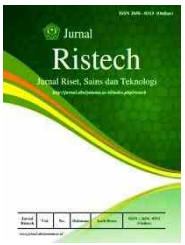
Jurnal Ristech
(Jurnal Riset, Sains dan Teknologi)
Available online at www.jurnal.abulyatama.ac.id/index.php/ristech
ISSN 2656 - 0313 (Online)
Universitas Abulyatama



UJI KEAMANAN WEBSITE TERHADAP SERANGAN SQL INJECTION : STUDI KASUS WEBSITE PENJUALAN BUKU

Armiyati, Juniana Husna, Banta Cut
Sistem Informasi, Fakultas Teknik , Universitas Abulyatama
Jl. Blang Bintang Lama Km. 8,5 Telp (0651) 21255 Lampoh Keudee, Aceh Besar- 23372
e-mail : armiyati403@gmail.com

ABSTRACT

The Book Sales Website is a website used as a medium for buying and access between buyers and sellers, given that the website can be accessed widely. Therefore, it is necessary to pay attention to website security, one of which is to do SQL Injection, SQL Injection is a vulnerability that occurs when an attacker has the ability to influence Structured Query Language (SQL), a query that passes an application to a back-end database. The purpose of this study is to find loopholes, then find out how to test website security, and find solutions to overcome problems with website security on book sales websites. From the book selling website, 1 website is vulnerable to attack attack. The results of testing the website selling books have a vulnerability type High 44%, Medium types 17%, and Low types 39%. The security gap will be tested in order to obtain future solutions for the development of safer websites.

Keywords : Testing, Security, Website, SQL Injection.

ABSTRAK

Website Penjualan Buku merupakan *website* yang digunakan sebagai media sarana untuk membeli dan akses antara pembeli dan penjual, mengingat website tersebut dapat diakses secara luas. Oleh karena itu, perlu memperhatikan keamanan *website,* salah satunya adalah dengan melakukan *SQL Injection, SQL Injection* adalah kerentanan yang terjadi ketika penyerang memiliki kemampuan untuk mempengaruhi *Structured Query Language (SQL)*, *query* yang melewati suatu aplikasi ke *database back-end.* Tujuan dari penelitian ini adalah untuk menemukan celah, kemudian mengetahui cara pengujian keamanan *website*, dan mengetahui solusi mengatasi masalah terhadap keamanan *website* pada website penjualan buku. Dari *website* penjualan buku didapatkan 1 website yang rentan terhadap serangan *attacker*. Hasil pengujian *website* penjualan buku terdapat kerentanan jenis High 44 %, jenis Medium 17 %, dan jenis Low 39 %. Celah keamanan tersebut akan diuji sehingga memperoleh solusi kedepan guna pengembangan *website* yang lebih aman.

Kata kunci : Pengujian, Keamanan, Website, SQL Injection.

1. PENDAHULUAN

Perkembangan teknologi yang semakin canggih memungkinkan proses kegiatan berjalan sangat cepat. Hadirnya teknologi membuat pekerjaan semakin mudah. Kemudahan yang ditawarkan tenologi tentunya seiring dengan bahaya yang disisipkan melalui berbagai hal. Terlebih jika bahaya tersebut tersistem sehingga kecenderungan

pengguna tidak menyadarinya dengan adanya bahaya yang sudah masuk dan mengintainya. Sistem dapat didefinisikan sebagai seperangkat komponen (sumber daya) terkait, dengan batas yang jelas dan bekerja sama untuk mencapai tujuan tertentu melalui sebuah inputan dalam proses transformasi yang teroganisir. Sedangkan Sistem Informasi lebih menekankan pada pengelolaan sumber daya (resource) yang ada menjadi produk informasi.

Layanan informasi yang terhubung dengan internet dapat diakses melalui website. Karena website sering sekali menjadi target serangan yang dilakukan oleh attacker. Website bisa disebut suatu layanan sajian informasi yang menggunakan konsep tautan (hyperlink) yang mempermudah pengguna internet untuk melakukan pencarian informasi. Maka dari itu website sering diserang untuk diambil informasi atau data secara paksa. Hal itu juga yang terjadi pada website penjualan buku yang rawan akan serangan attacker. Website penjualan buku merupakan website yang digunakan sebagai media sarana untuk membeli dan akses antara pembeli dan penjual. Mengingat website ini dapat diakses secara luas, maka dinilai perlu memperhatikan keamanan website. Terdapat beberapa cara yang digunakan untuk menganalisa keamanan website tersebut. Salah satu caranya adalah dengan menggunakan serangan SQL Injection.

SQL Injection adalah kegiatan menyisipkan perintah SQL kepada suatu statement SQL yang ada pada aplikasi yang sedang berjalan. Dengan kata lain SQL Injection ini merupakan suatu teknik pengeksploitasi pada web aplikasi yang didalam nya menggunakan database untuk penyimpanan datanya (Affandi, 2008).

