BAB II

KAJIAN PUSTAKA

A. Tinjauan Pustaka

Dengan dipilih nya judul penelitian ini, peneliti telah mencari dan menemukan beberapa penelitian yang terkait yang pernah dilakukan sebelumnya. Penelitian pertama Penelitian yang dilakukan oleh Riska Handayani, Zul Rachmat, Wahyuddin pada tahun 2022 dengan judul Perancangan Aplikasi *E-Learnin*g Berbasis *Website* Pada SMP Negeri 3 Watansoppeng. Dikembangkan aplikasi *e-learning* untuk SMP Negeri 3 Watansoppeng yang bertujuan untuk mengoptimalkan proses belajar mengajar, *e-learning* yang dirancang diharapkan dapat membantu baik untuk peserta didik maupun tenaga pengajar dalam mengikuti proses pembelajaran meskipun tidak berada di ruang kelas. Dengan mengakses *website e-learning* peserta didik tetap dapat mengikuti kelas dan tenaga pengajar tetap bisa mendistribusikan materi maupun soal-soal Latihan untuk peserta didik (Handayani et al., 2022). Hasil perancangan tersebut diperoleh sebuah sistem *e-learning* yang dapat digunakan oleh SMP Negeri 3 Watansoppeng namun dalam perancangan ini hanya sebatas pengembangan *website* dan untuk sisi keamanan hanya dilakukan diferensiasi kewenangan pengguna tanpa adanya implementasi keamanan lain untuk *platform e-learning*.

Penelitian yang dilakukan oleh Arfan Dwi Madya, Bagas Djoko Haryanto, Devi Putri Ningsih, Fried Sinlae pada tahun 2023 dengan judul

Keefektifan Metode Proteksi Data dalam Mengatasi Ancaman Cybersecurity. Dilakukan penekanan pentingnya keamanan *cyber* dalam menjaga data, privasi, dan kelancaran layanan. Ancaman *cyber* mencakup berbagai jenis, seperti fisik, logikal, dan Operasional (Dwi Madya et al., 2023). Namun dalam penelitian ini hanya sebatas penekanan pada pentingnya keamanan *cyber* dalam menjaga data, privasi, dan kelancaran layanan.

Penelitian lain yang dilakukan oleh Arief Budiman, Syaiful Ahdan, Muhammad Aziz tahun 2021 dengan judul Analisis Celah Keamanan Aplikasi *Web E-Learning* Universitas ABC Dengan *Vulnerability Assesment.* Pada penelitian ini, membahas mengenai *vulnerability analysis* dengan menggunakan metode *vulnerability assessment* yang dimana peneliti menggunakan beberapa tahapan dengan rincian *Vulnerability Scanning*, *Vulnerability Port Service*, dan Persentase *Vulnerability Scanning* (Budiman et al., 2021). Pada penelitian ini hanya dilakukan Analisa celah tanpa adanya implementasi atau perbaikan keamanan untuk aplikasi *web e-learning* milik universitas ABC dan peneliti juga mengharapkan agar pemilik sistem melakukan perbaikan dan evaluasi terhadap sistem yang mereka miliki sesuai dengan hasil yang didapatkan dari penelitian.

Pada penelitian yang dilakukan oleh Maurice Frayssinet Delgado, Doris Esenarro, Francisco Fernando Juárez Regalado, Mónica Díaz Reátegui 2021 dengan judul *Methodology Based On The NIST*

Cybersecurity Framework As A Proposal For Cybersecurity Management In Government Organization. Dilakukan analisa dan usulan terkait penggunaan *NIST Cybersecurity Framework*. Penelitian ini bertujuan untuk mengusulkan penggunaan metodologi berbasis Kerangka Kerja *NIST* untuk manajemen keamanan *cyber* yang memadai di organisasi pemerintah dalam kerangka penyediaan layanan *digital* (Frayssinet Delgado et al., 2021). Namun Dalam penelitian ini hanya sebatas analisa dan usulan terkait penggunaan *NIST Cybersecurity Framework*.

Pada penelitian yang dilakukan oleh Vicky Mahendra, Benfano Soewito 2023 dengan judul Penerapan Kerangka Kerja *NIST Cybersecurity* dan *CIS Controls* Sebagai Manajemen Risiko Keamanan Siber. Dilakukan pengukuran kematangan keamanan siber pada infrastruktur aplikasi sehingga dapat mengurangi kemungkinan terjadinya serangan siber (Mahendra & Soewito, 2023). Pada penelitian ini dilakukan analisa dan manajemen resiko terkait kerentanan pada aplikasi, pada penelitian ini juga dilakukan mitigasi terhadap kerentanan yang terdapat dalam aplikasi.

