LAPORAN PRAKTEK KERJA LAPANGAN

ANALISIS KEAMANAN *WEBSITE* KEMENTERIAN SEKRETARIAT NEGARA DENGAN *ACUNETIX WEB VULNERABILITY SCANNER*

KEMENTERIAN SEKRETARIAT NEGARA

Periode 2 Januari – 2 Februari 2018

Oleh :

AKBAR KOTO

1511512006

Dosen Pembimbing :

RAHMI EKA PUTRI, M.T.

NIP. 198407232008012001

JURUSAN SISTEM KOMPUTER

FAKULTAS TEKNOLOGI INFORMASI

UNIVERSITAS ANDALAS

2018

LAPORAN PRAKTEK KERJA LAPANGAN

ANALISIS KEAMANAN *WEBSITE* KEMENTERIAN SEKRETARIAT NEGARA DENGAN *ACUNETIX WEB VULNERABILITY SCANNER*

KEMENTERIAN SEKRETARIAT NEGARA

Periode 2 Januari – 2 Februari 2018

Disusun untuk memenuhi persyaratan kelulusan
Matakuliah Praktek Kerja Lapangan

Oleh :

AKBAR KOTO

1511512006

JURUSAN SISTEM KOMPUTER

FAKULTAS TEKNOLOGI INFORMASI

UNIVERSITAS ANDALAS

2018

SURAT PERNYATAAN
LAPORAN PRAKTEK KERJA LAPANGAN (PKL)

Yang bertandatangan di bawah ini :

Nama : Akbar Koto

NIM : 1511512006

Menyatakan dengan sesungguhnya bahwa :

1. Laporan PKL ini saya buat dengan sebenarnya dan berdasarkan sumber yang benar.
2. Objek tempat saya melaksanakan PKL berbentuk CV/PT/Pemerintahan dan dinyatakan masih aktif beroperasional hingga saat ini.
3. Data perusahaan dalam laporan PKL ini benar adanya dan bersifat valid.
4. Laporan ini bukan merupakan hasil plagiat/menjiplak karya ilmiah orang lain.
5. Laporan ini merupakan hasil kerja saya sendiri (bukan buatan/ dibuatkan orang lain)
6. Buku referensi yang saya gunakan untuk Lap.PKL ini merupakan buku yang terbit dalam 5 (lima) tahun terakhir ini.

Demikian pernyataan ini saya buat dalam keadaan sadar dan tanpa paksaan dari pihak manapun dan apabila dikemudian hari ternyata saya kedapatan telah melanggar salah satu dari pernyataan saya ini, saya bersedia untuk menerima sanksi skorsing, DO (Drop Out), hingga Penghapusan gelar akademik yang saya peroleh dari Perguruan Tinggi ini.

Jakarta , April 2018

Yang menyatakan,

Akbar Koto

1511512006

LEMBAR PENGSEHAN

LAPORAN PRAKTEK KERJA LAPANGAN

ANALISIS KEAMANAN *WEBSITE* KEMENTERIAN SEKRETARIAT NEGARA DENGAN *ACUNETIX WEB VULNERABILITY SCANNER*

Periode 2 Januari – 2 Februari 2018

Oleh :

AKBAR KOTO

1511512006

Mengetahui,

Dosen Pembimbing	Ketua Program Studi
RAHMI EKA PUTRI, M.T,	**DODY ICHWANA PUTRA, S.T, M.T**
NIP. 198407232008012001	**NIP. 198611072015041001**

Ketua Jurusan

Sistem Komputer

RATNA AISUWARYA, M.Eng

NIP. 198410302008122002

HALAMAN PENGESAHAN

LAPORAN PRAKTEK KERJA LAPANGAN

ANALISIS KEAMANAN *WEBSITE* KEMENTERIAN SEKRETARIAT NEGARA DENGAN *ACUNETIX WEB VULNERABILITY SCANNER*

Periode 2 Januari – 2 Februari 2018

Oleh :

AKBAR KOTO

1511512006

Laporan Praktek Kerja Lapangan ini telah diseminarkan dan disetujui oleh Dosen Penguji serta disahkan oleh Ketua Jurusan Sistem Komputer, Fakultas Teknologi Informasi Universitas Andalas.

Demikianlah lembaran pengesahan ini dibuat untuk diketahui bersama.

Padang, April 2018

Pembimbing,

Rahmi Eka Putri, M.T.

NIP. 198407232008012001

LEMBAR PENGESAHAN

LAPORAN PRAKTEK KERJA LAPANGAN

ANALISIS KEAMANAN *WEBSITE* KEMENTERIAN SEKRETARIAT NEGARA DENGAN *ACUNETIX WEB VULNERABILITY SCANNER*

Periode 2 Januari – 2 Februari 2018

Oleh :

AKBAR KOTO

1511512006

Menyetujui,

PEMBIMBING PKL

IRMA DWI SANTI, S.Kom., M.ICTM

NIP 180004560

ABSTRAK

Keamanan merupakan salah satu facktor peting yang harus diperhatikan dalam membangun sebuah *website*. Hal tersebut menjadi sebuah tantangan tersendiri bagi para pengembang *website*, karena tidak ada jaminan yang pasti akan definisi 'aman' itu sendiri. "Tidak ada sistem yang benar-benar aman", bukanlah sebuah pernyataan semata, namun telah dirasakan dalam realitas. *Website* Kemensetneg merupakan *website* yang digunakan sebagai media dan sarana informasi Negara. Mengingat *website* ini dapat diakses secara luas, maka dinilai perlu memperhatikan keamanan *website*. Terdapat beberapa cara yang dapat digunakan untuk melakukan pengujian terhadap 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*. Dengan dilakukannya analisis ini, diharapkan dapat diperoleh kelemahan dari *website* Kemensetneg. Kelemahan tersebut akan di analisis sehingga diperoleh solusi kedepan guna pengembangan *website* yang lebih aman.

Kata kunci : analisis, keamanan, website, SQL injection

KATA PENGANTAR

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

Puji syukur penulis ucapkan ke hadirat Allah SWT Yang Maha Pengasih lagi Maha Penyayang, yang telah melimpahkan rahmat dan karuniaNya, sehingga penulis dapat menyelesaikan laporan praktek kerja lapangan yang berjudul "Analisis Keamanan *Website* Kementerian Sekretariat Negara dengan *Acunetix Web Vulnerability Scanner*". Shalawat dan salam kepada Nabi Muhammad SAW yang telah memberi tuntunan dan pencerahan kepada umat manusia.

Penulis menyadari bahwa tanpa bantuan dan bimbingan dari berbagai pihak, sulit bagi penulis untuk dapat menyelesaikan laporan PKL ini. Oleh karena itu, penulis mengucapkan terima kasih kepada:

1. ALLAH S.W.T yang telah memberikan rahmat dan karunia bagi kita bersama.
2. Orang Tua dan saudara atas dukungannya untuk pelaksanaan kerja praktek ini.
3. Ibu Rahmi Eka Putri, M.T selaku dosen pembimbing kerja praktek ini.
4. Bapak Nur Hadianto, Bapak Suhariono dan Ibu Irma Dwi Santi., S.Kom., M.ICTM selaku pembimbing PKL di Kemensetneg.
5. Para staf dan karyawan Kemensterian Sekretariat Negara di Biro Dukungan Informasi.
6. Farlie Angriawan, Ridho Maulana dan Bima Agastya Fiandra yang telah menjadi rekan satu tim pada praktek kerja lapangan ini.
7. Inge Frastika Fitri selaku saudari BP dan sebagai teman sharing.
8. Teman-teman sesama Angkatan 2015 Jurusan Sistem Komputer Fakultas Teknologi Informasi Universitas Andalas.
9. Senior dan junior Jurusan Sistem Komputer Fakultas Teknologi Informasi Universitas Andalas

Penulis menyadari bahwa dalam penulisan laporan PKL ini masih jauh dari sempurna. Oleh karena itu penulis memohon maaf apabila ada kekurangan maupun kesalahan dalam penyajiannya, serta mengharapkan kritik dan saran yang bermanfaat untuk menyempurnakan laporan PKL ini.

