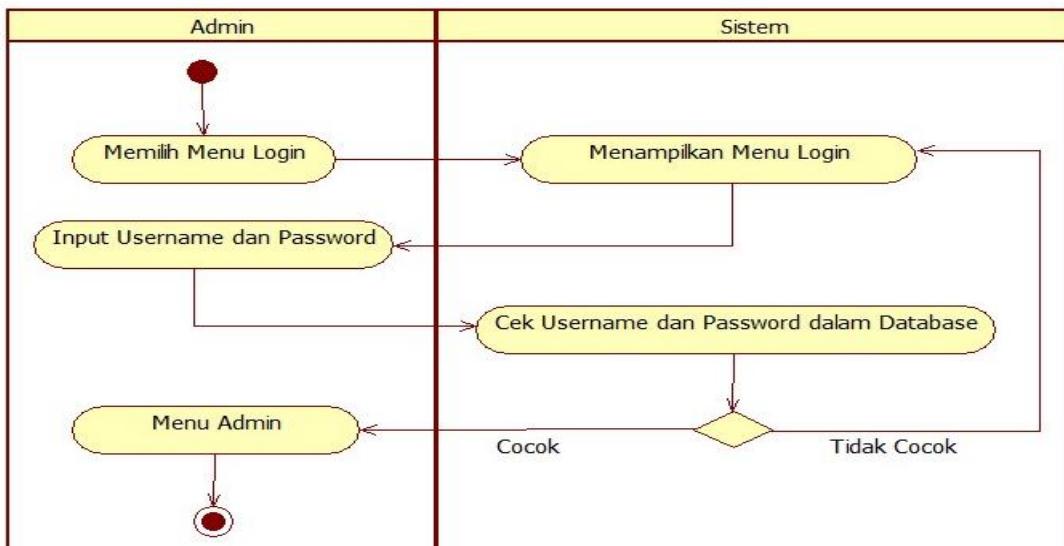


Gambar 1 Use case diagram Pengelolaan Konten Website

Use case diagram pengelolaan konten website toko terdiri dari admin, pelanggan dan *guest*. *Actor* admin bertugas untuk memanajemen isi dari website secara keseluruhan. *Actor* pelanggan memanajemen isi dari profil sendiri, melihat promosi khusus, memesan barang dan melakukan konfirmasi pembayaran. Sedangkan *actor guest* adalah pengunjung website yang ingin mendapatkan informasi yang ada toko. Untuk memahami lebih detil aktivitas *actor*, berikut adalah deskripsi dari *use case* website:

