

LAPORAN KERJA PRAKTEK

SECURITY ASSESMENT MENGGUNAKAN OPEN WEB APPLICATION SECURITY PROJECT ZED ATTACK PROXY (OWASP ZAP)

STUDI KASUS DI CV. CIPTA DAYA INFORMATIKA

Diajukan untuk memenuhi persyaratan kelulusan
Matakuliah TIF335 Kerja Praktek

Oleh :
Sabda Alam / C1A160015



**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS BALE BANDUNG
2019**

LEMBAR PENGESAHAN

PROGRAM STUDI TEKNIK INFORMATIKA

SECURITY ASSESMENT MENGGUNAKAN OPEN WEB APPLICATION
SECURITY PROJECT ZED ATTACK PROXY (OWASP ZAP)

STUDI KASUS DI CV. CIPTA DAYA INFORMATIKA

Oleh :

Sabda Alam / C1A160015

disetujui dan disahkan sebagai

Laporan Kerja Praktek

Bandung, Agustus 2019

Koordinator Kerja Praktek

Yaya Suharya S.Kom., M.T.

NIDN: 0407047706

LEMBAR PENGESAHAN

CV. CIPTA DAYA INFORMATIKA

SECURITY ASSESMENT MENGGUNAKAN OPEN WEB APPLICATION
SECURITY PROJECT ZED ATTACK PROXY (OWASP ZAP)

STUDI KASUS DI CV. CIPTA DAYA INFORMATIKA

oleh :

Sabda Alam / C1A160015

disetujui dan disahkan sebagai

Laporan Kerja Praktek

Padalarang, Agustus 2019

Pembimbing Lapangan

Elsa Herlyanti

ABSTRAKSI

Kerja Praktek dilaksanakan di CV. Cipta Daya Informatika, perusahaan yang bergerak di bidang telekomunikasi dan komputer. Kerja Praktek dimulai dari tanggal 14 Maret 2019 sampai dengan tanggal 14 April 2019.

Kerja praktek yang dilakukan adalah melakukan penelitian untuk mencari kerentanan website profil perusahaan CV. Cipta Daya Informatika yaitu <http://www.cdi.co.id>. Aplikasi yang digunakan adalah OWASP ZAP (*Open Web Application Security Project Zed Attack Proxy*).

Selama penelitian, metodologi yang digunakan adalah VAPT (*Vulnerability Assesment and Penetration Testing*). Tahap pertama Penentuan Ruang Lingkup (*Scope*). Tahap kedua Pengintaian Sistem (*Reconnaissance*). Tahap ketiga Pencarian Kerentanan Keamanan (*Vulnerability Detections*). Tahap keempat Analisis Perencanaan dan Perencanaan Pengujian (*Information Analysis and Planning*). Tahap kelima *Penetration Testing*. Tahap keenam Eksploitasi Kerentanan (*Privilege Escalation*). Dan tahap terakhir Penyusunan Laporan (*Reporting*).

Pada akhir kerja praktek dihasilkan dokumentasi aset yang dianggap berisiko sebagai bahan evaluasi untuk perbaikan dan penanganan pada ancaman keamanan website profil perusahaan CV. Cipta Daya Informatika.

Kesimpulan dari keseluruhan proses kerja praktek adalah untuk menghasilkan website profil perusahaan yang efektif, perlu diperhatikan aspek keamanan untuk melindungi aset yang dinilai penting.

Kata kunci: *Vulnerability Assesment, Penetration Testing, OWASP ZAP, VAPT*

KATA PENGANTAR

Puji syukur kehadiran Tuhan Yang Maha Esa yang telah melimpahkan rahmat dan hidayah-Nya sehingga penyusun dapat menyelesaikan Laporan Kerja Praktek ini dengan tepat waktu. terselesaikannya laporan ini tentu tidak lepas dari bantuan banyak pihak. Berkat bantuan dan bimbingan mereka, penyusun dapat menyusun dan menyelesaikan Laporan Kerja Praktek ini. Oleh karena itu, penyusun mengucapkan terima kasih yang sebesar-besarnya kepada:

1. Allah SWT yang telah memberikan karunia-Nya selama proses pengerjaan laporan ini.
2. Keluarga di rumah yang telah mendukung dan memberikan do'a selama proses pengerjaan laporan.
3. Dr. H. Nasep Rachmat, Ir., MM., M.Si. (Brigjen. TNI (Purn)) selaku Rektor Universitas Bale Bandung.
4. Yudi Herdiana, S.T, M.T. selaku Dekan Fakultas Teknologi Informasi Universitas Bale Bandung.
5. Yaya Suharya S.Kom, M.T. selaku Pembimbing Lapangan Sekaligus Dosen Pembimbing Kerja Praktek yang telah membantu selama pelaksanaan Kerja Praktek sampai penyusunan laporan.

Penyusun menyadari sepenuhnya bahwa laporan ini masih jauh dari kata sempurna, oleh karena itu kritik dan saran dari semua pihak yang bersifat membangun selalu penyusun harapkan demi kesempurnaan laporan ini.

Bandung, Juli 2019

Penyusun

SABDA ALAM
NIM: C1A160015

DAFTAR ISI

ABSTRAKSI.....	III
KATA PENGANTAR	IV
DAFTAR ISI.....	V
DAFTAR GAMBAR	VII
DAFTAR TABEL.....	VIII
BAB I PENDAHULUAN	I-1
I.1 Latar Belakang.....	I-1
I.2 Lingkup.....	I-2
I.3 Tujuan.....	I-3
BAB II ORGANISASI DAN LINGKUNGAN KERJA PRAKTEK	II-1
II.1 Sekilas Perusahaan	II-1
II.2 Sejarah Perusahaan	II-2
II.3 Visi Misi Perusahaan	II-3
II.3.1 Visi.....	II-3
II.3.2 Misi	II-3
II.4 Maksud Dan Tujuan Perusahaan	II-3
II.5 Struktur Organisasi Perusahaan.....	II-4
II.6 Lingkup Pekerjaan.....	II-4
II.7 Deskripsi Pekerjaan	II-5
II.8 Jadwal Kerja	II-6
BAB III PENGETAHUAN/TEORI PENUNJANG KERJA PRAKTEK	III-1
III.1 Teori Penunjang Kerja Praktek.....	III-1
III.2 Tinjauan Pustaka.....	III-1
III.3 Dasar Teori	III-3
III.3.1 <i>Information Technology Security Assesment</i>	III-3
III.3.2 VAPT (<i>Vulnerability Assesment and Penetration Testing</i>).....	III-5
III.3.3 Website	III-11
III.3.4 OWASP ZAP (<i>Open Web Application Security Project Zed Attack Proxy</i>).....	III-15

III.3.5	Browser	III-20
III.3.6	Sublime Text.....	III-24
III.3.7	Jaringan Internet	III-26
III.3.8	HTML (<i>Hypertext Markup language</i>)	III-28
III.4	Kakas Yang Digunakan	III-30
BAB IV PELAKSANAAN KERJA PRAKTEK.....		IV-1
IV.1	Input.....	IV-1
IV.2	Proses.....	IV-1
IV.2.1	Penentuan Ruang Lingkup (<i>Scope</i>).....	IV-2
IV.2.2	Pengintaian Sistem (<i>Reconnaissance</i>)	IV-2
IV.2.3	Pencarian Kerentanan Keamanan (<i>Vulnerability Detection</i>) Menggunakan <i>Tools Software</i> OWASP ZAP	IV-2
IV.2.4	Analisis dan Perencanaan <i>Penetration Testing</i>	IV-4
IV.2.5	<i>Penetration Testing</i>	IV-15
IV.2.6	Eksplorasi Kerentanan (<i>Privilege Escalation</i>).....	IV-17
IV.2.7	Pelaporan Hasil Kerja Praktek	IV-18
IV.3	Pencapaian Hasil.....	IV-18
BAB V PENUTUP.....		V-1
V.1	Kesimpulan Dan Saran Mengenai Pelaksanaan Kerja Praktek	V-1
V.1.1	Kesimpulan Pelaksanaan Kerja Praktek	V-1
V.1.2	Saran Pelaksanaan Kerja Praktek	V-1
V.2	Kesimpulan Dan Saran Mengenai Substansi Selama Kerja Praktek..	V-2
V.2.1	Kesimpulan Mengenai <i>Security Assesment</i> Di CV. Cipta Daya Informatika.....	V-2
V.2.2	Saran Mengenai <i>Security Assesment</i> Di CV. Cipta Daya Informatika	V-3
LAMPIRAN A. TOR		A-1
LAMPIRAN B. LOG ACTIVITY		B-1

DAFTAR GAMBAR

Gambar 2.1 Struktur Organisasi CV. Cipta Daya Informatika	II-4
Gambar 3.1 Fase Information Technology Security Assesment.....	III-4
Gambar 3.2 Tahapan VAPT.....	III-5
Gambar 3.3 Logo OWASP ZAP	III-15
Gambar 3.4 Skema OWASP ZAP	III-16
Gambar 3.5 Contoh Beberapa Browser	III-21
Gambar 3.6 Logo Sublime Text.....	III-24
Gambar 4.1 Tampilan Awal OWASP ZAP	IV-3
Gambar 4.2 Daftar Kerentanan Website CV. Cipta Daya Informatika.....	IV-3
Gambar 4.3 Keseluruhan Tingkat Resiko Keamanan.....	IV-15
Gambar 4.4 Contoh Tampilan ClickJacking CV. Cipta Daya Informatika ...	IV-16
Gambar 4.5 Script HTML Tampilan ClickJacking.....	IV-17

DAFTAR TABEL

Tabel 4.1 Daftar Kerentanan Website CV. Cipta Daya Informatika	IV-4
Tabel 4.2 Tingkat Kemungkinan Dan Dampak	IV-11
Tabel 4.3 Faktor Kemungkinan Threat agent	IV-11
Tabel 4.4 Faktor Kemungkinan Vulnerability	IV-12
Tabel 4.5 Faktor dampak Technical Impact Factors.....	IV-13
Tabel 4.6 Faktor Dampak Business Impact Factors.....	IV-14

BAB I

PENDAHULUAN

I.1 Latar Belakang

Perkembangan Teknologi semakin hari semakin maju. Salah satunya yaitu internet yang merupakan teknologi yang perkembangannya paling pesat saat ini. Orang dari berbagai kota besar maupun kecil mudah sekali mengakses internet. Bahkan dengan akses internet yang disediakan oleh penyedia jasa telepon/telekomunikasi, orang-orang di pelosok telah bisa mengakses baik lewat komputer maupun lewat *handphone* yang sekarang berkembang pesat. Bisa dipastikan hampir semua orang yang menggunakan *smartphone* telah menggunakan internet. Dengan demikian internet merupakan media yang bisa diakses semua orang. Dengan tersedianya media yang bisa diakses semua orang, maka perusahaan yang ingin dikenal secara luas maupun perusahaan yang ingin menjaga hubungan dengan pelanggannya perlu membuat Website yang berisi informasi profil perusahaan maupun penawaran serat proses transaksi jasa/produk yang diberikan.

CV. Cipta Daya Informatika, perusahaan yang bergerak di bidang telekomunikasi dan komputer, bergerak dalam bidang usaha barang dan jasa berupa: *hardware*, *software* komputer dan telekomunikasi sebagai pemrograman, analisis sistem, teknisi, konsultan, instruktur, pengujian, perancang, penjual, jasa multimedia (warnet, wartel, game online, penyelenggara VOIP (*Voice Internet Protocol*)), ISP (*Internet Service Provider*) dan perawat di bidang teknologi informasi dan telekomunikasi umumnya, khususnya di bidang komputer adalah perusahaan yang menerapkan pemanfaatan perkembangan internet menggunakan aplikasi website. Namun perlu diperhatikan untuk aspek keamanan pada aplikasi website diperlukan adanya dokumentasi tentang daftar aset aplikasi website yang dianggap berisiko di CV. Cipta Daya Informatika, karena dokumentasi tentang daftar aset yang dianggap berisiko dinilai penting sebagai bahan evaluasi untuk meningkatkan keamanan pada aplikasi website di CV. Cipta Daya Informatika.

Namun di CV. Cipta Daya Informatika belum mempunyai dokumentasi aset kritis yang berisi daftar aset aplikasi website yang dianggap berisiko untuk mencegah adanya gangguan pada salah satu aset aplikasi website. Dokumentasi aset yang dianggap berisiko sangat dibutuhkan untuk pencegahan dan penanganan pada ancaman dan risiko keamanan aplikasi website jika sewaktu-waktu terjadi penyerangan dan penyadapan.

Oleh karena itu, dalam pelaksanaan Kerja Praktek kali ini penyusun mengambil judul “Security Assesment Menggunakan Open Web Application Security Project Zed Attack Proxy (OWASP ZAP) Studi Kasus di CV. Cipta Daya Informatika” untuk mencari dan pendokumentasian kerentanan di website perusahaan milik CV. Cipta Daya Informtika.

Kerangka kerja yang digunakan dalam penelitian ini adalah VAPT (*Vulnerability Assesment and Penetration Testing*). Aplikasi yang digunakan untuk mengetahui kerentanan keamanan pada aset Website adalah OWASP ZAP (*Open Web Application Security Project Zed Attack Proxy*). OWASP ZAP adalah aplikasi untuk menemukan Vulnerability dalam suatu web application. Setelah diketahui hasil dari Vulnerability dari aplikasi website maka tahap selanjutnya adalah dilakukan *Penetration Testing*.

I.2 Lingkup

Lingkup materi dari pelaksanaan Kerja Praktek yang dilaksanakan di CV. Cipta Daya Informatika ini menyangkut hal berikut :

1. Penelitian dilakukan pada website CV. Cipta Daya Informatika yaitu (<http://www.cdi.co.id>)
2. Penelitian dilakukan mengacu pada metodologi penelitian VAPT (*Vulnerability Assesment and Penetration Testing*).
3. *Vulnerability Assesment* pada website CV. Cipta Daya Informatika menggunakan *tools* OWASP ZAP.

4. Penelitian dilakukan di dalam ataupun di luar jaringan internet milik CV. Cipta Daya Informatika.
5. Hasil penelitian berupa laporan tertulis.

I.3 Tujuan

Kerja Praktek yang dilakukan di CV. Cipta Daya Informatika ini bertujuan untuk membuat laporan dokumentasi aset dalam aplikasi website yang dianggap berisiko untuk dijadikan bahan evaluasi penanganan dan pencegahan ancaman penyerangan atau penyadapan terhadap aplikasi website profil perusahaan CV. Cipta Daya Informatika.

Penelitian Kerja Praktek ini juga diharapkan dapat membantu Perusahaan CV. Cipta Daya Informatika dalam mengevaluasi aplikasi website perusahaan dari perspektif keamanan informasi. Selain itu, penelitian ini juga dapat diharapkan sebagai bahan pertimbangan dalam pengembangan perusahaan terkait dengan keamanan informasi, baik secara teknis maupun non teknis.

BAB II

ORGANISASI DAN LINGKUNGAN KERJA PRAKTEK

II.1 Sekilas Perusahaan

Berawal di daerah Sekeloa Bandung pada tahun 2002 – 2004 mendirikan Usaha Mandiri “*Friends Computer*” disingkat “FC“, yang didirikan oleh Hilman, Evi Isnandar, Yudi Subekti, Zaenal dan Yaya Suharya. Kemudian Usaha Mandiri “*Friend Computer*”, diganti menjadi Usaha Mandiri “Media Teknologi Digital” disingkat “Metal” pada 1 Oktober 2005 di Jl. Budi Cilember No. 62 Cilember – Bandung. Pendiri Usaha Mandiri “Media Teknologi Digital”, yaitu Yudi Subekti, S.Kom, Evi Isnandar, S.T dan Yaya Suharya, S.Kom. Usaha Mandiri “Media Teknologi Digital”, berkembang dari tahun 2005 s/d 2009. Sejalan perkembangan waktu, pada Rabu 7 April 2010, Usaha Mandiri “Media Teknologi Digital”, berubah nama menjadi Usaha Mandiri “Bina Insan Telematika”, yang disingkat “BIT”

Kemudian Usaha Mandiri “Bina Insan Telematika” atau disingkat BIT, diganti nama menjadi CV. CDI (Cipta Daya Informatika), penamaan CDI bermula dari kode bilangan 001 yang merupakan kode bilangan biner atau *binary digit*. Dalam istilah komputer *binary digit* yaitu satuan terkecil ukuran data digital. CV. Cipta Daya Informatika, berdiri dengan Akta Notaris Sri Hendarti Prawiryo, SH, M.Kn, No. 55, Tanggal 15 Februari 2012, serta akta perubahan dari Notaris Ribi Azwar, SH, M.Kn, No. 434, Tanggal 22 Agustus 2014. Surat Izin Usaha Perdagangan (SIUP) dengan Nomor : 00116/ 10-17/ PK/ II/ 2012, tertanggal 23 Februari 2012, Nomor : 00454/ 10-17/ PK/ VII/ 2016, tertanggal 25 Juli 2016, Tanda Daftar Perusahaan (TDP) Persekutuan Komanditer (CV) dengan Nomor : 103134701315, tanggal 24 Februari 2012, Nomor : 103134602482, tanggal 26 Juli 2016, Surat Keterangan Domisili Perusahaan (SKDP) dengan Nomor : 583/ 12/ DS/ II/ 2012, tertanggal 20 Februari 2012, Surat Keterangan Status Tanah / Bangunan dengan Nomor : 593.12/ 12/ DS/ II/ 2012, tertanggal 20 Februari 2012, Surat Izin Gangguan (HO) dengan nomor : 503/ 020/ E.P2D/ 2012, tertanggal 20 Februari 2012, Nomor

Pokok Wajib Pajak (NPWP) dengan Nomor : 31.469.072.8.421.000, Nomor Rekening : 007.137.869.1001, Bank BJB cabang Cimindi atas nama : CV. Cipta Daya Informatika.