Semoga laporan PKL ini dapat bermanfaat bagi kita semua dan bagi penulis sendiri tentunya.

Padang, April 2018

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I
PENDAHULUAN

1.1 Latar Belakang

Website adalah salah cara untuk menampilkan suatu informasi dari suatu perusahaan atau instansi di *internet*. Diibaratkan *website* adalah sebuah tempat di *internet* dimana siapa saja di dunia ini dapat mengunjunginya. Keamanan merupakan salah satu indikator penting dalam membangun sebuah *website*, mengingat akses ke *internet* yang terbuka bebas bagi masyarakat umum. Selain itu, saat ini *website* tidak hanya dijadikan layanan untuk memberikan informasi statis, tetapi telah berkembang dengan ditambahkannya fitur-fitur untuk melakukan transaksi secara *on-line*. Sampai saait ini tidak ada *website* yang dapat dikatakan benar-benar aman.

Website Kementerian Sekretariat Negara (Kemensetneg) dengan domain setneg.go.id merupakan *website* yang digunakan sebagai media dan sarana publikasi informasi Negara. Mengingat *website* ini dapat diakses secara luas, maka dinilai perlu memperhatikan keamanan *website*-nya. Terdapat beberapa cara yang dapat digunakan untuk melakukan pengujian terhadap keamanan *website*. Salah satunya adalah dengan menggunakan *software* yang bernama *Acunetix Web Vulnerability Scanner*.

Keamanan data dan informasi sangat penting dalam menjaga ketahanan sebuah *website*. Oleh karena itu, maka dinilai perlu untuk menguji keamanan *website* Kemensetneg, serta melakukan analisa terhadap kelemahan sistem yang ada, sehingga dapat diperoleh tindakan selanjutnya untuk perbaikan sistem.

1.2 Ruang Lingkup

Ruang lingkup laporan ini adalah penggunaan *software Acunetix Web Vulnerability Scanner* pada *website* Kementerian Sekretariat Negara.

1.3 Tujuan

Adapun tujuan pembuatan Laporan dan kegiatan Praktek Kerja Lapangan (PKL) ini adalah sebagai berikut :

1. Menerapkan dan mengimplementasikan bidang ilmu sistem komputer.
2. Memahami penggunaan *software Acunetix Web Vulnerability Scanner* dan melakukan pengujian terhadap keamanan *website* Kemensetneg.
3. Menganalisa hasil dari pengujian keamanan *website* Kemensetneg.
4. Menambah pengetahuan dalam mengenal lingkungan kerja dan cara kerja dalam suatu tempat kerja atau instansi.

BAB II

PROFIL KEMENTERIAN SEKRETARIAT NEGARA (KEMENSETNEG)

2.1 Sejarah

Kementerian Sekretariat Negara adalah kementerian yang dipimpin oleh Menteri Sekretaris Negara, dan berkedudukan di bawah serta bertanggung jawab kepada Presiden. Sejak awal dibentuknya hingga sekarang, tugas Kementerian Sekretariat Negara pada umumnya adalah memberikan dukungan teknis, administrasi, dan analisis kepada Presiden dan Wakil Presiden dalam menyelenggarakan kekuasaan Negara.

Kementerian Sekretariat Negara dibentuk sejak awal Negara Republik Indonesia berdiri dengan nama Sekretariat Negara. Proklamasi Kemerdekaan bangsa Indonesia pada tanggal 17 Agustus 1945 merupakan tonggak awal berdirinya negara Republik Indonesia yang merdeka dan berdaulat. Sehari setelah Proklamasi Kemerdekaan, pada tanggal 18 Agustus 1945, Ir. Soekarno diangkat sebagai Presiden dan Drs. Mohammad Hatta diangkat sebagai Wakil Presiden. Pada tanggal 2 September 1945, Presiden Soekarno membentuk Kabinet Pemerintah Republik Indonesia yang pertama. Dalam pembentukan Kabinet pertama ini, diangkat seorang Sekretaris Negara dan Juru Bicara Presiden.

Dalam perjalanan sejarahnya, Kementerian Sekretariat Negara mengalami beberapa kali perubahan, baik tugas pokok, fungsi, kedudukan, maupun struktur kelembagaan. Perubahan itu sangat dipengaruhi oleh situasi politik yang terjadi di tanah air. Awalnya, Sekretariat Negara hanya berfungsi untuk membantu tugas-tugas administrasi kepresidenan. Pada akhirnya, menjadi sebuah kementerian yang memberikan dukungan teknis, administrasi, dan analisis kepada Presiden dan Wakil Presiden.

2.2 Struktur Organisasi

Gambar 2.1 Struktur Organisasi

Pada kerja praktek lapangan ini, kami ditempatkan pada Biro Dukungan Informasi (DI) yang berada pada Kemensterian Sekretariat Negara.

2.3 Visi, Misi dan Logo Perusahaan

1. Visi

   Kementerian Sekretariat Negara yang andal dalam memberikan pelayanan kepada Presiden dan Wakil Presiden dalam mewujudkan Indonesia yang Berdaulat, Mandiri dan Berkepribadian berlandaskan Gotong Royong.

2. Misi

   a. Memberikan dukungan teknis dan administrasi serta analisis yang cepat, akurat dan responsif, kepada Presiden dan Wakil Presiden dalam pengambilan kebijakan penyelenggaraan pemerintahan negara.

   b. Memberikan pelayanan kerumahtanggaan dan keprotokolan yang optimal kepada Presiden dan Wakil Presiden.

c. Memberikan dukungan teknis dan administrasi kepada Presiden dalam menyelenggarakan kekuasaan tertinggi atas Angkatan Darat, Angkatan Laut, dan Angkatan Udara.
d. Menyelenggarakan pelayanan yang efektif dan efisien di bidang pengawasan, administrasi umum, informasi, dan hubungan kelembagaan.
e. Meningkatkan kualitas sumber daya manusia dan prasarana Kementerian Sekretariat Negara.

3. Logo Kemensetneg RI

KEMENTERIAN
SEKRETARIAT NEGARA RI

Gambar 2.2 Logo Kemensetneg RI

2.4 Tugas dan Fungsi Kemensetneg RI

1. Tugas

Kementerian Sekretariat Negara mempunyai tugas menyelenggarakan dukungan teknis dan administrasi serta analisis urusan pemerintahan di bidang kesekretariatan negara untuk membantu Presiden dan Wakil Presiden dalam menyelenggarakan pemerintahan negara.

2. Fungsi

Dalam melaksanakan tugas tersebut, Kementerian Sekretariat Negara menyelenggarakan fungsi :

a. Dukungan teknis dan administrasi kerumahtanggaan, keprotokolan, pers, dan media kepada Presiden.
b. Dukungan teknis dan administrasi kerumahtanggaan dan keprotokolan, serta analisis kebijakan kepada Wakil Presiden dalam membantu Presiden menyelenggarakan pemerintahan negara.
c. Dukungan teknis dan administrasi kepada Presiden dalam menyelenggarakan kekuasaan tertinggi atas Angkatan Darat, Angkatan Laut, dan Angkatan Udara, dalam hal pengangkatan dan pemberhentian perwira Tentara Nasional Indonesia dan Kepolisian Republik Indonesia, penganugerahan gelar, tanda jasa dan tanda kehormatan, yang wewenang penetapannya berada pada Presiden, serta koordinasi pengamanan Presiden dan Wakil Presiden beserta keluarga termasuk Tamu Negara setingkat Kepala Negara/Kepala Pemerintahan negara asing.
d. Dukungan teknis, administrasi, dan analisis dalam penyiapan izin prakarsa dan penyelesaian Rancangan Peraturan Perundang-Undangan, penyiapan pendapat hukum, penyelesaian Rancangan Keputusan Presiden mengenai grasi, amnesti, abolisi, rehabilitasi, ekstradisi, remisi perubahan dari pidana penjara seumur hidup menjadi pidana sementara, dan naturalisasi, serta permintaan persetujuan kepada Sekretaris Kabinet atas permohonan izin prakarsa penyusunan Rancangan Peraturan Perundang-undangan dan atas substansi rancangan peraturan perundang-undangan.
e. Dukungan teknis, administrasi, dan analisis dalam penyelenggaraan hubungan dengan lembaga negara, lembaga non struktural, lembaga daerah, organisasi kemasyarakatan, organisasi politik, dan penyelenggaraan hubungan masyarakat, serta penanganan pengaduan masyarakat kepada Presiden, Wakil Presiden dan/atau Menteri.
f. Dukungan teknis dan administrasi serta analisis dalam pengangkatan, pemberhentian, dan pensiun pejabat negara, pejabat pemerintahan, pejabat lainnya, dan Aparatur Sipil Negara yang wewenang penetapannya berada pada Presiden.