Penelitian yang pernah dilakukan oleh Putri dkk, (2012) Analisis Forensik Jaringan Studi Kasus Serangan SQL Injection pada Server Universitas Gadjah Mada, dapat diketahui bahwa hasil analisis data log serangan SQL Injection yang menuju ke server Universitas Gadjah Mada (www.ugm.ac.id), dilakukan menggunakan tools seperti Havij dan SQLMap. Tools yang dibuat adalah parsing pcap yang dapat memecah file log dalam bentuk pcap berdasarkan tanggal, IP addres, mac address dan nomor port, sedangkan tools kedua yaitu port scanning yang dapat mengetahui port yang terbuka maupun yang tertutup pada suatu host atau server, dan yang terakhir adalah tools untuk mengubah file log pcap ke bentuk database sehingga data log bisa dianalisis secara lebih mendalam.

Selanjutnya penelitian yang dilakukan oleh Putra, SSH (2017) Penanggulangan Serangan XSS, CSRF, SQL Injection Menggunakan Metode Blackbox pada Marketplace IVENMU. Penanggulangan ancaman serangan Cross Site Scripting (XSS), Cross Site Request Forgery (CSRF) dan SQL Injection telah diimplementasikan. IVENMU mampu bertahan terhadap serangan Cross Site Scripting (XSS), Cross Site Request Forgery (CSRF) dan SQL Injection. IVENMU mampu bertahan secara aman.

Berdasarkan uraian dari penelitian sebelumnya, dapat disimpulkan bahwa dengan menggunakan tools Havij dan SQLMap dapat memecah file log dalam bentuk pcap berdasarkan tanggal, IP address, mac address dan nomor port serta dapat mengetahui port yang terbuka maupun yang tertutup pada sustu host atau server. Dengan mengimplementasikan IVENMU dapat menanggulangi ancaman serangan Cross Site Scripting (XSS), Cross Site Request Forgery (CSRF) dan SQL Injection.pada *Microsoft Word* yang menggunakan ”.” sebagai tanda desimal dan bukan ”,”. Aturan penulisan desimal dalam Jurnal APLIKA mengikuti aturan penulisan Matematika).

2. Landasan Teori

2.1 Keamanan Website

Keamanan web adalah proses mengamankan data rahasia yang disimpan secara online dari akses dan modifikasi data yang tidak sah. Hal ini dilakukan dengan menerapkan langkah-langkah kebijakan yang ketat (Kortisa, 2016).

2.2 Keamanan Jaringan

Jaringan komputer merupakan sekumpulan komputer otonom yang saling terhubung melalui media komunikasi dengan menggunakan protokol sebagai identitas setiap komputer yang terhubung pada jaringan tersebut. Manfaat jaringan komputer antara lain adalah memungkinkan pemakaian bersama atas sumber daya yang ada. Sumber daya dalam hal ini dapat berupa perangkat keras, perangkat lunak dan data atau informasi. Keamanan jaringan merupakan upaya memberikan keterjaminan jaringan atas gangguan gangguan yang mungkin muncul (Oktavinanda,2014).

2.3 Kejahatan Dunia Maya

Istilah keamanan biasa digunakan untuk hal-hal yang berhubungan dengan kejahatan, segala bentuk pencurian, dan lain-lain. Keamanan website adalah suatu cabang teknologi yang dikenal dengan nama keamanan informasi yang diterapkan pada website. Sasaran keamanan website antara lain adalah perlindungan terhadap informasi/data. Semakin maju sebuah teknologi yang diiringi dengan bertambahnya nilai informasi maka akan memicu juga munculnya jenis kejahatan baru. Secara khusus, kejahatan yang mengancam jaringan internet atau yang menggunakan jaringan intenet untuk melakukan kejahatan dunia maya. Kejahatan dunia maya merupakan kejahatan yang dilakukan oleh seseorang dengan menggunakan fasilitas internet yang bersifat melintas batas negara, dilakukan secara illegal, menggunakan peralatan komputer dan internet, menyebabkan kerugian, dan sulit dibuktikan secara hukum, Kejahatan dunia maya (cybercrime) ini menjadi ancaman tersendiri bagi keamanan sebuah website (Elu, 2013).

2.4 Website

Website merupakan suatu layanan sajian informasi yang menggunakan konsep tautan (hyperlink) yang mempermudah pengguna internet untuk melakukan pencarian informasi. Suatu website merupakan kumpulan halaman web yang saling terhubung dan file-file nya saling terkait yang dapat disertai dengan file gambar , video ataupun file-file yang lain baik bersifat statis ataupun dinamis. Informasi atau file-file yang terdapat dalam website tersimpan dalam sebuah server web yang secara umum ditulis dengan format HTML atau Hypertext Markup Language. Hyperlink adalah sebuah acuan dalam dokumen hypertext ke dokumen yang lain yang berbentuk grafis ataupun teks dalam dokumen tersebut yang biasanya ditandai dengan adanya garis bawah dan atau berwarna biru. Pada suatu web secara umum terdiri dari page atau halaman yang ditempatkan pada suatu server web yang dapat diakses melalui jaringan internet ataupun jaringan wilayah local yang merupakan file teks yang berisi tag-tag dengan format HTML (Elu, 2013).

2.5 Internet

Internet adalah sistem global jaringan komputer yang saling berhubungan yang menggunakan standart *Internet Protocol Suite* (TCP/IP) untuk melayani pengguna di seluruh dunia. Ini adalah jaringan dari jaringan yang terdiri dari jutaan pribadi, umum, akademik, bisnis, dan jaringan pemerintah, dari local untuk lingkup global, yang dihubungkan untuk sebuah array yang luas dari teknologi jaringan elektronik dan optik. Internet membawa berbagai macam sumber informasi dan layanan, seperti antar linked hypertext dokumen dari *Word Wide Web* (WWW) dan infrastruktur untuk mendukung surat elektronik. Jaringan internet adalah media yang paling cepat terinovasi kesegala lini dan paling adaptif dengan kebutuhan masyarakat, sehingga hampir semua media dan kebutuhan masyarakat dapat di koneksikan ke dalam jaringan-jaringan internet (Riska, 2013).