CV. Cipta Daya Informatika, berhubungan dengan bidang telekomunikasi dan komputer bergerak dalam bidang usaha barang dan jasa berupa : *hardware*, *software computer* dan telekomunikasi sebagai pemrogram, analis sistem, teknisi, konsultan, instruktur, penguji, perancang, penjual, jasa multimedia (warnet, wartel, game online, penyelenggara VOIP (*Voice Internet Protocol*)), ISP (*Internet Service Provider*) dan perawat di bidang teknologi informasi dan telekomunikasi umumnya, khususnya di bidang komputer. Serta penggunaan informasi dalam beberapa macam bidang, seperti bioinformatika, informatika medis, informasi pemerintahan, informasi konstruksi, informasi transportasi, dan informasi berbagai disiplin ilmu.

II.2 Sejarah Perusahaan

Pendiri CV. Cipta Daya Informatika, yaitu Andri Kurniawan, S.Pd sebagai Komisaris, Yaya Suharya, S.Kom., M.T., sebagai Direktur, Dadan Juansah, S.Pd, S.ST sebagai Wakil Direktur, Yudi Subekti, S.Kom sebagai *Manager ICT*, Erik Pratama, S.Pd, M.T, sebagai *Manager Operational* dan Firman Danny, S.Pd sebagai *Manager Marketing*. CV. Cipta Daya Informatika, merupakan usaha untuk melakukan sesuatu atau kemampuan bertindak untuk menemukan bentuk baru dari objek kreatifitas dengan menerapkan disiplin ilmu *computer engineering*, *computer science*, *software engineering*, *information system* dan *information technology*. CV. Cipta Daya Informatika, diresmikan pada Minggu, 08 April 2012 di BERLIAN SPORT & HALL, Jl.Raya Purwakarta No.251 Kampung Cikamuning, Desa Ciburuy, Kecamatan Padalarang, Kabupaten Bandung Barat 40553. CV Cipta Daya Informatika mengalami perubahan pengurus, anggaran dasar dan lokasi yang disahkan oleh Notaris Ribi Azwar, S.H., M.Kn, dengan nomor 434, pada tanggal 24 Agustus 2014. Pengurus CV. Cipta Daya Informatika, yaitu Angga Dwi Jayanto, S.S sebagai Komisaris, Yaya Suharya, S.Kom., M.T. sebagai Direktur, Dadan

Juansah, S.Pd, S.ST sebagai Wakil Direktur, Andri Kurniawan, S.Pd sebagai Sekretaris, Yudi Subekti, S.Kom sebagai *Manager ICT*, Erik Pratama, S.Pd, M.T, sebagai *Manager Operational* dan Firman Danny, S.Pd sebagai *Manager Marketing*.

II.3 Visi Misi Perusahaan

II.3.1 Visi

Menjadi bisnis terdepan dalam barang dan jasa komersil *hardware, software computer* dan telekomunikasi umumnya, khususnya pemanfaatan ilmu komputer untuk bidang pendidikan yang sesuai dengan perkembangan teknologi informasi dan komunikasi serta teknologi informatika dan komputer pada tahun 2022.

II.3.2 Misi

Menyediakan dan memenuhi standar kebutuhan bisnis hardware, software computer dan telekomunikasi sebagai pemrogram, analis sistem, teknisi, konsultan, instruktur, penguji, perancang, penjual, jasa multimedia (warnet, wartel, game online, penyelenggara VOIP (*Voice Internet Protocol*)), ISP (*Internet Service Provider*) dan perawat di bidang teknologi informasi dan telekomunikasi umumnya, khususnya di bidang komputer yang profesional, kompeten, terpercaya dan berkualitas dalam skala lokal maupun nasional.

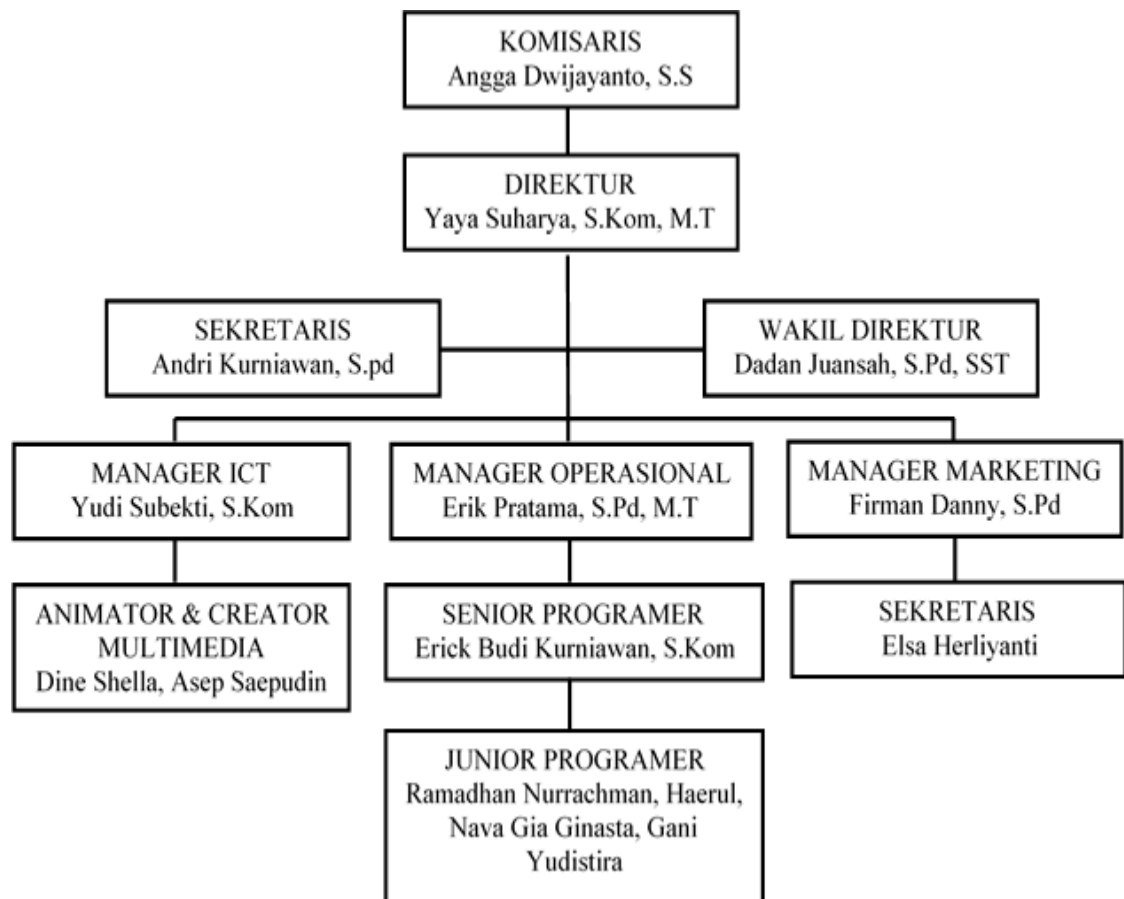
II.4 Maksud Dan Tujuan Perusahaan

1. Mengembangkan sumber daya manusia/*brainware* secara optimal.
2. Menciptakan kreasi baru *software computer*.
3. Meningkatkan kemampuan ilmu pengetahuan dalam bidang teknologi informasi dan komunikasi serta ilmu komputer.
4. Meningkatkan keterampilan/*skills* pada bidang barang dan jasa bisnis telekomunikasi, *hardware* dan *software computer*.
5. Meningkatkan metode proses belajar mengajar dalam bidang Pendidikan.

6. Membuka usaha mandiri dengan merealisasikan lapangan kerja baru.

II.5 Struktur Organisasi Perusahaan

Struktur Organisasi CV. Cipta Daya Informatika



Gambar 2.1 Struktur Organisasi CV. Cipta Daya Informatika

II.6 Lingkup Pekerjaan

Peserta Kerja Praktek melaksanakan pekerjaan adalah di CV. Cipta Daya Inforatika dan dibimbing langsung oleh Bapak Yaya Suharya S.T., M.T. selaku direktur di perusahaann tersebut selama Kerja Praktek berlangsung. Tempat peserta Kerja Praktek melakukan pekerjaan adalah di bagian Keamanan Aplikasi website yang melakukan penelitian dan pendokumentasian aset kritis yang dianggap berisiko.

II.7 Deskripsi Pekerjaan

Secara garis besar, pekerjaan yang telah dilakukan dapat dibagi dalam 3 tahap yaitu:

1. Eksplorasi, serta pencarian baik metodologi pengembangan perangkat lunak maupun teknologi yang akan digunakan dalam teori penunjang Kerja Praktek.
2. Melakukan penelitian dengan cara memanfaatkan hasil eksplorasi menggunakan metodologi VAPT (*Vulnerability Assesment and Penetration testing*) yakni dengan beberapa tahap:
 - a. Penentuan Ruang Lingkup (*Scope*), pada penelitian ini telah ditentukan Ruang Lingkup (*Scope*) seperti apa yang tertera pada subbab Lingkup. Pengujian akan berfokus pada aplikasi website profil perusahaan milik CV. Cipta Daya Informatika.
 - b. Pengintaian Sistem (*Reconnaissance*), Pada tahap ini penyusun akan mencari informasi dasar target dan mengumpulkan informasi.
 - c. Pencarian Kerentanan Keamanan (*Vulnerability Detection*), Pada tahap ini penyusun akan melakukan proses pencarian kerentanan keamanan dengan menggunakan tools yaitu OWASP ZAP, nantinya digunakan untuk mendeteksi berbagai kerentanan dari Website CV. Cipta Daya Informatika.
 - d. Analisis Perencanaan dan Perencanaan Pengujian (*Information Analysis and Planning*), pada tahap ini penyusun akan menguraikan Kerentanan Keamanan yang telah dilakukan sebelumnya tentang kemungkinan-kemungkinan serangan yang dapat dilakukan.
 - e. *Penetration Testing*, Pada tahap ini penyusun akan melakukan simulasi penyerangan terhadap target yang diuji yaitu aplikasi website profil perusahaan CV. Cipta Daya Informatika.
 - f. Eksploitasi Kerentanan (*Privilege Escalation*) yaitu pemanfaatan kerentanan. Pemanfaatan yang dimaksud adalah untuk mengambil informasi dari web aplikasi CV. Cipta Daya Informatika.

- g. Penyusunan Laporan (*Reporting*), pada tahap ini penyusun menyusun laporan hasil dari pengujian yang sudah dilakukan pada web aplikasi profil perusahaan CV. Cipta Daya Informatika.
3. Pelaporan kegiatan dan hasil kerja praktek, baik kepada CV. Cipta Daya Informatika maupun kepada Program Studi Teknik Informatika Universitas Bale Bandung. Pelaporan ini dilakukan baik melalui presentasi maupun pembuatan laporan kerja praktek.

II.8 Jadwal Kerja

Kerja praktek dilaksanakan dari tanggal 14 Maret 2019 sampai dengan 14 April 2019 selama 4 minggu.

Secara umum, kegiatan yang dilakukan selama kerja praktek adalah sebagai berikut:

1. Minggu pertama:
 - Pengenalan lingkungan kerja.
 - Pemberian tugas dari perusahaan.
2. Minggu kedua:
 - Instalasi *tools* yang akan digunakan penelitian.
 - Eksplorasi cara penggunaan aplikasi.
3. Minggu ketiga:
 - Fase peninjauan website.
 - Fase pemeriksaan website.
 - Fase pengujian.
4. Minggu keempat:
 - Penyusunan laporan.

Adapun detail Kegiatan Kerja Praktek dalam skala mingguan dapat dilihat pada lampiran B. Secara keseluruhan, realisasi jadwal kerja sesuai dengan rencana yang telah disusun. Selama kerja praktek yang dilakukan oleh penyusun sendiri.

BAB III

PENGETAHUAN/TEORI PENUNJANG KERJA PRAKTEK

III.1 Teori Penunjang Kerja Praktek

Selama pelaksanaan kerja praktek di CV. Cipta Daya Informatika, peserta kerja praktek menggunakan pengetahuan yang diperoleh selama masa perkuliahan. Pengetahuan dan teori yang digunakan antara lain:

1. Keamanan Jaringan

Teori tentang keamanan Jaringan diperoleh di mata kuliah FTI317 Jaringan Komputer.

2. Konsep Pemrograman Internet

Teori tentang Pemrograman Internet yang diperoleh di mata kuliah FTI319 Pemrograman Internet.

3. Konsep Sistem Informasi

Teori tentang pembangunan sistem informasi yang baik diperoleh di mata kuliah FTI312 Sistem Informasi Manajemen.

III.2 Tinjauan Pustaka

Jurnal penelitian tentang audit keamanan informasi pada 66 sistem informasi milik pemerintah mengungkapkan bahwa web aplikasi yang dikelola pemerintah beberapa masih memanfaatkan *open source framework* yang keamanannya belum terjamin. Pencarian kerentanan keamanan dan rekapitulasi tingkat kerentanan menggunakan *tools software* Nessus. Hasil yang didapatkan adalah 37 web aplikasi menghasilkan tingkat *high*, 20 aplikasi web mendapat tingkat *medium*, dan 9 lainnya mendapat tingkat *low*. Jumlah tersebut terus meningkat seiring berjalannya waktu karena banyak instansi pemerintah yang mulai beralih menggunakan sistem informasi untuk pengelolaan data. Tujuan dari jurnal ini adalah untuk evaluasi untuk meminimalisir peluang terjadinya serangan pada web aplikasi yang dikelola oleh pemerintah (Anggrahito, 2018).

Penelitian tentang penggunaan *tools* Nessus untuk pencarian kerentanan keamanan dalam rangka pelengkapan dokumentasi sebagai bahan pengembangan web yang dilakukan oleh Lane Harrison dkk. dari Oak Ridge National Laboratory. Hasil dari *scanning vulnerability* menggunakan *tools* Nessus menunjukkan bahwa web *localhost* memiliki berbagai kerentanan keamanan. Namun dokumentasi tentang hasil yang didapatkan dirahasiakan karena dikhawatirkan dapat dimanfaatkan oleh penyerang (Harrison, Spahn, Iannacone, Downing, & Goodall, 2012).

Penelitian yang dilakukan Tashia Indah Nasiti mengemukakan bahwa Universitas Gadjah Mada memiliki websiste yang berisi data tentang nomor jaminan sosial, kartu kredit dan data sensitif lainnya. Oleh sebab itu dibutuhkan sebuah kegiatan untuk melakukan pengujian keamanan untuk mengevaluasi sistem keamanan pada website tersebut. Kegiatan ini menggunakan tools OWASP ZAP untuk mencari kerentanan keamanan. Terdapat kurang lebih sepuluh kerentanan keamanan yang ditemukan pada website tersebut, tujuan dari penelitian ini adalah mengevaluasi dan memastikan proses keamanan yang dilakukan oleh website tersebut sudah berjalan dengan baik (Nasiti, 2016).

Penelitian lain yang juga menggunakan metode VAPT adalah penelitian dari *Institute For Development and Research in Banking Technology*. Penelitian tersebut menjelaskan bahwa peningkatan konektivitas Sistem Informasi di seluruh dunia, juga meningkatkan ancaman terhadap integritas dan kerahasiaan data. Untuk menjaga keamanan dan meminimalisir ancaman yang ada, maka dilakukan pengujian kerentanan secara berkala pada aset yang dimilikinya. Penelitian ini menggunakan tools Net-Nirikshark 1.0 yang digunakan untuk menganalisis sistem keamanan yang sedang berjalan. Tools tersebut dapat mendeteksi kerentanan pada web aplikasi. Semua aspek Teknis dan Operasional Net-Nirikshark 1.0 dijelaskan dalam makalah ini bersama dengan Output dari sampel uji VAPT yang dilakukan di www.webscantest.com menggunakan Net-Nirikshark 1.0. metode ini berhasil mengeksploitasi kerentanan keamanan pada web tersebut (Shah & Mehtre, 2015).

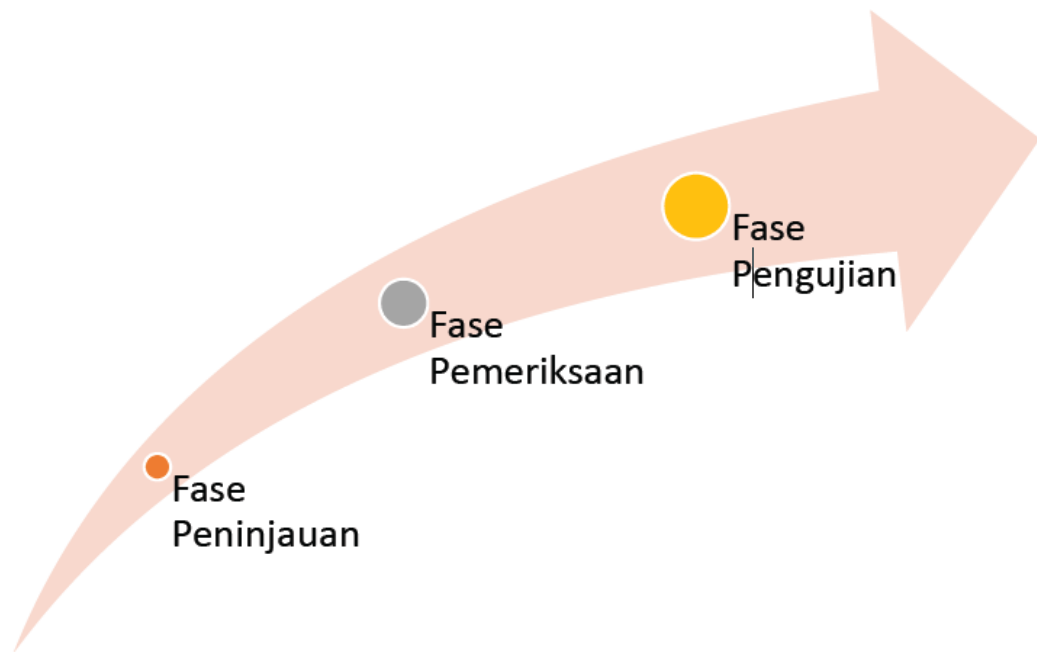
III.3 Dasar Teori

III.3.1 *Information Technology Security Assesment*

Information Technology Security Assesment atau dalam bahasa indonesia disebut sebagai penilaian teknologi informasi adalah sebuah penilaian yang berorientasi kepada risiko (Abdel-Aziz, 2011). Konsentrasi penilaian keamanan adalah terdapat pada celah keamanan yang dapat menimbulkan risiko beragam jika terjadi kegagalan proses teknologi informasi yang bisa terjadi karena beberapa faktor, seperti; faktor *hardware*, *software*, lingkungan bahkan serangan dari dalam maupun luar organisasi. Fokus analisis risiko adalah mengacu pada aset-aset yang menjalankan proses teknologi informasi (Sosonkin, 2005). Aset-aset tersebut perlu diperhatikan karena berperan penting dalam proses teknologi informasi yang berlangsung secara terus menerus.