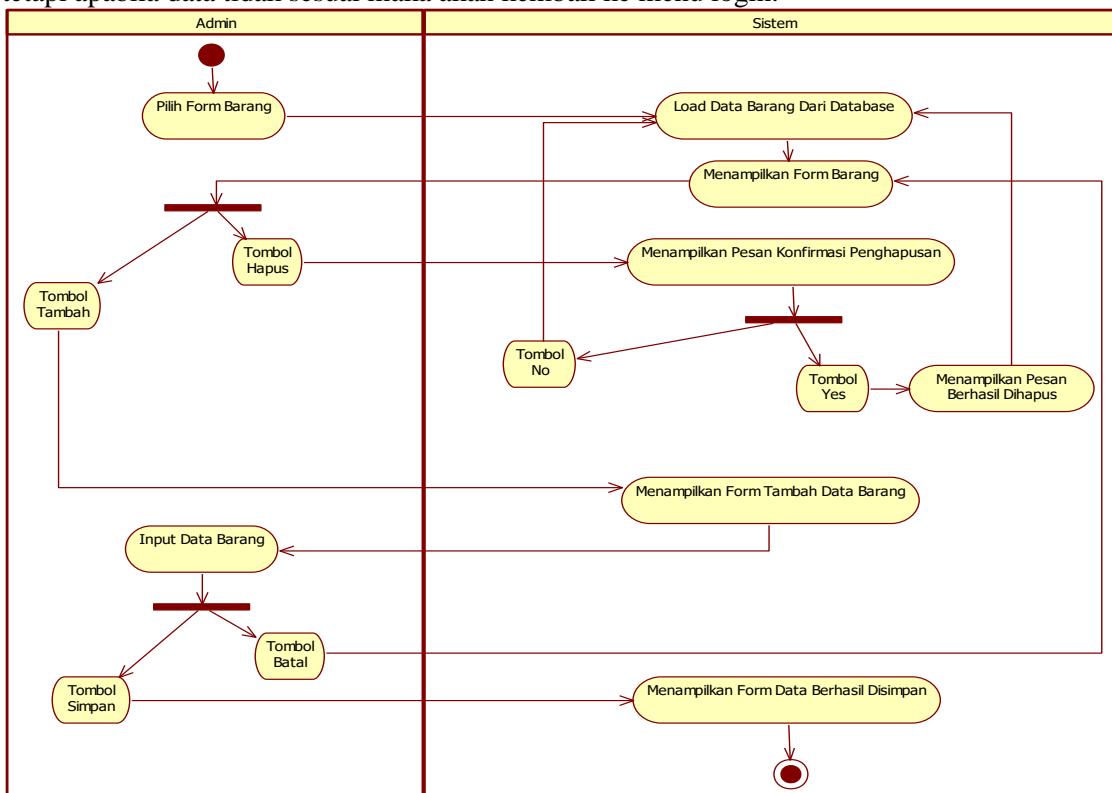
Activity Diagram menggambarkan berbagai alur aktivitas dalam sistem yang sedang dirancang, bagaimana masing-masing alur berawal, decision yang mungkin terjadi, dan bagaimana mereka berakhir. *Activity Diagram* juga dapat menggambarkan proses paralel yang mungkin terjadi pada beberapa eksekusi. *Activity Diagram* merupakan *state diagram* khusus, di mana sebagian besar *state* adalah *action* dan sebagian besar transisi di-trigger oleh selesainya *state* sebelumnya (*internal processing*). Oleh karena itu *Activity Diagram* tidak menggambarkan *behaviour internal* sebuah sistem (dan interaksi antar subsistem) secara eksak, tetapi lebih menggambarkan proses-proses dan jalur-jalur aktivitas dari level atas secara umum.

Pencegahan Serangan Cross Site Scripting dengan Teknik Metacharacter pada Sistem e-Grocery



Gambar 2 Activity Diagram Login Admin

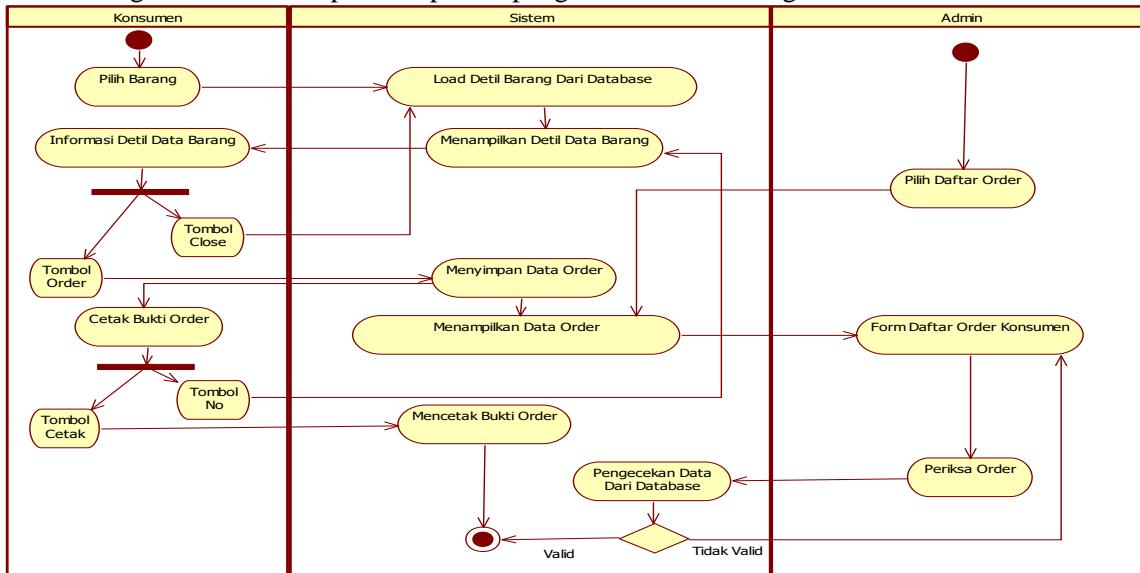
Admin memilih menu login dan sistem menampilkan form login. Setelah form login tampil, admin mengisi data username dan password. Sistem melakukan pengecekan terhadap username dan password, apabila data sesuai dengan database, maka menu admin ditampilkan, tetapi apabila data tidak sesuai maka akan kembali ke menu login.



