BAB 2

TINJAUAN PUSTAKA

2.1 Penelitian Terkait

Merujuk pada studi penelitian sebelumnya yang digunakan sebagai referensi dengan tujuan untuk memperhatikan kekurangan dan kelebihan antara penelitian sebelumnya dan penelitian saat ini.

Tabel 2.1 Penelitian Terkait

Penelitian 1	
Penulis (Tahun)	Zulkifli & Samsir (2020)
Judul	Implementasi Sistem Keamanan *SQL Injection* Dalam Berbasis Web
Metode	Penelitian ini menggunakan serangan *SQL Injection.*
Hasil	Dalam penelitian ini, secara penjelasan lebih berfokus ke tahap implementasi dan tahap pengujian sistem. Kemudian model kedua, dilakukan *SQL Injection* pada *website* terhadap *login admin* dengan teknik penerapan *maxlength* dan *input type number*. Pada *form login website* yang telah dilakukan pengujian dengan menginputkan *username* dan *password* yang tidak tersedia dalam *database* dan hasilnya menunjukkan *invalid login*, yang berarti gagal untuk *login*. Kemudian pada pengujian kedua dilakukan dengan menginputkan *username* dan *password* yang ada di *database* dan hasilnya valid dan menampilkan halaman *admin*, artinya berhasil *login* dengan benar.
Penelitian 2	
Penulis (Tahun)	Hermawan (2021)

Tabel 2.1 Penelitian Terkait (Lanjutan)

Penelitian 2	
Judul	Teknik Uji Penetrasi Web Server Menggunakan *SQL Injection* Dengan *SQLmap* Di *Kalilinux*
Metode	Penelitian ini menerapkan metode *Dynamic Application Security Testing* (*DAST*) pada tahap *vulnerability detection*.
Hasil	Dalam penelitian ini, untuk melakukan uji penetrasi yaitu menggunakan *software Vmware* 15, membuat *topology* simulasi dalam penyerangan menggunakan dua komputer *virtual* di *VMWare*. Penyerang melakukan perintah menggunakan *tools SQLmap* dengan query yang diinjeksikan ke server target untuk menunjukkan *database* yang ada di web server. Berdasarkan hasil dari simulasi penyerangan *penetration testing* ini pengambil alihan server target terbukti berhasil dilakukan oleh penyerang yang dengan mudah dapat menguasai server setelah berhasil memperoleh informasi data *user* melalui serangan *SQL Injection*.
Penelitian 3	
Penulis (Tahun)	Andria dkk. (2021)
Judul	Pengujian Keamanan Basis Data Sistem Informasi Berbasis Web
Metode	Penelitian ini menerapkan metode *DAST* (*Dynamic Application Security Testing*).
Hasil	Dalam penelitian ini, dilakukan pengujian keamanan basis data *website* mulai dari tahapan *information gathering*, *vulnerability detection*, *exploitation*, sampai *reporting*. Berdasarkan pengujian yang telah dilakukan

Tabel 2.1 Penelitian Terkait (Lanjutan)

Penelitian 3	
Hasil	menggunakan aplikasi Termux dan tools SQLMap untuk menemukan celah keamanan pada *website* target, diperoleh informasi dari *vulnerability detection* bahwa ditemukannya hasil *bug SQL Injection* pada situs web target, *bug SQL Injection* ini yang disebut celah kerentanan terhadap lapisan basis data dalam *website* tersebut. Sehingga dapat dilakukan eksploitasi untuk mendapatkan akses ke dalam basis data lebih lanjut dengan mengakses *table*, *column*, sampai *record* pada basis data web.
Penelitian 4	
Penulis (Tahun)	Ojagbule et al. (2018)
Judul	*Vulnerability Analysis of Content Management Systems to SQL Injection Using SQLMAP*
Metode	Penelitian ini menerapkan metode *penetration testing* dengan menggunakan serangan *SQL Injection*.
Hasil	Kerentanan pada halaman *login default* dari ketiga situs, bahwa serangan *SQL Injection* tidak berhasil mendapatkan akses ke *database back-end*. Hal ini dikarenakan, secara default situs sudah diaktifkan *WAF* (*Web Application Firewall*) atau *IPS* / *IDS* yang menjaga aplikasi web dari serangan *SQL Injection*.
Penelitian 5	
Penulis (Tahun)	Zhang & Zhang (2018)
Judul	*SQL Injection Attack Principles and Preventive Techniques for PHP Site*