Pada penelitian yang dilakukan oleh Andria, Wahyu Ambar Ningrum, Iqbal Mubarok 2021 dengan judul Pengujian Keamanan Basis Data Sistem Informasi Berbasis Web. Dilakukan pengujian keamanan basis data pada sistem informasi berbasis web dengan melakukan simulasi pada situs web yang memiliki celah kerentanan menggunakan media perangkat Smartphone bersistem operasi Android dengan bantuan aplikasi Termux yang didalamnya di install tool SQLMap (Andria et al., 2021). Pada

penelitian ini digunakan sistem informasi berbasis *web* yang memang dirancang oleh developer untuk digunakan sebagai media belajar melakukan *penetration testing*.

B. Landasan Teori

1. Analisa

Secara umum analisis adalah tindakan mengamati suatu objek dengan cara mendeskripsikan bagian-bagian penyusunnya dan menyusun kembali komponen-komponen tersebut agar dapat dipelajari secara detail. Dalam arti lain, analisis adalah kemampuan untuk memecah atau mendeskripsikan suatu dokumen menjadi komponen-komponen yang lebih kecil untuk memudahkan pemahaman dan pembelajaran. (Syafitri, 2020)

Sedangkan dikutip dari Wikipedia, Analisis melibatkan pengamatan perilaku suatu objek dengan mendeskripsikan komposisinya dan menata ulang komponen-komponennya untuk dipelajari atau dipelajari secara rinci. Kata analisis berasal dari bahasa Yunani Kuno *ἀνάλυσις* (menganalisis, "memecahkan" atau "menguraikan" dari ana- "berdiri, secara menyeluruh" dan lysis "melonggarkan"). (Wikipedia, 2024c)

Menurut peneliti, analisa adalah proses sistematis dalam memahami, menafsirkan, dan mengevaluasi informasi dan data untuk mendapatkan pemahaman yang lebih mendalam tentang suatu topik atau isu tertentu. Dalam pengertian yang lebih luas, analisa melibatkan pemecahan data

menjadi bagian-bagian yang lebih kecil, mengidentifikasi pola, hubungan, dan tren, serta membuat kesimpulan dan rekomendasi berdasarkan hasil tersebut.

2. *Cybersecurity*

Keamanan siber adalah praktik melindungi perangkat komputer, perangkat seluler, *server*, sistem elektronik, jaringan, dan data dari berbagai jenis serangan *digital* berbahaya. Serangan *digital* berbahaya ini sering disebut serangan *cyber*. (Diapoldo et al., n.d., 2022.)

Sedangkan menurut Dicoding, Keamanan siber berasal dari dua kata dalam bahasa Inggris: *cyber* yang berarti dunia maya (*internet*) dan *security* yang berarti keamanan. Sederhananya, keamanan siber adalah suatu bentuk perlindungan terhadap sistem yang terhubung ke *Internet*. Ini termasuk perangkat keras, perangkat lunak, dan data yang kita miliki. (Dicoding Intern, 2023)

Berdasarkan kesimpulan diatas, peneliti dapat menyimpulkan bahwa *Cybersecurity* adalah kebijakan dan prosedur yang dirancang untuk melindungi sistem komputer, jaringan, perangkat elektronik dan data dari serangan, penggunaan yang tidak sah, kerusakan atau pencurian. *Cybersecurity* berfokus pada menjaga kerahasiaan, integritas, dan ketersediaan informasi yang disimpan dan dipertukarkan secara elektronik.

3. *Framework*

Menurut Annisa, pengertian dari *framework* adalah seperangkat instruksi atau fungsi dasar yang mengatur aturan-aturan tertentu dan interaksi satu sama lain. (Annisa, 2023)

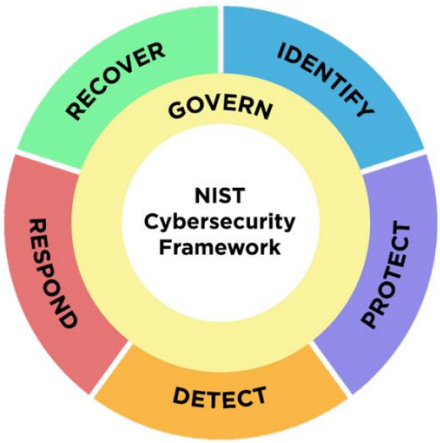
Sedangkan menurut Rony Setiawan, *framework* adalah kerangka kerja yang digunakan untuk pengembangan *website*. Kerangka kerja ini dibuat untuk membantu pengembang *web* menulis baris kode. Dengan menggunakan *framework coding* maka akan lebih mudah, cepat dan terstruktur. (Rony Setiawan, 2021)