Gambar 3 Activity Kelola Barang

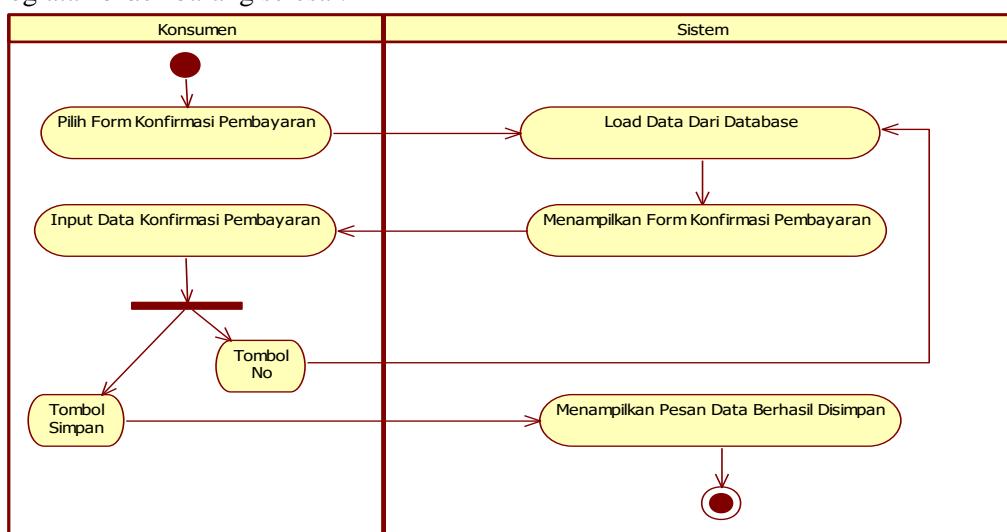
Pengelolaan data barang oleh admin dimulai dari pemilihan form data barang. Form data barang ditampilkan lengkap dengan data yang diambil dari *database*. Pada form data barang, admin dapat menghapus barang atau menambah data barang. Apabila admin menambah data barang maka *form* data barang akan ditampilkan. Admin mengisi data sesuai dengan

item yang terdapat pada *form* tambah data barang. Setelah data barang diisi dengan lengkap, maka admin mengklik tombol simpan dan proses pengelolaan data barang selesai.



Gambar 4 Activity Order Barang

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 menampilkan *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.