Tabel 2.1 Penelitian Terkait (Lanjutan)

Penelitian 5	
Metode	Penelitian ini menerapkan metode serangan *SQL Injection*.
Hasil	Penelitian ini membahas penyebab terjadinya serangan *SQL Injection* pada kode *PHP*, yang pada umumnya pengguna biasanya menggunakan metode *GET*, metode *POST*, dan metode *Cookie* untuk mengirimkan data menuju ke server. Berdasarkan hasil pengujian secara manual dalam sistem aplikasi web untuk mengetahui kerentanan *SQL Injection* dan hasil pengujian menunjukkan halaman sistem informasi web tidak memiliki kerentanan. Oleh karena itu penelitian ini juga membahas teknik menggunakan kerentanan *SQL Injection* dan teknik pencegahan terhadap kerentanan *SQL Injection*.
Penelitian 6	
Penulis (Tahun)	Gunawan et al. (2018)
Judul	*Penetration Testing using Kali Linux: SQL Injection, XSS, Wordpres, and WPA2 Attacks*
Metode	Penelitian ini menerapkan metode *penetration testing* pada *kali linux* menggunakan serangan *SQL Injection*, *XSS* dan *WPA2*.
Hasil	Penelitian ini membahas *penetration testing* dengan serangan *SQL Injection* menggunakan *Burp Suite* terhadap web berbasis java. Dari hasil serangan yang menggunakan *SQL Injection*, pada *file log server* dianalisis lebih lanjut menggunakan *Deep Log Analyzer* berisi folder *SQL injection*. Dari alat *SQLMap* diterima

Tabel 2.1 Penelitian Terkait (Lanjutan)

Hasil	sebanyak 399 *hits*. Kemudian saat serangan *XSS* dilakukan, *file log* akses tidak mencatat sesuatu yang signifikan, oleh karena itu *Deep Log Analyzer* tidak dapat merekam hal-hal yang mencurigakan atau berbahaya.

Dari beberapa penelitian terkait yang telah diuraikan diatas, maka dapat diambil kesimpulan bahwa terdapat letak persamaan dan perbedaan antara penelitian terdahulu. Meskipun sebagian dari penelitian terkait mempunyai persamaan pada *tools* yang digunakan dan serangan yang sama berupa *SQL Injection*. Oleh karena itu, penelitian ini akan dilakukan dengan menggunakan metode *SQL Injection* dengan membuat beberapa skema diantaranya adalah membuat *website* sendiri dan dijalankan pada web server, melakukan penyerangan terhadap *website* yang sangat rentan, dan terakhir mencoba melakukan serangan *SQL Injection* pada *website* yang dianggap sangat aman.

2.2 Landasan Teori

2.2.1 Internet

Internet adalah jaringan yang digunakan untuk mendapatkan informasi di seluruh dunia dengan protokol *TCP* melalui perangkat keras sebagai perantara. Dalam artikel yang berjudul "*What Is the Internet? Meaning, Working, and Types*" diakses pada tanggal 24 Februari 2023 yang ditulis oleh BasuMallick (2023), bahwa Internet adalah jaringan komputer, *server*, telepon, dan perangkat pintar secara global yang saling terhubung melakukan komunikasi satu sama lain dengan menggunakan *Transmission Control Protocol* (*TCP*) standar untuk memungkinkan pertukaran data dan file yang cepat di antara layanan lainnya.

Internet juga disebut sebagai jaringan komputer yang terhubung. Koneksi internet yang terhubung dapat berjalan ketika pengguna di *workstation* mana pun mampu menerima data dari setiap sistem lain (pengguna yang bekerja sering berinteraksi dengan komputer). Infrastruktur internet terdiri dari kabel transmisi

data berupa *fiber optic* atau kabel tembaga serta berbagai infrastruktur jaringan seperti *Local Area Network* (*LAN*), *Wide Area Network* (*WAN*), *Metropolitan Area Network* (*MAN*). Terkadang layanan nirkabel seperti *4G* dan 5G serta *WiFi* memerlukan pemasangan kabel fisik serupa untuk terhubung ke Internet. Salah satu organisasi yang menerapkan internet yaitu *Internet Corporation for Assigned Names and Numbers* (*ICANN*) di negara Amerika Serikat, organisasi tersebut mengontrol internet dan teknologi terkaitnya menggunakan alamat *IP* (Ravat, 2023).