Secara umum, "*Framework*" mengacu pada struktur konseptual yang memberikan pedoman, aturan, atau prinsip untuk mengatur dan membimbing proses, pengembangan, atau pemecahan masalah dalam bidang tertentu. *Framework* dapat membantu dalam membuat rencana, menyederhanakan kompleksitas, dan menerapkan praktik efektif secara konsisten.

4. ***NIST Cybersecurity Frameworks***

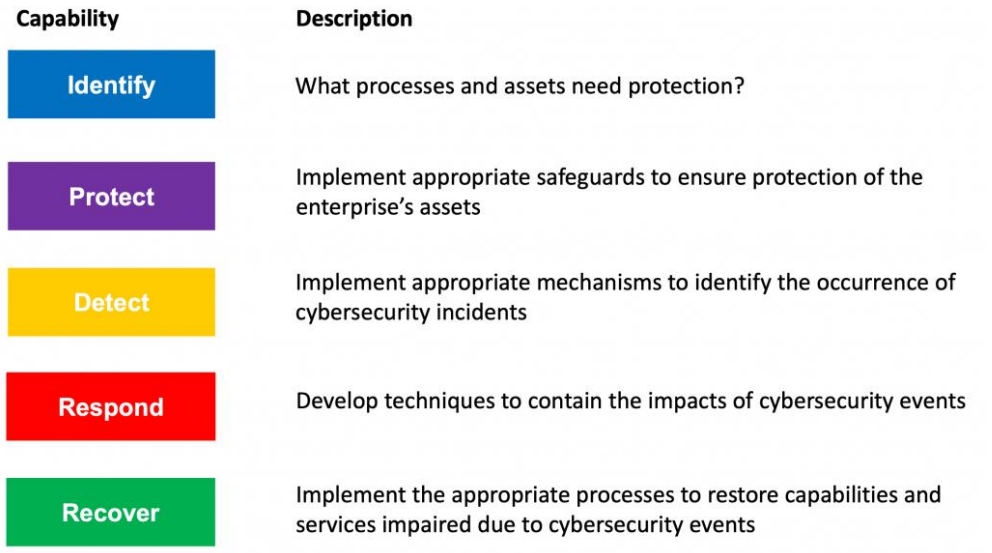
Dikutip dari Wikipedia, *NIST Cybersecurity Framework* (*CSF*) adalah serangkaian pedoman untuk mengurangi risiko keamanan *cyber* organisasi, yang diterbitkan oleh Institut Nasional Standar dan Teknologi Amerika Serikat (*NIST*) berdasarkan standar, pedoman, dan praktik yang sudah ada. (Wikipedia, 2024d)

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Cybersecurity Supply Chain Risk Management	GV.SC
	Roles, Responsibilities, and Authorities	GV.RR
	Policies, Processes, and Procedures	GV.PO
	Oversight	GV.OV
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO



Gambar 2.1 *Framework NIST Cybersecurity*

Sedangkan menurut Rexy, Kerangka Keamanan Siber *NIST* adalah sebuah panduan yang diterbitkan oleh *National Institute of Standards and Technology* (*NIST*) di Amerika Serikat. Kerangka kerja ini dirancang untuk membantu organisasi dalam meningkatkan keamanan siber mereka secara terstruktur dan terukur. (Rexy, 2023)



Gambar 2.2 Deskripsi Setiap Fungsi Dalam *NIST Cybersecurity Framework*

Menurut peneliti, *NIST Cybersecurity Framework* adalah sebuah Kerangka kerja yang dirancang untuk membantu bisnis mengelola dan meningkatkan keamanan siber mereka. Tujuan utamanya adalah untuk memberikan panduan tentang bagaimana organisasi dapat mengelola risiko keamanan dalam infrastruktur informasi dan teknologi mereka.