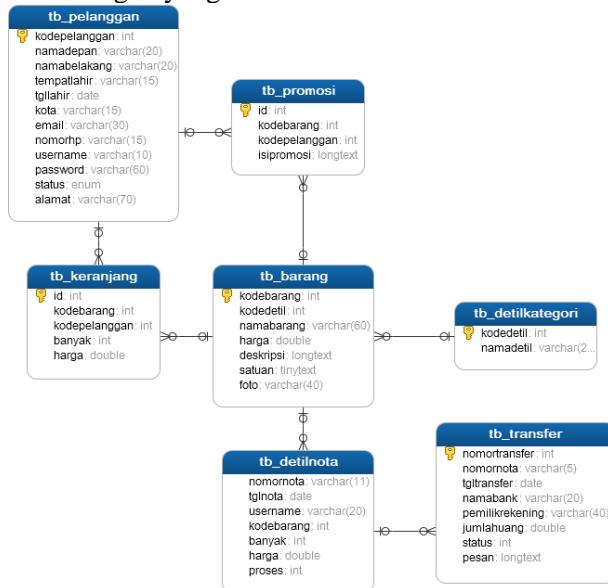
Gambar 5 Activity Konfirmasi Pembayaran

Konsumen memilih *form* konfirmasi pembayaran untuk memberitahukan bahwa barang yang *diorder* telah dilakukan pembayaran sesuai dengan nilai yang ada pada bukti *order*. Sistem menampilkan *form* konfirmasi pembayaran dan konsumen mengisikan data sesuai dengan *item* yang terdapat pada *form* konfirmasi pembayaran. Setelah selesai diinputkan maka konsumen dapat mengklik tombol simpan data sistem menampilkan pesan bahwa data telah berhasil

Pencegahan Serangan Cross Site Scripting dengan Teknik Metacharacter pada Sistem e-Grocery

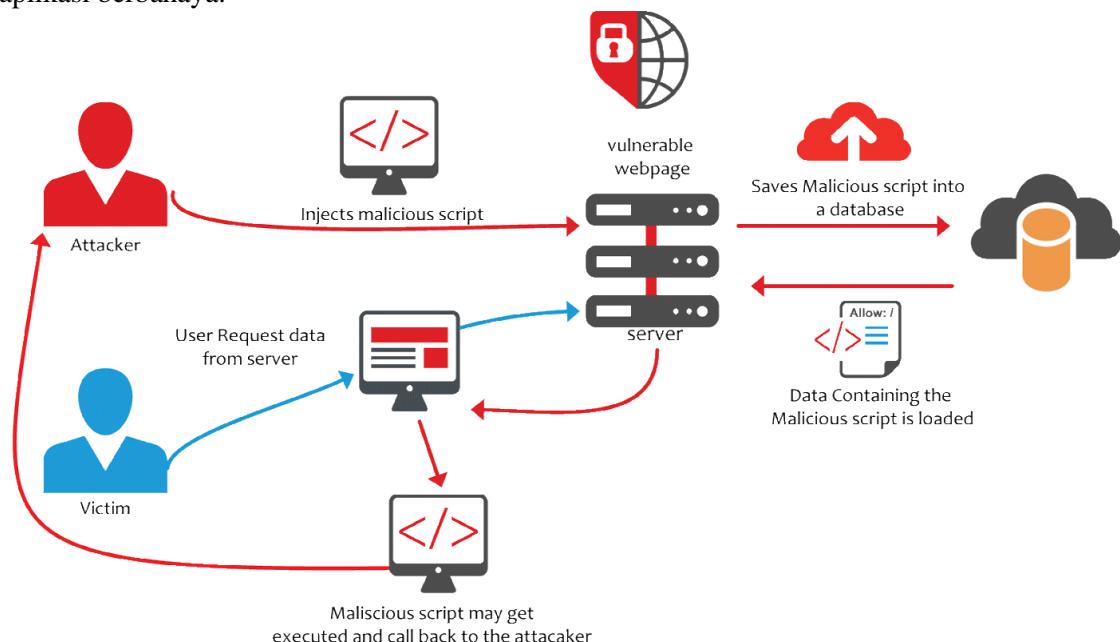
disimpan.

Diagram Hubungan Entitas adalah suatu dokumentasi data dengan mengidentifikasi entitas data dan memperhatikan hubungan yang ada diantara entiti tersebut.