Internet mengirimkan berbagai jenis informasi dan media antar perangkat yang terhubung ke jaringan. Internet akan berjalan dengan jaringan *Internet Protocol* (*IP*) dan jaringan perutean paket *Transport Control Protocol* (*TCP*). Setiap kali pengguna yang mengunjungi sebuah situs web, komputer atau ponsel akan meminta *server* untuk menggunakan protokol ini. Menurut (Fanggidae et al., 2019), *server* adalah sistem komputer yang ada di jaringan komputer untuk memberikan layanan kepada pengguna yang biasa disebut *client*.

2.2.2 Cyber Crime

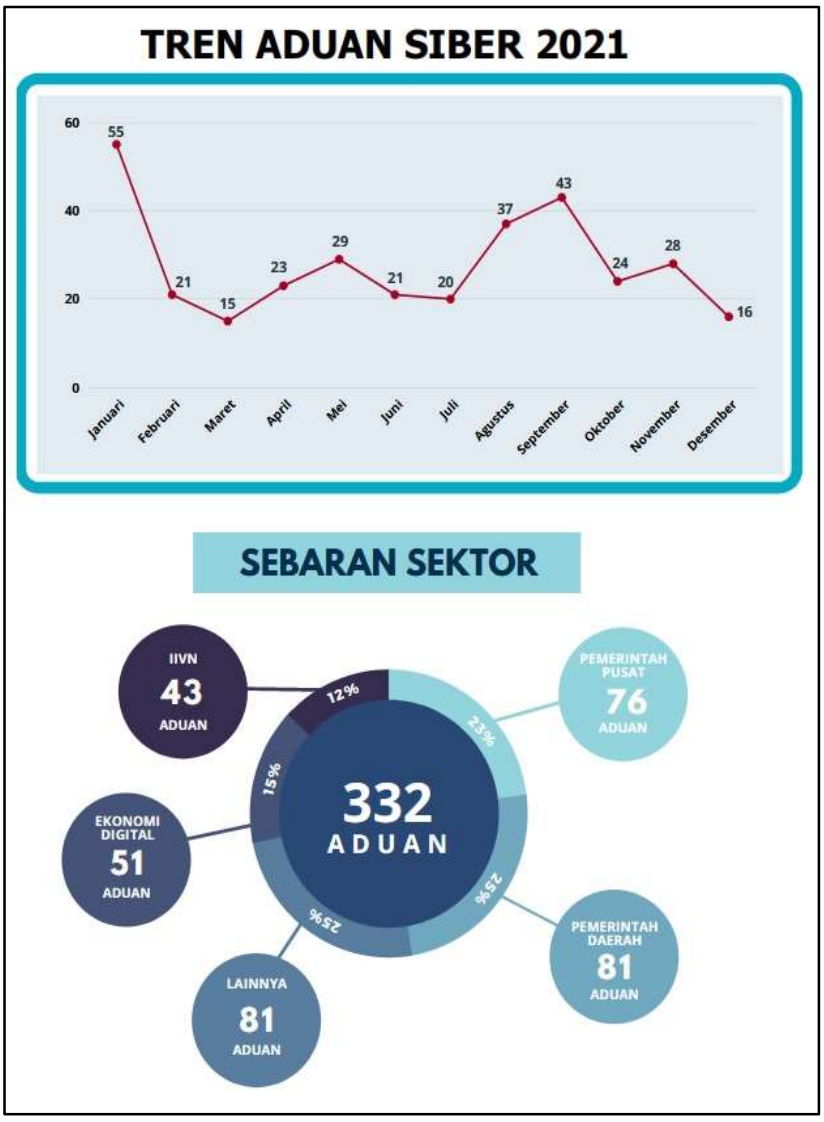
Perkembangan teknologi informasi di sisi lain mengubah tatanan dan perilaku masyarakat. Bahkan tidak berhenti sampai di situ, tetapi juga mengubah realitas ekonomi, budaya, politik, dan hukum. Oleh karena itu, dibalik manfaat positifnya, teknologi internet juga memiliki dampak negatif yang kecil. Salah satunya digunakan sebagai sarana untuk melakukan kejahatan yang selanjutnya disebut *cyber crime* atau kejahatan jaringan informasi. Selain disebut sebagai *cyber criminal*, istilah ini juga disebut sebagai *computer crime*, yaitu suatu jenis kejahatan manusia yang dilakukan di dunia maya atau internet dengan menggunakan komputer untuk menghasilkan uang. Dengan mendapatkan keuntungan sebanyak-banyaknya dari orang lain, baik dengan menipu, menipu publik, meretas akun orang lain, atau mengacaukan sistem informasi negara (Koto, 2021).