g. Pembinaan, penataan dan pengembangan Aparatur Sipil Negara, organisasi, tata laksana, dan akuntabilitas kinerja di lingkungan Kementerian Sekretariat Negara.
h. Pembinaan dan pemberian dukungan teknis dan administrasi di bidang perencanaan, keuangan, ketatausahaan, kerumahtanggaan, penyediaan prasarana dan sarana, serta pengembangan pemerintahan berbasis elektronik di lingkungan Kementerian Sekretariat Negara, serta pemberian dukungan prasarana dan sarana untuk pejabat negara tertentu, dan dukungan administrasi kepada Dokter Kepresidenan.
i. Pengelolaan barang milik/kekayaan negara yang menjadi tanggung jawab Kementerian Sekretariat Negara.
j. Penyelenggaraan koordinasi kerja sama teknik antara Pemerintah Indonesia dengan Mitra Pembangunan, dan penanganan administrasi perjalanan dinas luar negeri.
k. Pengawasan atas pelaksanaan tugas di lingkungan Kementerian Sekretariat Negara.
l. Pelaksanaan fungsi lain yang diberikan oleh Presiden dan Wakil Presiden serta oleh peraturan perundang-undangan.

2.5 Lokasi Perusahaan

Kementrian Sekretariat Negara Republik Indonesia beralamat di Jl. Veteran No. 17 - 18 Jakarta Pusat

2.6 Deskripsi Pekerjaan

Selama melakukan Praktek Kerja Lapangan (PKL) di Kementrian Sekretariat Negara RI, penulis ditempatkan pada bagian Biro Dukungan Informasi Sekretariat Negara Republik Indonesia, bagian ini bertugas sebagai pusat penyediaan informasi dan menjalankan operasi terkait jaringan. Dalam Pelaksanaan PKL penulis merancang bagaimana pembuatan aplikasi dan merancangnya menggunakan aplikasi Android Studio.

Kegiatan yang dilakukan selama PKL adalah sebagai berikut :

1. Mempelajari dasar-dasar dalam penggunaan apliksai Android Studio.
2. Memahami bagian-bagian tools pada Android Studio beserta fungsinya.
3. Merancang dan membuat aplikasi dasar dalam pembuatan aplikasi GPS *tracking*.
4. Melakukan pengujian aplikasi pada perangkat Android.
5. Mempresentasikan hasil dan demo dari rancangan aplikasi yang telah dirancang.

2.7 Jadwal Kerja

Rincian kegiatan selama melakukaan Praktek Kerja Lapangan (PKL), Kementrian Sekretariat Negara Republik Indonesia (KEMENSETNEG RI) :

Tabel 1. Kegiatan PKL

No.	Minggu	Kegiatan yang dilakukan
1	Pertama	a. Pengenalan Biro Dukungan Informasi Kementerian Sekretariat Negara Republik Indonesia
2	Kedua	a. Pengenalan mengenai *website* dan jaringan Kementerian Sekretariat Negara Republik Indonesia b. Pemberian tugas selama kerja praktek lapangan
3	Ketiiga	a. Pengerjaan tugas yang diberikan (tahap awal) b. Survei jaringan dengan teknisi Biro Dkungan Informasi Kementerian Sekretariat Negara Republik Indonesia
4	Keempat	a. Melanjutkan pembuatan tugas yang diberikan b. Presentasi tahap awal tugas yang diberikan
5	Kelima	a. Menyelesaikan pembuatan tugas (tahap akhir) yang diberikan b. Presentasi tahap akhir dari tugas yang diberikan

BAB III
PELAKSANAAN PRAKTEK KERJA LAPANGAN

3.1 Pengertian *Website*

Website adalah kumpulan informasi yang berbentuk halaman-halaman elektronik atau *web page*. Sebuah *website* umumnya terhubung pada sebuah alamat penunjuk yang spesifik. Alamat penunjuk tersebut dinamakan *domain*. *Website* pada umumnya terdiri dari format teks, gambar, tabel, grafik, kutipan, video, musik dan format visual lainnya yang menarik bagi pengunjung *website* tersebut.

Sebuah *website* biasanya bisa diakses secara umum, kebanyakan *website* dapat diakses melalui *public internet protocol (IP)* dalam sebuah jaringan internet. Namun tidak menutup kemungkinan bahwa *website* tersebut diakses secara *offline* melalui jaringan LAN. *Website* bisa berupa *website* pribadi, komersial, pemerintahan dan *website* lainnya yang dibuat untuk kepentingan *profit* maupun *non-profit* yang dipublikasikan secara umum. Selain itu, *website* juga dapat dibuat untuk tujuan khusus seperti misalnya untuk hiburan, pendidikan dan juga kepentingan sosial.

3.2 Jenis-jenis *Website*

Berdasarkan penampilan dan respon ketika diakses, *website* bisa dikategorikan ke dalam dua jenis utama yaitu *static website* dan *dynamic website*.

1. *Static Website*

   Static Website pada umumnya merupakan informasi yang disimpan di dalam *server* dengan format tertentu yang nantinya akan tampil secara identik untuk semua pengguna atau *users*. *Website* jenis ini umumnya dikembangkan dengan menggunakan Bahasa pemrograman *Hypertext Markup Language (HTML)* atau pun *Cascanding Style Sheets (CSS)*.

   Pada umumnya *static website* ini akan menampilkan bentuk yang sama ketika kita mengunjunginya. Meskipun pengelola *website* melakukan

pembaharuan informasi, biasanya penampilan yang muncul pada saat kita mengakses *website* tipe ini tetap sama. Jika pengelola ingin mengubah penampilan dari *website* ini, maka pengelola harus mengubahnya melalui kode-kode program yang tentunya menuntut pengelola untuk memahami prinsip-prinsip pemrograman sebuah *website*.

Website jenis ini mempunyai prototipe yang hampir mirip, yaitu memiliki sekitar setidaknya lima halaman utama. Halaman-halaman tersebut biasanya digunakan untuk menuliskan informasi mengenai produk, kontak, sejarah dan informasi-informasi umum mengenai *website* tersebut. Di dalam *website* tersebut juga bisa dimuat informasi multimedia seperti musik dan video. Namun pada *website* jenis ini umumnya video dan musik langsung dimainkan secara otomatis. Dan pada umumnya tidak memungkinkan interaksi secara lebih fleksibel antara pengunjung dan *website* itu sendiri.

2. *Dynamic website*

Berbeda dengan *static website, dynamic website* mempunyai kemampuan untuk menyesuaikan dirinya sesuai dengan keadaan *users* mengakses *website* tersebut dengan memanfaatkan *database*. Jika pada *static website*, kebanyakan diatur menggunakan *HTML* dan *CSS*, maka pada *dynamic website* ini penampilannya juga diatur menggunakan Bahasa pemrograman seperti *Perl, PHP, Javascript, Phyton* dan lain sebagainya. Dengan begitu, pengembang *website* bisa membuat halaman dengan konsep visual dan kemampuan interaksi tinggi dengan penggunanya. Beberapa fitur yang biasanya terdapat pada *dynamic website* adalah *cookies,* fasilitas *live chatting,* kolom komentar, form registrasi dan lain sebagainya.