2.6 Subgraph Vega

Vega adalah sebuah platform open source untuk menguji keamanan aplikasi web. Vega dapat membantu dalam menemukan dan memvalidasi SQL Injection, Cross Site Scripting(XSS), inadvertently disclosed sensitive information, and other vulnerabilities, dan kerentanan lainnya. Di tulis dengan bahasa pemograman JAVA, berbasis GUI, dan berjalan pada Linux, OS X, dan Windows.

Vega termasuk scanner otomatis dan cepat, dan intercepting proxy untuk tactical inspection. Vega dapat dikembangkan dengan menggunakan powerful API, dalam bahasa web : Javascript. Vega di kembangkan oleh Subgraph di Montreal (Unknown, 2015).

2.7 SQL

SQL merupakan singkatan Structured Query Language. Di dalam dunia database istilah query dapat diartikan "Permintaan Data". SQL merupakan bahasa tingkat empat yang berfungsi menampilkan hasil atau melakukan sesuatu pada

data yang tidak diinginkan. SQL query terdiri dari satu atau beberapa SQL Statements yang secara efektif mengintruksikan tugas yang harus di lakukan oleh server database. Pada SQL Statements juga dikenal regular expressions (regex) yang merupakan pola dari karakter-karakter yang sama atau gagal untuk disamakan, bersamaan dengan karakter lain didalam teks. Regular expressions ini juga dapat digunakan untuk melakukan proses pengujian vulnerability sql injection pada suatu website (Elu, 2013).

2.8 SQL Injection

SQL Injection adalah kerentanan yang terjadi ketika penyerang memiliki kemampuan untuk mempengaruhi Structured Query Language (SQL), query yang melewati suatu aplikasi ke database *back-end.* Dengan memasukkan perintah SQL sebagai input sebuah web guna mendapatkan akses ke database, penyerang dapat memanfaatkan sintaks dan kemampuan dari SQL, serta kekuatan dan fleksibilitas untuk mendukung fungsi operasi database dan fungsionalitas sistem yang tersedia ke database (Dahlan, 2015).

Penyebab utama terjadi nya SQL Injection adalah tidak adanya penanganan terhadap karakter-karakter tanda petik satu (‘) dan juga karakter double minus (--) yang menyebabkan suatu aplikasi dapat disisipi dengan perintah SQL. Sehingga seorang hacker menyisipkan perintah SQL ke dalam parameter suatu form. SQL Injection memanfaatkan kelalaian dari website yang mengijinkan user untuk menginputkan data tertentu tanpa melakukan filter terhadap malicious character. Input tersebut biasanya di masukan pada box search atau bagian-bagian tertentu dari *website* yang berinteraksi dengan basis data SQL dari situs tersebut. Bug SQL Injection sangat berbahaya, karena teknik ini memungkinkan seseorang dapat login ke dalam sistem tanpa harus memiliki account (Yudistira, 2012).

2.9 Kegunaan SQL Injection

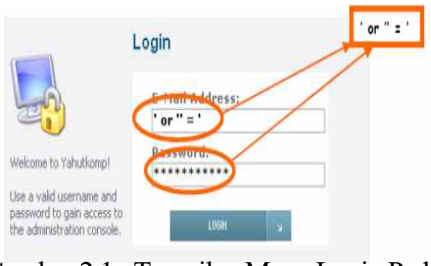
SQL Injection adalah menyisipkan query SQL kedalam sebuah aplikasi web melalui form input dan *URL (Uniform Resource Locator)* untuk mendapatkan informasi pada basis data . SQL Injection dapat diartikan suatu kegiatan menipu query dari basis data, sehingga seseorang dapat mengetahui dan mendapatkan informasi yang terdapat pada basis data. Menipu disini adalah menyisipkan kode SQL tambahan ke dalam kode yang asli pada sebuah aplikasi (Falistathuyunis, 2018).

2.10 Contoh Penyerangan Sql Injection

SQL Injection adalah jenis aksi hacking pada keamanan komputer dimana seorang penyerang bisa mendapatkan akses ke basis data didalam sistem. SQL Injection yaitu serangan yang mirip dengan XSS dalam bahwa penyerang memanfaatkan aplikasi vektor dan juga dengan common dalam serangan XSS (Masykuri, 2013).
Adapun contok sintaks pemograman PHP yang diterapkan para attacker dapat melakukan

penyerangan dengan menggunakan metode SQL Injection adalah sebagai berikut :

1. $SQL = "select * from login where username = "$username" and password = "$password"; , {dari GET atau POST variable}
2. Isikan password dengan string 'or" = '
3. Hasilnya maka SQL akan seperti ini = "select * from login where username = '$username' and password = 'pass' or' = ' "; ,{dengan SQL ini hasil selection akan selalu TRUE}
4. Dan hasilnya, para hacker bisa inject sintax SQL kedalam SQL dengan menggunakan menu Login pada website yang akan diserang. Seperti pada gambar dibawah ini :



Gambar 2.1 : Tampilan Menu Login Pada Website

Berdasarkan uraian diatas dapat disimpulkan bahwa dengan menggunakan metode Sql Injection pada menu Login sebuah website dengan memasukkan kode 'or" = ' pada password, sehingga hasil selection akan selalu TRUE. Dengan demikian, para hacker bisa masuk kedalam website yang diserangnya.

