BAB II
TINJAUAN PUSTAKA

2.1 Teori Dasar

2.1.1 Keamanan Web

Dikutip dari artikel Exabytes.co.id mengenai pengertian keamanan web, "Keamanan web atau web security yang juga dikenal sebagai "cyber security" ini pada dasarnya berarti melindungi situs web atau aplikasi web dengan mendeteksi, mencegah, dan menangani ancaman dunia maya seperti hacker".

Adapun beberapa jenis web security atau solusi teknis populer untuk mencegah threat atau ancaman meliputi:

1. Alat pengujian kotak hitam (black box testing).
2. Alat atau fuzzing tools.
3. Alat pengujian kotak putih (white box testing).
4. Firewall aplikasi web atau Web App Firewall (WAF).
5. Pemindai keamanan atau kerentanan (vulnerability or security scanner)
6. Alat peretas kata sandi (password hack tools)
7. Kemungkinan ancaman (possible threat)

Dalam membahas tentang arti web security, hal tersebut tentunya tidak terlepas juga daripada apa saja macam-macam metode ancaman pembobolan keamanan website. Diantaranya adalah:

1. *Cross-site Scripting*
2. *SQL Injection*
3. *Denial-of-Service (DoS) dan Distributed Denial-of-Service (DDoS)*
4. *Phishing*
5. *Malware*
6. *Memory Corruption*
7. *Buffer Overflow*

Dan alasan pentingnya keamanan web adalah untuk menjaga keamanan data customer, mendukung kredibilitas sebagai perusahaan yang terpercaya, mencegah terhentinya penjualan, mencegah *malware* berbahaya dan memberikan jaminan kompetitif. (Exabytes.co.id, 2021).

Terdapat sebuah organisasi nirlaba Bernama OWASP (*Open Web Application Security Project)* yang berfokus pada keamanan web app dan saat ini menjadi standar keamanan web app dunia.

Dikutip langsung sebuah penjelasan OWASP dari website resminya, "OWASP sebuah organisasi nirlaba yang fokus pada keamanan web app. OWASP

banyak menyediakan sumber daya agar dapat mempelajari lebih lanjut tentang keamanan web app."

Sebagai salah satu prinsipnya yang dipegang, OWASP memastikan bahwa semua informasi dan materi pembelajarannya yang diberikan dapat diakses dengan mudah dan gratis sehingga semua orang dapat meningkatkan keamanan website, dan materi yang OWASP sediakan berupa dokumentasi, tools, video, dan forum.

2.1.2 Pemindaian

Definisi atau arti pemindaian dalam Kamus Besar Bahasa Indonesia adalah sebuah proses, cara, perbuatan, memindai. Dan definisi dari kata memindai adalah melihat dengan cermat dan lama; memandangi. (KBBI.web.id, 2022)

Bisa didapatkan arti pemindaian dengan konteks yang lebih detail dari kamus *Oxford's English dictionary*, kata *scan* (memindai) memiliki arti yaitu melihat semua bagian dari (sesuatu) dengan hati-hati untuk mendeteksi beberapa fitur. (OED.com, 2022)

Dalam konteks judul tugas akhir ini, arti pemindaian kerentanan keamanan web adalah sebuah proses melihat satu persatu bagian komponen web untuk mendapati/mendeteksi adanya celah keamanan yang membuat web menjadi rentan untuk diretas.