Pada *dynamic website* ini, pengembang bisa membuat agar beberapa halaman tampil selayaknya halaman statis seperti pada *static website,* tetapi kemudian digabungkan dengan *engine* untuk menampilkan sekumpulan artikel terakhir yang diterbitkan, atau yang lebih dikenal dengan istilah *blog engine*. Dengan menggunakan tipe *website* seperti ini, maka akan berpotensi membuat pengunjung betah membaca konten di dalam

website. Selain itu pada *dynamic website* ini juga bisa menambahkan perbaruan aktivitas yang tercatat pada *website.*

3.3 Manfaat *Website*

Manfaat *website* yang paling utama adalah untuk menyebarkan informasi melalui dunia digital. Dengan adanya dunia digital yang bisa diakses melalui jaringan internet ini, maka arus pertukaran informasi dapat dilakukan secara internasional dan tidak terbatas oleh batasan tempat.

Melalui *website,* orang di seluruh dunia bisa saling bertukar informasi terkini sehingga tidak ketinggalan perkembangan teknologi, budaya dan ilmu pengetahuan yang sedang meroket di segala belahan dunia. Kini selain sebagai media untuk bertukar informasi, *website* juga bisa menjadi media untuk promosi dan mengembangkan bisnis. Di samping itu, *website* juga ramai digunakan sebagai ruang untuk mengekspresikan diri atau yang kini popular dengan sebutan media sosial.

Namun yang tidak kalah penting adalah *website* juga bisa digunakan sebagai tempat untuk mendapatkan komunitas yang sesua dengan minat yang dimiliki. Yang jelas *website* memberikan banyak manfaat positif jika kita mampu menggunakannya secara bijak dan atau tujuan yang positif.

3.4 Macam-macam domain *website*

Berikut adalah contoh macam-macam domain *website* yang ada pada saat sekarang ini :

1. .co.id : Biasanya digunakan untuk badan usaha yang memiliki badan hokum sah.
2. .go.id : Khusus digunakan untuk Lembaga Pemerintahan RI.
3. .ac.id : Dipakai untuk Lembaga Pendidikan.
4. .or.id : Dipakai untuk segala macam organisasi yang tidak termasuk kategori ".co.id",".go.id",".mil.id",".ac.id" dan sebagainya.

5. .war.net.id : Dipakai untuk industry warung internet (warnet) yang ada di Indonesia.
6. .sch.id : Dipakai khusus untuk Lembaga Pendidikan SD, SMP dan SMA atau SMK.
7. .web.id: Biasanya digunakan untuk organisasi, badan usaha, ataupun perseorangan yang melakukan kegiatan di WWW.

3.5 Web Server

Web server merupkan salah satu kebutuhan yang digunakan oleh user untuk *website* yang mempunyai kapasitas penyimpanan yang besar dan juga akses yang cepat untuk trafik yang besar dalam mencegah terjadinya *down* pada suatu *website* atau aplikasi.

1. Pengertian Server dan Web Server

   Web server atau server web merupakan perangkat lunak (*software*) dalam server yang berfungsi untuk menerima permintaan (*request*) berupa halaman web melalui protokol HTTP atau HTTPS dari client yang lebih dikenal dengan nama browser, kemudian mengirimkan kembali atau merespon hasil permintaan tersebut ke dalam bentuk halaman-halaman web yang pada umumnya berupa dokumen HTML atau PHP.

2. Fungsi Web Server

   Fungsi utama dari *web server* adalah untuk memindahkan atau mentransfer berkas yang diminta oleh pengguna melalui protokol komunikasi tertentu. Oleh karena itu, dalam satu halaman web biasanya terdiri dari berbagai macam jenis berkas seperti teks, gambar, video, audio, file dan lain-lain, maka pemanfaatan *web server* berfungsi juga untuk mentransfer keseluruhan aspek pemberkasan dalam halaman tersebut, termasuk gambar, teks, video, audio, file dan lain sebagainya. Beberapa contoh *web server* yang paling banyak digunakan diantaranya adalah :

   - Apache
   - Apache Tomcat

- Nginx
- Lighttpd
- Litespeed
- Microsoft Internet Information Services (IIS)

3.6 Web Security

Web Security adalah cabang Keamanan Informasi yang secara khusus menangani keamanan *website* , aplikasi web dan layanan web . Pada tingkat tinggi, keamanan aplikasi Web mengacu pada prinsip-prinsip keamanan aplikasi tetapi berlaku mereka secara khusus untuk Internet dan web sistem.

3.7 Web Vulnerability

Web Vulnerabilitya dalah suatu kelemahan program atau infrastruktur yang memungkinkan terjadinya exploitasi sistem. kerentanan (*vulnerability*) ini terjadi akibat kesalahan dalam merancang, membuat atau mengimplementasikan sebuah sistem. *Vulnerability* atau 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 tersebut. *Open Web Application Security Project* (OWASP) adalah project open source yang dibangun untuk menemukan penyebab dari tidak amannya sebuah software dan menemukan cara menanganinya.Berikut ini adalah 9 celah dan cara agar kita dapat mengatasi masalah tersebut.

1. Unvalidated Input

   Semua aplikasi web menampilkan data dari HTTP request yang dibuat oleh user dan menggunakan data tersebut untuk melakukan operasinya. Hacker dapat memanipulasi bagian-bagian pada request (*query string, cookie information, header*) untuk membypass mekanisme keamanan.

   Berikut ini tiga jenis penyerangan yang berhubungan dengan masalah ini:

   - Cross site scripting

- Buffer overflows
- Injection flaws

2. Broken Access Control

Banyak aplikasi yang mengkategorikan user-usernya ke dalam role yang berbeda dan level yang berbeda untuk berinteraksi dengan content yang dibedakan dari kategori-kategori tersebut. Salah satu contohnya, banyak aplikasi yang terdapat user role dan admin role : hanya admin role yang diijinkan untuk mengakses halaman khusus atau melakukan action administration.

Masalahnya adalah beberapa aplikasi tidak efektif untuk memaksa agar otorisasi ini bekerja. Contohnya, beberapa program hanya menggunakan sebuah *checkpoint* dimana hanya user yang terpilih yang dapat mengakses : untuk proses lebih lanjut, user harus membuktikan dirinya terotorisasi dengan menggunakan user name dan password. Akan tetapi, Mereka tidak menjalankan pengecekan dari *checkpoint* sebelumnya : dimana apabila user berhasil melewati halaman login, mereka dapat bebas menjalankan operasi.

Masalah lain yang berhubungan dengan *access control* adalah :

- Insecure Ids – Beberapa site menggunakan id atau kunci yang menunjuk kepada user atau fungsi. ID dapat juga ditebak, dan jika hacker dapat mudah menebak ID dari user yang terautorisasi, maka site akan mudah diserang.
- File permissions – Kebanyakan web dan aplikasi server percaya kepada external file yang menyimpan daftar dari user yang terotorisasi dan resources mana saja yang dapat dan/atau tidak dapat diakses. Apabila file ini dapat dibaca dari luar, maka hacker dapat memodifikasi dengan mudah untuk menambahkan dirinya pada daftar user yang diijinkan. Langkah-langkah apa saja yang dapat dilakukan untuk mengatasinya? Pada contoh-contoh tadi, kita dapat mengembangkan filter atau komponen yang dapat dijalankan pada sensitive resources. Filter atau komponen tadi dapat menjamin hanya user yang terotorisasi dapat

mengakases. Untuk melindungi dari insecure Ids, kita harus mengembangkan aplikasi kita agar tidak percaya pada kerahasiaan dari Ids yang dapat memberi access control. Pada masalah file permission, file-file tersebut harus berada pada lokasi yang tidak dapat diakses oleh web browser dan hanya role tertentu saja yang dapat mengaksesnya.

