ANALISIS KEAMANAN *WEBSITE* DI UNIVERSITAS MUHAMMADIYAH SURAKARTA

Makalah

Program Studi Teknik Informatika

Fakultas Komunikasi dan Informatika

Diajukan oleh:

Detty Metasari

Fatah Yasin Irsyadi, S.T., M.T.

Ir. Jatmiko, M.T.

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS KOMUNIKASI DAN INFORMATIKA

UNIVERSITAS MUHAMMADIYAH SURAKARTA

2014

HALAMAN PENGESAHAN

Publikasi ilmiah dengan judul :

ANALISIS KEAMANAN *WEBSITE*

DI UNIVERSITAS MUHAMMADIYAH SURAKARTA

Yang dipersiapkan dan disusun oleh :

Detty Metasari

L200 090 039

Telah disetujui pada :

Hari :

Tanggal :

Pembimbing I	Pembimbing II
Fatah Yasin, S.T., M.T.	**Ir. Jatmiko, M.T.**
NIP/NIK : 738	NIK/NIK : 622

Publikasi ilmiah ini telah diterima sebagai salah satu persyaratan

Untuk memperoleh gelar sarjana

Tanggal :

Mengetahui

Ketua Program Studi

Teknik Informatika

Heru Supriyono, S.T.,M.Sc.Ph,D

NIK : 970

ANALISIS KEAMANAN *WEBSITE* DI UNIVERSITAS MUHAMMADIYAH SURAKARTA

Detty Metasari, Fatah Yasin Irsyadi, Jatmiko

Program Studi Teknik Informatika, Fakultas Komunikasi dan Informatika

Universitas Muhammadiyah Surakarta

E-Mail : **detty.metasari@gmail.com**

ABSTRAK

Pada saat ini *website* menjadi salah satu media informasi *modern* yang berkembang sangat cepat. Dalam pembuatan website tidak hanya sisi *desain* dan informasi yang dipentingkan tetapi aspek keamanan dari sebuah website itu sendiri mempunyai peranan yang sangat penting dalam sebuah website. Kebutuhan keamanan sebuah website timbul dari kebutuhan untuk melindungi data. Pertama, dari kehilangan dan kerusakan data. Kedua, adanya pihak yang tidak hendak mengakses dan merubah data. Permasalahan lainnya mencakup perlindungan data dari *delay* yang berlebih pada saat mengakses atau menggunakan data, atau mengatasi gangguan *Denial of Service*.

Metode yang dilakukan pada pengujian ini akan menggunakan *tool* berupa perangkat lunak dan cara-cara tertentu yang digunakan untuk menguji keamanan sebuah *website.* Untuk melakukan analisis keamanan *website*, *software* yang digunakan adalah *Acunetix website vulnerability scanner*.

Hasil dari pengujian adalah ditemukannya berbagai level kerentanan dari level kerentanan *Low* pada *domain* ums.ac.id sampai level kerentanan *High* pada sub domain lainnya yang berupa sub domain fakultas. Dari hasil analisis yang diperoleh dapat dilihat berbagai *web alerts* yang terdapat pada sebuah *website*. Adapun berbagai *web alerts* yang berhasil ditemukan berupa *SQL Injection, Cross Site Scripting* dan berbagai *web alerts* lainnya.

Kata kunci : *website*, keamanan *website, Acunetix, web alert, SQL Injection, Cross Site Scripting*.

PENDAHULUAN

Keamanan informasi dalam sebuah *website* menjadi sangat penting. Keamanan informasi sebuah *website* merupakan salah satu prioritas yang sangat utama bagi seorang *web development*. Jika seseorang mengabaikan keamanan tersebut maka seorang *hacker* dapat mengambil data penting dan bahkan mangacak-acak tampilan *web* tersebut.

Ada tiga tujuan penting tercapainya keamanan informasi (Vacca,2009):

1. *Confidentiality* (kerahasiaan) yaitu informasi hanya tersedia unutk orang atau sistem yang memang perlu akses ke sana.
2. *Integrity* (kesatuan) yaitu informasi hanya dapat ditambah atau diperbaharui oleh orang yang telah diautorisasi.
3. *Avability* (ketersediaan) yaitu informasi harus tersedia dalam waktu yang tepat ketika dibutuhkan.

Universitas Muhammadiyah Surakarta merupakan salah satu Perguruan Tinggi Swasta yang menyediakan informasi dalam sebuah tampilan *website*, baik informasi untuk pengenalan Universitas kepada masyarakat luas ataupun informasi yang berkaitan tentang perkuliahan. Selain *website* dengan alamat ums.ac.id juga terdapat profil per fakultas yang ditampilkan dalam sebuah *website* tersendiri dengna subdomain yang sama.