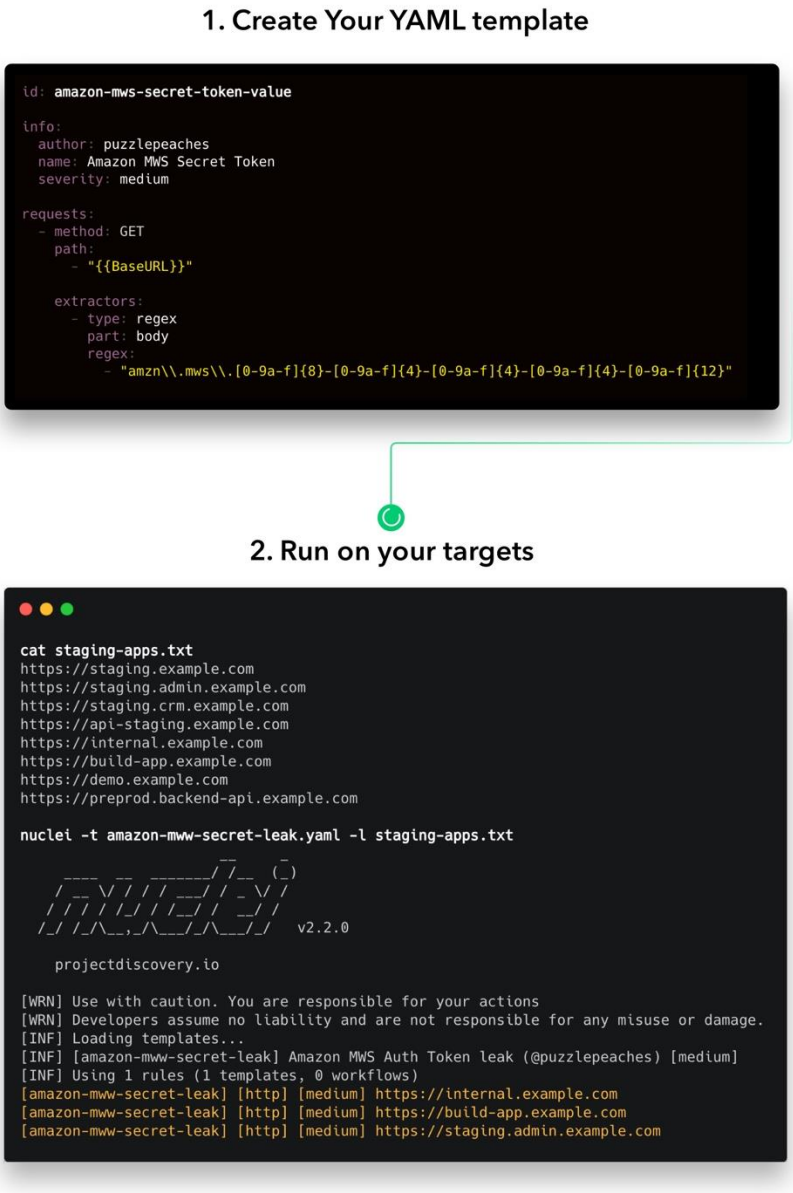
2.1.3 Nuclei

Nuclei adalah sebuah utilitas (*tools*) *Command Line Interface* (CLI) di *desktop* yang biasa digunakan oleh para profesional dibidangnya seperti *Security Engineer*, *Bug Bounty Hunters*, *Penetration Testers* dalam mempermudah pekerjaannya pemindaian/pencarian kerentanan (*vulnerability*) sistem keamanan website yang ditarget. (Projectdiscovery.io, 2022)

Cara kerja Nuclei yaitu Nuclei mengirimkan *requests* (permintaan) ke alamat web url yang ditarget untuk melakukan pemindaian kerentanan skala besar dan cepat, yang dapat memindai protokol termasuk TCP, SSH, DNS, HTTP, SSL, dan lainnya.

Nuclei memliki klasifikasi tingkatan kekerasan/keparahan (*severity*) dalam kerentanan pada suatu website, antara lain dimulai yang paling lemah:

1. *Info*
2. *Low*
3. *Medium*
4. *High*
5. *Critical*



Gambar 2.1 Cara Kerja Nuclei

Jadi, semakin kerasnya kerentanan yang ditemukan oleh Nuclei, maka semakin gentingnya hal itu harus diperbaiki segera untuk menghindari hal-hal yang tidak diinginkan.

2.1.4 *Software Development Life Cycle* (SDLC)

Pengertian SDLC dalam artikel yang dimuat oleh Dicoding mengenai SDLC, "SDLC adalah proses pengubahan dan pembuatan sistem, model, serta metodologi yang digunakan untuk mengembangkan *software*."