Gambar 6 Diagram Hubungan Entitas (DHE)

Model Penerapan Keamanan Dengan Teknik Cross Site Scripting (XSS), XSS merupakan salah satu jenis serangan injeksi code (code injection attack). XSS dilakukan oleh penyerang dengan cara memasukkan kode HTML atau client script code lainnya ke suatu situs. Serangan ini akan seolah-olah datang dari situs tersebut. Akibat serangan ini antara lain penyerang dapat mem-bypass keamanan di sisi klien, mendapatkan informasi sensitif, atau menyimpan aplikasi berbahaya.



Gambar 7 Teknik Cross Site Scripting (XSS)

XSS ini disebabkan oleh tidak adanya filter/penyaringan pada kode PHP, berikut contoh kode PHP yang Vulnerable terhadap bug XSS :

```

1 <?php
2     $komentar = $_POST['komentar'];
3     "<script>
4         alert('bug xss');
5     </script>";
6     echo $komentar;
7 ?>
```

Kode diatas sangat terbuka sekali karena tidak ada filter/konversi pada saat pengambilan data (echo \$komentar;), pengguna/penyerang bisa saja dengan leluasa menyisipkan sebuah kode jahat berupa javascript/iframe. Untuk Memperbaiki bug tersebut maka diperlukan tambahan pada kode PHP nya seperti htmlspecialchars (\$string, ENT_QUOTES), sehingga kodennya menjadi seperti ini :

```

1 <?php $komentar = $_POST['komentar'];
2     <script>
3         alert('bug xss');
4     </script>
5     echo htmlspecialchars($komentar, ENT_QUOTES);
6     //browser tidak memberi sebuah alert/dialog 'bug xss'.
7     //lantas dikonvert menjadi kode HTML entities.
8 ?>
```

Penggunaan htmlspecialchars (\$string, ENT_QUOTES) dalam penelitian ini berlaku pada setiap penyimpanan dan pengaksesan pada variabel. Berikut ini penggunaan htmlspecialchars (\$string, ENT_QUOTES) secara penuh:

```

function fixtags($text){
    $text = htmlspecialchars($text);
    $text = preg_replace("/=/", "=\"", $text);
    $text = preg_replace("/quot;/", "&quot;\\"", $text);
    $tags = "/&lt;(\w*)(\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;
}
```

Ada sebuah function bernama fixtags dimana function tersebut dapat dipergunakan untuk memfilter berbagai macam jenis data (simbol, angka, huruf, karakter dan lain-lain). Ketika fuction ini dipanggil pada suatu proses, maka setiap data yang ingin ditampung pada variabel akan dilakukan seleksi sehingga hanya data yang diijinkan yang boleh diterima. Disinilah letak keamanannya dan berikut ini contoh pemanggilan fungsi:

```

<?php
    $namagambar = fixtags($_FILES["namafile"]["name"]);
    $kodebarang = fixtags($_POST['kodebarang']);
    $namabarang = fixtags($_POST['namabarang']);
    $harga = fixtags($_POST['harga']);
    $banyak = fixtags($_POST['banyak']);
?>
```

Pada pemanggilan function fixtags, terlihat bahwa sebelum data disimpan kedalam setiap variabel, maka data tersebut akan disaring berdasarkan isi dari function fixtags. Dengan teknik seperti ini akan cukup terjamin keamanan. Hanya data yang diijinkan yang boleh ditampung pada variabel.

Interface Design, mendefinisikan *interface-interface* diantara komponen sistem dan spesifikasi *interface* tidak boleh ambigu. Merancang antarmuka merupakan bagian yang paling penting dari merancang sistem. Biasanya hal tersebut juga merupakan bagian yang paling sulit karena dalam merancang antarmuka harus memenuhi tiga persyaratan: sebuah antarmuka harus sederhana, sebuah antarmuka harus lengkap, dan sebuah antarmuka harus memiliki kinerja yang cepat. Alasan utama mengapa antarmuka sulit untuk dirancang adalah karena setiap antarmuka adalah sebuah bahasa pemrograman yang kecil: antarmuka menjelaskan sekumpulan objek-objek dan operasi-operasi yang bisa digunakan untuk memanipulasi objek.