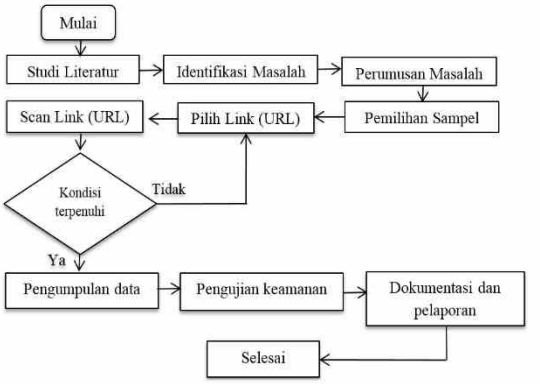
3. Metodelogi Penelitian

3.1 Metode Penelitian

Metode penelitian adalah langkah yang dimiliki dan dilakukan oleh peneliti dalam rangka untuk mengumpulkan informasi atau data serta melakukan investigasi pada data yang telah didapatkan tersebut. Metode penelitian memberikan gambaran rancangan penelitian yang meliputi antara lain: prosedur dan langkah-langkah yang harus ditempuh, waktu penelitian, sumber data, dan dengan langkah apa data-data tersebut diperoleh dan selanjutnya diolah dan dianalisis (Hidayat, 2017).

3.2 Tahapan Penelitian

Tahapan penelitian yangn dilakukan oleh penulis berdasarkan serangan *SQL Injection* yang diteliti adalah sebagai berikut :



Gambar 3.1 Diagram Alir Penelitian

3.3 Metode Pengumpulan Data

Metode penelitian yang digunakan adalah sebagai berikut :

1. Investigasi

   Investigasi adalah salah satu cara mengumpulkan data dengan mengumpul data-data tertulis. Contoh data-data tertulis adalah laporan, memo, manual, dan peraturan perusahaan, pengumuman. dll

2. Dokumen

   Dokumen merupakan sumber data yang digunakan untuk melengkapi penelitian, baik berupa sumber tertulis, film, gambar (foto), dan karya-karya monumental, yang semua itu memberikan informasi (Yuni4ti, 2013).

3.4 Kebutuhan Sistem

Peralatan yang di perlukan adalah sebagai berikut :

1. Laptop untuk melakukan proses scanning
2. Subhgraph Vega
3. OS Windows 8.1 pro 64 bit.

3.5 Tempat dan Jadwal Penelitian

Dalam menyusun proposal skripsi ini penulis mengamati Website penjualan di mulai dari tanggal 5 maret – 13 mei 2019. Waktu untuk penulis mengamati website penjualan pada pukul 08.00 – 17.00 wib setiap hari.

3.6 Teknik Pengumpulan Data

Teknik pengumpulan data yang dilakukan penulis adalah teknik Purposive Sampling, purposive sampling adalah teknik sampling non random sampling dimana peneliti menentukan pengambilan sampel dengan cara menetapkan ciri-ciri khusus yang sesuai dengan tujuan penelitian sehingga diharapkan dapat menjawab permasalahan penelitian (Hidayat, 2017).

1. Lokasi Analisis

   Analisis dilakukan pada website penjualan yang masih dapat diakses secara umum dan bisa diakses dimana saja.

2. Populasi Analisis

   Populasi merupakan individu atau objek yang merupakan sifat-sifat umum wilayah generalisasi yang terdiri atas objek atau subjek yang mempunyai kualitas dan karakteristik tertentu untuk dipelajari dan ditarik kesimpulan. Populasi yang ditetapkan dalam melakukan analisis ini adalah website penjualan yang dapat digunakan sebagai sarana untuk informasi pembelian buku dan dapat diakses secara umum.

3. Sampel

   Dalam melakukan analisis penulis mengambil sampel dengan menggunalan teknik Purposive Sampling dilakukan dengan cara mengambil subjek bukan didasarkan atas, random, atau daerah tetapi didasarkan atas adanya tujuan dan pertimbangan tertentu. Maka sampel yang digunakan dalam proses pengujian ada 1 website penjualan. Pemilihan 1 website ini berdasarkan pada kebutuhan penulis. Berikut ini adalah nama beserta website yang diuji :

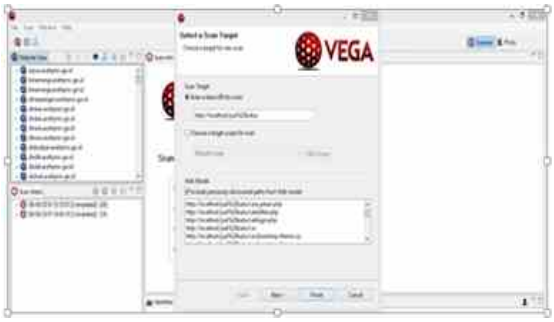
No.	Nama Website	Link Website
1.	Website penjualan buku	http://localhost/jual%20buku/