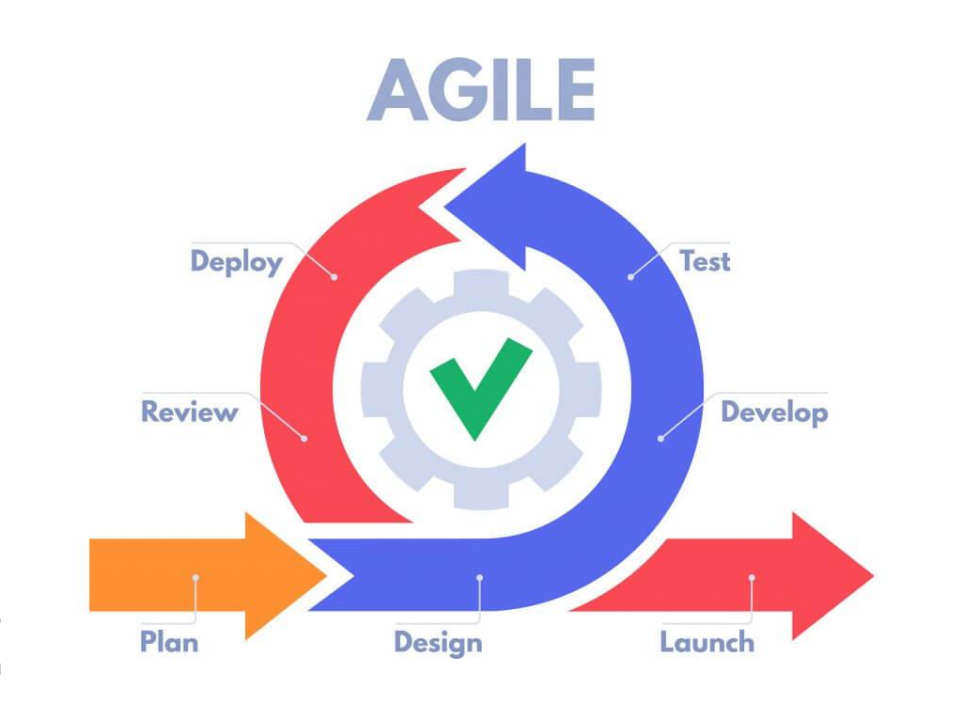
"Singkatnya, dalam dunia rekayasa *software*, ia merupakan langkah-langkah yang bisa diterapkan para *engineer* dan *developer* untuk merancang dan mengelola *software.*"

"SDLC ditujukan untuk menghasilkan *output* sistem berkualitas tinggi yang sesuai dengan ekspektasi para pengguna dan *stakeholder."*

"SDLC juga memiliki beberapa tahap kerja, termasuk *planning, design, testing, building,* dan *deployment*."

"Model SDLC yang terkenal meliputi *waterfall model, spiral model,* dan *agile model."* (Dicoding.com, 2021)

- *System Planning*
  Tahap awal yaitu (system planning) perencanaan sistem dengan pengumpulan kebutuhan dan informasi pengguna sistem yang nantinya sebagai dasar dalam pengembangan sistem.
- *System Analysis*
  Tahap selanjutnya (system analysis) analisis sistem yaitu melakukan analisis sistem yang sedang berjalan, hasil dari analisis digunakan sebagai acuan dalam system design.
- *System Design*
  Tahap system desain yaitu diagram digunakan sebagai representasi dari desain proses dan desain database dan gambar digunakan sebagai representasi dari desain visual (mockup) pada sistem yang dirancang atau dikembangkan.
- *Implementation*
  Proses implementasi sistem merupakan proses perancangan perangkat dalam melakukan pekerjaan sistem seperti penulisan kode program yang didasarkan dari hasil system design.
- *Maintenance*
  Tahapan maintenance merupakan perawatan sistem untuk mengatasi masalah yang muncul agar langsung diperbaiki pada perangkat lunak dan pengembangan sistem dimulai kembali dari tahap perencanaan sistem.



Gambar 2.2 Metode SDLC (*Software Development Life Cycle*) Agile

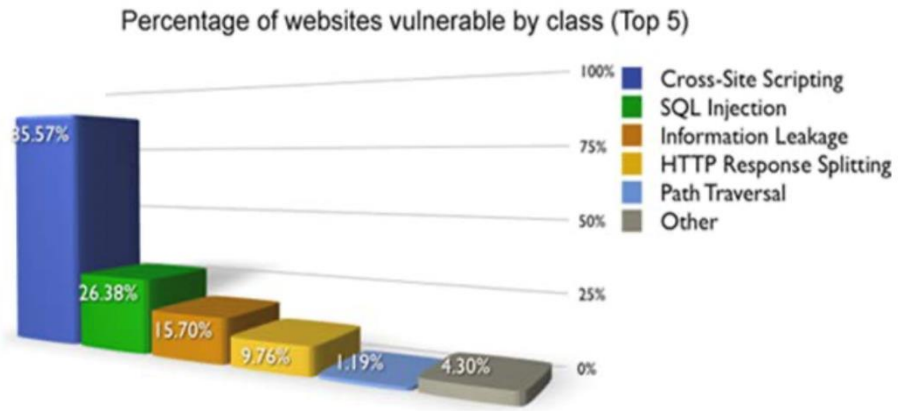
"Model *Agile* merupakan model pengembangan jangka pendek yang memerlukan adaptasi cepat dan pengembangan terhadap perubahan dalam bentuk apapun, sehingga jika terjadi ada perubahan ditengah pengembangan modul fitur akan cepat teratasi dan cepat juga dilakukan pengetesan." (Ries, Eric, 2011)