Tahap Penyebaran (*Deployment*) adalah tahap dimana sistem dibuat tersedia bagi komunitas pengguna. Tergantung pada komunitas pengguna, ini mungkin memerlukan tambahan sumber daya IT. Proses penyebaran harus direncanakan dengan baik sehingga meminimalkan downtime dan dampak untuk mengakhiri produktivitas pengguna. Hal ini tidak hanya mencakup perangkat keras dan perangkat lunak tetapi pengguna akhir. Pengujian kode yang akan dilakukan oleh tim tester seperti yang telah disebutkan di atas. Tes ini dilakukan terhadap sistem informasi E-Grocery yang berfokus kepada fitur dan fungsi sistem secara keseluruhan. Acceptance test ini berasal dari user stories yang telah diimplementasikan.

Back End adalah istilah halaman belakang pada situs web yang memungkinkan seseorang untuk masuk sebagai administrator dan melakukan perubahan informasi dalam website. Untuk memiliki tingkatan halaman yang aman, setidaknya halaman *Back-end* dilindungi dengan *https* dan juga *SSL* yang akan membuat enkripsi menjadi aman, dan juga *password* administrator yang berformat MD5. Dengan memiliki halaman *Back-end* akan memudahkan seorang user untuk meng-update situs web. Admin memiliki peran dalam mengelola data barang, mengelola data konsumen, promosi dan mengelola data pesanan konsumen. Agar data bisa terjaga integritas dan keamanannya, maka harus ada menu login untuk bisa masuk ke halaman utama admin. Form login hanya dipergunakan demi keamanan data.

Testing registrasi konsumen dimaksudkan untuk memastikan apakah form registrasi sudah dapat dipergunakan dengan baik atau belum. Berikut ini adalah proses testing registrasi konsumen:

Registrasi Pelanggan

Nama Awal	Rangga
Nama Belakang	Hardianto
Tempat/Tgl. Lahir	Sintang / 2003-08-15
Kota	Sintang
Email	rangga@gmail.com
Telp	-
Alamat	Baning - Sintang
Username	rangga
Password	*****

Submit

Gambar 8 Testing Registrasi Konsumen

Jika tombol submit diklik maka data yang telah diinputkan seperti pada form diatas akan disimpan ke dalam database. Untuk memastikan apakah benar data tersebut tersimpan ke dalam

database, maka hal ini dapat dilakukan dengan cara login menggunakan account perusahaan dan lihat di dalam daftar konsumen. Berikut ini adalah daftar konsumen:

Nama Pelanggan	Kota	Email	Username	Telp / HP	Kontrol
Erianti Setia	Pontianak	erianti@yahoo.com	erianti	-	
Greboris Yahya	Pontianak	greboris@yahoo.com	greboris	-	
Rangga Hardianto	Sintang	rangga@gmail.com	rangga	-	
Rendy Natalio	Pontianak	rendy@yahoo.com	rendy	-	
Trionata Yuda	Pontianak	trionata@yahoo.co.id	trionata	-	
Yeremia Gunawan	Pontianak	yeremia@gmail.com	yeremia	-	

Showing 1 to 6 of 6 entries

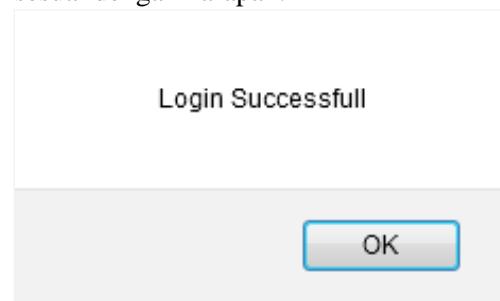
[Previous](#) [Next](#)