Information technology security assessment adalah pengukuran untuk suatu model keamanan pada sebuah sistem di organisasi atau perusahaan (Miles, Rogers, Fuller, Hoagberg, & Dykstra, 2004). Model keamanan adalah cara bagaimana keamanan sistem informasi diimplementasikan pada sebuah organisasi. Pengukuran ini bertujuan untuk memberikan informasi tentang celah keamanan sistem informasi yang terdapat pada organisasi atau perusahaan tersebut yang kemudian hasil pengukuran akan digunakan untuk meningkatkan keamanan dari sistem informasi.

Security assessment bergantung kepada tiga fase penilaian utama yang saling terkait, yaitu fase peninjauan, fase pemeriksaan, fase pengujian. Tiga fase tersebut dapat secara akurat menilai teknologi, orang, dan proses yang merupakan bagian dari keamanan sebagaimana dijelaskan dibawah.



Gambar 3.1 Fase *Information Technology Security Assessment*

1. Fase Peninjauan

Fase peninjauan merupakan proses melakukan pengumpulan data dan informasi terkait sistem yang akan dilakukan proses *Assesment*. Proses ini dapat berupa wawancara kepada pihak organisasi. Informasi yang dikumpulkan mencakup evaluasi kebijakan, prosedur, aplikasi, dan jaringan untuk menemukan kerentanan. Fase ini dilakukan untuk memahami bagaimana sistem bekerja (Abdel-Aziz, 2011).

2. Fase Pemeriksaan

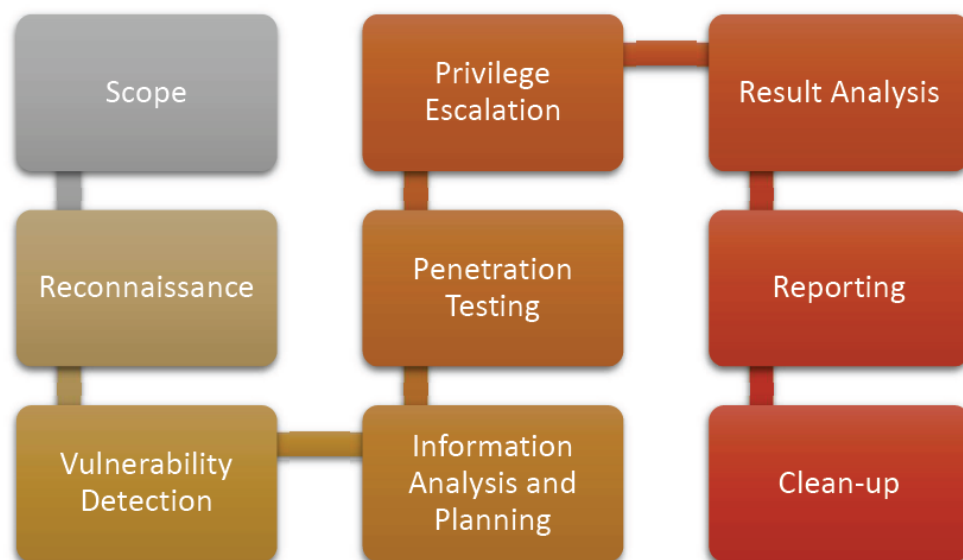
Fase pemeriksaan adalah proses teknis langsung yang melihat organisasi secara khusus dari tingkat sistem atau jaringan untuk mengidentifikasi kerentanan keamanan yang ada adalah sistem tersebut. Ini termasuk melakukan analisis teknis dari *firewall*, sistem deteksi, dan *router*. Ini juga mencakup pemindaian kerentanan jaringan pelanggan (Abdel-Aziz, 2011).

3. Fase Pengujian

Fase pengujian sering juga disebut *Penetration Testing* adalah proses di mana seseorang menirukan seorang musuh yang mencari kerentanan keamanan, yang memungkinkan masuk ke sistem atau jaringan (Abdel-Aziz, 2011).

III.3.2 VAPT (*Vulnerability Assessment and Penetration Testing*)

Sesuai dengan namanya, VAPT (*Vulnerability Assessment and Penetration Testing*) adalah kerangka kerja dalam melakukan uji keamanan terhadap suatu sistem web application (Goel & Mehte, 2015). VAPT merupakan gabungan dari dua aktivitas *Vulnerability Assessment* dan *Penetration Testing*. *Vulnerability Assessment* merupakan aktivitas pemindaian pada sebuah web aplikasi yang meliputi proses pemeriksaan sebuah kerentanan keamanan dari suatu web aplikasi tersebut. Sedangkan *Penetration Testing* adalah suatu proses percobaan atau simulasi penyerangan terhadap kerentanan yang terdapat pada web aplikasi dan mengeksploitasinya. tujuannya adalah untuk mendapat informasi penting pada sebuah web aplikasi. Proses pengujian menggunakan kerangka kerja VAPT terdapat 9 tahapan yang perlu dilakukan (Goel & Mehtre, 2015). Penjabaran mengenai 9 tahapan tersebut ada pada Gambar 3.1.



Gambar 3.2 Tahapan VAPT

Vulnerability assessment (penilaian kerentanan) adalah proses mengidentifikasi, mengukur, dan memprioritaskan (atau memberi peringkat) kerentanan dalam suatu sistem. Kegiatan *Vulnerability assessment* meliputi, *information technology systems, energy supply systems, water supply systems,*

transportation systems, dan *communication systems*. Penilaian tersebut dapat dilakukan oleh berbagai organisasi yang berbeda, dari organisasi kecil hingga besar. Kerentanan dari perspektif disaster management berarti menilai ancaman berdasarkan potensi bahaya terhadap lingkungan dan infrastruktur. Hal tersebut dapat dilakukan di bidang politik, sosial, ekonomi atau lingkungan.

Vulnerability assessment Penilaian biasanya dilakukan sesuai dengan langkah-langkah berikut:

1. Mendaftarkan aset dan kemampuan (sumber daya) dalam suatu sistem.
2. Menetapkan nilai terukur (atau setidaknya urutan tingkat) dan pentingnya sumber daya tersebut
3. Mengidentifikasi kerentanan atau potensi ancaman terhadap setiap sumber daya
4. Memitigasi atau menghilangkan kerentanan untuk sumber daya yang paling berharga

Vulnerability assessments memberikan gambaran terkait kelemahan keamanan dalam lingkungan organisasi, juga memberikan arahan dalam menilai risiko dan ancaman yang terus berkembang. Proses ini memberikan pemahaman mengenai aset organisasi, sistem keamanan dan risiko yang dihadapi, serta mengurangi kemungkinan adanya *cybercriminal* yang akan menyerang sistem perusahaan.

Vulnerability assessments dilakukan saat adanya temuan-temuan di dalam sistem atau kerentanan jaringan, proses penilaian mencakup penggunaan berbagai alat, pemindai, dan metodologi untuk mengidentifikasi kerentanan, ancaman, dan risiko.

Beberapa jenis vulnerability assessments adalah sebagai berikut:

1. *Network-based scans* digunakan untuk mengidentifikasi kemungkinan serangan keamanan jaringan. Jenis peninjauan ini juga dapat mendeteksi sistem yang rentan pada jaringan kabel atau nirkabel.

2. *Host-based scans* digunakan untuk mencari dan mengidentifikasi kerentanan di *server*, *workstation* atau *host* jaringan lainnya. Jenis peninjauan ini biasanya akan memeriksa *port* dan layanan yang mungkin terlihat oleh *Network-based scans*, tetapi penilaian ini menawarkan tingkat visibilitas yang lebih besar pada pengaturan konfigurasi dan menampung riwayat sistem yang telah diamati.
3. *Wireless network scans* pada jaringan Wi-Fi organisasi biasanya fokus pada titik-titik serangan infrastruktur jaringan nirkabel. Selain mengidentifikasi jalur akses yang terindikasi, pengamatan jaringan nirkabel juga dapat memvalidasi bahwa jaringan perusahaan terkonfigurasi dengan aman.
4. *Application scans*, dapat digunakan untuk menguji situs web dan mendeteksi kerentanan perangkat lunak serta kesalahan dalam konfigurasi aplikasi jaringan atau web.
5. *Database scans*, dapat digunakan untuk mengidentifikasi titik lemah dalam basis data sehingga dapat mencegah serangan berbahaya, seperti serangan injeksi SQL.

Vulnerability assessments sering kali menyertakan komponen pengujian penetrasi (*penetration testing*) untuk mengidentifikasi kerentanan dalam prosedur atau proses organisasi yang mungkin tidak terdeteksi dengan pengamatan jaringan atau sistem. Proses ini terkadang disebut sebagai *vulnerability assessments* atau *penetration testing*, atau VAPT. *Vulnerability assessments* bertujuan untuk menemukan risiko kerentanan dalam jaringan dan merekomendasikan mitigasi atau remediasi yang tepat untuk mengurangi atau menghilangkan risiko.

Organisasi harus menggunakan *vulnerability testing* secara berkala untuk memastikan keamanan jaringan, terutama ketika dilakukan perubahan, sebagai contoh, layanan yang ditambahkan, peralatan yang baru dipasang atau *port* yang terbuka. Sebaliknya, *penetration testing* melibatkan identifikasi kerentanan dalam suatu jaringan dengan mencoba mengeksploitasi untuk menyerang

sistem. Namun, *penetration testing* tidak hanya sebatas penilaian kerentanan saja. Meskipun dilakukan bersamaan dengan *vulnerability assessments*, tujuan utama *penetration testing* adalah untuk memeriksa apakah kerentanan benar-benar ada dan untuk membuktikan bahwa mengeksploitasi dapat merusak aplikasi atau jaringan.

Sementara penilaian kerentanan biasanya otomatis untuk mencakup berbagai kerentanan yang belum ditampung, *penetration testing* umumnya menggabungkan teknik otomatis dan manual untuk membantu penguji menyelidiki lebih jauh ke dalam kerentanan dan mengeksploitasinya untuk mendapatkan akses jaringan ke dalam lingkungan yang terkendali.

Penetration Testing (pentest) adalah suatu kegiatan dimana seseorang mencoba mensimulasikan serangan yang bisa dilakukan terhadap jaringan organisasi/perusahaan tertentu untuk menemukan kelemahan yang ada pada sistem jaringan tersebut. Orang yang melakukan kegiatan ini disebut *penetration tester* (pentester). *Penetration Testing* mempunyai standar resmi sebagai acuan dalam pelaksanaannya. Standar ini bisa dilihat di <http://pentest-standard.org>.

Perusahaan-perusahaan besar yang menyimpan data-data sensitif (seperti Bank) tentu tidak ingin jaringannya dibobol oleh orang tidak bertanggung jawab yang kemudian bisa mengambil alih kontrol jaringan dan menimbulkan kerugian yang sangat besar. Oleh karena alasan itu perusahaan menginvestasikan dana untuk memperkuat sistem jaringannya. Salah satu metode paling efektif adalah melakukan pentest. Dengan melakukan pentest, celah-celah keamanan yang ada dapat diketahui dan dengan demikian dapat diperbaiki secepatnya. Seorang pentester mensimulasikan serangan yang dapat dilakukan, menjelaskan resiko yang bisa terjadi, dan melakukan perbaikan sistem tanpa merusak infrastruktur jaringan perusahaan tersebut.

Penetration Testing memiliki standar (PTES) yang digunakan sebagai acuan dalam pelaksanaannya yang dibagi ke dalam beberapa tahap:

1. *Pre-engagement Interactions*

Tahap dimana seorang pentester menjelaskan kegiatan pentest yang akan dilakukan kepada client (perusahaan). Disini seorang pentester harus bisa menjelaskan kegiatan-kegiatan yang akan dilakukan dan tujuan akhir yang akan dicapai.

2. *Intelligence Gathering*

Tahap dimana seorang pentester berusaha mengumpulkan sebanyak mungkin informasi mengenai perusahaan target yang bisa didapatkan dengan berbagai metode dan berbagai media. Hal yang perlu dijadikan dasar dalam pengumpulan informasi adalah: karakteristik sistem jaringan, cara kerja sistem jaringan, dan metode serangan yang bisa digunakan.

3. *Threat Modeling*

Tahap dimana seorang pentester mencari celah keamanan (*vulnerabilities*) berdasarkan informasi yang berhasil dikumpulkan pada tahap sebelumnya. Pada tahap ini seorang pentester tidak hanya mencari celah keamanan, tetapi juga menentukan celah yang paling efektif untuk digunakan.

4. *Vulnerability Analysis*

Tahap dimana seorang pentester mengkombinasikan informasi mengenai celah keamanan yang ada dengan metode serangan yang bisa dilakukan untuk melakukan serangan yang paling efektif.

5. *Exploitation*

Tahap dimana seorang pentester melakukan serangan pada target. Walaupun demikian tahap ini kebanyakan dilakukan dengan metode *brute force* tanpa memiliki unsur presisi. Seorang pentester profesional hanya akan melakukan *exploitation* ketika dia sudah mengetahui secara pasti apakah serangan yang dilakukan akan berhasil atau tidak. Namun tentu saja ada kemungkinan tidak terduga dalam sistem keamanan target. Walaupun begitu, sebelum melakukan

serangan, pentester harus tahu kalau target mempunyai celah keamanan yang bisa digunakan. Melakukan serangan secara membabi-buta dan berharap sukses bukanlah metode yang produktif. Seorang pentester profesional selalu menyempurnakan analisisnya terlebih dahulu sebelum melakukan serangan yang efektif.

6. *Post Exploitation*

Tahap dimana seorang pentester berhasil masuk ke dalam sistem jaringan target dan kemudian melakukan analisis infrastruktur yang ada. Pada tahap ini seorang pentester mempelajari bagian-bagian di dalam sistem dan menentukan bagian yang paling *critical* bagi target (perusahaan). Disini seorang pentester harus bisa menghubungkan semua bagian-bagian sistem yang ada untuk menjelaskan dampak serangan/kerugian yang paling besar yang bisa terjadi pada target (perusahaan).

7. *Reporting*

Reporting adalah bagian paling penting dalam kegiatan pentest. Seorang pentester menggunakan report (laporan) untuk menjelaskan pada perusahaan mengenai pentesting yang dilakukan seperti: apa yang dilakukan, bagaimana cara melakukannya, resiko yang bisa terjadi dan yang paling utama adalah cara untuk memperbaiki sistemnya.

Ada dua jenis tipe pentest, yaitu: *overt* dan *covert*. *Overt* pentest dilakukan dengan sepengetahuan perusahaan. *Covert pentest* dilakukan tanpa sepengetahuan perusahaan. Kedua tipe pentest ini memiliki kelebihan dan kelemahan satu sama lain.

1. *Overt Penetration Testing*

Pada *overt* pentest, seorang pentester bekerja bersama dengan tim IT perusahaan untuk mencari sebanyak mungkin celah keamanan yang ada. Salah satu kelebihan adalah pentester mengetahui informasi sistem jaringan yang ada secara detail dan dapat melakukan serangan tanpa khawatir akan di-blok.

Salah satu kelemahannya adalah tidak bisa menguji respon dari tim IT perusahaan jika terjadi serangan sebenarnya. Saat jumlah waktu dalam kegiatan pentest dibatasi, akan lebih efektif menggunakan tipe *overt*.

2. *Covert Penetration Testing*

Pada *covert* pentest, seorang pentester melakukan kegiatan pentest tanpa sepengetahuan perusahaan. Artinya tes ini digunakan untuk menguji respon dari tim IT perusahaan jika terjadi serangan sebenarnya. *Covert test* membutuhkan waktu yang lebih lama dan skill yang lebih besar daripada *overt test*. Kebanyakan pentester profesional lebih merekomendasikan *covert test* daripada *overt test* karena benar-benar mensimulasikan serangan yang bisa terjadi. Pada *covert test*, seorang pentester tidak akan berusaha mencari sebanyak mungkin celah keamanan, tetapi hanya akan mencari jalan termudah untuk masuk ke dalam sistem, tanpa terdeteksi.

III.3.3 Website

Website atau situs adalah kumpulan halaman yang menampilkan informasi data teks, data gambar diam atau gerak, data animasi, suara, video dan atau gabungan dari semuanya, baik yang bersifat statis maupun dinamis yang membentuk satu rangkaian bangunan yang saling terkait dimana masing-masing dihubungkan dengan jaringan-jaringan halaman (*hyperlink*).