Penelitian ini akan membahas bagaimana menganalisis sebuah *website* menggunakan *software website vulnerability scanner*.

TELAAH PENELITIAN

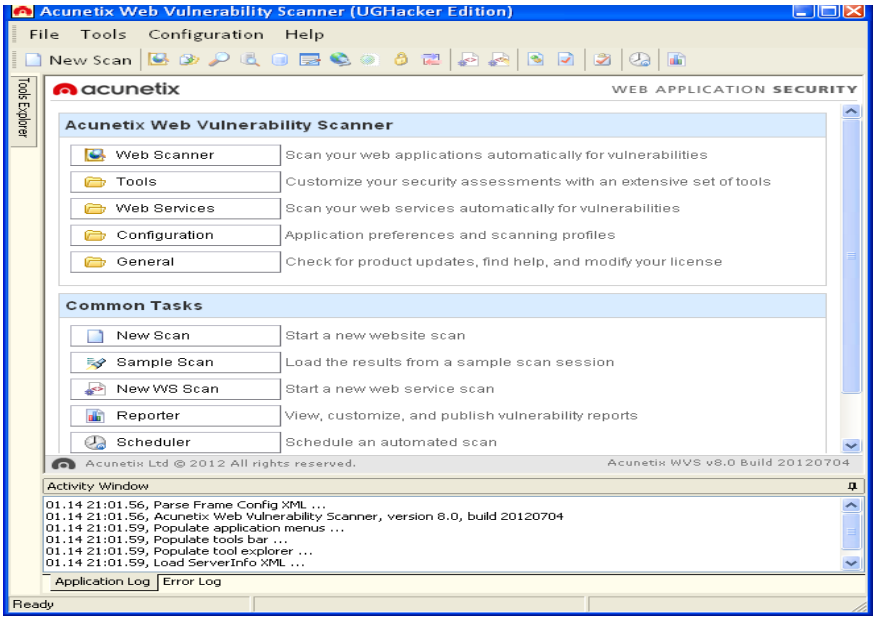
Sutanta (2008) meneliti tentang keamanan sistem aplikasi (study kasus aplikasi *e-learning* di IST AKPRIND Yogyakarta) penelitian ini melakukan analisis terhadap aspek-aspek keamanan sistem yang meliputi keamanan *web server*, program aplikasi dan *database* akademik yang digunakan di IST AKPRIND. Berdasarkan hasil penelitian ini diketahui bahwa tingkat ancaman terhadap *webserver* berada pada level 2 (*medium*). Hal tersebut menunjukkan bahwa

aplikasi *e-learning* IST AKPRIND masih terdapat celah-celah yang memungkinkan terjadinya ancaman dan akses illegal yang berpotensi merusak.

Susanty, Widya dan Ayu (2012) meneliti tentang pengujian keamanan sistem *web server* yang dikelola oleh PT. Web Architect Technology. Penelitian ini melakukan pengujian terhadap *web* dan *port* pada *website* serta *Content Management System* (CMS) Wall Street Institute Indonesia. Berdasarkan hasil penelitian diketahui bahwa *website* dan CMS Wall Street belum dapat dikatakan aman, hal ini dibuktikan dengan masih ditemukannya beberapa kerentanan *web alerts* dan *open port* terkait *website* dan CMS tersebut yang dapat menjadi celah keamanan yang dapat menimbulkan kerusakan yang fatal.

METODE PENELITIAN

Pada pengujian ini peneliti akan menggunakan *tool* berupa perangkat lunak dan cara-cara tertentu yang digunakan untuk menguji keamanan sebuah *website*. Untuk melakukan analisis keamanan *website*, *software* yang digunakan adalah *Acunetix website vulnerability scanner*. Tampilan awal Acunetix *website vulnerbilty scanner* akan ditampilkan pada gambar 1.