3. Broken Aunthentication dan Session Management

Authentication dan *session management* menunjuk kepada semua aspek dari pengaturan *user authentikasi dan management of active session*. Berikut ini beberapa hal yang perlu diperhatikan :

- Password strength – Aplikasi kita harus memberikan level minimal dari keamanan sebuah password, dimana dapat dilihat dengan cara melihat panjang dari password dan kompleksitasnya. Contohnya sebuah aplikasi dimana terdapat user baru yang akan mendaftar : aplikasi tidak mengijinkan password dengan panjang 3-4 karakter atau kata- kata simpel yang dapat mudah ditebak oleh hacker.
- Password use – Aplikasi kita harus membatasi user yang mengakses aplikasi melakukan login kembali ke sistem pada tenggang waktu tertentu. Dengan cara ini aplikasi dapat dilindungi dari serangan brute force dimana hacker bisa menyerang berulang kali untuk berhasil login ke sistem. Selain itu, log in yang gagal sebaiknya dicatat sebagai informasi kepada administrator untuk mengindikasikan kemungkinan serangan yang terjadi.
- Password storage – password tidak boleh disimpan di dalam aplikasi. Password harus disimpan dalam format terenkripsi dan disimpan di file lain seperti file database atau file password. Hal ini dapat memastikan bahwa informasi yang sensitif seperti password tidak disebarkan ke dalam aplikasi.

  Issue lain yang berhubungan : password tidak boleh dalam bentuk hardcoded di dalam source code.

- Session ID Protection – server biasanya menggunakan session Id untuk mengidentifikasi user yang masuk ke dalam session. Akan tetapi jika session ID ini dapat dilihat oleh seseorang pada jaringan yang sama, orang tersebut dapat menjadi seorang client. Salah satu cara yang dapat digunakan untuk mencegah terlihatnya session ID oleh seseorang pada suatu jaringan yang sama adalah menghubungkan komunikasi antara sever dan client pada sebuah SSL-protected channel.

4. Cross Site Scripting

   Cross site scripting terjadi ketika seseorang membuat aplikasi web melalui script ke user lain. Hal ini dilakukan oleh penyerang dengan menambahkan content (seperti JavaScript, ActiveX, Flash) pada request yang dapat membuat HTML output yang dapat dilihat oleh user lain. Apabila ada user lain yang mengakses content tersebut, browser tidak mengetahui bahwa halaman tersebut tidak dapat dipercaya. Cara yang bisa digunakan untuk mencegah serangan cross site scripting adalah dengan melakukan validasi data masuk dari user request (seperti header, cookie, user parameter, ...). Cara *negative approach* tidak digunakan : mencoba untuk memfilter active content merupakan cara yang tidak efektif.

5. Buffer Overflows

   Penyerang dapat menggunakan *buffer overflows* untuk merusak aplikasi web. Hal ini dilakukan karena penyerang mengirimkan request yang membuat server menjalankan kode-kode yang dikirimkan oleh penyerang. Kelemahan buffer overflow biasanya sulit dideteksi dan sulit dilakukan oleh hacker. Akan tetapi penyerang masih bisa mencari kelemahan ini dan melakukan buffer overflow pada sebagian aplikasi web. Terima kasih atas desain dari Java environment, dimana aplikasi yang berjalan pada J2EE server aman dari jenis serangan ini. Untuk memastikan keamanan, cara yang paling baik adalah melakukan pengawasan apabila terdapat patch atau bug report dari produk server yang digunakan.

6. Injection Flaws

Salah satu kelemahan yang populer adalah injection flaw, dimana hacker dapat mengirimkan atau menginject request ke operating system atau ke external sumber seperti database.

7. Insecure Storage

Aplikasi web biasanya perlu menyimpan informasi yang sensitif seperti password, informasi kartu kredit, dan yang lain. Dikarenakan item-item tersebut bersifat sensitif item-item tersebut perlu dienkripsi untuk menghindari pengaksesan secara langsung. Akan tetapi beberapa metode enkripsi masih lemah dan masih bisa diserang.Berikut ini beberapa kesalahan yang sering terjadi :

- Kesalahan untuk mengenkripsi data penting
- Tidak amannya kunci, *certificate*, dan *password*
- Kurang amannya lokasi penyimpanan data
- Kurangnya penghitungan dari randomisasi
- Kesalahan pemilihan algoritma
- Mencoba untuk menciptakan algoritma enkripsi yang baru.

8. Denial of Service

Denial of Service merupakan serangan yang dibuat oleh hacker yang mengirimkan request dalam jumlah yang sangat besar dan dalam waktu yang bersamaan.Dikarenakan request-request tersebut, server menjadi kelebihan beban dan tidak bisa melayani user lainnya.Serangan DoS mampu menghabiskan bandwidth yang ada pada server. Selain itu dapat juga menghabiskan memory, koneksi database, dan sumber yang lain. Pada umumnya sangat sulit untuk melindungi aplikasi dari serangan ini. Akan tetapi masih ada cara yang dapat dilakukan seperti membatasi resource yang dapat diakses user dalam jumlah yang minimal. Merupakan ide / cara yang

bagus untuk membuat load quota yang membatasi jumlah load data yang akan diakses user dari sistem.

9. Insecure Configuration Management

Biasanya kelompok (*group*) yang mengembangkan aplikasi berbeda dengan kelompok yang mengatur hosting dari aplikasi. Hal ini bisa menjadi berbahaya, dikarenakan keamanan yang diandalkan hanya dari segi aplikasi : sedangakan dari segi server juga memiliki aspek keamanan yang perlu diperhatikan. Adanya kesalahan dari konfigurasi server dapat melewati aspek keamanan dari segi aplikasi.Berikut ini adalah kesalahan konfigurasi server yang bisa menimbulkan masalah: :

- Celah keamanan yang belum dipatch dari software yang ada pada server – administrator tidak melakukan patch software yang ada pada server.
- Celah keamanan server dimana bisa menampilkan list dari direktori atau juga serangan berupa directory traversal.
- File-file backup atau file contoh (*sample file*), file-file script, file konfigurasi yang tertinggal / tidak perlu.
- Hak akses direktori atau file yang salah.
- Adanya service yang seperti *remote administration* dan *content management* yang masih aktif.
- Penggunaan *default account* dan *default password*.
- Fungsi *administrative* atau fungsi *debug* yang bisa diakses.
- Adanya pesan *error* yang informatif dari segi teknis.
- Kesalahan konfigurasi SSL certificate dan setting enkripsi.
- Penggunaan self-signet certificates untuk melakukan autentikasi.
- Penggunaan default certificate.

3.8 Cookies

1. Pengertian Cookies

Cooikies diciptakan agar *website* dapat mengetahui aktivitas yang telah dilakukan user pada waktu sebelumnya. Aktivitas ini misalnya mengklik suatu tombol, login, ata halaman mana yang telah dibuka oleh user pada bulan bahkan tahun lalu.

Cookies juga bisa saja menyimpan informasi diri anda sendiri seperti nama, alamat e-mail, alamat rumah atau kantor, nomor telepon yang dapat digunakan untuk mengidentifikasi atau mengontak anda. Hal ini bisa terjadi apabila anda memberikan informasi di dalam sebuah *website.*

2. Fungsi Cookies

Cookies diciptakan untuk menghemat waktu Anda saat browsing di internet. Cara kerja cookies adalah *storing and sending*, alias menyimpan dan mengirim. Sehingga jika Anda mengunjungi suatu situs web, Anda tidak perlu lagi melakukan setting dan lain sebagainya dengan catatan Anda sudah pernah berkunjung ke situs tersebut sebelumnya.