Bersifat statis apabila isi informasi website tetap, jarang berubah, dan isi informasinya searah hanya dari pemilik website. Bersifat dinamis apabila isi informasi website selalu berubah-ubah, dan isi informasinya interaktif dua arah berasal dari pemilik serta pengguna website. Contoh website statis adalah berisi profil perusahaan, sedangkan website dinamis adalah seperti media sosial (Facebook, Instagram, Twitter dll), portal berita (detik, cnnindonesia, tribunnews, dll), forum diskusi, dan e-commerce (bukalapak, tokopedia). Dalam sisi pengembangannya, website statis hanya bisa diupdate oleh pemiliknya saja, sedangkan website dinamis bisa diupdate oleh pengguna maupun pemilik. Untuk

menyediakan sebuah website, maka harus tersedia unsur-unsur penunjangnya, adalah sebagai berikut:

1. *Domain Name*

Domain Name atau bisa disebut dengan Nama domain atau URL (*Uniform Resource Locator*) adalah alamat unik di dunia internet yang digunakan untuk mengidentifikasi sebuah website, atau dengan kata lain *domain name* adalah alamat yang digunakan untuk menemukan sebuah website pada dunia internet.

Nama domain diperjual belikan secara bebas di internet oleh perusahaan penyedia pendaftaran *domain name* dengan status sewa tahunan. Setelah Nama Domain itu terbeli di salah satu penyedia jasa pendaftaran, maka pengguna disediakan sebuah kontrol panel untuk administrasinya. Jika pengguna lupa/tidak memperpanjang masa sewanya, maka nama domain itu akan di lepas lagi ketersediaannya untuk umum.

Nama domain sendiri mempunyai identifikasi ekstensi/akhiran sesuai dengan kepentingan dan lokasi keberadaan website tersebut. Contoh nama domain ber-ekstensi internasional adalah com, net, org, info, biz, name, ws. Contoh nama domain ber-ekstensi lokasi Negara Indonesia adalah:

- .id : Ditujukan untuk umum yang melakukan kegiatannya di internet.
- .co.id : Untuk Badan Usaha/bisnis yang mempunyai badan hukum sah.
- .ac.id : Untuk Lembaga Pendidikan setara sekolah tinggi/universitas.
- .go.id : Khusus untuk Lembaga Pemerintahan Republik Indonesia.
- .mil.id : Khusus untuk Lembaga Militer Republik Indonesia.
- .or.id : Untuk segala macam organisasi.
- .sch.id : Untuk Lembaga Pendidikan setara sekolah dasar, menengah, atas, dan kejuruan.
- .web.id : Ditujukan untuk umum yang melakukan kegiatannya di internet.
- .desa.id : Ditujukan untuk pemerintahan desa.

2. *Web Hosting*

Web Hosting adalah ruangan (*space*) yang terdapat dalam *harddisk* komputer *server*, sebagai tempat menyimpan berbagai data, file-file, gambar, video, audio, data email, statistik, database dan lain sebagainya yang akan ditampilkan di website. Komputer *server* ini harus *online* 24 jam tersimpan di sebuah *data center* yang terkoneksi ke dunia internet. Besarnya data yang bisa dimasukkan tergantung dari besarnya paket *web hosting* yang disewa di perusahaan penyedia *web hosting*. Semakin besar *web hosting* semakin besar pula beragam data yang dapat disimpan.

Web Hosting juga diperoleh dengan menyewa. Pengguna akan memperoleh kontrol panel yang terproteksi dengan *username* dan *password* untuk administrasi websitenya. Besarnya hosting ditentukan ruangan *harddisk* dengan ukuran MB (*Mega Byte*) atau GB (*Giga Byte*). Lama penyewaan *web hosting* rata-rata dihitung per bulan atau tahun. Penyewaan hosting dilakukan dari perusahaan-perusahaan penyewa *web hosting* yang banyak dijumpai baik di Indonesia maupun Luar Negeri. Lokasi peletakan pusat data (*data center*) web hosting bermacam-macam. Ada yang di Jakarta, Singapore, Inggris, Amerika, dengan harga sewa bervariasi.

3. Bahasa Program (*Web program*) beserta Desain Website (*Web Design*).

Web Program adalah bahasa yang digunakan untuk menerjemahkan setiap perintah dalam website yang pada saat diakses. Jenis bahasa program sangat menentukan statis, dinamis atau interaktifnya sebuah website. Semakin banyak ragam bahasa program yang digunakan maka akan terlihat website semakin dinamis, dan interaktif serta terlihat bagus.

Beragam bahasa program saat ini telah hadir untuk mendukung kualitas website. Jenis jenis bahasa program yang banyak dipakai para desainer website antara lain HTML, ASP, PHP, JSP, Java Scripts, Java applets, XML, Ajax dsb. Bahasa dasar yang dipakai setiap situs adalah HTML sedangkan PHP, ASP, JSP dan

lainnya merupakan bahasa pendukung yang bertindak sebagai pengatur dinamis, dan interaktifnya situs.

Bahasa-bahasa program tersebut produksi informasi dan fungsi-fungsi tertentu di website. Supaya informasi dan fungsi tersebut enak dilihat oleh pengguna internet maka perlu membungkus bahasa program dengan desain grafis yang indah dan fungsional mudah dioperasikan. Desain website menentukan kualitas dan keindahan sebuah website. Desain sangat berpengaruh kepada penilaian pengunjung akan bagus tidaknya sebuah website dan tampil responsif di semua alat (komputer/laptop/smartphone/tablet). Untuk membuat website biasanya dapat dilakukan sendiri atau menyewa jasa website *designer*.

Perlu diketahui bahwa kualitas tampilan website sangat ditentukan oleh kualitas *designer*. Semakin banyak penguasaan *web designer* tentang beragam program/perangkat lunak pendukung pembuatan website maka akan dihasilkan website yang semakin berkualitas, demikian pula sebaliknya. Jasa *web designer* ini yang umumnya memerlukan biaya yang tertinggi dari seluruh biaya pembangunan situs dan semuanya itu tergantung kualitas *designer*.

4. *Content Management System*

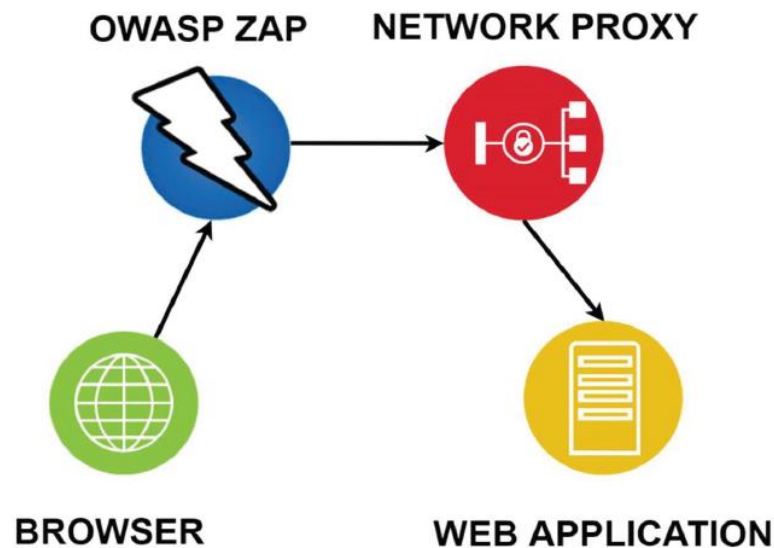
Pembuatan website secara modern sudah dipermudah dengan kehadiran program CMS (*Content Management System*). Program tersebut mampu menggabungkan web program dan web design jadi satu. Penggunaannya cukup diinstal melalui kontrol panel website ataupun manual. Contoh program CMS adalah WordPress, Drupal, Joomla, dll. CMS dibangun oleh para profesional web programmer dan web designer untuk mempermudah orang awam memiliki website. Tutorial website CMS bisa ditemukan di internet dan toko-toko buku.

III.3.4 OWASP ZAP (*Open Web Application Security Project Zed Attack Proxy*)



Gambar 3.3 Logo OWASP ZAP

OWASP (*Open Web Application Security Project*) merupakan organisasi atau komunitas terbuka yang didirikan pada tanggal 1 Desember 2001 berfokus pada bidang keamanan aplikasi. OWASP tidak berafiliasi dengan perusahaan manapun demi kebebasan dari tekanan dan mampu bersifat objektif dalam memberikan informasi mengenai keamanan yang erat kaitannya dengan dunia teknologi informasi. Sedangkan ZAP (*Zed Attack Proxy*) adalah aplikasi *open source* untuk melakukan pencarian kerentanan pada website dengan cara *scanner* otomatis pada aplikasi ZAP tersebut. ZAP dirancang khusus untuk pengujian aplikasi web. Pada intinya, ZAP adalah apa yang dikenal sebagai “*Proxy Man-in-the-Middle*”. Ini berdiri antara tester browser dan aplikasi web sehingga dapat mencegat dan memeriksa pesan yang akan dikirim antara browser dan aplikasi web, memodifikasi isi jika diperlukan, dan kemudian meneruskan paket-paketnya ke tujuan. Seperti Gambar..., jika ada jaringan lain *proxy* yang sudah digunakan, seperti di banyak lingkungan perusahaan, ZAP dapat dikonfirmasi untuk terhubung ke *proxy*.



Gambar 3.4 Skema OWASP ZAP

Sebagai salah satu bukti dari komitmen mereka, OWASP telah menyediakan beberapa dokumen untuk membantu para developer dalam membuat website dan aplikasi yang aman. Berikut ini 5 dokumen yang sering disebut sebagai panduan penting untuk para developer.

1. *OWASP Developer Guide*

Panduan ini dikhususkan untuk *developer* yang merupakan salah satu dokumen pertama yang harus Anda download jika Anda ingin mempunyai website dan aplikasi yang aman. Pertama kali dirilis sudah lebih dari 15 tahun lalu, mereka banyak melakukan revisi dari tahun 2014 supaya panduannya sesuai untuk saat ini. *Guide* tersebut dibuat supaya para *developer* dapat membangun website atau *software* untuk organisasi mereka dengan memakai *coding* yang mempunyai sistem yang aman. Guide tersebut berisikan prinsip-prinsip yang harus anda ikuti dalam proses *coding*.

2. *OWASP ASVS (Application Security Verification Standard)*

ASVS merupakan sebuah daftar persyaratan untuk memberi tahu kepada para *developer* apakah sebuah aplikasi itu telah aman untuk dipakai oleh organisasi, vendor, dan customer. ASVS sudah dipisahkan ke beberapa level untuk

menjelaskan dengan lebih detail dari berbagai jenis aplikasi dan *software*. Ada tiga level yang mereka jelaskan yaitu *opportunistic level* (*software* umum), *standard level* (aplikasi yang mengandung data sensitif), dan *advanced level* (berbagai aplikasi seperti aplikasi rumah sakit, *software* dan aplikasi bank, situs dan *software* pemerintahan, dan lainnya). ASVS bisa dibilang merupakan resource untuk keamanan website karena mereka menjelaskan langkah demi langkah.

3. *Security Knowledge Framework*

Security Knowledge Framework merupakan sebuah *tool* yang di-rancang untuk membantu *developer* membuat *software* yang aman. *Framework* ini dibuat berdasarkan standard ASVS sehingga *developer* dapat dengan mudah mengerti serta mengimplementasikan persyaratan keamanannya.

4. *Developer Cheat Sheet Series*

Organisasi ini meminta bantuan dari berbagai pakar keamanan website di seluruh dunia untuk membuat *guide* yang lengkap, juga membahas berbagai kelemahan, dan *protocol* keamanan, serta bagaimana mereka ada di berbagai bahasa programming terkenal. *Cheat sheet* ini di rancang daengan bentuk *bullet points* jadi *developer* dapat mengerti *best practices* kemanan serta syarat-syaratnya dengan lebih mudah.

5. OWASP Top 10

OWASP Top 10 merupakan sebuah panduan bagi para *developers* dan *security team* mengenai kelemahan-kelemahan pada web aplikasi yang rentan diserang dan harus segera disiasati. Berbagai kelemahan ini memudahkan penyusup untuk menanamkan *malware*, mencuri data, atau mengambil alih sepenuhnya situs atau komputer Anda. Dokumen ini biasanya diupdate secara rutin oleh sebuah tim yang terdiri dari berbagai pakar keamanan website di seluruh dunia. Mereka merekomendasikan berbagai perusahaan untuk memperhatikan kesepuluh masalah yang ada pada dokumen tersebut untuk mengamankan website dan data

mereka dari ancaman penyusup. Berikut ini penjelasan singkat dari kesepuluh ancaman keamanan situs yang ada pada OWASP Top 10 tahun 2017:

a. *Injection*

Serangan ini biasa terjadi jika ada data yang tidak terpercaya dikirimkan ke sebuah *code interpreter* melewati sebuah formulir input atau cara input data ke situs lainnya. Misalnya, seorang penyusup bisa memasukkan kode database SQL melewati sebuah formulir yang sebenarnya hanya meminta data *plaintext*. Jika formulir input tersebut tidak diamankan dengan baik maka kode SQL nya bisa dijalankan. Ini merupakan contoh serangan *injection* SQL. Nah, serangan *injection* ini dapat dicegah dengan cara memvalidasi dan membersihkan data yang telah dimasukkan oleh *user*. Validasi tersebut adalah menolak berbagai data yang terlihat mencurigakan. Membersihkan data berarti menghapus semua data mencurigakan tersebut. Selain itu, admin *database* juga dapat meminimalkan jumlah informasi yang mungkin telah *terexpose* ke serangan *injection*.

b. *Broken Authentication*

Kelemahan di sistem login bisa memberikan *hacker* akses ke akun *user*. Selain itu, mereka bisa juga menguasai seluruh sistem dengan meng-*hack* akun admin. Untuk mengetahui kelemahan *authentication*, Anda bisa memakai 2-*factor authentication* (2FA).

c. *Sensitive Data Exposure*

Jika sebuah website menyimpan berbagai data *sensitive* user-nya, tentu akan berbahaya jika mereka tidak menjaga keamanannya. Untuk mengurangi kemungkinan resiko pencurian data, Anda dapat mengenskripsi data-data sensitifnya. *Developer* juga harus memastikan bahwa situs tidak menyimpan data-data *sensitive* yang tidak dibutuhkan.

d. *XML External Entities*

Ini merupakan serangan ke website dan aplikasi yang menganalisa input XML. Input ini dapat mereferensikan *entity external* untuk dapat mengetahui

kelemahan yang ada pada input XMLnya. *Entiti external* tersebut biasanya berupa unit penyimpanan, seperti *hard drive*. Analisa input XML dapat dibuat seakan-akan mereka mengirimkan data ke *entity external* yang tidak dipercaya, dimana mereka dapat mengirim data-data *sensitive* ke *hacker* langsung. Cara terbaik untuk mengatasi hal ini adalah dengan mempunyai web aplikasi yang memiliki jenis data yang tidak terlalu kompleks.

e. *Broken Access Control*

Access control ini mengacu ke sistem control yang mengakses informasi dan fungsionalitasnya. *Access control* yang bermasalah memungkinkan *hacker* untuk melewati proses *autorisasi* serta melakukan hal-hal yang biasanya hanya dapat dilakukan oleh admin.

f. *Security Misconfiguration*

Kesalahan konfigurasi keamanan merupakan kelemahan yang paling kerap terjadi di antara kelemahan lain di daftar ini. Biasanya itu terjadi jika Anda hanya memakai *default* konfigurasi tanpa melihat kebutuhan dari website.

g. *Cross Site Scripting*

Kelemahan ini akan terjadi pada web aplikasi jika web aplikasi mengizinkan *user* untuk menambahkan kode *custom* ke sebuah path URL atau ke situs yang dilihat oleh *user* lain. Kelemahan ini biasanya dimanfaatkan untuk menjalankan kode *JavaScript* berbahaya pada browser korban. Misalnya, jika seorang *hacker* mengirim *email* ke korban dengan memakai nama bank tertentu dan menyertakan link ke situs bank tersebut, mereka bisa saja menaruh kode *JavaScript* berbahaya di dalamnya. Jika perlindungan website bank kurang baik, nasabah Anda akan menjadi korbannya.

h. *Insecure Deserialization*

Untuk mengerti masalah dari kelemahan ini, kita harus mengetahui dulu apa pengertian dari serialisasi dan deserialisasi. Serialisasi merupakan proses dimana objek diambil dari kode aplikasi lalu di-*convert* ke format lain sehingga dapat digunakan untuk keperluan lain, contohnya menyimpan data

ke sebuah *disk*. Deserialisasi berarti sebaliknya, meng-*convert* sebuah data yang sudah diserialisasi kembali objek yang dipakai oleh aplikasinya. *Insecure deserialization* atau deserialisasi yang kurang aman dapat diserang dengan memanfaatkan data dari sumber yang tidak dipercaya. Ini dapat menyebabkan terjadinya serangan DDoS. Untuk mencegah hal ini, Anda perlu melarang deserialisasi pada data yang tidak dipercaya.

i. *Using Components With Known Vulnerabilities*

Kebanyakan web *developer* memakai komponen semacam *libraries* dan *frameworks* di web aplikasi mereka. Komponen-komponen ini merupakan kumpulan *software* yang membantu *developers* untuk bekerja dengan lebih efisien. Beberapa *hacker* biasanya mencari kelemahan yang ada pada komponen-komponen tersebut supaya mereka dapat melakukan serangan. Oleh karena itulah, *developer* harus selalu memastikan bahwa komponen-komponen tersebut sudah diupdate supaya tetap aman.

j. *Insufficient Logging and Monitoring*

Kebanyakan web aplikasi tidak mengambil langkah selanjutnya untuk mendeteksi penembusan data. Rata-rata orang baru menyadarinya jika terjadi penembusan di situs mereka setelah 200 hari. Ini tentunya memberikan *hacker* banyak waktu untuk melakukan penyerangan. OWASP telah merekomendasikan *developer* untuk mengimplementasi *logging* dan monitoring serta rencana *response insiden* supaya mereka mengetahui jika ada penyerangan yang terjadi pada aplikasi mereka.