Tabel 3.1 Sampel Website penjualan buku yang diuji

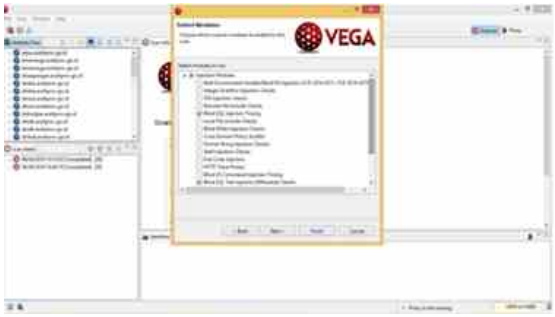
3.7 Proses Pengujian

Pada tahap ini penulis mulai melakukan pengujian menggunakan Subhgraph Vega terhadap keamanan website penjualan buku. Berikut ini langkah-langkah melakukan pengujian :

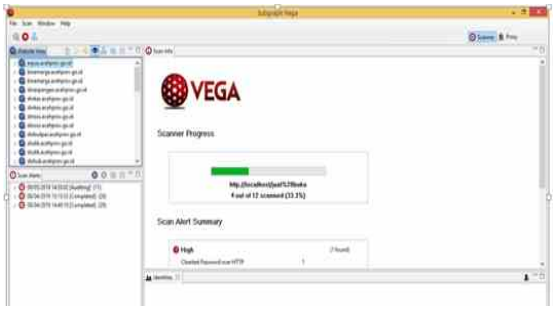
Gambar 3.2 : Tampilan awal pada aplikasi Subgraph Vega



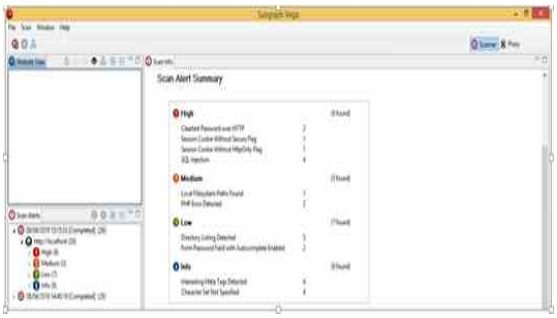
Gambar 3.3 : Tampilan untuk mengisi link (Url) Website yang akan di scan.



Gambar 3.4 : Tampilan pemilihan untuk serangan.



Gambar 3.5 : Tampilan proses pengujian



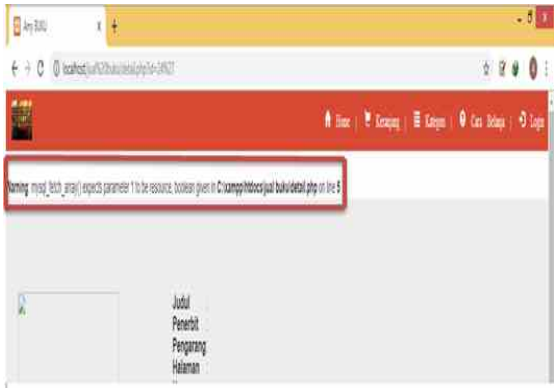
Gambar 3.6 : Tampilan hasil pengujian

3.8 Implementasi Dari Sql Injection

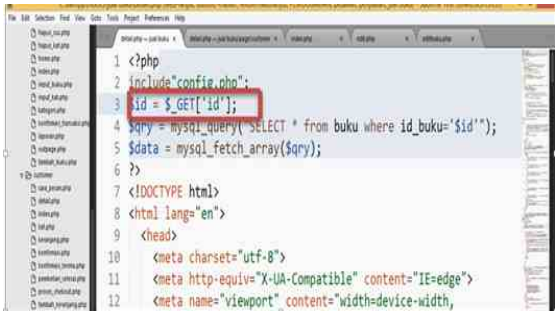
Pada tahap ini mulai melakukan serangan kode SQL Injection pada localhost dengan Url http://localhost/jual%20buku/. Berikut ini langkah-langkah melakukan implementasi :

Gambar 3.7 : Tampilan halaman website penjualan buku

Gambar 3.8 : Tampilan halaman website setelah dimasukan tanda petik satu

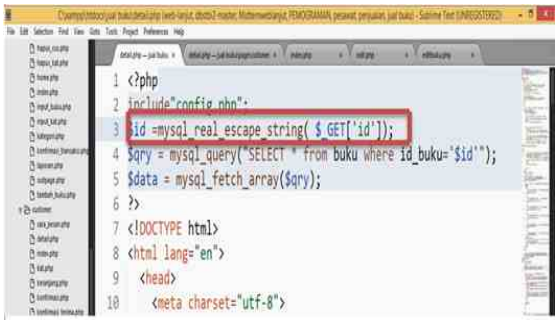


Gambar 3.9 : Tampilan halaman website yang terinjeksi sintak Sql Injection



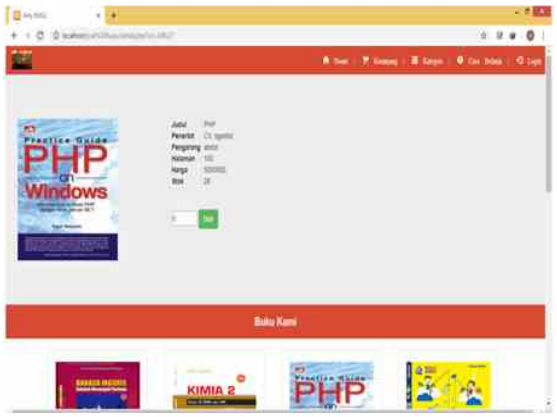
```
<?php
include"config.php";
$id = $_GET['id'];
$qry = mysql_query("SELECT * from buku where id_buku='$id'");
$data = mysql_fetch_array($qry);
?>
<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width,
```