Gambar 1 tampilan awal *Acunetix Website Vulnerability Scanner*

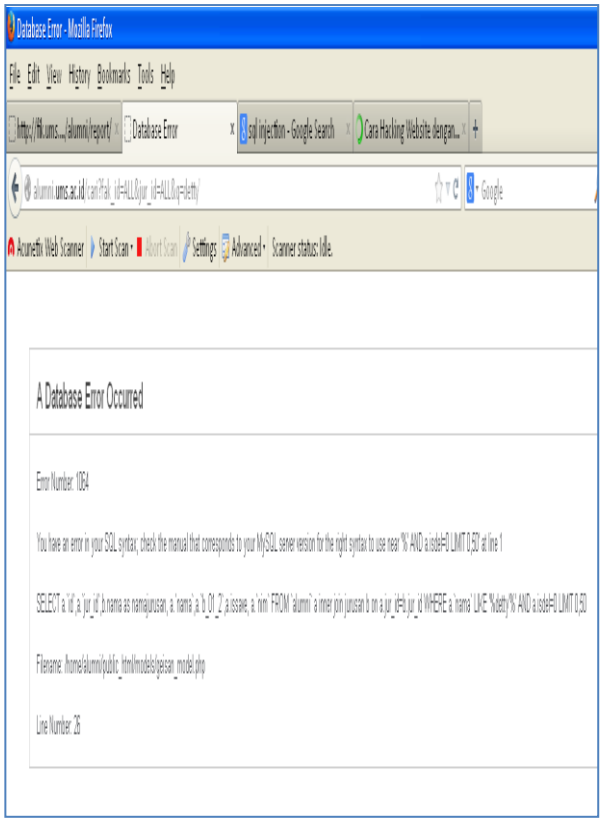
HASIL PENELITIAN

Hasil analisis terhadap *website* ums.ac.id menunjukkan bahwa *website* tersebut dalam level kerentanan *Low*. Hal ini ditunjukkan dengan hanya ditemukan *web alerts* dengan kategori *Low* dan *Informational*.

Pada *website* dengan alamat alumni.ums.ac.id berada pada level kerentanan yang tinggi ditunjukkan dengan ditemukannya *web alerts* seperti *SQL Injection* dan *Cross Site Scripting*.

Gambar 2 *SQL Injection*

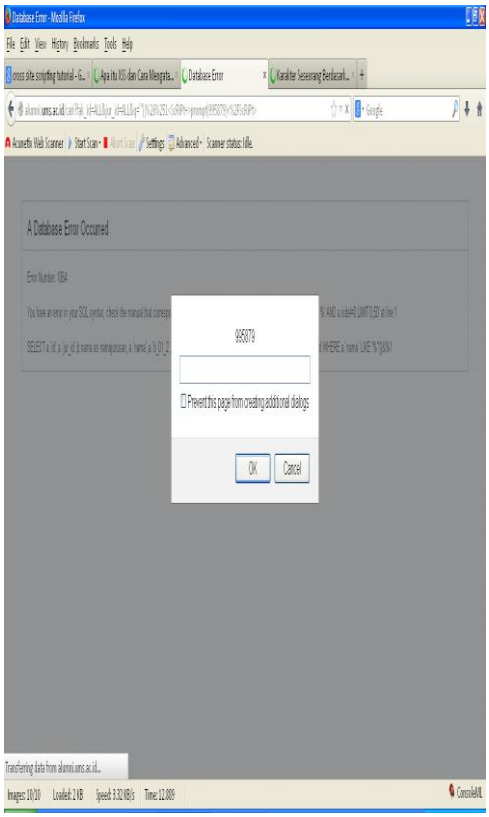
Pada gambar 2 dilakukan penyerangan menggunakan *SQL Injection* dengan cara menyertakan karakter ‘ sebagai contoh mengetikkan detty’ pada kolom masukkan nama anda. Setelah diproses akan memunculkan *database error* seperti gambar 3.



Gambar 3 *Database error* pada alumni.ums.ac.id/cari/

Pada *website* dengan alamat alumni.ums.ac.id juga ditemukan *web alerts* dengan kategori tinggi yaitu *Cross Site Scripting*. Hal ini

dapat dilakukan dengan menyertakan script'"()&%1<ScRiPt>prompt(995879)</ScRiPt> pada kolom masukkan nama anda di sini. Setelah diproses maka akan menampilkan seperti gambar 4 yang menunjukkan *website* tersebut rentan terhadap serangan *Cross Site Scripting*.