Contohnya, ketika Anda membuka Instagram atau jejaring sosial lainnya dan login, selanjutnya Anda akan logout Instagram dan secara otomatis email tersimpan serta kita menghemat waktu untuk tidak menulis email kembali Atau pengaturan bahasa pada Instagram. Jika sebelumnya Anda menggunakan setting bahasa indonesia, maka saat Anda membuka Instagram selanjutnya, settingan bahasa akan tetap pada bahasa Indonesia.

Selain itu, ukuran file cookies juga sangat kecil, dengan ukuran tidak dapat lebih besar dari *4096 Bytes (4KB)* per website yang dikunjungi. Ada batas jumlah total cookies pada harddisk klien. Jumlah ini juga berbeda-beda pada setiap browser, tetapi biasanya terbatas pada sekitar tiga ratus cookies. Jika nomor ini telah terlampaui, sebuah cookies yang lebih tua akan dihapus sebelum yang baru dibuat. Cookies memiliki tanggal kadaluarsa. Tanggal ini telah ditetapkan, sehingga browser dapat menghapus cookies yang kadaluarsa atau tua ketika mereka tidak lagi dibutuhkan oleh server web. Jika tanggal kadaluarsa kosong, cookies akan dihapus saat sambungan dengan server

ditutup. Hal ini terjadi ketika jendela atau tab situs ditutup oleh pengguna, atau ketika pengguna menutup seluruh browser.

3.9 Acunetix Web Vulnerability Scanner

1. Pengertian Acunetix Web Vulnerability Scanner

   Acunetix Web Vulnerability Scanner adalah sebuah alat layanan aplikasi web untuk pengujian keamanan otomatis yang mengaudit aplikasi web Anda dengan memeriksa kerentanan seperti SQL Injection, Cross site scripting, dan kerentanan web yang dieksploitasi lainnya. Acunetix merupakan alat otomatis yang dapat membantu perusahaan memindai aplikasi web mereka untuk mengidentifikasi dan menyelesaikan kerentanan dieksploitasi.

   Acunetix Vulnerability Scanner juga telah menjadi alat pilihan bagi banyak pelanggan di Pemerintahan, Militer, Pendidikan, Telekomunikasi, Perbankan, Keuangan, dan perusahaan E-Commerce, dan termasuk perusahaan-perusahaan besar lainnya dari berbagai negara.

   Acunetix Vulnerability Scanner juga dapat mendeteksi dan melaporkan berbagai macam kerentanan dalam aplikasi yang dibangun pada arsitektur seperti WordPress, PHP, ASP.NET, Java Frameworks, Ruby on Rails dan masih banyak lainnya. Acunetix Vulnerability Scanner membawa fitur-set yang luas dari kedua alat pengujian penetrasi otomatis dan manual, memungkinkan analis keamanan untuk melakukan penilaian kerentanan yang lengkap, dan melakukan perbaikan acaman yang terdeteksi dan memberikan laporan lengkap mengenai hasil dari scan secara jelas.

2. Alasan menggunakan Acunetix Web Vulnerability Scanner

   Kejahatan hacking yang selalu terus meningkat dari waktu ke waktu dan jumlah korban yang juga selalu meningkat Masalah kerentanan keamanan website setiap hari menjadikan masalah serius yang harus di atasi.Firewall, SSL dan server lock-down tidak cukup mampu untuk mencegah aplikasi web dan situs dari serangan hacker.

Berikut adalah beberapa fitur utama yang ditawarkan oleh Acunetix Web Vulnerability Scanner:

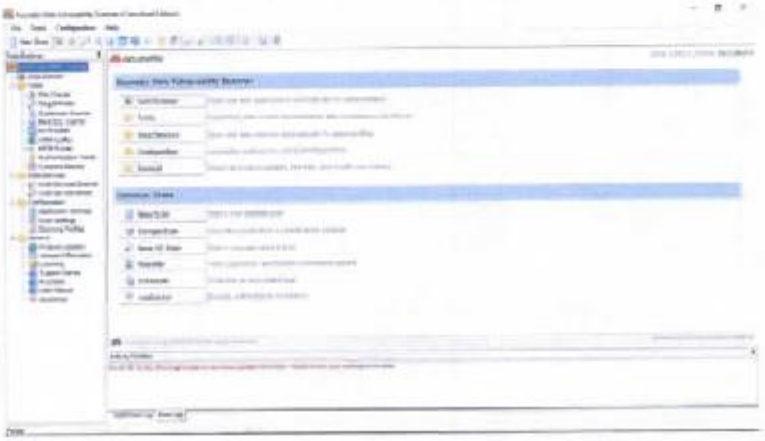
- Teknologi Acusensor
- Industri yang paling canggih dan mendalam dalam SQL injection dan pengujian Cross site scripting.
- Mendukung HTML5 penuh dengan Acunetix DeepScan Teknologi
- Aplikasi scanning komprehensif baik untuk Halaman Single dan situs berbasis JavaScript
- Mendukung Mobile web site
- Dapat mendeteksi kerentanan Blind XSS dengan layanan AcuMonitor
- Dapat mendeteksi otomatis kerentanan XSS berbasis DOM
- Alat pengujian penetrasi Canggih, seperti HTTP Editor dan HTTP Fuzzer
- Fasilitas pelaporan ekstensif termasuk laporan kepatuhan PCI
- Multi-berulir dan petir scanner cepat merangkak ratusan ribu halaman dengan mudah.

BAB IV
HASIL DAN PEMBAHASAN

4.1 Pembahasan

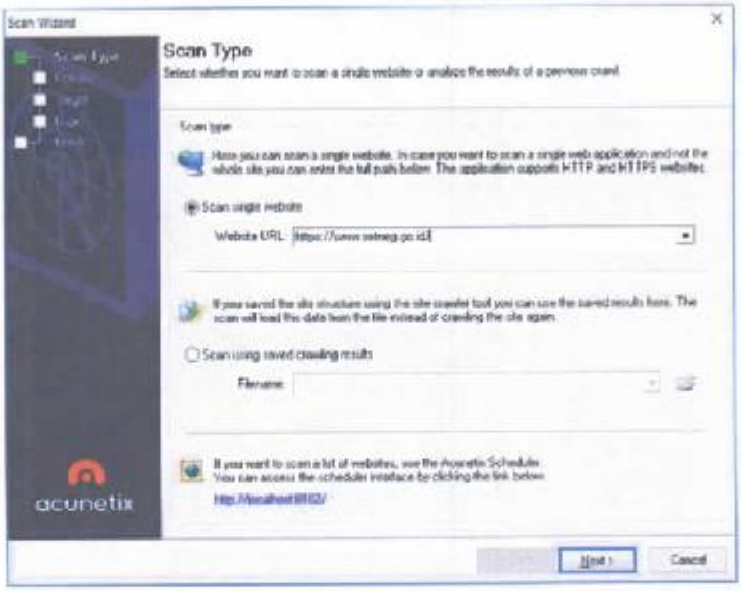
Untuk memulai pengujian terhadap *website* Kementerian Sekretariat Negara adalah dengan mengikuti langkah-langkah berikut ini :

1. Aplikasi *Acunetix Web Vulnerability Scanner* dibuka atau dijalankan, maka akan didapatkan tampilan seperti pada gambar di bawah ini :