2.2 Tinjauan Studi / Pustaka

2.2.1 Jurnal Mendeteksi Kerentanan Keamanan Aplikasi Website Menggunakan Metode OWASP (Open Web Application Security Project) Untuk Penilaian Risk Rating

Dalam jurnal ini menyebutkan untuk memperkirakan kemungkinan dampak kerentanan dengan menggunakan metode OWASP dari masing-masing faktor yang dibagi dalam tiga bagian risiko yaitu *risk severity high*, *risk severity medium*, dan *risk severity low*.

Dan dalam jurnal ini dapat disimpulkan mengenai factor-faktor yang dapat menyebabkan rentannya tingkat keamanan pada aplikasi berbasi website, yaitu diantaranya kesalahan pada penulisan sebuah kode program dan juga *misconfiguration*. (Ghozali, B., Kusrini, K., & Sudarmawan, S, 2019)



Gambar 2.3 Persentase kerentanan website yang paling banyak diserang

Serta kesalahan kerentanan yang terdapat pada penulisan kode program dalam sebuah pengembangan perancangan aplikasi berbasis website sering dimanfaatkan oleh penyerang/hacker, dalam hal ini serangan yang sering menjadi celah dan dimanfaatkan oleh penyerang/hacker berdasarkan diagram yang dirilis oleh webappsec.org (Januari 2010) diantaranya adalah *XSS (35,57%)*, *SQL Injection (26,38%)* dan *Information Leakage (15,70%)*.

2.2.2 Jurnal Tanggung Jawab Tokopedia Terhadap Kebocoran Data Pribadi Konsumen

Dalam jurnal ini membahas mengenai bagaimana Tokopedia harus bertanggung jawab terhadap kasus kebocoran data pribadi konsumen yang diakibatkan peretasan dari celah kerentanan keamanan sistem Tokopedia yang dimana Indonesia saat ini sudah memiliki aturan soal perlindungan Data Pribadi. (Fathur, Muhammad, 2020)

Penulis mendapatkan kesimpulan pentingnya agar suatu sistem sercara berkala memelihara keamanan sistem yang kalau tidak, kedua belah pihak secara tidak mungkin akan mendapatkan kerugian akibat peretasan dari kerentanan keamanan sistem aplikasi ini.

Dari kerugian kedua pihak ini, seperti pihak Konsumen dirugikan atas datanya disalahgunakan oleh orang yang bertanggung jawab dan juga dari pihak yang memiliki sistem yang diretas dirugikan atas dilayangkannya gugatan kepada Menteri Komunikasi dan Informatika Republik Indonesia untuk menuntut pertanggungjawaban selaku Penyelenggara Sistem Elektronik hal ini sesuai dengan UU 19/2016 tentang Informasi dan Transaksi Elektronik, PP 71 Tahun 2019 tentang

Penyelenggaraan Sistem dan Transaksi Elektronik, dan Permenkominfo No.20 Tahun 2016 tentang Perlindungan Data Dalam Sistem Elektronik.

2.2.3 Jurnal *Security Assessment of Libyan Government Websites*

Dalam jurnal ini membahas terkait sebuah proses transformasi layanan konvesional pemerintahan libya seperti contoh layanannya antara lain pencatatan sipil, transaksi keuangan dan penanganan informasi pribadi menjadi digital / *e-government*. Dan juga membahas masalah kerentanan keamanan website yang dihadapi. (Ahmed Ali, Abdullah & Zamri Murah, Mohammad, 2018)

Dalam analisis tingkat kerentanan pada website pemerintah dengan menggunakan aplikasi testing yaitu Acunetix dan Netsparker untuk mengetahui celah-celah pada website tersebut.

Dan didapati bahwa tingkat keamanan dalam website pemerintah dari 16 website terdapat 7 website yang memiliki keamanan yang tinggi, selain itu sisa dari website tersebut memiliki kerentanan tinggi dapat ditemukan 5 website tersebut yang belum menerapkan enkripsi SSL yang mengakibatkan hilangnya data, gangguan layanan, kehilangan privasi.

Penulis menyimpulkan sangat pentingnya dilakukannya *security assessment* terhadap suatu sistem agar terhindar dari hal-hal yang merugikan.