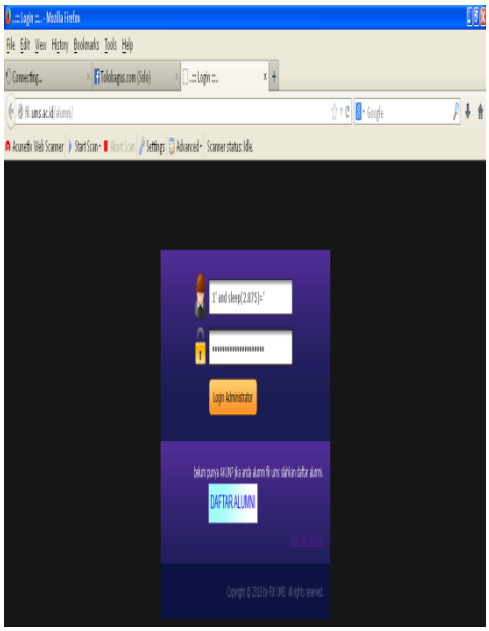


Gambar 4 *Cross Site Scripting* pada alumni.ums.ac.id

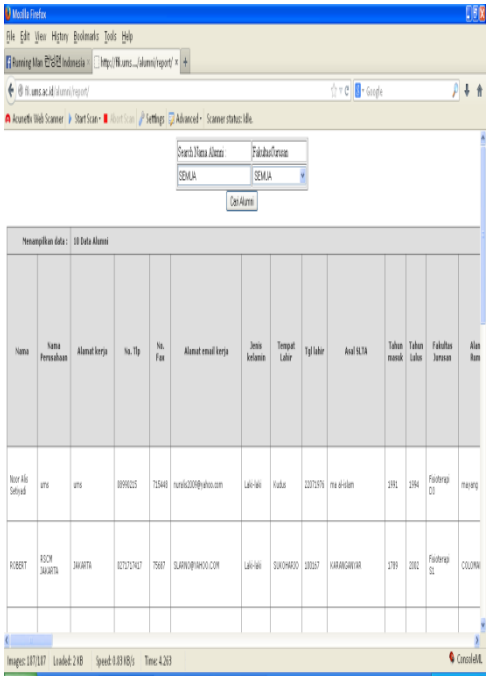
Pada *website* dengan alamat geografi.ums.ac.id yang berada pada level kerentanan tinggi juga menunjukkan bahwa *website* tersebut berpontensi terkena serangan *Cross Site Scripting* dengan ditunjukkan gambar 5.

Gambar 5 *Cross Site Scripting pada* geografi.ums.ac.id

Pada *website* dengan alamat fik.ums.ac.id/alumni/ juga berada pada level *High* ditunjukkan dengan adanya potensi berupa serangan *SQL Injection*. Serangan ini dilakukan dengan mengetikkan karakter tertentu pada username dan password hl ini menyebabkan dapat mengakses halaman/alumni/ tanpa harus mendaftar sebagai *user* terlebih dahulu. Ditampilkan pada gambar 6 dan gambar 7.

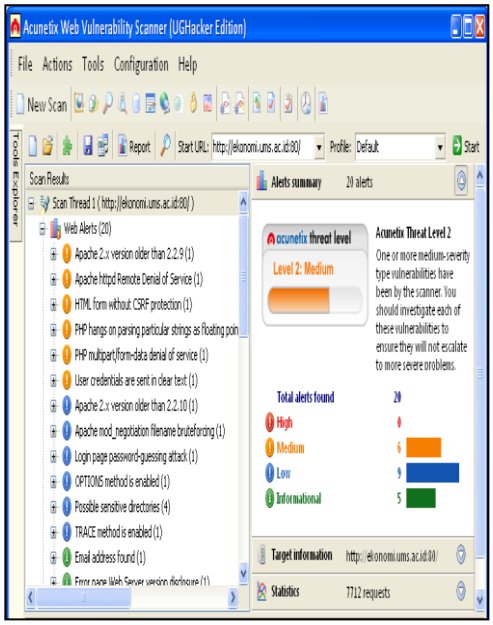


Gambar 6 halaman *login* fik.ums.ac.id/alumni/



Gambar 7 fik.ums.ac.id/alumni/

Pada gambar 8 menunjukkan hasil scanning *website* dengan alamat ekonomi.ums.ac.id berada pada level *medium* dengan jumlah *web alerts* sebanyak 20. Dengan rincian 6 *web alerts* level *medium*, 9 *web alerts* pada level *Low* dan 5 *alerts informational*.



Gambar 8 ekonomi.ums.ac.id

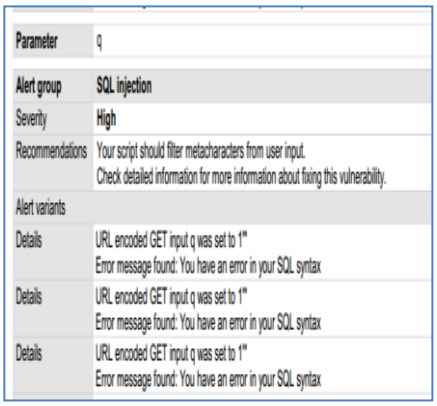
Rekomendasi berdasarkan tingkatan resiko keamanan mengacu pada hasil rekomendasi yang terdapat pada *Software Acunetix*.