III.3.5 Browser

Browser adalah aplikasi perangkat lunak digunakan untuk mencari, mengambil dan juga menampilkan informasi di World Wide Web, termasuk halaman Web, gambar, video dan file lainnya. Sebagai model klien/server, browser ini jangka klien pada komputer yang kontak server Web dan permintaan informasi. Web server mengirimkan informasi kembali ke browser Web yang menampilkan hasilnya pada komputer atau internet perangkat yang mendukung browser.

Contohnya adalah Microsoft Internet Explorer, Google Chrome, Apple Safari dan Opera, Netscape Navigator, Mozilla Firefox.



Gambar 3.5 Contoh Beberapa Browser

Penjelajah web pertama bernama bernama WorldWideWeb (tanpa spasi) diciptakan oleh Tim *Berners-Lee*. Nama penjelajah tersebut kemudian diubah menjadi *Nexus*. Pada tahun 1993, *Marc Andreessen* melakukan inovasi penjelajah web dengan merilis Mosaic (kemudian Netscape), "perampan web populer pertama di dunia", yang membuat sistem Internet lebih mudah digunakan dan dapat diakses oleh lebih banyak orang. Penjelajah web Andreessen memicu ledakan popularitas di Internet pada tahun 1990-an. Andreessen, pemimpin tim Mosaic di NCSA, segera mendirikan perusahaan sendiri, bernama Netscape, dan merilis Mosaic-yang kemudian mempengaruhi Netscape Navigator pada tahun 1994, yang dengan cepat menjadi penjelajah yang paling populer di dunia, dengan menguasai 90% dari seluruh penggunaan penjelajah web di dunia.

Microsoft menanggapinya dengan menciptakan Internet Explorer pada tahun 1995, juga sangat dipengaruhi oleh Mosaic, dan memulai perang penjelajah web pertama dalam industri Internet. Dibundel dengan Windows, Internet Explorer

memperoleh dominasi di pasar penjelajah web. Raihan penggunaan Internet Explorer memuncak hingga lebih dari 95% pengguna pada tahun 2002.

Opera memulai debutnya pada tahun 1996, meskipun belum pernah mencapai penggunaan secara luas, memiliki kurang dari 2% pangsa penggunaan browser pada Februari 2012 menurut Net Applications. Versi mini Opera (Opera Mini) memberikan tambahan pangsa pasar, pada bulan April 2011 sebesar 1,1% pada penggunaan penjelajah web secara keseluruhan, tetapi terfokus pada pasar ponsel yang tumbuh cepat. Opera Mini terinstal pada lebih dari 40 juta ponsel. Opera Mini ini juga tersedia di beberapa sistem lain, termasuk konsol video game Nintendo Wii.

Pada tahun 1998, Netscape meluncurkan apa yang kemudian akan menjadi Mozilla Foundation dalam upaya menghasilkan browser kompetitif dengan menggunakan model perangkat lunak sumber terbuka. Penjelajah web tersebut akhirnya akan berkembang menjadi Firefox. Hingga Agustus 2011, Firefox memiliki pangsa pasar 28% penjelajah web dunia. Dilanjut Safari yang merilis versi beta pada Januari 2003. Hingga April 2011, Safari memiliki pangsa dominan untuk penjelajah web berbasis Apple, dan menguasai lebih dari 7% dari pasar penjelajah web dunia.

Pendatang baru di pasar penjelajah web adalah Google Chrome. Pertama kali dirilis pada bulan September 2008, popularitas Chrome meningkat secara signifikan dari tahun ke tahun, dengan menggandakan pangsa penggunaannya dari 8% menjadi 16% pada bulan Agustus 2011. Peningkatan ini berbanding terbalik dengan popularitas Internet Explorer yang cenderung menurun dari bulan ke bulan. Pada Desember 2011, Google Chrome menyalip Internet Explorer 8 sebagai web browser yang paling banyak digunakan namun tetap lebih rendah jika dibandingkan dengan jumlah gabungan semua versi Internet Explorer yang digunakan.

Penjelajah web bisa dibedakan lewat fitur-fitur yang disediakan. Penjelajah modern dan halaman web biasanya menggunakan banyak fitur dan teknik yang tidak ada pada masa-masa awal web. Disebabkan adanya perang penjelajah web, fitur-fitur web dan penjelajah web semakin cepat dikembangkan.

Berikut daftar beberapa elemen dan fitur-fitur tersebut:

- ActiveX
- Autocompletion (Pengisian otomatis) URL dan formulir data
- Markah buku untuk mengikuti lokasi yang sering diakses
- Cascading Style Sheets (CSS)
- Kuki yang membolehkan sebuah website untuk mengetahui seorang pengguna lama
- Tembolok web - Halaman web "disimpan" dalam memori ketika penyusun membukanya agar dapat diakses lagi walaupun sedang luring
- Digital certificate (Sertifikat Digital)
- Pemuatan gambar menggunakan format gambar yang sudah terkenal seperti GIF, PNG, JPEG, SVG
- Flash
- Favicon
- Font, ukuran, warna
- Formulir untuk mengirimkan informasi
- Frame dan Iframes
- Gambar
- Integrasi dengan aplikasi desktop lainnya
- Offline browsing (Penjelajah Tertutup) terhadap isi web yang sudah disimpan terlebih dahulu
- Java applet
- JavaScript untuk isi yang lebih dinamis
- Pengaturan pengunduhan
- Penyaringan iklan (Ad filtering)
- Plug-in

- Sejarah kunjungan ke halaman-halaman web terakhir
- Session management
- Tabbed browsing
- Tabel
- XHTML dan XML
- DHTML
- HTTPS

III.3.6 Sublime Text



Gambar 3.6 Logo Sublime Text

Sublime Text adalah aplikasi editor untuk kode dan teks yang dapat berjalan di berbagai platform *operating system* dengan menggunakan teknologi *Python* API. Terciptanya aplikasi ini terinspirasi dari aplikasi Vim, Aplikasi ini sangatlah fleksibel dan *powerfull*. Fungsionalitas dari aplikasi ini dapat dikembangkan dengan menggunakan *sublime-packages*. Sublime Text bukanlah aplikasi *opensource* dan juga aplikasi yang dapat digunakan dan didapatkan secara gratis, akan tetapi beberapa fitur pengembangan fungsionalitas (*packages*) dari aplikasi ini merupakan hasil dari temuan dan mendapat dukungan penuh dari komunitas serta memiliki linsensi aplikasi gratis.

Sublime Text mendukung berbagai bahasa pemrograman dan mampu menyajikan fitur *syntax highlight* hampir di semua bahasa pemrograman yang didukung ataupun dikembangkan oleh komunitas seperti: C, C++, C#, CSS, D, Dylan, Erlang, HTML, Groovy, Haskell, Java, JavaScript, LaTeX, Lisp, Lua, Markdown, MATLAB, OCaml, Perl, PHP, Python, R, Ruby, SQL, TCL, Textile and XML. Biasanya bagi bahasa pemrograman yang didukung ataupun belum terdukung secara default dapat lebih dimaksimalkan atau didukung dengan menggunakan *add-ons* yang bisa didownload sesuai kebutuhan user.

Berikut beberapa fitur yang diunggulkan dari aplikasi Sublime Text:

- *Goto Anything*
Fitur yang sangat membantu dalam membuka file ataupun menjelajahi isi dari file hanya dengan beberapa *keystrokes*.
- *Multiple Selections*
Fitur ini memungkinkan user untuk mengubah secara interaktif banyak baris sekaligus, mengubah nama variabel dengan mudah, dan memanipulasi file lebih cepat dari sebelumnya.
- *Command Palette*
Dengan hanya beberapa *keystrokes*, user dapat dengan cepat mencari fungsi yang diinginkan, tanpa harus menavigasi melalui menu.
- *Distraction Free Mode*
Bila *user* memerlukan fokus penuh pada aplikasi ini, fitur ini dapat membantu user dengan memberikan tampilan layar penuh.
- *Split Editing*
Dapatkan hasil yang maksimal dari monitor layar lebar dengan dukungan editing perpecahan. Mengedit sisi file dengan sisi, atau mengedit dua lokasi di satu file. Anda dapat mengedit dengan banyak baris dan kolom yang user inginkan.
- *Instant Project Switch*

Menangkap semua file yang dimasukkan kedalam *project* pada aplikasi ini. Terintegrasi dengan fitur *Goto Anything* untuk menjelajahi semua file yang ada ataupun untuk beralih ke file dalam *project* lainnya dengan cepat.

- *Plugin API*

Dilengkapi dengan *plugin API* berbasis Phyton sehingga membuat aplikasi ini sangat tangguh.

- *Customize Anything*

Aplikasi ini memberikan *user* fleksibilitas dalam hal pengaturan fungsional dalam aplikasi ini.

- *Cross Platform*

Aplikasi ini dapat berjalan hampir disemua *operating system* modern seperti Windows, OS X, dan Linux *based op*.

III.3.7 Jaringan Internet

Internet (Singkatan dari *interconnected network*) adalah sistem jaringan komputer yang saling terhubung secara global dengan menggunakan paket protokol internet (TCP/IP) untuk menghubungkan perangkat di seluruh dunia. Ini adalah jaringan dari jaringan yang terdiri dari jaringan *privat*, *publik*, akademik, bisnis, dan pemerintah lokal ke lingkup global, dihubungkan oleh beragam teknologi elektronik, nirkabel, dan jaringan optik. Internet membawa beragam sumber daya dan layanan informasi, seperti dokumen hiperteks yang saling terkait dan aplikasi World Wide Web (WWW), surat elektronik, telepon, dan berbagi berkas.

Asal usul Internet berasal dari penelitian yang ditugaskan oleh pemerintah federal Amerika Serikat pada tahun 1960-an untuk membangun komunikasi yang kuat dan toleran terhadap kesalahan dengan jaringan komputer. Jaringan prekursor utama, ARPANET, awalnya berfungsi sebagai tulang punggung untuk interkoneksi jaringan akademik dan militer regional pada 1980-an. Pendanaan *National Science Foundation Network* sebagai tulang punggung baru pada 1980-an, serta pendanaan swasta untuk ekstensi komersial lainnya, mendorong

partisipasi dunia dalam pengembangan teknologi jaringan baru, dan penggabungan banyak jaringan.

Keterkaitan jaringan komersial dan perusahaan pada awal 1990-an menandai dimulainya transisi ke Internet modern, dan menghasilkan pertumbuhan eksponensial yang berkelanjutan ketika generasi komputer institusional, personal, dan seluler terhubung ke jaringan. Meskipun Internet banyak digunakan oleh akademisi sejak 1980-an, komersialisasi memasukkan layanan dan teknologinya ke dalam hampir setiap aspek kehidupan modern.

Sebagian besar media komunikasi tradisional, termasuk telepon, radio, televisi, surat kertas dan surat kabar dibentuk ulang, didefinisikan ulang, atau bahkan dilewati oleh Internet, sehingga melahirkan layanan baru seperti email, telepon Internet, televisi Internet, musik online, surat kabar digital, dan situs web streaming video. Surat kabar, buku, dan penerbitan cetak lainnya beradaptasi dengan teknologi situs web, atau dibentuk kembali menjadi *blogging*, *feed web*, dan agregator berita *online*. Internet telah memungkinkan dan mempercepat bentuk interaksi pribadi baru melalui pesan instan, forum Internet, dan jejaring sosial. Belanja online telah tumbuh secara eksponensial baik untuk pengecer besar, usaha kecil dan pengusaha, karena memungkinkan perusahaan untuk memperluas kehadiran "batu bata dan mortir" mereka untuk melayani pasar yang lebih besar atau bahkan menjual barang dan jasa sepenuhnya online. Layanan bisnis-ke-bisnis dan keuangan di Internet mempengaruhi rantai pasokan di seluruh industri.

Internet tidak memiliki tata kelola terpusat tunggal dalam implementasi teknologi atau kebijakan untuk akses dan penggunaan; setiap jaringan konstituen menetapkan kebijakannya sendiri. Definisi melampaui batas dari dua ruang nama utama di Internet, ruang alamat Protokol Internet (alamat IP) dan Sistem Penamaan Domain (DNS), diarahkan oleh organisasi pengelola, *Internet Corporation for Assigned Names and Numbers* (ICANN). Dasar-dasar teknis

dan standarisasi protokol inti adalah kegiatan dari *Internet Engineering Task Force* (IETF), sebuah organisasi nirlaba dari para peserta internasional yang berafiliasi secara terbuka yang dapat diajak bekerjasama oleh siapa saja dengan kontribusi berkeahlian teknis.

Internet dijaga oleh perjanjian bilateral atau multilateral dan spesifikasi teknikal (protokol yang menerangkan tentang perpindahan data antara rangkaian). Protokol-protokol ini dibentuk berdasarkan perbincangan *Internet Engineering Task Force* (IETF), yang terbuka kepada umum. Badan ini mengeluarkan dokumen yang dikenali sebagai RFC (*Request for Comments*). Sebagian dari RFC dijadikan Standar Internet (*Internet Standard*), oleh Badan Arsitektur Internet (*Internet Architecture Board* - IAB). Protokol-protokol Internet yang sering digunakan adalah seperti, IP, TCP, UDP, DNS, PPP, SLIP, ICMP, POP3, IMAP, SMTP, HTTP, HTTPS, SSH, Telnet, FTP, LDAP, dan SSL.

Beberapa layanan populer di Internet yang menggunakan protokol di atas, ialah email/surat elektronik, *Usenet*, *Newsgroup*, berbagi berkas (*File Sharing*), WWW (*World Wide Web*), Gopher, akses sesi (*Session Access*), WAIS, finger, IRC, MUD, dan MUSH. Di antara semua ini, email/surat elektronik dan World Wide Web lebih kerap digunakan, dan lebih banyak servis yang dibangun berdasarkannya, seperti milis (*Mailing List*) dan Weblog. Internet memungkinkan adanya servis terkini (*Real-time service*), seperti web radio, dan webcast, yang dapat diakses di seluruh dunia. Selain itu melalui Internet dimungkinkan untuk berkomunikasi secara langsung antara dua pengguna atau lebih melalui program pengirim pesan instan seperti Camfrog, Pidgin (Gaim), Trilian, Kopete, Yahoo! Messenger, MSN Messenger Windows Live Messenger, Twitter, Facebook dan lain sebagainya.

III.3.8 HTML (*Hypertext Markup language*)

HTML dibuat oleh Tim Berners-Lee, seorang ahli fisika di lembaga penelitian CERN yang berlokasi di Swiss. Dia memiliki ide tentang sistem *hypertext* yang

berbasis internet. *Hypertext* merujuk pada teks yang memuat referensi (*link*) ke teks lain yang bisa diakses langsung oleh *viewer*. Tim merilis versi pertama HTML pada tahun 1991, dan di dalamnya terdiri atas 18 HTML *tag*. Sejak saat itu, setiap kali bahasa HTML merilis versi teranyarnya, selalu ada tag dan *attribute* (*tag modifier*) terbaru.

Dokumen HTML adalah file yang diakhiri dengan ekstensi .html atau .htm. Ekstensi file ini bisa dilihat dengan menggunakan web browser apa pun (seperti Google Chrome, Safari, atau Mozilla Firefox). Browser tersebut membaca file HTML dan me-render kontennya sehingga *user* internet bisa melihat dan membacanya.

Biasanya, rata-rata situs web menyertakan sejumlah halaman HTML yang berbeda-beda. Contohnya, beranda utama, halaman ‘tentang kami’, halaman kontak yang semuanya memiliki dokumen HTML terpisah. Masing-masing halaman HTML terdiri atas seperangkat *tags* (bisa disebut juga *elements*), yang mengacu pada *building block* halaman website. Tag tersebut membuat hirarki yang menyusun konten hingga menjadi bagian, paragraf, heading, dan block konten lainnya. Sebagian besar element HTML memiliki tag pembuka dan penutup yang menggunakan syntax `<tag></tag>`. Elemen teratas dan terbawah adalah division sederhana (`<div></div>`) yang bisa Anda gunakan untuk mark up bagian konten yang lebih besar.

Sama seperti hal teknis lainnya dalam dunia web, HTML juga punya kelebihan dan kekurangan diantaranya:

1. Kelebihan

- Bahasa yang digunakan secara luas dan memiliki banyak sumber serta komunitas yang besar.
- Dijalankan secara alami di setiap web browser.
- Memiliki *learning curve* yang mudah.
- *Open-source* dan sepenuhnya gratis.

- Bahasa *markup* yang rapi dan konsisten.
- Standard web yang resmi di-maintain oleh World Wide Web Consortium (W3C).
- Mudah diintegrasikan dengan bahasa *backend*, seperti PHP dan Node.js.

2. Kekurangan

- Paling sering digunakan untuk halaman web statis. Untuk fitur dinamis, Anda bisa menggunakan JavaScript atau bahasa *backend*, seperti PHP.
- HTML tidak memungkinkan *user* untuk menjalankan *logic*. Akibatnya, semua halaman web harus dibuat terpisah meskipun menggunakan elemen yang sama, seperti *header* dan *footer*.
- Fitur-fitur baru tidak bisa digunakan secara cepat di sebagian browser.
- Terkadang perilaku browser susah untuk diprediksi (misalnya, browser lama tidak selalu bisa render tag yang lebih baru).

III.4 Kakas Yang Digunakan

Kakas atau *tools* yang digunakan dalam proses *Security Assesment* pada website profil perusahaan CV. Cipta Daya Informatika antara lain:

1. OWASP ZAP (*Open Web Application Security Project Zed Attack Proxy*)

Aplikasi OWASP ZAP (*Open Web Application Security Project Zed Attack Proxy*) yang digunakan adalah versi 2.8.0.

2. Browser

Aplikasi Browser yang digunakan penyusun dalam penelitian kali ini adalah Google Chrome.

3. Sublime Text

Aplikasi Sublime Text digunakan untuk membuat *script* serangan *clickjacking*.

4. Komputer/Laptop

Komputer/Laptop adalah alat utama yang digunakan untuk proses penelitian.