Dengan pesatnya perkembangan teknologi Web 2.0, jaringan aplikasi secara bertahap menjadi bagian integral dari kehidupan kita. Pada saat yang sama,

aplikasi web menghadapi tantangan lain. Seperti yang dilaporkan oleh organisasi standar keamanan OWASP, serangan injeksi termasuk di antara sepuluh kerentanan teratas pada tahun 2013 dan 2017, dan serangan *SQL Injection* adalah salah satu jenis serangan injeksi yang utama (Li et al., 2019).

Gambar 2.1 Statistik jenis serangan pada aduan siber tahun 2021
Sumber: (Sandy, 2022)

Pada gambar 2.1 yang menunjukkan jenis serangan yang dilaporkan pada Badan Siber dan Sandi Negara (BSSN) telah menerima 332 pengaduan tindakan *cyber crime* pada tahun 2021. Jenis serangan yang paling sering dilaporkan adalah serangan *SQL Injection*, dengan 79 pengaduan. BSSN menerima aduan *Cyber* ini dari *Cyber Plant Center* melalui telepon, *email* atau langsung ke BSSN. Pelaporan tersebut dilakukan secara individu ataupun organisasi (Sandy, 2022).



Gambar 2.2 Statistik tren aduan sebaran sektor siber 2021
Sumber: (Sandy, 2022)

Selain itu, pada gambar 2.2, terdapat 332 pengaduan siber yang diterima BSSN, pengaduan terbanyak berasal dari “Pemerintah Daerah” dan “Lainnya”, masing-masing sebanyak 81 pengaduan. Diikuti oleh "Pemerintah Pusat" dengan 76 pengaduan, "Ekonomi Digital" dengan 51 pengaduan dan "Infrastruktur Informasi Vital Nasional (IIVN)" dengan 43 pengaduan (Sandy, 2022).

Terdapat beberapa penyebab terjadinya tindakan *cyber crime* antara lain kemudahan dalam mengakses internet yang tidak terbatas, kesalahan pengguna komputer, keamanan yang mudah diabaikan dan tidak memerlukan peralatan

canggih, pelaku termasuk orang yang cenderung cerdas, sangat ingin tahu dan fanatik terhadap teknologi informasi, lemahnya sistem *cyber security* yang digunakan, kurangnya kesadaran dan perhatian serta penegakan hukum dari masyarakat (Dermawan, 2018).

2.2.3 Vulnerability

Keamanan jaringan adalah area keamanan teknologi informasi yang harus dijaga dengan baik. Dengan adanya keamanan jaringan maka istilah *vulnerability* banyak didengar oleh seluruh dunia. Dalam artikel yang berjudul "*Vulnerability*: Pengertian, Penyebab, Contoh, Cara Mengatasi" yang diakses pada 3 Maret 2023 oleh Fitriani (2021), bahwa *vulnerability* atau yang disebut dengan *bug* adalah suatu kesalahan ataupun cacat pada kerangka suatu aplikasi yang menyebabkan pertahanannya menjadi lemah atau rentan, sehingga menggunakan program *antivirus* merupakan salah satu cara agar mampu memperbaiki *bug* tersebut.

Vulnerability ini dapat disebabkan karena kesalahan dalam perancangan atau dalam pembuatan dan implementasi sistem. Dalam artikel yang berjudul "Jenis-jenis *Vulnerability* pada Keamanan Jaringan" yang diakses pada 4 Maret 2023 oleh Irfansyah (2023), menjelaskan terkait *bug* atau *vulnerability* biasanya tercipta didalam perangkat lunak. *Vulnerability* pada perangkat lunak tergolong berbahaya karena dapat dieksploitasi dari jarak jauh. Dan terdapat beberapa *vulnerability* pada *software* karena mempunyai celah keamanan yang berisiko tinggi antara, lain *vulnerability* yang terdapat pada aplikasi *web*, *vulnerability* yang terdapat pada *firmware*, *vulnerability* yang terdapat pada sistem operasi, *vulnerability* yang terdapat pada *brainware*, *vulnerability* yang terdapat pada *software*.