Gambar 3.10 : Tampilan coding sintaks sebelum diperbaiki



```
<?php
include"config.php";
$id =mysql_real_escape_string( $_GET['id']);
$qry = mysql_query("SELECT * from buku where id_buku='$id'");
$data = mysql_fetch_array($qry);
?>
<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
```

Gambar 3.11 : Tampilan coding setelah sintaks diperbaiki



Gambar 3.12 : Tampilan halaman website setelah diperbaiki

3.9 Cara Mengatasi Sql Injection

```
= mysql_real_escape_string(
```

Fungsi dari mysql_real_escape_string tersebut adalah digunakan untuk memberi perlindungan/mencegah karakter Sql Injection terhadap karakter tanda petik satu (‘) sebelum mengirim query ke mysql yang dapat membahayakan data dari serangan Sql Injection. Mysql_real_escape_string memproteksi karakter yang membahayaka kan Sql ketika di running.

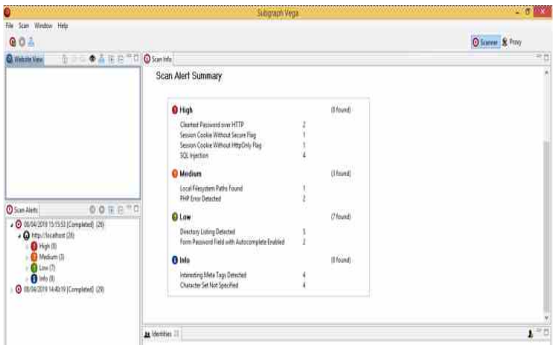
4. Hasil dan Pembahasan

4.1 Pembahasan

Pada bagian ini akan diuraikan hasil yang telah dilakukan berdasarkan pengujian yang telah dikemukakan pada bab sebelumnya. Pembahahasan diarahkan pada permasalahan terhadap keamanan website dengan serangan *SQL Injection* yang terdapat di 1 (satu) website penjualan buku.

4.2 Scanner Website

Berdasarkan hasil scanner website yang berhasil di dapatkan dari website penjualan buku. Dengan ini akan membahas hasil yang di dapat melalui proses scanner dengan memakan waktu 4-5 jam.



Gambar 4.1 : Hasil scanner website penjualan buku

Jenis *High* ditemukan 4 (empat), jenis *Medium* ditemukan 2 (dua), jenis, *Low* ditemukan 2 (dua). jenis *Information* ditemukan 2 (dua). Dari keempat jenis tersebut yang paling berbahaya adalah jenis *High* atau bisa disebut juga paling beresiko untuk diserang. Didalam jenis *High* terdapat *Sql Injection* dengan permasalahan didapat totalnya ada 4 (empat) yang bermasalah berarti bisa di kategorikan *website* tersebut masih belum aman dari para *attacker.*

4.3 Hasil Pengujian Website

Dari hasil pengujian *website* yang berlangsung dapat dirangkum jumlah url yang bermasalah pada website penjualan buku, maka dapat dijelaskan pada tabel dibawah ini. Untuk mempermudah proses yang didapat maka hasilnya akan di masukkan dalam tabel, berikut tabelnya :

No	Nama Website	Jumlah Url yang bermasalah					
		High	%	Medium	%	Low	%
1.	Website Penjualan Buku	8	44	3	17	7	39

Tabel 4.1 : Jumlah Url yang bermasalah pada website penjualan buku

Dari keseluruhan Url, ada 8 (delapan) Url yang bermasalah pada kerentanan jenis *High,* 3 (tiga) Url pada kerentanan jenis *Medium*, dan 7 (tujuh) url pada kerentanan jenis *Low*. Dari 8 (delapan) Url yang bermasalah pada kerentanan jenis High terdapat 4 *Sql Injection*, 1 *Session Cookie Without Secure Flag*, 2 *Cleartext Password Over HTTP*, dan 1 *Session Cookie Without Httponly Flag.*

Namun demikian, yang diuji dalam penelitian ini hanya serangan dari *Sql Injection* yang terdiri dari 4 celah yaitu detail.php, index.php, editbuku.php, dan edit.php. Proses selanjutnya adalah tingkat kerentanan sebuah website dari jumlah Url yang bermasalah yang menggunakan persen (%) dimasukkan ke dalam diagram bentuk pie supaya mudah dilihat dan dipahami.

Gambar 4.2 : Persentase tingkat kerentanan pada Website

Dari hasil gambar diagram diatas dapat disimpulkan bahwa tingkat kerentanan persentase hasil analisa website pada website penjualan buku terdapat kerentanan jenis High 44 %, Medium 17 %, dan Low 39 %.