5. Jaringan Internet

Karena penelitian berhubungan dengan keamanan jaringan pada website, untuk itu internet juga diperlukan untuk pencarian kerentanan dan *penetration testing*.

BAB IV

PELAKSANAAN KERJA PRAKTEK

IV.1 Input

Rencana *Security Assesment* Menggunakan aplikasi OWASP ZAP ini diberikan langsung oleh pihak perusahaan CV. Cipta Daya Informatika, baik secara tertulis maupun secara lisan. Salah satu kebutuhan yang paling mendasar adalah belum adanya dokumentasi aset kritis yang berisi daftar aset Website yang dianggap berisiko untuk mencegah adanya gangguan atau ancaman penyerangan dan penyadapan pada salah satu aset Website CV. Cipta Daya Informatika.

Informasi yang dibutuhkan untuk proses *Security Assesment* diberikan oleh direktur CV. Cipta Daya Informatika yang sekaligus sebagai pembimbing selama pelaksanaan kerja praktek. Dasar teori selama perkuliahan juga penting untuk membaca dan menganalisa keamanan jaringan pada website profil perusahaan CV. Cipta Daya Informatika.

Kegiatan kerja praktek yakni *Security Assesment* dilakukan di rumah masing-masing karena sebelumnya ada diskusi terkait penelitian tersebut termasuk *job desc* masing-masing. Sehingga peserta kerja praktek sudah mengetahui apa yang harus dilakukan dan dikerjakan sebelumnya.

IV.2 Proses

Setelah melakukan pengenalan lingkungan kerja pada awal pelaksanaan kerja praktek, selanjutnya proses kerja praktek dapat dibagi menjadi beberapa tahap, mengacu pada metodologi yang digunakan yaitu VAPT (*Vulnerability Assesment and Penetration Testing*).

IV.2.1 Penentuan Ruang Lingkup (*Scope*)

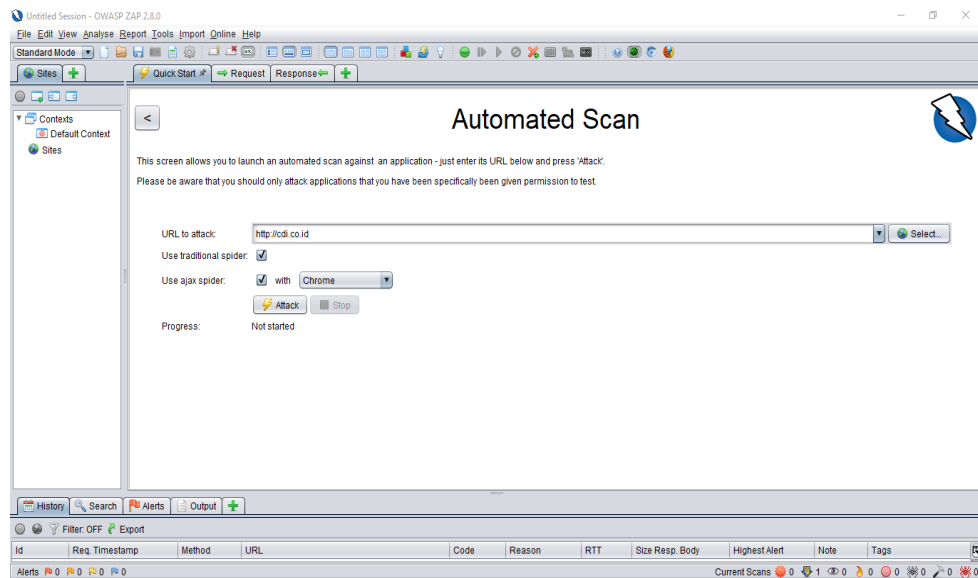
Pada penelitian kali ini telah ditentukan Ruang Lingkup (*Scope*) seperti yang sudah tertera pada subbab Batasan Masalah. Penyusun menerapkan ruang lingkup penelitian pada Web aplikasi profil perusahaan CV. Cipta Daya Informatika untuk menjadi target pengujian. Cakupan untuk *penetration testing* terbatas pada pencarian hak akses dan kerentanan pada website CV. Cipta Daya Informatika tersebut.

IV.2.2 Pengintaian Sistem (*Reconnaissance*)

Tahap ini dilakukan untuk mencari informasi dasar target dengan cara mewawancarai secara langsung dari pihak CV. Cipta Daya Informatika untuk mencari masalah apa yang terjadi di web profil tersebut. Peneliti mendapatkan informasi tidak ada masalah atau ancaman yang terjadi namun pihak CV. Cipta Daya Informatika menginginkan ada pendokumentasian kerentanan pada web profilnya untuk mencegah adanya peretasan atau penyadapan.

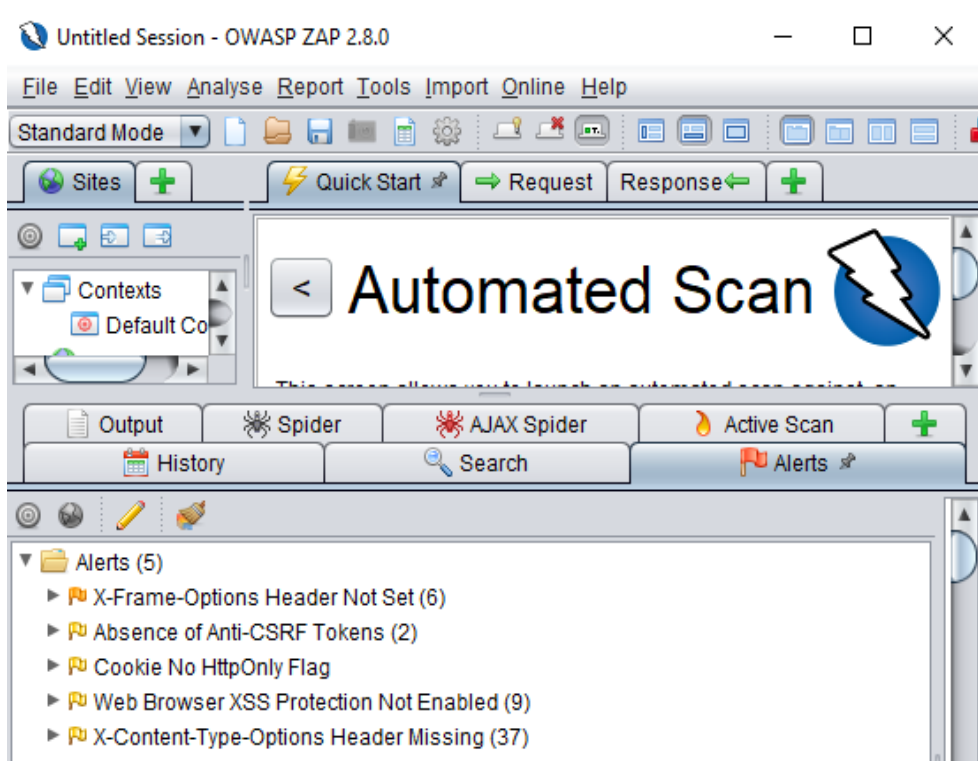
IV.2.3 Pencarian Kerentanan Keamanan (*Vulnerability Detection*) Menggunakan *Tools Software OWASP ZAP*

Pada tahap pencarian kerentanan keamanan akan dilakukan *Vulnerability Scanning* menggunakan OWASP ZAP (*Open Web Application Security Project Zed Attack Proxy*). Tujuan dilakukan *vulnerability scanning* adalah untuk mencari kerentanan keamanan dan menjadikan salah satu celah sebagai bahan untuk melakukan *penetration testing* dan berikut selanjutnya apa yang harus dilakukan untuk menangani kerentanan tersebut jika berhasil dilakukan simulasi penyerangan atau *penetration testing*. Tahap awal pencarian kerentanan keamanan dilakukan dengan cara membuka aplikasi OWASP ZAP, selanjutnya memasukkan URL Web profil CV. Cipta Daya Informatika ditampilkan awal pada OWASP ZAP di Gambar 4.1.



Gambar 4.1 Tampilan Awal OWASP ZAP

Setelah itu langsung tekan tombol “Attack” untuk memulai pencarian kerentanan dan tunggu proses pemindaian selesai. Setelah selesai proses pemindaian pada Gambar 4.2 muncul daftar kerentanan keamanan di bagian *Tab Menu “Alert”*.



Gambar 4.2 Daftar Kerentanan Website CV. Cipta Daya Informatika

Pada hasil pencarian kerentanan menggunakan OWASP ZAP terdapat beberapa kerentanan pada web CV. Cipta Daya Informatika seperti yang terlihat pada gambar 4.2 dimana pada setiap kerentanan mempunyai level tersendiri. Di aplikasi OWASP ZAP sendiri ada 3 level kerentanan diantaranya *low*, *medium*, dan *high* dan cara membedakan level tersebut terdapat pada warna pada di kerentanan itu sendiri dimana *low* dengan warna kuning, *medium* dengan warna oren, dan *high* dengan warna merah seperti yang tertera pada tabel 4.1

Tabel 4.1 Daftar Kerentanan Website CV. Cipta Daya Informatika

No.	Nama Kerentanan	Level	Deskripsi
1	<i>X-Frame-Options Header Not Set</i>	Medium	Kerentanan ini berpotensi terkena serangan <i>ClickJacking</i> .
2	<i>Absence of Anti CSRF Tokens</i>	Low	Kerentanan ini mengindikasikan tidak ada token <i>Anti-CSRF</i> yang di temukan pada <i>HTML Submission Form</i>
3	<i>Cookie No HttpOnly Flag</i>	Low	Kerentanan ini mengindikasikan web tersebut tidak menggunakan <i>HttpOnly</i>
4	<i>Web Browser XSS Protection Not Enabled</i>	Low	Kerentanan ini mengindikasikan <i>XSS Protection</i> tidak diaktifkan
5	<i>X-Content-Type-Options Header Missing</i>	Low	Kerentanan ini mengindikasikan <i>X-Content-Type-Options</i> tidak di tambahkan

IV.2.4 Analisis dan Perencanaan *Penetration Testing*

Pada tahap ini setelah melakukan *Vulnerability Detection* pada web CV. Cipta Daya Informatika menggunakan aplikasi OWASP ZAP, maka didapatkan kerentanan-kerentanan seperti tertera pada Tabel 4.1.

1. *X-Frame-Options Header Not Set*

X-frame-options, adalah *header respons* HTTP, juga disebut sebagai *header* keamanan HTTP, yang telah ada sejak tahun 2008. Pada 2013 secara resmi diterbitkan sebagai RFC 7034, tetapi bukan standar internet. Header ini memberi tahu browser bagaimana berperilaku saat menangani konten situs Anda. Alasan utama untuk awal adalah untuk memberikan perlindungan *clickjacking* dengan tidak mengizinkan rendering halaman dalam bingkai. Hal ini dapat mencakup render halaman dalam `<frame>`, `<iframe>` atau `<object>`. *Iframe* digunakan untuk menyematkan dan mengisolasi konten pihak ketiga ke dalam situs web. Contoh hal-hal yang menggunakan *iframe* mungkin termasuk tombol berbagi media sosial, Google Maps, pemutar video, pemutar audio, iklan pihak ke-3.

X-frame-options memiliki tiga arahan yang berbeda di mana dapat memilih dari harus dikirim sebagai header HTTP, karena browser akan mengabaikannya jika ditemukan dalam tag META. Penting juga untuk dicatat bahwa arahan tertentu hanya didukung di browser tertentu. Meskipun tidak perlu mengirim *header respons* ini di seluruh situs Anda, PRAKTEK terbaik adalah setidaknya mengaktifkannya di halaman yang membutuhkannya.

a. Deny

Arahan ini benar-benar menonaktifkan pemuatan halaman dalam bingkai, terlepas dari situs apa yang berusaha. Di bawah ini adalah tampilan permintaan tajuk apakah ini diaktifkan.

b. Sameorigin

Arahan ini memungkinkan halaman yang akan dimuat dalam bingkai tentang asal-usul yang sama seperti halaman itu sendiri. Di bawah ini adalah tampilan permintaan tajuk apakah ini diaktifkan.

c. Allow-From

Allow-From memungkinkan halaman untuk hanya dimuat dalam bingkai tentang asal-usul tertentu dan atau domain. Ini memungkinkan untuk mengunci situs hanya dari asal terpercaya. Tapi hati-hati dengan arahan ini.

Jika menerapkannya dan browser tidak mendukungnya, maka tidak akan memiliki pertahanan *clickjacking* di tempatnya.

2. *Absence of Anti CSRF Tokens*

Pemalsuan permintaan lintas situs (CSRF) adalah kerentanan keamanan web yang memungkinkan penyerang membujuk pengguna untuk melakukan tindakan yang tidak ingin mereka lakukan. Ini memungkinkan penyerang untuk sebagian menghindari kebijakan asal yang sama, yang dirancang untuk mencegah situs web yang berbeda saling mengganggu.

Dalam serangan CSRF yang berhasil, penyerang menyebabkan pengguna korban untuk melakukan suatu tindakan secara tidak sengaja. Misalnya, ini mungkin untuk mengubah alamat email pada akun mereka, untuk mengubah kata sandi mereka, atau untuk melakukan transfer dana. Bergantung pada sifat tindakan, penyerang mungkin bisa mendapatkan kontrol penuh atas akun pengguna. Jika pengguna yang dikompromikan memiliki peran istimewa dalam aplikasi, maka penyerang mungkin dapat mengambil kendali penuh atas semua data dan fungsionalitas aplikasi.

Token CSRF adalah nilai unik, rahasia, dan tak terduga yang dihasilkan oleh aplikasi sisi *server* dan ditransmisikan ke klien sedemikian rupa sehingga dimasukkan dalam permintaan HTTP berikutnya yang dibuat oleh klien. Ketika permintaan nanti dibuat, aplikasi sisi *server* memvalidasi bahwa permintaan menyertakan token yang diharapkan dan menolak permintaan jika token hilang atau tidak *valid*.

Token CSRF dapat mencegah serangan CSRF dengan membuatnya tidak mungkin bagi penyerang untuk membuat permintaan HTTP yang sepenuhnya *valid* yang cocok untuk memberi makan kepada pengguna korban. Karena penyerang tidak dapat menentukan atau memprediksi nilai token CSRF pengguna, mereka tidak dapat membuat permintaan dengan

semua parameter yang diperlukan untuk aplikasi untuk memenuhi permintaan tersebut.

Token CSRF harus diperlakukan sebagai rahasia dan ditangani dengan cara yang aman sepanjang siklus hidupnya. Suatu pendekatan yang biasanya efektif adalah untuk mengirimkan token kepada klien dalam bidang tersembunyi dari formulir HTML yang dikirimkan menggunakan metode POST. Token kemudian akan dimasukkan sebagai parameter permintaan ketika formulir dikirimkan.

Untuk keamanan tambahan, bidang yang berisi token CSRF harus ditempatkan sedini mungkin dalam dokumen HTML, idealnya sebelum bidang input yang tidak tersembunyi dan sebelum lokasi mana pun di mana data yang dapat dikendalikan pengguna disematkan dalam HTML. Ini mengurangi berbagai teknik di mana penyerang dapat menggunakan data yang dibuat untuk memanipulasi dokumen HTML dan menangkap bagian dari isinya. Pendekatan alternatif, menempatkan token ke string kueri URL, agak kurang aman karena string kueri:

- Dicatat di berbagai lokasi di sisi klien dan server.
- Dapat ditransmisikan ke pihak ketiga dalam tajuk Referer HTTP.
- Dapat ditampilkan di layar dalam browser pengguna.

Beberapa aplikasi mengirimkan token CSRF dalam header permintaan khusus. Ini menyajikan pertahanan lebih lanjut terhadap penyerang yang berhasil memprediksi atau menangkap token pengguna lain, karena browser biasanya tidak mengizinkan header khusus untuk dikirim lintas domain. Namun, pendekatan ini membatasi aplikasi untuk membuat permintaan yang dilindungi CSRF menggunakan XHR (sebagai lawan dari formulir HTML) dan mungkin dianggap terlalu rumit untuk banyak situasi.

3. *Cookie No HttpOnly Flag*

HttpOnly adalah bendera yang ditambahkan ke *cookie* yang memberi tahu browser untuk tidak menampilkan *cookie* melalui skrip sisi klien (dokumen *cookie* dan lainnya). Agenda di balik *HttpOnly* bukanlah untuk menumpahkan *cookie* ketika cacat XSS ada, karena seorang *hacker* mungkin dapat menjalankan skrip mereka tetapi manfaat mendasar dari memiliki kerentanan XSS (kemampuan mencuri *cookie* dan membajak sesi yang saat ini ditetapkan) hilang. Ketika mengatur *cookie* dengan *flag HttpOnly*, itu memberitahu browser bahwa *cookie* khusus ini hanya boleh diakses oleh server. Upaya apa pun untuk mengakses *cookie* dari skrip sisi klien dilarang keras. Tentu saja, ini mengandaikan Anda memiliki peramban web modern.

Menurut Jaringan Pengembang Microsoft, *HttpOnly* adalah *flag* tambahan yang disertakan dalam *header* respons HTTP *Set-Cookie*. Menggunakan *flag HttpOnly* saat membuat *cookie* membantu mengurangi risiko skrip sisi klien mengakses *cookie* yang dilindungi (jika browser mendukungnya). Jika sebuah browser tidak mendukung *HttpOnly* dan sebuah situs web mencoba untuk mengatur *cookie HttpOnly*, bendera *HttpOnly* akan diabaikan oleh browser, sehingga menciptakan *cookie* tradisional yang dapat diakses skrip. Akibatnya, *cookie* (biasanya *cookie* sesi Anda) menjadi rentan terhadap pencurian modifikasi oleh skrip berbahaya.