Untuk menghindari celah keamanan yang terdapat pada suatu sistem maka dapat dilakukan *vulnerability assessment* secara berkala agar cepat mengetahui kerentanan yang paling berbahaya sebelum terjadi peretasan. Menurut Nagpure & Kurkure (2018), *vulnerability assessment* adalah metode yang menguji keamanan aplikasi interaktif seperti *e-banking*, siaran berita, dan web belanja online.

2.2.4 Website

Menurut Asmara (2019), *website* adalah kumpulan yang berisi halaman-halaman web yang ditemukan dalam nama domain yang menampilkan informasi. Secara teknis, *website* dikenal juga dengan kumpulan halaman web terkait yang dikelompokkan berdasarkan nama atau alamat web secara unik untuk mengidentifikasi *web server*.

Web server terdiri dari *software* dan *hardware* yang menggunakan *HTTP* (*Hypertext Transfer Protocol*) dan protokol lain untuk memberikan respons terhadap permintaan klien yang dibuat melalui *World Wide Web*. Fungsi utama *web server* adalah untuk menampilkan berbagai konten *website* dengan cara menyimpan, memproses, dan mengirimkan halaman web kepada pengguna. Selain *HTTP*, *web server* juga mendukung *SMTP* (*Simple Mail Transfer Protocol*) dan *FTP* (*File Transfer Protocol*), yang digunakan dalam *email*, transfer file, dan penyimpanan. *Web server* terbagi menjadi dua tipe yaitu *web server* dinamis dan *web server* statis (Alexander S. Gillis, 2020).

Setiap *website* yang tersedia dalam internet dibuat untuk maksud atau tujuan tertentu. Dalam artikel Tonjoo yang berjudul "10 Fungsi, Manfaat dan Keuntungan Memiliki *Website* Yang Perlu Anda Ketahui" oleh Andayani (2021), menjelaskan tentang *website* yang mempunyai fungsi utama yaitu sebagai sarana dalam memberikan informasi, sebagai sarana komunikasi secara *real time*, sebagai sarana dalam bertransaksi secara *online* (*Ecommerce*), sebagai *branding* yang menampilkan profil sebuah perusahaan atau instansi, sebagai sarana *marketing* / promosi tanpa batas, sebagai *virtual asset* atau sumber keuntungan bagi bisnis.

2.2.5 Database

Sederhananya, data dapat berupa fakta yang terkait dengan objek apapun yang dipertimbangkan misalnya seperti nama, umur, tinggi, berat badan dan lain-lain. Data sangat penting karena berisi informasi pribadi. Data juga dapat berupa gambar, *file*, *pdf*, dan lain-lain. Menurut Setyawati dkk. (2020), *database* adalah sekumpulan tabel data yang berisi informasi terkait dan *database* dapat terdiri dari satu atau lebih tabel.

Adapun *database* berdasarkan jenis dari pendekatan yang paling umum seperti *database* relasional (*database* relasional terdiri dari tabel yang datanya sesuai dengan kategori yang telah ditentukan sebelumnya), *database* terdistribusi (*database* terdistribusi biasanya disimpan di beberapa lokasi fisik dan pemrosesan didistribusikan atau direplikasi ke lokasi berbeda di jaringan), *database cloud* (*database cloud* biasanya berjalan pada platform komputasi awan). Layanan *database cloud* menyediakan akses ke dalam *database*, dan *database NoSQL*. Selain itu terdapat lima komponen utama dalam *database* yang meliputi, *hardware*, *software*, data, prosedur dan bahasa untuk mengakses *database* (Saxena, 2022). Salah satu contoh dari *database* relasional yaitu DBMS.

Database Management System (*DBMS*), sering disebut sebagai *Database Management* dalam bahasa Indonesia, adalah perangkat lunak yang mengelola dan mengeksekusi *query database*. Perangkat lunak *DBMS* digunakan untuk mengelola basis data secara efektif dan efisien, mulai dari pembuatan basis data hingga operasi terkait seperti memasukkan data, mengedit data, menghapus data, dengan kueri secara efektif. *Relasional Database Management System* (*RDBMS*), yang merepresentasikan data dalam bentuk tabel tertaut, adalah salah satu jenis *DBMS* yang paling populer saat ini. Tabel terdiri dari baris (*record*) dan kolom (*field*) yang berisi data (B. Rawat et al., 2021).