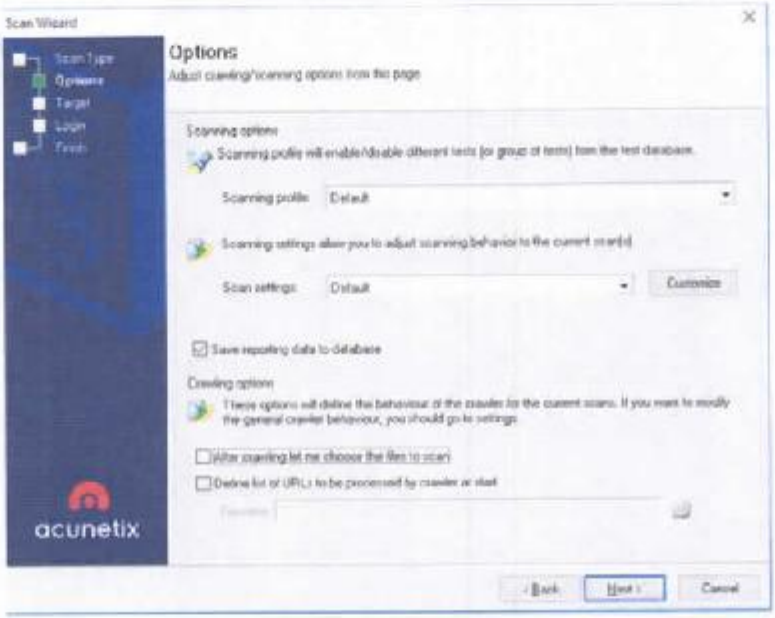
Gambar 4.1 Tampilan Awal Aplikasi *Acunetix*

2. Menu *New Scan* dipilih untuk memulai pengujian



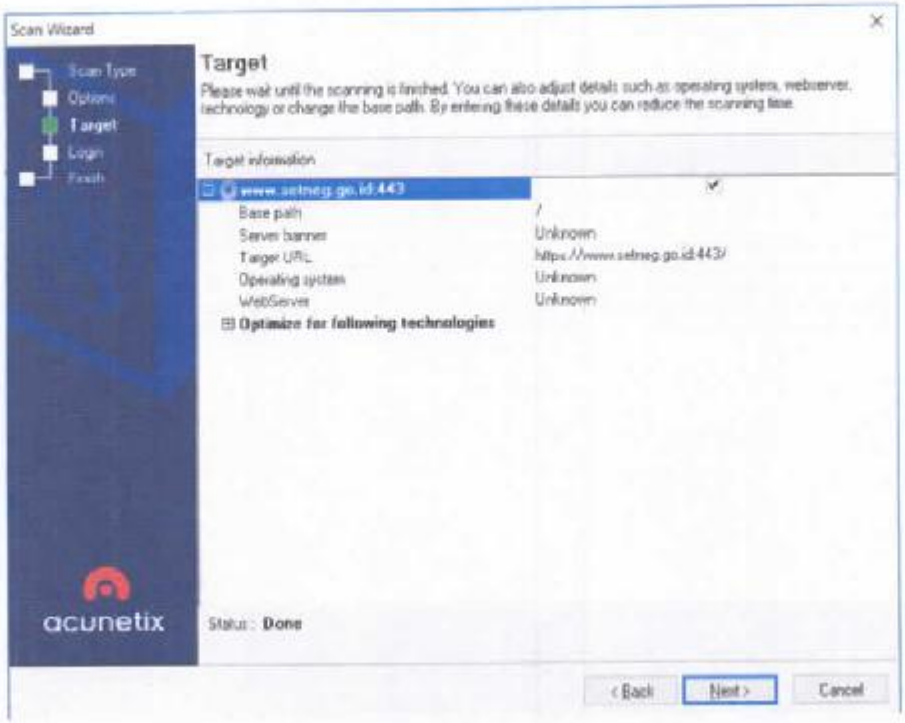
Gambar 4.2 Penginputan *URL Website*

3. Pada gambar 4.2, terdapat 2 opsi yang dapat dipilih, yaitu :
   a. Scan single website, dimana opsi ini digunakan untuk memindai suatu *website.*
   b. Scan using saved crawling result, dimana opsi ini digunakan untuk memindai *website* yang telah dipindai sebelumnya.
4. Kemudian alamat *URL website* yang akan diuji dimasukkan seperti pada gambar 4.2, dimana disini menggunakan *website* Kemensetneg yaitu *https://www.setneg.go.id.*
5. Kemudian tombol *next* diklik untuk melanjutkan proses.



Gambar 4.3 *Scanning Option*

6. Pada gambar 4.3, *Scanning option* dan *settings* diatur *default.*
7. Kemudian tombol *next* diklik, sehingga aplikasi akan menampilkan informasi *website* yang akan diuji.



Gambar 4.4 Informasi *Website*

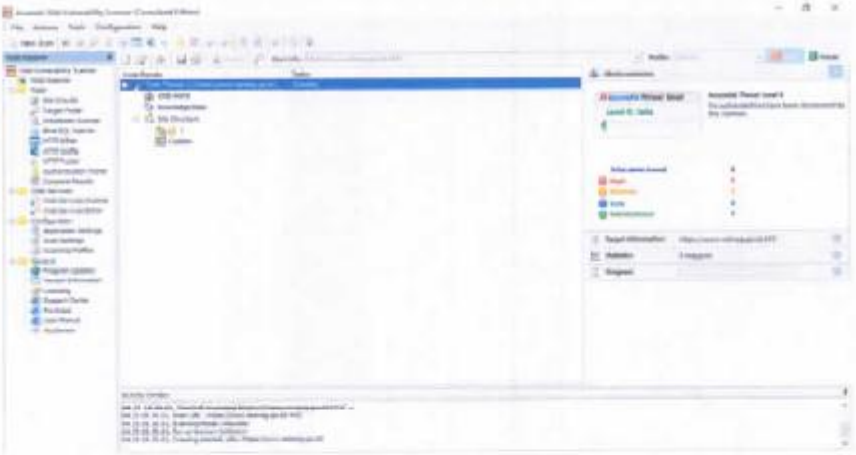
8. Setelah informasi *website* ditampilkan, tombol *next* diklik untuk melanjutkan proses.

Gambar 4.5 Informasi *Login*

9. Pada gambar 4.5, *Login sequence* diatur *no login sequence.*
10. Kemudian tombol *next* diklik untuk melanjutkan proses.

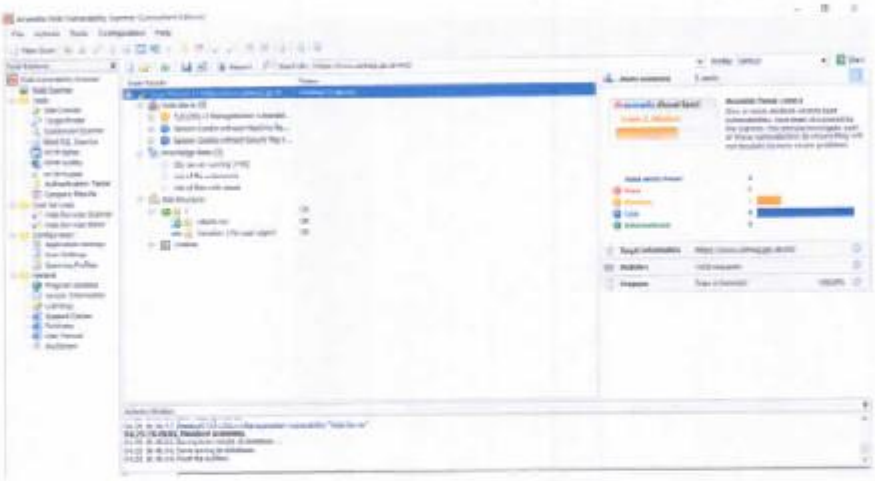
Gambar 4.6 *Finish setup*

11. Kemudian tombol *finish* diklik agar menyelesaikan proses *setup.*
12. Setelah itu aplikasi akan berjalan untuk men-*scan website* yang akan diuji.