1. *SQL injection*

   Tingkat resiko : *High*

   Resiko : dapat menggangu integritas *database* atau keterbukaan informasi.

   Rekomendasi : menfilter karakter yang digunakan pengakses.



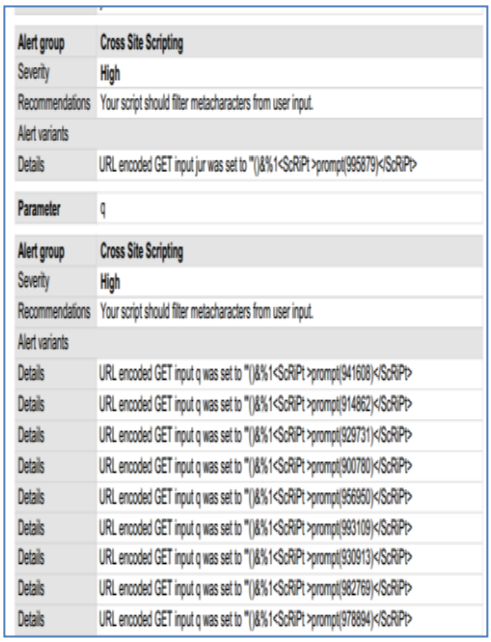
Parameter	q
Alert group	SQL injection
Severity	High
Recommendations	Your script should filter metacharacters from user input. Check detailed information for more information about fixing this vulnerability.
Alert variants	
Details	URL encoded GET input q was set to 1" Error message found: You have an error in your SQL syntax
Details	URL encoded GET input q was set to 1" Error message found: You have an error in your SQL syntax
Details	URL encoded GET input q was set to 1" Error message found: You have an error in your SQL syntax

2. *Cross Site Scripting*

   Tingkat resiko : *High*

   Resiko : penyerang dapat mencuri *cookie session* dan mengambil alih akun, meniru penguna sehingga memungkinkan untuk menmodifikasi halaman *website*.

   Rekomendasi : menfilter karakter yang digunakan mengakses.



Alert group	Cross Site Scripting
Severity	High
Recommendations	Your script should filter metacharacters from user input.
Alert variants	
Details	URL encoded GET input jur was set to "()&%1<ScRiPt >prompt(995879)</ScRiPt>
Parameter	q
Alert group	Cross Site Scripting
Severity	High
Recommendations	Your script should filter metacharacters from user input.
Alert variants	
Details	URL encoded GET input q was set to "()&%1<ScRiPt >prompt(941608)</ScRiPt>
Details	URL encoded GET input q was set to "()&%1<ScRiPt >prompt(914862)</ScRiPt>
Details	URL encoded GET input q was set to "()&%1<ScRiPt >prompt(929731)</ScRiPt>
Details	URL encoded GET input q was set to "()&%1<ScRiPt >prompt(900780)</ScRiPt>
Details	URL encoded GET input q was set to "()&%1<ScRiPt >prompt(956850)</ScRiPt>
Details	URL encoded GET input q was set to "()&%1<ScRiPt >prompt(993109)</ScRiPt>
Details	URL encoded GET input q was set to "()&%1<ScRiPt >prompt(930913)</ScRiPt>
Details	URL encoded GET input q was set to "()&%1<ScRiPt >prompt(982769)</ScRiPt>
Details	URL encoded GET input q was set to "()&%1<ScRiPt >prompt(978884)</ScRiPt>

KESIMPULAN

Berdasarkan hasil analisis yang telah dilakukan diketahui bahwa keamanan *website* di Universitas Muhammadiyah Surakarta belum dapat dikatakan aman, hal ini di tunjukkan dengan masih adanya sub domain fakultas yang berada pada level *High* dengan ditemukannya *web alerts* berbahaya pada beberapa website fakultas dan level *Medium* yang mengandung informasi sensitif. Hanya *website* dengan alamat ums.ac.id saja yang berada pada level Low.

DAFTAR PUSTAKA

Susanty, Yiyin, Widya & Ayu. 2012, *Pengujian Keamanan Sistem Web Server yang dikelola oleh PT. Web Architect Tecnology*, skripsi internship, Universitas Bina Nusantara, Jakarta.

Sutanta, Edhy 2008, *Analisis Keamanan Sistem Aplikasi (Study Kasus Aplikasi E-Learning di IST AKPRIND Yogyakarta)*, skripsi, Institut Sains & Teknologi AKPRIND, Yogyakarta.

Vacca, JR 2009. *Computer and Information Securty Handbook*, Elsevier, Inc, Wachington D.C.