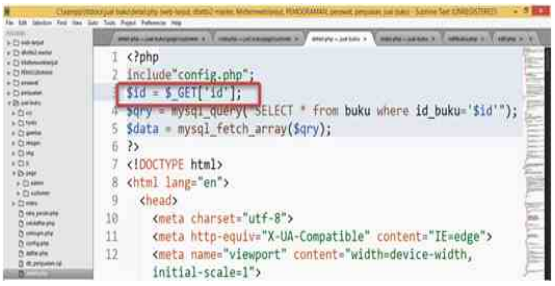
4.4 Kasus Sql Injection dan Cara Penyelesaiannya

Berdasarkan penelitian yang sudah dilakukan, terdapat beberapa kasus dari Sql Injection pada website penjualan buku. Berikut ini adalah celah keamanan dan cara penyelesaian dari kasus tersebut

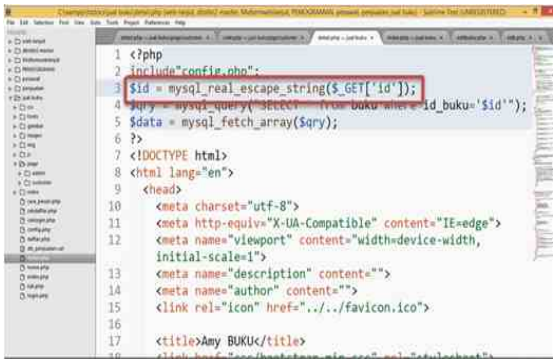
No	Celah Keamanan	Coding sebelum diperbaiki	Coding sesudah diperbaiki
1	Detail.php	$id=$_GET['id'];	$id=mysql_real_escape_string($_GET['id']) ;
2	Index.php	@$idkat=$_GET['id'] ;	@$idkat=mysql_real_escape_string ($_GET['id']) ;
3	Editbuku.php	$e=$_GET['id'];	$e=mysql_real_escape_string($_GET['id']);
4	Edit.php	$a=$_GET['id'];	$a=mysql_real_escape_string($_GET['id']);

Tabel 4.2 : Celah keamanan pada website penjualan buku

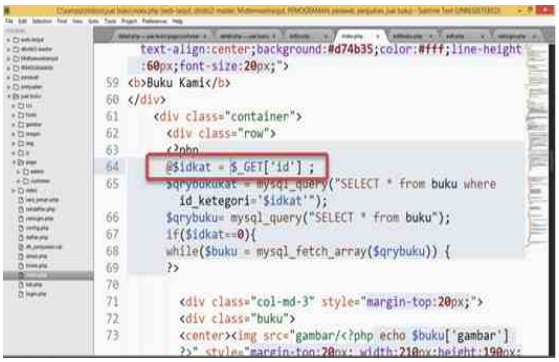
Dari tabel diatas dapat dilihat celah keamanannya, coding sebelum diperbaiki dan coding sesudah diperbaiki. Proses selanjutnya adalah pembuktian cara penyelesaian dari coding yang sebelum diperbaiki dan coding yang sudah diperbaiki. Berikut ini adalah contohnya :



Gambar 4.3 : Tampilan coding sebelum diperbaiki dari celah detail.php

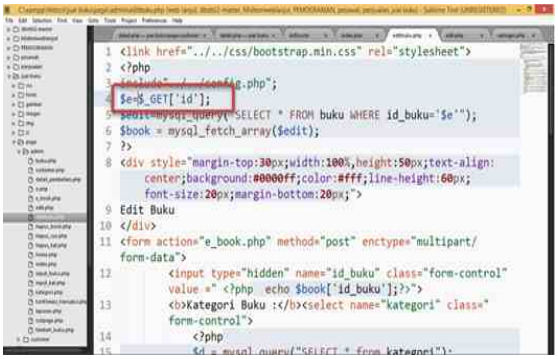


Gambar 4.4 : Tampilan coding sesudah diperbaiki dari celah detail.php

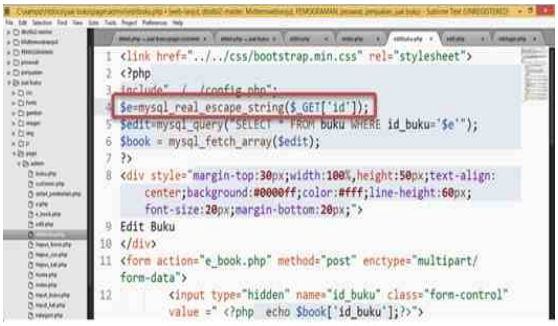


Gambar 4.5 : Tampilan coding sebelum diperbaiki dari celah index.php

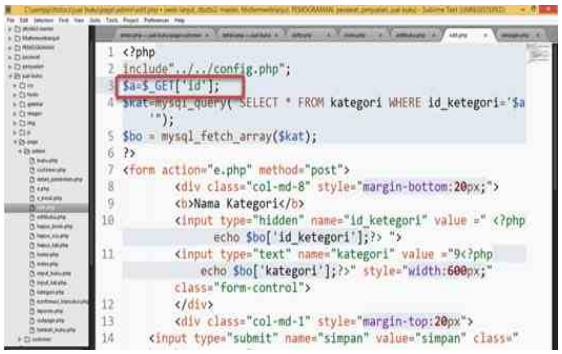
Gambar 4.6 :Tampilan coding yang sudah diperbaiki dari celah index.php