Gambar 4.7 Proses *Scanning*

13. Setelah aplikasi menyelesaikan proses *scanning*, maka akan didapatkan tampilan seperti pada gambar dibawah ini :



Gambar 4.8 Hasil *Scanning*

14. Pada gambar 4.8 akan ditampilkan hasil dari tingkat keamanan *website* yang diuji, dimana aplikasi *Acunetix Web Vulnerability Scanner* akan memberikan hasil berupa tingkatan ancaman sebagai berikut :
    a. *High Level,* merupakan tingkat ancaman yang paling tinggi.
    b. *Medium Level,* merupakan tingkat ancaman menengah.
    c. *Low Level,* merupakan tingkat ancaman yang paling rendah.
    d. *Informational,* merupakan ancaman untuk penyebaran informasi melalui pencarian

4.2 Analisa

Hasil pengujian dari *website* Kemensetneg dengan URL *https://www.setneg.go.id* didapatkan hasil tingkat ancaman yang berada pada *Medium Level 2.*

Gambar 4.9 Tingkat Ancaman

Berikut adalah rincian dari ancaman yang telah ditemukan dari pengujian *website* Kemensetneg dengan menggunakan aplikasi *Acunetix Web Vulnerability Scanner* :

1. TLS1/SSLv3 Renegotiation Vulnerability

TLS1/SSLv3 Renegotiation Vulnerability

Severity	**Medium**
Type	Configuration
Reported by module	TLS1_SSL3_Renegotiation

Gambar 4.10 TLS1/SSLv3 Renegotiation Vulnerability

Hal ini dapat menyebabkan penyerang untuk menanamkan *plaintext* ke dalam aliran protocol aplikasi. Ancaman ini juga bias mengakibatkan situasi dimana penyerang dapat memberikan perintah ke server seolah-olah dari sumber yang sah, seperti mendapatkan informasi *HTTP*. Masalah ini termasuk dalam tingkat ancaman level *Medium.*

2. Session Cookie without HttpOnly flag set

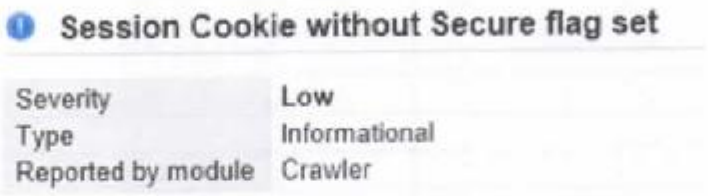
Session Cookie without HttpOnly flag set

Severity	Low
Type	Informational
Reported by module	Crawler

Gambar 4.11 Session Cookie without HttpOnly flag set

Hal ini dapat menyebabkan penyerang untuk mendapatkan file *cookie user.* Dimana file *cookie* ini berisi data dari pengguna atau *user.* Hal ini masih tergolong dalam ancaman tingkat rendah atau *low,* tetapi lebih baik untuk memberikan keamanan terhadap *file cookie* agar tidak terjadi hal yang tidak diinginkan.

3. Session Cookie without Secure flag set



Gambar 4.12 Session Cookie without Secure flag set

Hal ini tidak jauh berbeda dengan kondisi pada ancamana ke-2, perbedaannya terletak pada *file cookie* yang diamankan. Pada *HttpOnly flag set,* hanya melindungi *file cookie* pada *Http,* sedangkan *Secure flag set* dapat melindngi *file cookie* dari *Http* maupun *Https.* Biarpun ancaman ini termasuk ke dalam level rendah *Low,* ada baiknya jug ajika memberi atau meningkatkan keamanan pada ancaman ini.

BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil analisis data pengujian *website* maka dapat disimpulkan sebagai berikut:

1. Aplikasi *Acunetix Web Vulnerability Scanner* merupakan aplikasi yang digunakan untuk melakukan pengujian terhadap ancaman atau celah keamanan dari suatu *website.*
2. Aplikasi *Acunetix Web Vulnerability Scanner* dapat memberikan rekomendasi atau solusi dari hasil pengujian suatu *website.*
3. Tingkat celah keamanan dari *website* Kemensetneg dengan URL *https://www.setneg.go.id* berada pada level *Medium.*

5.2 Saran

Berdasarkan kesimpulan yang didapatkan diatas dapat dikemukakan beberapa saran, yaitu :

1. Melakukan pengujian terhadap *website* yang dilakukan secara berkala, agar dapat mengetahui kerentanan dari *website* agar tidak terjadi pembobolan yang tidak diinginkan.
2. Tingkat kerentanan *website* kemensetneg sudah memasuki level *Medium* oleh karena itu sebaiknya Kemensetneg memperbaiki atau memperbarui sistem keamanan pada *website*-nya.

DAFTAR PUSTAKA

Basavala, S.R., Kumar, N. & Agarrwal, A. 2012. *Finding Vulnerabilities in Rich Internet Applications (Flex/AS3) Using Static Techniques.* I.J.Modern Education and Computer Science.

Dahlan, Mohdkk. 2014. *Pengujian dan Analisa Keamanan Website Terhadap Serangan SQL Injection.* UniversitasMuriaKudus : Kudus.

Kementerian Sekretariat Negara. 2018. Diakses April 2018. Pada https://www.setneg.go.id.

Stuttard D., Pinto M. 2011. *The Web Application Hacker's Handbook Second Edition.* John Wiley & Sons, Inc. Indianapolis, America.

LAMPIRAN

Dokumentasi

1. Presentasi dari tugas yang diberikan oleh Biro Dukungan Informasi Kementerian Sekretariat Negara Republik Indonesia.

C. KARTU KENDALI PKL

UNIVERSITAS ANDALAS
Program Studi Sistem Komputer
Kampus UNAND Limau Manis

F3

KARTU KENDALI PRAKTEK KERJA LAPANGAN (PKL)

Nama : Akbar Kolo
No.BP : 1511512006
Nama Perusahaan/Instansi : Biro Informasi dan Teknologi, Sekretariat Kementrian
Pembimbing PKL : 1. Nur Hadianto
2. Suhariono

No.	Hari/Tanggal	Kegiatan	Tanda Tangan Pembimbing
1.	Selasa - Jumat 2-5 Januari 2018	Pengenalan ruang lingkup kerja Biro DI Kemensetneg	1.
2.	Senin - Jumat 8-12 Januari 2018	1. Pengenalan Jaringan gedung Setneg 2 Pemberian project aplikasi android	2.
3.	Senin - Jumat 15-19 Januari 2018	1. Pengerjaan Project aplikasi android (Pembuatan tahap dasar aplikasi android) 2. Survei dengan teknisi Kemensetneg	3.
4.	Senin - Jumat 22-26 Januari 2018	1. Pengerjaan project aplikasi android (melanjutkan pembuatan aplikasi) 2. Presentasi project aplikasi android tahap1	4.
5.	Senin - Jumat 29 Januari - 2 Februari 2018	1. Pengerjaan project aplikasi android (finishing aplikasi Android Technician Tracker 2. presentasi tahap akhir.	5.
6.			6.
7.			7.
8.			8.

D. FORM PENILAIAN PKL

UNIVERSITAS ANDALAS
Program Studi Sistem Komputer
Kampus UNAND Limau Manis

F4

FORM PENILAIAN PRAKTEK KERJA LAPANGAN (PKL)

Nama : Akbar Koto
No.BP : 1511512006
Nama Perusahaan/Instansi : Biro Informasi dan Teknologi, Sekretariat Kementrian
Pembimbing PKL : 1. Nur Hadianto
2. Suhariono

No	Jenis Penilaian	Nilai Angka	Nilai Huruf
1	Kemampuan dan etika bergaul	83	A-
2	Kemampuan beradaptasi	78	B+
3	Kemampuan berinisiatif	82	A-
4	Kemampuan menyampaikan pendapat	77	B+
5	Pengetahuan tentang pekerjaan	85	A
6	Kemampuan kerjasama dalam kelompok	87	A
7	*Kesungguhan dalam bekerja*	87	A
8	Kedisiplinan	82	A-
9	Sopan santun	85	A
10	Tanggung jawab	80	A-
11	Kehadiran	85	A
12	Keselamatan kerja	80	A-
13	Laporan kerja	84	A-

Ekivalen Nilai:

A	: 85 – 100	C+	: 60 – 64
A-	: 80 – 84	C	: 55 – 59
B+	: 75 – 79	C-	: 50 – 54
B	: 70 – 74	D	: 40 – 49
B-	: 65 – 69	E	: < 40

Padang,
Pembimbing PKL,

(SUHARIONO)