5. *Linux*

Dikutip dari Wikipedia, Linux adalah keluarga sistem operasi mirip *Unix* yang gratis dan *open source* berdasarkan *kernel Linux,* yang pertama kali dikembangkan oleh Linus Torvalds pada tahun 1991. (Wikipedia, 2024b)

Sedangkan menurut Aorinka Anendya, Linux adalah sebuah sistem operasi bersifat open source. Yang membedakan sistem operasi ini yaitu Windows dan iOS biasanya hanya digunakan untuk end-user sedangkan Linux dapat dimanfaatkan dalam pengembangan perangkat maupun oleh end-user. (Anendya, 2024)

Menurut peneliti, *linux* adalah sistem operasi komputer berbasis *open source* berdasarkan *kernel linux*. *kernel linux* sendiri awalnya dikembangkan oleh Linus Torvalds pada tahun 1991 dan sejak itu menjadi salah satu sistem operasi terpopuler di seluruh dunia, terutama di lingkungan *server* dan komputasi berbasis *cloud*.

Pada penelitian ini digunakan sistem operasi *Kali Linux, Kali Linux* adalah sistem operasi *open source* yang dapat digunakan untuk pengujian penetrasi sistem dan jaringan komputer. Terdapat lebih dari

300 alat dengan fungsi terkait yang dapat digunakan untuk melakukan pengujian keamanan pada sistem jaringan. *Kali Linux* dikembangkan dan disponsori oleh *Offensive Security*. (Andria, 2020)

6. *E-Learning*

Menurut Eka Septiani, *E-learning* dalam arti luas mencakup proses pembelajaran yang dilakukan dengan menggunakan media elektronik, seperti menggunakan *internet*, baik secara formal maupun informal. (Septiani, 2018)

Sedangkan menurut kutipan dari jurnal lain *E-learning* merupakan metode pembelajaran dengan menggunakan media elektronik (audio visual) melalui *internet*.. (Setiawan et al., 2019)

Menurut peneliti, istilah *e-learning* sendiri memiliki arti electronic learning atau pembelajaran elektronik. Merupakan metode pembelajaran yang memanfaatkan teknologi digital seperti komputer dan internet untuk memberikan materi pembelajaran kepada siswa.

7. Aplikasi

Menurut Wikipedia, Aplikasi adalah sebuah subkelas perangkat lunak komputer yang secara langsung menggunakan kemampuan komputer untuk melakukan tugas yang diinginkan oleh pengguna. Biasanya dibandingkan dengan perangkat lunak sistem yang mengintegrasikan berbagai fitur komputer tetapi tidak secara langsung menerapkan fitur tersebut untuk melakukan tugas yang diperintahkan oleh pengguna. (Wikipedia, 2023)

Menurut Mila Rosyida, Aplikasi adalah merujuk pada program komputer yang dirancang untuk berjalan pada perangkat seluler seperti smartphone atau tablet. Aplikasi dapat memiliki berbagai fungsi, seperti permainan, media sosial, e-commerce, pendidikan, kesehatan, dan masih banyak lagi. (Mila Rosyida, 2023)

Sedangkan menurut peneliti, Aplikasi adalah program komputer yang dirancang untuk melakukan tugas tertentu atau menyediakan layanan kepada pengguna. Hal ini berupa perangkat lunak desktop, perangkat lunak seluler, atau aplikasi web yang dijalankan melalui browser internet. Fungsi dan tujuan aplikasi bervariasi mulai dari produktivitas, hiburan, dan komunikasi hingga pengelolaan dan pemrosesan data.

8. Aplikasi Berbasis *Web*

Menurut Robith Adani aplikasi *web* sendiri diartikan sebagai aplikasi yang dikembangkan dalam *HTML*, *PHP*, *CSS*, atau *JS* yang memerlukan *server web* dan *browser* untuk menjalankannya, seperti *Chrome*, *Firefox*, atau *Opera*. Aplikasi *web* dapat berjalan di *Internet* atau jaringan area lokal (*LAN*).. (Adani, 2018)

Dikutip dari Wikipedia, aplikasi berbasis web adalah aplikasi yang diakses menggunakan *browser web* melalui jaringan seperti *internet* atau *intranet*. Ini juga merupakan aplikasi perangkat lunak komputer yang dikodekan dalam bahasa yang didukung *browser web* (*ASP*, *Perl*,

Java, *JavaScript*, *PHP*, *Python*, *Ruby,* dll.) dan bergantung pada browser tempat aplikasi tersebut ditampilkan. (Wikipedia, 2024a)