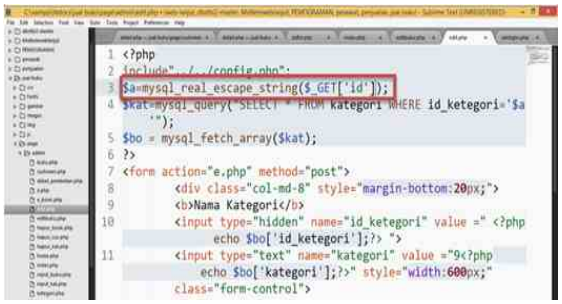
Gambar 4.7 : Tampilan coding sebelum diperbaiki dari celah editbuku.php



Gambar 4.8 : tampilan coding sesudah diperbaiki dari celah editbuku.php



Gambar 4.9 : tampilan coding sebelum diperbaiki dari celah edit.php



Gambar 4.10 : Tampilan coding sesudah diperbaiki dari celah edit.php

5. Kesimpulan dan Saran

5.1 Kesimpulan

Berdasarkan hasil kegiatan "Uji Keamanan Website Terhadap Serangan *Sql Injection* : Studi Kasus Website Penjualan Buku" dapat diketahui sampai saat ini tingkat keamanan pada beberapa website penjualan untuk saat ini masih belum aman. Penulis dapat menyimpulkan beberapa hal sebagai berikut :

1. Dengan adanya pengujian ini diharapkan tingkat keamanan pada sebuah website dapat ditingkatkan atau melakukan update secara berkala sehingga memperkecil resiko terhadap serangan attacker.
2. Dapat dijadikan pedoman sebagai pemantau jaringan yang dapat disimpulkan bahwa website dikatakan relatif aman.
3. Persentase hasil analisa website pada website penjualan buku terdapat kerentanan jenis High 44%, jenis Medium 17%, dan jenis Low 39 %.
4. Serangan Sql Injection cukup berbahaya karena attacker bisa memanipulasi data dengan memasukkan tanda petik satu pada url.
5. .Hasil implementasi serangan Sql Injection pada aplikasi penjualan buku, yaitu serangan Sql Injection cukup berbahaya karena ketika attacker memasukan tanda petik satu pada url, maka attacker tersebut sudah bisa memanipulasi data dan mendapatkan informasi dari basis data.

5.2 Saran

1. Diharapkan agar analisa yang sudah dilakukan supaya dapat dimanfaatkan dan digunakan sebagai pedoman untuk meningkatkan keamanan website.
2. Dalam menjaga keamanan website perlu memperhatikan perawatan atau melakukan service web secara teratur. Untuk solusi yang lainnya sintaks harus periksa dan perbaiki secara berkala atau melakukan perbaruan terhadap bahasa pemograman.
3. Untuk menjaga tingkat keamanan sebuah website di perlukan orang-orang yang berkompeten atau ahli dibidang website.

4. Kelemahan website terletak pada bahasa pemogramannya atau sintaks yang digunakan masih belum sempurna. Cara memperbaikinya adalah dengan menyempurnakan sintaks tersebut dengan teliti.

DAFTAR PUSTAKA

Affandi, ahmad, 2008. Sql injection dan cara pencegahannya. Tugas akhir. Palembang. Universitas sriwijaya.

Arikunto, suharsimi. "metodologi penelitian". Jakarta: pt. Rineka cipta (2013).

Dahlan, moh, dkk. 2014. Pengujian analisa keamanan website terhadap serangan sql injection studi kasus : website umk. Skripsi. Gondangmanis. Universitas muria kudus.

Elu, am. 2013. Rancang bangun aplikasi pendeteksian vulnerbility structured query language (sql) injection untuk keamanan website. Issn: 1907-2430.114

Elu, am. 2013. Rancang bangun aplikasi pendeteksian vulnerbility structured query language (sql) injection untuk keamanan website. Issn: 1907-2430.113

Hidayat, rahmat. 2014. Keamanan jaringan "mengenal firewall dan cara kerjanya". Makalah.

Ismail6033, 2017. Makalah teknik pengumpulan data. Makalah

Kortisa, yogi. 2016. Deteksi sql injection pada web menggunakan metode code review dan penetration testing. Skripsi. Batam. Politeknik.

Masykuri, lh. 2013. Mencegah sql injection pada sebuah website menggunakan pattern regex. Makalah

Masykuri, lh. 2013. Mencegah sql injection pada sebuah website menggunakan pattern regex. Makalah

Riska, dkk. 2013. Studi tentang pengguna internet oleh pelajar. Issn: 0000-0000.2

Putri, ru, dkk. 2012. Analisis forensik jaringan studi kasus serangan sql injection pada server universitas gadjah mada. Issn: 1978-1520.110

Putra, ssh. 2017. Penanggulangan serangan xss, csrf, sql injection menggunakan metode blackbox pada marketplace ivenmu. Issn: 2355-9977.299

Unknown, 2014. Teknik pengambilan sampel dengan metode purposive sampling. Dari http://www.portal-statistik.com. (diakses 17 mei).

Unknown, 2015. Cara menggunakan vega web scanner. Dari http://www.skilledmaster.blogspot.com. (diakses 10 juli)

Yudistira, alfandi, 2012. Analisis keamanan otentikasi dan basis data pada web simple-o menggunakan sql injection. Skripsi. Depok. Fakultas teknik program studi teknik komputer.