2.2.6 Structured Query Language (SQL)

SQL merupakan kepanjangan dari *Structured Query Language* atau dikenal juga dengan bahasa perintah yang digunakan untuk mengelola data dalam *database*. Menurut Pamungkas (2018), *SQL (Structured Query Language)* adalah bahasa terstruktur yang dapat digunakan untuk mengakses data *database* dan entitas dalam *database*. *SQL* juga merupakan bahasa standar yang digunakan dalam *database* yang ada, sehingga memudahkan bahkan saat berpindah dari satu *database* ke *database* lainnya.

SQL mampu membantu mengontrol informasi yang tersimpan dalam *database*, sehingga pengguna dapat dengan mudah mengambil data secara spesifik yang diinginkan sesuai kebutuhannya dengan model *database* relasional.

Menurut Idrus dkk. (2019), *database* relasional adalah *database* yang di mana data akan disimpan dalam bentuk tabel dan ada hubungan antar tabel serta aspek yang terlibat dalam *database* relasional meliputi tabel, kolom, tipe data, lebar data, *primary key*, *secondary key*, *foreign key*, *index*, relasi, dan tipe relasi. Sehingga perintah *SQL* menjadi pilihan dalam mengelola basis data.

Perintah *SQL* yang sangat sederhana telah menjadi pilihan populer untuk pemrograman basis data selama bertahun-tahun. Karena itu, *SQL* sebagai bahasa *database* tersendiri dari bahasa pemrograman lain. Bahasa *SQL* populer karena mempuyai beberapa manfaat dalam penggunaannya pada *database* seperti bahasa yang *portable* sehingga dapat digunakan di server, komputer pribadi, laptop, dan juga ponsel, untuk menggunakan bahasa *SQL* tidak harus mempunyai keterampilan dalam pengkodean, *SQL* melakukan pemrosesan *query* yang cepat dengan tetap menjaga akurasi data, dan sangat mudah diakses karena kompatibel dengan *database* seperti *Microsoft Access*, *MySQL*, dan lainnya (Menon, 2022).

2.2.7 SQL Injection

SQL Injection adalah kegiatan meretas yang dilakukan dalam aplikasi *client* dengan memodifikasi perintah *SQL* dalam *database* aplikasi klien, untuk melakukan teknik yang dieksploitasi oleh aplikasi yang mendasarinya, di mana sistem menggunakan *database* untuk menyimpan data (Bastian dkk., 2020).

Serangan *SQL Injection* mempunyai beberapa metode dalam menemukan kerentanan *database*. Menurut Hu et al. (2020) terdapat beberapa metode untuk melakukan serangan *SQL Injection* terhadap kerentanannya antara lain *tautologies*, *union queries*, *error-based*, *boolean-based*, *time-based*, *out of band exploitation technique*, *out of band*, *piggy – backed queries attacks*, *stored procedure injection*, *encoding attacks*.

Jika terjadi serangan *SQL Injection* dengan metode tertentu maka akan menimbulkan berbagai ancaman yang datang. Menurut Lika dkk. (2018), terdapat beberapa ancaman dari serangan *SQL Injection* seperti *identify spoofing*, mengubah data asli, memodifikasi data, mendapatkan akses secara penuh, penolakan layanan, mendapatkan akses atas informasi yang sangat sensitif.

2.2.8 Penetration Testing

Penetration testing (juga dikenal dengan *pentest*) adalah proses yang secara terstruktur untuk menguji keseluruhan dari bagian sistem komputasi yang mencari kerentanan seperti konfigurasi sistem, *bug software* dan *hardware*, serta proses operasionalnya dalam mengidentifikasi kelemahan tersebut (Al Shebli & Beheshti, 2018).