Menurut *Michael Howard*, Manajer Program Keamanan Senior di grup *Secure Windows Initiative* di Microsoft, mayoritas XSS menyerang target pencurian *cookie* sesi. *Server* dapat membantu mengurangi masalah ini dengan mengatur *flag HttpOnly* pada *cookie* yang dibuatnya, yang mengindikasikan *cookie* tidak boleh diakses oleh klien. Jika browser yang mendukung *HttpOnly* mendeteksi *cookie* yang berisi *flag HttpOnly*, dan kode skrip sisi klien mencoba membaca *cookie*, maka browser mengembalikan string kosong sebagai hasilnya. Ini menyebabkan serangan

gagal dengan mencegah kode jahat (biasanya XSS) mengirim data ke situs web penyerang.

4. *Web Browser XSS Protection Not Enabled*

Web Browser XSS Protection dirancang untuk memungkinkan *cross-site scripting* (XSS) filter dibangun ke browser web modern. Ini biasanya diaktifkan secara default. Ini didukung oleh Internet Explorer 8+, Chrome, dan Safari. *Cross-site scripting* juga dikenal sebagai XSS, pada dasarnya adalah cara untuk menyuntikkan kode yang akan melakukan tindakan di browser pengguna atas nama situs web. Kadang-kadang ini terlihat oleh pengguna dan kadang-kadang bisa benar-benar tanpa disadari di latar belakang. Ada banyak jenis kerentanan XSS, di bawah ini adalah dua yang paling umum.

- a. Reflektif XSS, Ini biasanya jenis yang paling umum. Biasanya ini berada dalam parameter permintaan HTTP dan digunakan oleh skrip sisi *server* untuk mem-parsing dan menampilkan halaman hasil untuk pengguna.
- b. Persistent XSS, Ini adalah ketika data dari penyerang benar-benar disimpan di *server* dan kemudian ditampilkan kepada pengguna, meniru halaman normal.

Kerentanan XSS lainnya termasuk berbasis DOM, *server* tersimpan, *server* terpantul, klien tersimpan, klien terpantul, dan subset klien. Menurut perincian CVE , basis data kerentanan keamanan, sejak 2009 telah tercatat lebih dari 9.903 serangan XSS besar dicatat. Setelah DDoS dan eksekusi kode, serangan XSS sangat umum.

5. *X-Content-Type-Options Header Missing*

X-Content-Type-Options adalah *header* HTTP yang digunakan untuk meningkatkan keamanan situs web. *Header X-Content-Type-Options* digunakan untuk melindungi terhadap kerentanan sniffing MIME.

Kerentanan ini dapat terjadi ketika situs web memungkinkan pengguna untuk mengunggah konten ke situs web namun pengguna menyamarkan jenis file tertentu sebagai sesuatu yang lain . Ini dapat memberi mereka kesempatan untuk melakukan skrip lintas situs dan kompromi situs web.

Namun, tajuk keamanan ini membantu mencegah jenis serangan ini dengan menonaktifkan fungsionalitas *sniffing* MIME pada Internet Explorer dan browser Chrome sehingga browser diperlukan untuk menggunakan tipe MIME yang dikirim melalui *server* asal seperti contoh berikut:

- a. Klien Chrome membuat permintaan ke *server* web untuk aset (mis. Image.jpg).
- b. Respons dikirim kembali dengan tajuk X-Content-Type-Options: nosniff. Ini mencegah klien dari "mengendus" aset untuk mencoba dan menentukan apakah jenis file adalah sesuatu selain apa yang dinyatakan oleh *server*.
- c. Browser kemudian menerima tipe MIME yang ditentukan oleh *server* asal dan menampilkan aset kepada pemirsa.

Sayangnya, *X-Content-Type-Options* tidak melindungi terhadap semua kerentanan terkait *sniffing*. Seperti disebutkan sebelumnya, saat ini hanya berjalan di Chrome dan versi Internet Explorer tertentu. Oleh karena itu, jika browser yang tidak didukung mengakses aset yang mengirim kembali *header respons* khusus ini, itu tidak akan berpengaruh.

Dari tabel 4.1 diatas dijelaskan bahwa ada beberapa kerentanan aset website profil beserta kemungkinan-kemungkinan yang terjadi. Kerentanan yang ditemukan dapat di kelompokkan menjadi 3 kategori yaitu *low*, *medium* dan *high*, tingkatan resiko kerentanan dihitung dari dua faktor yaitu faktor estimasi kemungkinan dan faktor estimasi dampak. Setiap faktor memiliki pilihan dan setiap pilihan mempunyai rating 0 sampai 9, rating ini akan digunakan untuk menghitung tingkat resiko setiap faktor. Dari rating akan didapatkan level

kerentanan, berdasarkan OWASP, kerentanan dibagi menjadi 3 yaitu *low*, *medium*, *high* yang memiliki rating nilai berbeda-beda, seperti pada Tabel 4.2.

Tabel 4.2 Tingkat Kemungkinan Dan Dampak

0 to< 3	<i>LOW</i>
3 to< 6	<i>MEDIUM</i>
6 to< 9	<i>HIGH</i>

1. Faktor estimasi kemungkinan

Faktor-faktor untuk estimasi kemungkinan berhubungan dengan bagaimana kerentanan ditemukan dan dieksploitasi oleh penyerang. Faktor ini dibagi menjadi 2 kategori, yaitu *Threat Agent Factors* dan *Vulnerability Factors*. Kategori *Threat Agent Factors* memiliki 4 faktor yaitu *Skill level*, *Motive*, *Opportunity*, *Size*, pada Tabel 4.3.

Tabel 4.3 Faktor Kemungkinan *Threat agent*

Faktor	Pilihan	Rating
Skill level	Security penetration skills	9
	Network and programming skills	6
	Advanced computer user	5
	Some technical skills	3
	No technical skills	1
Motive	Low or no reward	1
	Possible reward	4
	High reward	9
Opportunity	Full acces or expensive resources required	0
	Special access or resources required	4
	Some access or resources required	7
	No access or resources required	9
Size	Developers	2
	System administrators	2
	Internet users	4

	Partners	5
	Authenticated user	6
	Anonymous internet users	9

Kategori *Vulnerability Factors* memiliki 4 faktor yaitu *Ease of discovery*, *Ease of exploit*, *Awareness*, *Intrusion detection* dan masing-masing factor memiliki pilihan, pada Tabel 4.4.

Tabel 4.4 Faktor Kemungkinan *Vulnerability*

Faktor	Pilihan	Rating
Ease of discovery	Practically impossible	1
	Difficult	3
	Easy	7
	Automated tools available	9
Ease of exploit	Theoretical	1
	Difficult	3
	Easy	5
	Automated tools available	9
Awareness	Unknown	1
	Hidden	4
	Obvious	6
	Public knowledge	9
Intrusion detection	Active detection in application	1
	Logged and reviewed	3
	Logged without review	8
	Not logged	9

2. Faktor Estimasi Dampak

Faktor untuk estimasi dampak dibagi menjadi 2 kategori, yaitu *Technical Impact Factors* dan *Business Impact Factors*. Kategori *Technical Impact Factors*

memiliki 4 faktor yaitu *loss of confidentiality*, *loss of integrity*, *loss of availability* dan *loss of accountability*, pada Tabel 4.5.

Tabel 4.5 Faktor Dampak *Technical Impact Factors*

Faktor	Pilihan	Rating
Loss of confidentiality	Minimal non-sensitive data disclosed	2
	Minimal critical data disclosed	6
	Extensive non-sensitive data disclosed	6
	Extensive critical data disclosed	7
	All data disclosed	9
Loss of integrity	Minimal slightly corrupt data	1
	Minimal seriously corrupt data	3
	Extensive slightly corrupt data	5
	Extensive seriously corrupt data	7
	All data totally corrupt	9
Loss of availability	Minimal secondary services interrupted	1
	Minimal primary services interrupted	5
	Extensive secondary services interrupted	5
	Extensive secondary services interrupted	7
	All services completely lost	9
Loss of accountability	Fully traceable	1
	Possibly traceable	7
	Completely traceable	9

Kategori *Business Impact Factors* memiliki 4 faktor yaitu *financial damage*, *reputation damage*, *non-complicance* dan *privacy violation*, dan setiap faktor memiliki pilihan, Tabel 4.6.

Tabel 4.6 Faktor Dampak *Business Impact Factors*

Faktor	Pilihan	Rating
Financial damage	Less than the cost to fix the vulnerability	1
	Minor effect in annual profit	3
	Significant effect on annual profit	7
	Bankruptcy	9
Reputation damage	Minimal damage	1
	Loss of major accounts	4
	Loss of goodwill	5
	Brand damage	9
Non-compliance	Minor violation	2
	Clear violation	5
	High profile violation	7
Privacy violation	One individual	3
	Hundreds of people	5
	Thousand of people	7
	Millions of people	9

Rating terakhir tingkat resiko kerentanan didapatkan dengan menggabungkan 2 faktor yaitu faktor estimasi kemungkinan dan faktor estimasi dampak. Penentuan akhir tingkat resiko kerentanan menggunakan rumus seperti berikut:

$$\text{Resiko} = \text{Kemungkinan} * \text{Dampak}$$

Jika dari faktor estimasi dampak ditemukan untuk kategori dampak teknis dan kategori dampak bisnis, maka kategori dampak bisnis menjadi prioritas, namun jika kategori dampak bisnis tidak ditemukan maka menggunakan kategori dampak teknis. Dari perhitungan 2 faktor dengan menggunakan rumus diatas didapatkan hasil seperti pada Gambar 4.3.

Dampak	TINGGI	Medium	Tinggi	Kritis
	MEDIUM	Rendah	Medium	Tinggi
	RENDAH	Catatan	Rendah	Medium
		RENDAH	MEDIUM	TINGGI
	Kemungkinan			

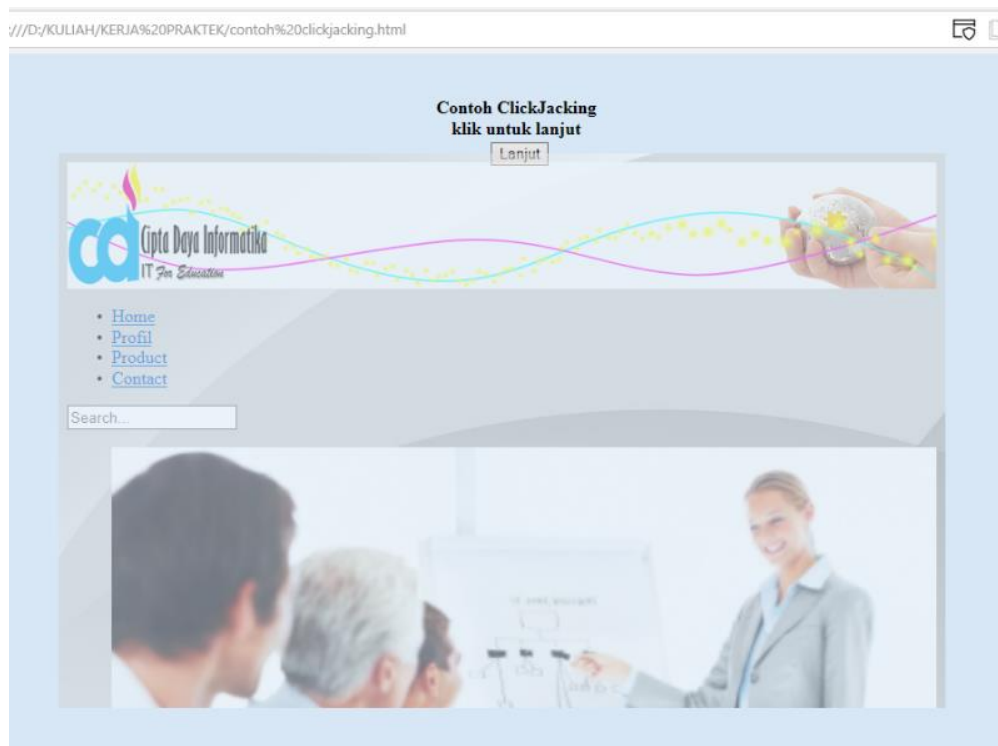
Gambar 4.3 Keseluruhan Tingkat Resiko Keamanan

IV.2.5 Penetration Testing

Penetration Testing (Pentest) adalah sebuah metode untuk melakukan evaluasi terhadap keamanan dari sebuah sistem dan jaringan komputer. Evaluasi dilakukan dengan cara melakukan sebuah simulasi serangan (*attack*). Hasil dari pentest ini sangat penting sebagai *feedback* bagi pengelola sistem untuk memperbaiki tingkat keamanan dari sistem komputernya. Laporan hasil Pentest akan memberikan masukan terhadap kondisi *vulnerabilitas* sistem sehingga memudahkan dalam melakukan evaluasi dari sistem keamanan komputer yang sedang berjalan. Aktivitas pentest kadang disebut juga dengan istilah *ethical hacking*.

Terdapat beberapa teknik dan metode untuk melakukan Pentest, diantaranya adalah apa yang disebut dengan *black box*, *white box* dan *grey box*. *Black box* testing adalah metode Pentest dimana diasumsikan tester tidak mengetahui sama sekali infrastruktur dari target pentest. Dengan demikian pada *black box* test ini tester harus mencoba untuk menggali dari awal semua informasi yang diperlukan kemudian melakukan analisis serta menentukan jenis *attack* yang akan dilakukan. Pada *White box* testing terjadi sebaliknya, tester telah mengetahui semua informasi yang diperlukan untuk melakukan pentest. Sementara *gray box* atau kombinasi dari kondisi *black box* dan *white box*. Pengertian lain dari *white box* adalah "*full disclosure*", *grey box* adalah "*partial disclosure*" dan *black box*

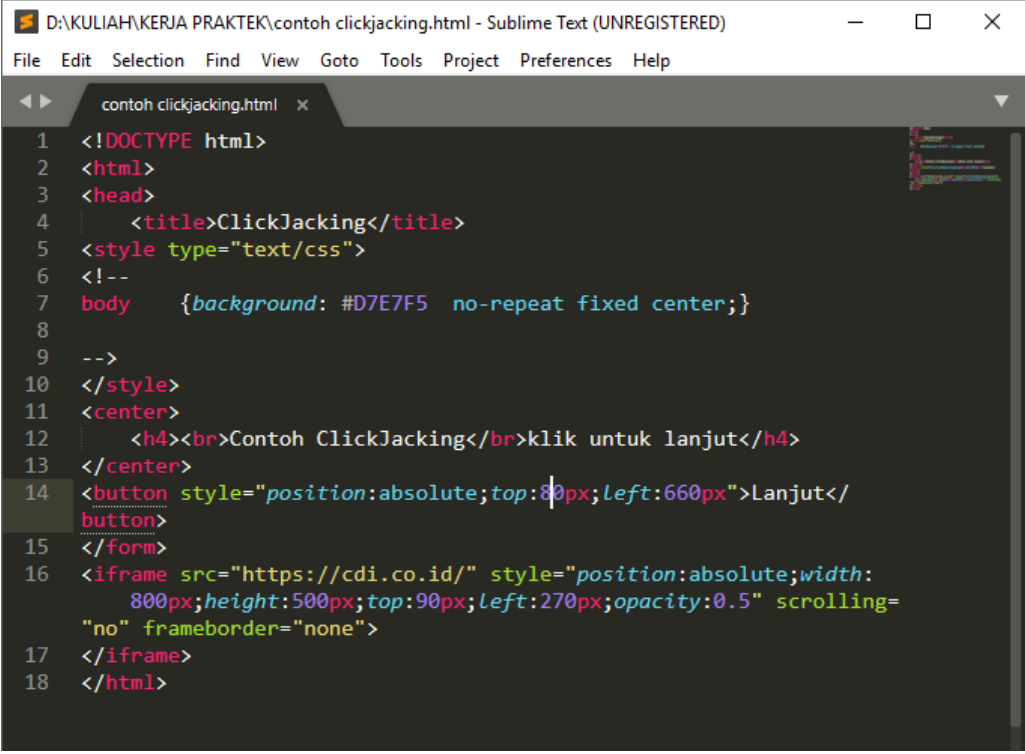
adalah ” *blind disclosure*”. Dari hasil analisis terdapat beberapa kerentanan berikut penjelasannya, salah satunya kita bisa memanfaatkan kelemahan *Absence of Anti CSRF Tokens* dan *X-Frame-Options Header* untuk melakukan *ClickJacking*. *ClickJacking* adalah aktifitas berbahaya yang dilakukan oleh seorang *Hacker* dengan tujuan untuk melakukan sebuah tindakan seperti menipu *User* internet untuk mengklik tombol atau *link* dan dibalik tombol itu terdapat sebuah *script* yang nantinya bila di klik oleh *user* internet maka akan mendapatkan sebuah informasi dari korban tersebut. *ClickJacking* di perkenalkan pertama kali oleh Jeremiah Grossman dan Robert Hansen pada tahun 2008, pada tahun 2002 telah di catat bahwa untuk membuat halaman transparan di dalam web atau diatas web itu akan mempengaruhi pengguna. Istilah *ClickJacking* diciptakan oleh Jeremiah dan Robert Hansen yang berasal dari kata “*Click*” yang artinya “klik” dan “*Jacking*” yang artinya “pembajakan”. Contoh tampilan *ClickJacking* seperti pada Gambar 4.4.