Gambar 9 Daftar Konsumen Setelah Testing Registrasi

Lihat data pada baris pertama yang diberikan tanda kotak dan ini membuktikan bahwa testing registrasi konsumen baru berhasil dengan baik dan sesuai dengan apa yang diinginkan. Testing konsumen login konsumen baru dimaksudkan untuk memastikan apakah konsumen yang baru resgistrasi dapat menggunakan account tersebut untuk bisa masuk kesistem dan mengakses fasilitas yang ada. Berikut ini adalah testing login konsumen baru:

Gambar 10 Testing Konsumen Login Konsumen Baru

Jika tombol login diklik maka sistem akan menampilkan pesan berhasil login dan ini membuktikan bahwa account konsumen yang baru melakukan proses registrasi dapat langsung dipergunakan dengan baik dan sesuai dengan harapan.



Gambar 11 Testing Konsumen Login Sukses

Testing konsumen memesan barang dimaksudkan untuk menguji apakah konsumen dapat melakukan pemesanan barang setelah konsumen berhasil login. Berikut ini adalah proses pemesanan barang:



Gambar 12 Testing Konsumen Memesan Barang

Jika tombol beli diklik maka data barang tersebut akan masuk kedalam keranjang belanja dan ini adalah sesuai dengan prosedur dalam proses pemesanan barang. Berikut ini adalah tampilan data barang yang berhasil masuk ke dalam keranjang belanja setelah mengklik tombol beli:

No.	Nama Barang	Banyak	Harga	Jumlah	Control
1	Mix Nut (Kacang Campur) - 2.82oz	2 Bungkus	Rp 10,000	Rp 20,000	
Proses		TOTAL Rp 20,000			

Gambar 13 Testing Keranjang Belanja

Adanya data yang ada didalam keranjang belanja dan sesuai dengan data yang ada pada detil barang seperti pada gambar diatas, menandakan bahwa proses pembelian berhasil dan sesuai dengan apa yang diharapkan. Jika tombol proses diklik maka data yang ada didalam keranjang belanja akan dipindahkan kedalam invoice sebagai bukti bahwa data barang tersebut benar dipesan dan data yang ada didalam keranjang belanja akan dikosongkan. Berikut ini adalah data invoice yang berhasil diproses dari form keranjang belanja:

INVOICE #00007

Konsumen :

Rangga Hardianto
Baning - Sintang - Sintang
-
rangga@gmail.com

Nomor Rekening:

BCA : 0321670200 a.n : Indiana
Mandiri : 1110006031271 a.n : Rohania
BRI : 0669.01.004717.111 a.n : Santi
BNI : 0669.01.004718.110 a.n : Rudi

Berikut ini adalah daftar barang yang telah anda pesan. Silahkan untuk melakukan pengecekan terhadap status pesanan anda.

Nomor	Nama Barang	Banyak	Harga	Jumlah
1	Mix Nut (Kacang Campur) - 2.82oz	2 Bungkus	Rp 10,000	Rp 20,000
TOTAL Rp 20,000				
Print		Payment Methods: 		

Gambar 14 Testing Data Invoice

Pesanan konsumen yang telah disetujui harus segera dilunasi oleh pihak konsumen dengan cara mengirimkan pembayaran melalui transfer ke rekening pihak toko. Setelah konsumen mentransfer uang, maka konsumen harus mengisikan data pembayaran melalui form konfirmasi pembayaran. Berikut ini adalah form konfirmasi pembayaran konsumen:

Konfirmasi Pembayaran Pesanan

Nomor Nota	#00007
Tgl Transfer	2018-08-17
Nama Bank	BRI
Pemilik Rekening	Rangga
Jumlah Uang	20000
Tinggal Pesan Anda	-
<input type="button" value="Submit"/>	

Gambar 15 Testing Konfirmasi Pembayaran

Pihak toko dapat melihat konsumen yang telah melakukan pembayaran terhadap pesanan mereka melalui form daftar pembayaran belum diproses. Form ini bermanfaat bagi pihak toko untuk mengetahui konsumen yang telah melunasi pesanannya.