Menurut S. Rawat et al. (2020), *penetration testing* dilakukan dengan *tools* seperti *Nikto*, *SQLMap*, dan *XSStrike*. Selain itu dalam melakukan *penetration testing* diperlukan tahapan ataupun proses dalam mencari kerentanan suatu sistem. Menurut (Khera et al., 2019), tahapan pada *penetration testing* meliputi *scope*, *reconnaissance*, *vulnerability detection*, *information analysis and planning*, *penetration testing*, *privilege escalation*, *result analysis*, *reporting*, dan *clean-up*. Adapun *tools* dalam *vulnerability detection* yang akan digunakan, yaitu:

1. *Nmap*

   Nmap adalah singkatan dari "*Network Mapper*". Nmap adalah alat penemuan jaringan dan audit keamanan *open source* gratis. Nmap menggunakan paket IP *raw* untuk menentukan *host* yang tersedia di jaringan. Ini digunakan untuk pemindaian *port* untuk menemukan *port* terbuka di *host*. *Nmap* juga menentukan layanan yang disediakan oleh *host* yang tersedia (nama dan versi aplikasi), sistem operasi dan versi sistem operasi yang digunakan, dan jenis filter *firewall*/paket yang digunakan. Nmap adalah alat yang fleksibel, sederhana, portabel, kuat, gratis, didukung, didokumentasikan dengan baik, dikenal dan populer. Nama belakang menyediakan pencarian *host*, layanan, dan identifikasi sistem operasi. Menggunakan skrip *nmap* menyediakan *vulnerability detection*, *services detection*, dan fitur lainnya (Chhillar & Shrivastava, 2021).

2. *Nikto*

   Nikto dapat digunakan secara gratis dan berfungsi sebagai *vulnerability scanner* yang bersifat *open source*. Nikto memindai server web untuk mencari potensi yang menimbulkan masalah berbahaya dan

kerentanan keamanan seperti kesalahan dari konfigurasi server dan *software*, program dan *file default*, *file* dan program yang tidak aman, serta server dan program yang telah habis masa berlakunya (Siva Prasad et al., 2018).

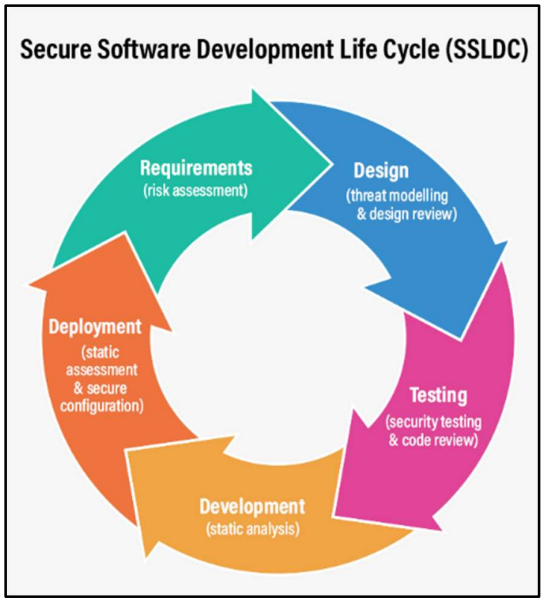
Selain itu, *tools* dalam *penetration testing* yang akan digunakan, yaitu:

1. *SQLmap*

   SQLmap berfungsi untuk melakukan metode *SQL Injection* dalam meretas *database* situs web, yang dimana saat menyalahgunakan server situs web akan ditambahkan perintah *SQL Injection* secara jelas. *Tools* ini merupakan *software* yang gratis untuk melakukan pengujian penetrasi yang mampu mendeteksi secara efektif untuk menemukan informasi dan mengakses sistem *record* untuk menjalankan urutannya (Samantha & Phanindra, 2018).

2.2.9 SSDLC

Menurut Banowosari & Gifari (2019), *SSDLC* (*Secure Software Development Lifecycle*) adalah model proses yang digunakan oleh organisasi atau perusahaan untuk membuat aplikasi yang aman, sehingga proses *SSDLC* menentukan bagaimana cara menyatukan keamanan ke dalam proses pengembangan *software*.



Gambar 2.3 Contoh tahapan proses dari SSDLC
Sumber: (Bora, 2021)

Dalam artikel yang berjudul "*Adopting secure software development lifecycle for safer path to production*" diakses pada tanggal 20 Maret 2023 oleh Bora (2021), bahwa *SSDLC* mempunyai tahapan dengan 5 fase yaitu *requirement collection and analysis*, *design*, *development*, *testing*, *deployment* & *maintenance* dan fase ini ditunjukkan pada gambar 2.3 diatas.