Gambar 4.4 Contoh Tampilan *ClickJacking* CV. Cipta Daya Informatika

Setelah korban berselancar di halaman web fiktif, korban berpikir bahwa ia berinteraksi dengan user interface terlihat, tetapi efektif ia melakukan tindakan

pada halaman tersembunyi. Karena halaman tersembunyi adalah halaman otentik, penyerang dapat menipu pengguna agar melakukan tindakan yang mereka tidak pernah inginkan untuk melakukan melalui "ad hoc" posisi elemen dalam halaman website. Gambar diatas adalah contoh tampilan yang dibuat untuk melakukan serangan *ClickJacking* dengan menggunakan *HTML*, untuk *Script* nya bisa dilihat pada Gambar 4.5.



```

1  <!DOCTYPE html>
2  <html>
3  <head>
4      <title>ClickJacking</title>
5  <style type="text/css">
6  <!--
7  body {background: #D7E7F5 no-repeat fixed center;}
8
9  -->
10 </style>
11 <center>
12     <h4><br>Contoh ClickJacking</br>klik untuk lanjut</h4>
13 </center>
14 <button style="position:absolute;top:80px;left:660px">Lanjut</
15 button>
16 </form>
17 <iframe src="https://cdi.co.id/" style="position:absolute;width:
18     800px;height:500px;top:90px;left:270px;opacity:0.5" scrolling=
    "no" frameborder="none">
19 </iframe>
20 </html>

```

Gambar 4.5 Script HTML Tampilan *ClickJacking*

IV.2.6 Eksploitasi Kerentanan (*Privilege Escalation*)

Pada tahap ini peneliti mampu mempraktekan sebuah serangan *ClickJacking*. Tetapi itu hanyalah sebuah tampilannya saja. Peneliti tidak mempraktekan *ClickJacking* yang sebenarnya terhadap aplikasi website profil perusahaan CV. Cipta Daya Informatika. Namun kurang lebih gambaran serangan *ClickJacking* seperti itu. Penyerang membuat tampilan web tidak terlihat di depan tampilan web CV. Cipta Daya Informatika dimana ketika kita meng'klik' pada tampilan web dari penyerang maka otomatis kita dibawa kealamat yang diinginkan oleh

penyerang dan ketika kita memasukan sebuah informasi maka informasi tersebut akan tembus kepada penyerang.

IV.2.7 Pelaporan Hasil Kerja Praktek

Proses pelaporan hasil kerja praktek dilakukan pada tahap akhir kerja praktek di CV. Cipta Daya Informatika. Pelaporan hasil kerja praktek ini dilakukan melalui presentasi di hadapan pembimbing kerja praktek. Pelaporan hasil kerja praktek dilakukan pula dengan pembuatan laporan kerja praktek.

IV.3 Pencapaian Hasil

Adapun hasil yang dicapai dari kerja praktek di CV. Cipta Daya Informatika ini berupa dokumentasi aset dalam aplikasi website yang dianggap berisiko untuk dijadikan bahan evaluasi penanganan dan pencegahan ancaman penyerangan atau penyadapan terhadap aplikasi website profil perusahaan CV. Cipta Daya Informatika diantaranya:

1. *X-Frame-Options Header Not Set*, dapat digunakan agar browser tidak membuat halaman dalam, atau situs dapat menggunakan ini untuk menghindari serangan *ClickJacking* dengan memastikan bahwa konten tidak tertanam ke situs lain. *X-Frame-Options Header* hanya dapat digunakan jika pengguna mengakses lewat browser yang mendukungnya.
2. *Absence of Anti CSRF Tokens*, adalah serangan Aplikasi Web sisi pengguna di mana penyerang menipu korban untuk mengeksekusi permintaan web jahat atas nama dirinya sendiri. Penyerang dapat mengirim tautan ke korban, dengan sedikit Rekayasa Sosial, ia akan membuat korban mengklik tautan tersebut. Kemudian korban secara tidak sengaja mengeluarkan permintaan ke server web yang tidak diinginkan.
3. *Cookie No HttpOnly Flag*, permasalahan ini mengindikasikan bahwa website tidak memiliki set *HttpOnly Flag*. Ketika *cookie* diatur dengan *HttpOnly Flag*, *cookie* memerintahkan browser bahwa *cookie* hanya dapat diakses oleh server dan bukan oleh sisi pengguna. Ini adalah perlindungan keamanan penting untuk sesi *cookie*.

4. *Web Browser XSS Protection Not Enabled*, adalah fitur Internet Explorer, Chrome dan Safari yang menghentikan halaman memuat ketika mendeteksi serangan *cross-site scripting* (XSS) yang tercermin. Meskipun perlindungan ini sebagian besar tidak perlu di browser modern karena sebagian besar sudah menerapkan *Content-Security-Policy* yang menonaktifkan penggunaan inline JavaScript ('*unsafe-inline*'), *XSS Protection* masih dapat dipakai sebagai perlindungan bagi pengguna browser web yang lebih tua.
5. *X-Content-Type-Options Header Missing* artinya rentan terhadap *sniffing MIME*. Ini dapat mencegah Internet Explorer dan Google Chrome dari *sniffing MIME*, respon dari tipe konten yang dideklarasikan. Ini juga berlaku untuk Google Chrome saat mengunduh ekstensi. Ini mengurangi paparan terhadap serangan unduhan *drive-by* dan situs-situs yang menyajikan konten yang diunggah pengguna.

Pada tahap *Penetration Testing* dilakukan serangan *Clickjacking*. Untuk mengantisipasi serangan tersebut ada dua cara yaitu:

1. Perlindungan sisi klien *Frame Busting*, metode sisi klien bisa efektif dalam beberapa kasus, tetapi dianggap bukan praktek terbaik, karena mereka dapat dengan mudah dilewati.
2. Pelindungan sisi server *X-Frame-Options*, metode sisi server direkomendasikan oleh para pakar keamanan sebagai cara yang efektif untuk bertahan melawan *clickjacking*. Header respons X-Frame-Options dilewatkan sebagai bagian dari respons HTTP halaman web, yang menunjukkan apakah browser boleh atau tidak merender halaman di dalam tag <FRAME> atau <IFRAME>.

Ada tiga nilai yang diizinkan untuk header X-Frame-Options:

- *DENY* = tidak mengizinkan domain apa pun untuk menampilkan halaman ini dalam sebuah bingkai
- *SAMEORIGIN* = memungkinkan halaman saat ini untuk ditampilkan dalam bingkai di halaman lain, tetapi hanya di dalam domain saat ini

- *ALLOW-FROM URI* = memungkinkan halaman saat ini ditampilkan dalam bingkai, tetapi hanya di URI tertentu.

Menggunakan opsi *SAMAORIGIN* untuk bertahan melawan *Cickjacking* memungkinkan penerbit konten untuk mencegah konten mereka sendiri dari digunakan dalam bingkai yang tidak terlihat oleh penyerang. Opsi *DENY* adalah yang paling aman, mencegah penggunaan halaman saat ini dalam bingkai. Lebih umum, *SAMAORIGIN* digunakan, karena memang memungkinkan penggunaan frame, tetapi membatasi mereka ke domain saat ini.

Keterbatasan *X-Frame-Options*:

- Untuk mengaktifkan opsi *SAMAORIGIN* di situs web, tajuk *X-Frame-Options* perlu dikembalikan sebagai bagian dari respons HTTP untuk setiap halaman individual (tidak dapat diterapkan lintas situs).
- *X-Frame-Options* tidak mendukung daftar putih dari domain yang diizinkan, jadi itu tidak berfungsi dengan situs multi-domain yang perlu menampilkan konten berbingkai di antara mereka.
- Hanya satu opsi yang dapat digunakan pada satu halaman, jadi, misalnya, tidak mungkin halaman yang sama ditampilkan sebagai bingkai baik di situs web saat ini dan situs eksternal.
- Opsi *ALLOW-FROM* tidak didukung oleh semua browser.
- *X-Frame-Options* adalah opsi yang sudah usang di sebagian besar browser.

BAB V

PENUTUP

V.1 Kesimpulan Dan Saran Mengenai Pelaksanaan Kerja Praktek

V.1.1 Kesimpulan Pelaksanaan Kerja Praktek

1. Mahasiswa dapat mengaplikasikan ilmu yang diperoleh selama perkuliahan untuk menyelesaikan permasalahan di dunia nyata.
2. Mahasiswa dapat mengetahui ilmu keterampilan yang dibutuhkan untuk memasuki dunia kerja di era globalisasi seperti:
 - Keterampilan berkomunikasi dan bekerja sama dengan orang lain.
 - Ilmu dasar mengenai bidang spesifik yang diperoleh selama perkuliahan. Misalnya ilmu dasar di bidang informatika, ilmu dasar di bidang ekonomi, dan sebagainya.
 - Keterampilan menganalisis permasalahan untuk dicari solusinya.
 - Ilmu pengetahuan umum.
 - Keterampilan mempelajari hal yang baru dalam dunia pekerjaan.
3. Mahasiswa menyadari pentingnya etos kerja yang baik, disiplin, dan tanggung jawab dalam menyelesaikan suatu pekerjaan.
4. Kerja praktek dapat melatih mahasiswa untuk bekerja sama dalam suatu tim, baik antar peserta kerja praktek maupun dengan karyawan lain di CV. Cipta Daya Informatika.
5. Mahasiswa memperoleh tambahan ilmu yang tidak diperoleh di proses perkuliahan. Pada kerja praktek yang dilakukan di CV. Cipta Daya Informatika, mahasiswa mendapatkan pengetahuan tambahan.

V.1.2 Saran Pelaksanaan Kerja Praktek

Adapun saran mengenai pelaksanaan kerja praktek antara lain:

1. Perlu ditumbuhkan kebiasaan belajar secara mandiri (*self-learning*) di kalangan mahasiswa, khususnya dalam mempelajari teknologi secara

aplikatif. Salah satu fasilitas yang tersedia yang mendukung proses pembelajaran secara mandiri ini adalah koneksi internet yang cukup cepat.

2. Perlu adanya kemampuan mahasiswa untuk menggabungkan seluruh ilmu yang pernah didapat di perkuliahan dalam proses *Security Assessment*.
3. Perlu adanya bimbingan secara lebih intensif bagi mahasiswa kerja praktek.
4. Jika memungkinkan, dalam pelaksanaan kerja praktek mahasiswa dapat dilibatkan dalam suatu proyek di mana mahasiswa dapat bekerja sama dengan pegawai lain.

V.2 Kesimpulan Dan Saran Mengenai Substansi Selama Kerja Praktek

V.2.1 Kesimpulan Mengenai *Security Assessment* Di CV. Cipta Daya Informatika

1. Hasil dari penelitian kerentanan keamanan pada website CV.Cipta Daya Informatika di dapatkan beberapa masalah diantaranya:

- *X-Frame-Options Header Not Set*
- *Absence Of Anti CSRF Tokens*
- *Cookie No HttpOnly Flag*
- *Web Browser XSS Protection Not Enabled*
- *X-Content-Type-Options Header Missing*

Diantara kerentanan-kerentanan tersebut ada yang level kerentanannya *medium* yaitu *X-Frame-Options Header Not Set*. Kerentanan tersebut dapat mengakibatkan terjadinya serangan *Clickjacking*. Penyusun telah melakukan *Penetration Testing* atau simulai penyerangan melalui celah tersebut dengan menggunakan serangan *Clickjacking* dan hasilnya website dari CV. Cipta Daya Informatika rentan terhadap serangan tersebut.

2. Website atau *Platform* mempunyai kelemahan tersendiri baik dalam *Frontend* maupun *Backend*.
3. Celah dalam website CV. Cipta Daya Informatika ada yang bisa diperbaiki maupun tidak bisa diperbaiki, tergantung dalam penggunaan website tersebut. Baik website yang menggunakan *Native* (dibuat *Full* oleh pihak

perusahaan itu sendiri) maupun yang sudah di sediakan pihak lain, seperti Wordpress atau Blogspot.

V.2.2 Saran Mengenai *Security Assesment* Di CV. Cipta Daya Informatika

Adapun saran mengenai pelaksanaan kerja praktek antara lain:

1. Dari hasil *Penetration Testing* dimana website CV. Cipta Daya Informatika terkena serangan *Clickjacking* yang dilakukan penyusun, adapun cara mengatasi masalah tersebut yang paling efektif adalah pada sisi *server*. Dimana hanya *server* yang dapat mengatasi permasalahan tersebut.
2. Perlu optimasi secara lebih lanjut terhadap website CV. Cipta Daya Informatika untuk mengatasi kerentanan-kerentanan tersebut.
3. Mempertimbangkan terhadap kerentanan-kerentanan yang ditemukan supaya tidak terjadi kerentanan yang lebih lemah.
4. Memasang *https* agar lebih terlindungi oleh *hosting*.

DAFTAR PUSTAKA

- [1] Goel, J N., & Mehtre, B. M. (2015). Vulnerability Assesment & Penetration Testing as a Cyber Defence Technology. *Procedia Computer Science*, 57,710-715. <https://doi.org/10.1016/j.procs.2015.07.458>
- [2] Grangers, S. (2001). Social Engineering Fundamentals, Part I:Hacker Tactics | Symantec Connect. *Social Engineering Fundamentals*, 1527. Retrieved from <https://s3.amazonaws.com/academia.edu.documents/s/33172114/04SocialEngineeringWebQuest.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1526824318&Signature=8cWE8Bum9sdq4wl3axkcxp3mhaQ%253D&response-content-disposition=inline%253B>
- [3] Anggrahito. (2018). Penerapan Vulnerability Assesment dan Penetration Test Bagi Pelaksanaan Audit Keamanan Informasi Sektor Pemerintah. *BADAN SIBER DAN SANDI NEGARA*.
- [4] Nasiti, T. I. (2016). *Web Application Vulnerability Assesment Used OWASP ZAP Application Security Verification Standar (ASVS) for UGM Websites. Universitas Gadjah Mada*
- [5] Shah, S., & Mehte, B. M. (2015). An Automated Approach to Vulnerability Assesment and Penetration Testing using Net-Nirikshak 1.0. *Proceedings of 2014 IEE International Conference on Advanced Communication, Control and Computing Technologies, ICACCCT 2014*, (978), 707-712. <https://doi.org/10.1109/ICACCCT.2014.7019182>
- [6] Galih S. P. (2018). Security Assesment Menggunakan Open Web Application Security Project Zed Attack Proxy (OWASP ZAP) Untuk Mencari Kerentanan Keamanan Web KRS Daring (Kartu Rencana Studi Daring) Di Institut Pendidikan XYZ
- [7] Unknown,. Yayasan OWASP, Retrived Juli 2019, from https://www.owasp.org/index.php/Main_Page.

- [8] Unknown,. IT Governance Indonesia, Penetration Testing, Retrived Juli 2019 from <https://itgid.org/vulnerabilty-assessment/>.
- [9] Octavianus, Boni (2014). Penetratio Testing, Retrived Juli 2019 from <https://coolnetkid.wordpress.com/2014/05/24/penetration-testing/>
- [10] Unknown,. BOC Indonesia, Website, Retrived Juli 2019 from [http://www.boc.web.id/pengertian-website-webhosting domainname/#sthash.g6th5nwq.dpuf](http://www.boc.web.id/pengertian-website-webhosting-domainname/#sthash.g6th5nwq.dpuf).
- [11] Ariata, C (2018). Hypertext Markup Language, Retrived Juli 2019 from <https://www.hostinger.co.id/tutorial/apa-itu-html/>

Lampiran A. TOR

TERM OF REFERENCE

Sebelum melaksanakan kerja praktek, penyusun melakukan beberapa metode penelitian diantaranya adalah observasi, interview, dan studi pustaka. Setelah mengamati dan mempelajari beberapa konsep lingkup pelaksanaan kerja praktek dan di setujui oleh instansi serta pembimbing lapangan. Penyusun melaksanakan kerja praktek dan memiliki tugas yang harus dikerjakan yaitu:

1. Mencari kerentanan keamanan website profil perusahaan CV. Cipta Daya Informatika.
2. Membuat dokumen daftar kerentanan-kerentanan sebagai bahan evaluasi.
3. Merekomendasi perusahaan CV. Cipta Daya Informatika terhadap kerentanan-kerentanan yang ditemukan.

Bandung, Juli 2019

Disetujui Oleh:

Mahasiswa Kerja Praktek

Pembimbing Lapangan

Sabda Alam
NIM: C1A160015

Elsa Herlyanti

Lampiran B. Log Activity

PEMETAAN WAKTU PELAKSANAAN PENYELESAIAN KERJA PRAKTEK (KP) MAHASISWA
FAKULTAS TEKNOLOGI INFORMASI

NO	URAIAN PEKERJAAN	BOBOT (%)	BULAN KE 1				BULAN KE 2				BULAN KE 3				BOBOT (%)
			1	2	3	4	5	6	7	8	9	10	11	12	
															100%
PERSIAPAN															
1	Pendaftaran	2,5	2,5												
2	Pembuatan Proposal	2,5		2,5											
3	Persetujuan Proposal	2,5			2,5										
4	Penentuan Pembimbing Internal	2,5				2,5									
TEMPAT KERJA PRAKTEK															
5	Survey Lokasi Kerja Praktek (KP)	5,0				2,5	2,5								
6	Penetapan Waktu Kerja Praktek dan penentuan Pembimbing KP	2,5					2,5								
WAKTU KERJA PRAKTEK															
7	Mempelajari Struktur Perusahaan	2,5					2,5								
8	Pengumpulan Data	5,0					1,3	1,3	1,3	1,3					
9	Analisis Data	7,5						1,9	1,9	1,9	1,9				50%
10	Desain	12,5						3,1	3,1	3,1	3,1				
11	Koding atau Pembuatan Model	25,0							6,3	6,3	6,3	6,3			
12	Prototype	2,5							0,6	0,6	0,6	0,6			
MENYUSUN LAPORAN															
13	Pemberkasan	7,5									3,8	3,8			
14	Presentasi	12,5											12,5		
15	Pelaporan	5,0											2,5	2,5	
16	Lain-Lain	2,5												2,5	
															0%
JUMLAH BOBOT		100	2,5	2,5	2,5	5,0	8,8	6,3	13,1	13,1	15,6	10,6	15,0	5,0	
BOBOT MINGGUAN KUMULATIF			2,5	5,0	7,5	12,5	21,3	27,5	40,6	53,8	69,4	80,0	95,0	100,0	