4. KESIMPULAN

Berdasarkan hasil kajian dan pembahasan dalam penelitian ini, maka dapat diambil beberapa kesimpulan sebagai Pengembangan Website e-grocery dengan cara melakukan analisis terhadap kebutuhan. Untuk mengetahui apa yang menjadi kebutuhan dari pengembangan website tersebut, dilakukan dengan cara pengumpulan data yang terdiri dari data primer dan data sekunder. Tahapan dalam perancangan e-grocery mengacu kepada metode pengembangan sistem Linear Sequential / Waterfall Model. Metode ini merupakan model klasik yang bersifat sistematis dan mudah dipahami karena berurutan dalam tahapan membangun software mulai dari proses *communication, planning, modeling, construction hingga proses deployment*. Hasil akhir adalah sebuah website e-grocery yang dapat dipergunakan oleh Aneka Mart Tebas untuk menjangkau masyarakat luas dalam memasarkan barang dan memberikan kemudahan bagi konsumen untuk mendapatkan barang dan bertransaksi. Dengan menggunakan website e-grocery pihak penjual dapat menjual barangnya secara online dan pihak konsumen mendapatkan kemudahan dalam melakukan pemesanan barang tanpa harus datang langsung ke alamat toko fisik dari Aneka Mart Tebas.

5. SARAN

Berdasarkan hasil pembahasan dan kesimpulan, maka dapat diambil beberapa saran sebagai Untuk mendukung pengoperasian secara maksimal dari website e-grocery perlu adanya dukungan koneksi internet yang memadai terutama bagi pihak toko. Dengan adanya pengembangan website yang merupakan sumber informasi maka pendokumentasian harus dilakukan dengan baik. Personil yang dilibatkan dalam manajemen konten dan pemeliharaan perlu memiliki pengetahuan dasar dibidang jaringan dan memahami dasar pemrograman website. Untuk memperoleh hasil yang maksimal perlu mencakup keseluruhan dari Linear Sequential / Waterfall Model dan juga diperlukan kajian lebih lanjut.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada dosen pembimbing, keluarga dan teman-teman yang telah memberi dukungan dalam menyelesaikan jurnal ini.

DAFTAR PUSTAKA

- [1] Kendall, Kenneth E., and Julie E. Kendall, 2003, “*Aplikasi dan Perancangan Sistem, Edisi Kelima*”, Jilid 1 dan 2, PT INDEKS.
- [2] Hays, T., Keskinocak, P., Lopez, V.M., (2004), “Strategies and Challenges of Internet Grocery Retailing Logistics”, Applications of Supply Chain Management and E-Commerce Research in Industry, Kluwer Academic Publishers, Dordrecht, The Netherlands, 2004.
- [3] Oetomo, 2002. “*Perancangan dan Pembangunan Sistem Informasi*”. Yogyakarta : CV Andi Offset.
- [4] Putri, S. Y., Ismail, S. J. I., & Rosmiati, M. (2015). Perlindungan Prototype Efb (electronic Flight Bag) Terhadap Serangan XSS (cross Site Script) Dengan Metode Black-box Testing. eProceedings of Applied Science, 1(3), 2299-2307.
- [5] Stuart McClure, Joel Scambray, George Kurtz. (2003). Hacking Exposed, McGraw-Hill.
- [6] Sugiyono, (2008). Metode Penelitian Bisnis. Bandung. Alfabeta.
- [7] Tolle, H., Kurniawan, T. A., & Zakaria, A. (2012). Peningkatan Keamanan Web Terhadap Serangan Cross Site Scripting (XSS). TEKNO, 9(1), 52-61.
- [8] Yulianingsih (2017). Melindungi Aplikasi dari Serangan Cross Site Scripting (XSS) Dengan Metode Metacharacter. Teknosi, 3(1), 83-88.