Menurut Andria dan Reza Kusuma, *Web* atau *website* adalah suatu program yang dibangun dan dikembangkan dalam bahasa pemrograman tertentu, yang hasilnya berupa halaman yang menampilkan sumber informasi tertentu yang dapat diakses dengan menggunakan koneksi *Internet* (*online*) atau tanpa koneksi *Internet* (*offline*). (Andria & Kusuma, 2019)

Sedangkan menurut peneliti, aplikasi berbasis *web* sendiri adalah sebuah jenis aplikasi yang dapat diakses melalui peramban *web* (*Browser*) tanpa perlu melakukan unduh atau install perangkat lunak tambahan pada perangkat pengguna. Aplikasi ini berjalan pada *server* jarak jauh dan menyediakan antar muka pengguna melalui halaman *web* yang dapat diakses oleh pengguna menggunakan *internet*. Hal ini berbeda dengan aplikasi *desktop* ataupun aplikasi *smartphone* yang mana harus diunduh dan *install* pada perangkat pengguna sebelum bisa memakainya.

C. Keaslian Penelitian

ANALISA KEBUTUHAN KEAMANAN DATA DAN APLIKASI DALAM PENGEMBANGAN E-LEARNING SDN 01 MANISREJO MENGGUNAKAN NIST CYBERSECURITY FRAMEWORK

Tabel 2.1 Matriks Literatur Review dan Posisi Penelitian

No	Judul	Peneliti, Media Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
1.	Perancangan Aplikasi *E-learning* Berbasis *Website* Pada SMP Negeri 3 Watansoppeng.	Riska Handayani, Zul Rachmat, Wahyuddin 2022.	Pengembangan *aplikasi e-learning* untuk SMP Negeri 3 Watansoppeng yang bertujuan untuk mengoptimalkan proses belajar mengajar, *e-learning* yang dirancang diharapkan dapat membantu baik untuk peserta didik maupun tenaga pengajar dalam mengikuti proses pembelajaran meskipun tidak berada di ruang kelas.	Aplikasi *e-learning* berbasis *website* dapat menjadi pengembangan sistem pembelajaran yang biasanya hanya dilakukan secara tatap muka, menjadi pembelajaran online. Dimana dalam penelitian ini penulis membangun *prototype* Aplikasi *e-learning* berbasis *website* yang diharapkan untuk kedepannya dapat dikembangkan menjadi	Dalam penelitian ini hanya sebatas pengembangan *website* dan untuk sisi keamanan hanya dilakukan diferensiasi kewenangan pengguna tanpa adanya implementasi keamanan lain untuk *platform e-learning*.	Perbedaan terletak pada implementasi keamanan yang diterapkan pada sistem, pada jurnal ini dilakukan analisa menyeluruh terkait keamanan data yang dibutuhkan dalam pengembangan *website e-learning*.

Tabel 2.1 Matriks Literatur Review dan Posisi Penelitian						
No	Judul	Peneliti, Media Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
				sebuah aplikasi yang dapat mengoptimalkan proses pembelajaran.		
2.	Keefektifan Metode Proteksi Data Dalam Mengatasi Ancaman *Cybersecurity*.	Arfan Dwi Madya, Bagas Djoko Haryanto, Devi Putri Ningsih, Fried Sinlae 2023.	Menekankan pentingnya keamanan *cyber* dalam menjaga data, privasi, dan kelancaran layanan. Ancaman *cyber* mencakup berbagai jenis, seperti fisik, logikal, dan Operasional.	Dalam menghadapi ancaman keamanan *cyber* yang semakin kompleks, diperlukan upaya yang komprehensif. Pentingnya pemahaman mengenai keamanan *cyber*, terutama dalam konteks proteksi data, menunjukkan perlunya strategi yang efektif. Ancaman *cyber* mencakup berbagai jenis, mulai dari serangan fisik, logikal, hingga operasional. Kesadaran pengguna, regulasi pemerintah, dan investasi dalam proteksi data	Dalam penelitian ini hanya sebatas penekanan pada pentingnya keamanan *cyber* dalam menjaga data, privasi, dan kelancaran layanan.	Perbedaan terletak pada analisa dan implementasi. pada penelitian ini dilakukan analisa menyeluruh dan implementasi terkait keamanan data yang dibutuhkan dalam pengembangan *website e-learning*.

Tabel 2.1 Matriks Literatur Review dan Posisi Penelitian						
No	Judul	Peneliti, Media Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
				menjadi kunci untuk melawan ancaman tersebut.		
3.	Analisis Celah Keamanan Aplikasi *Web E-learning* Universitas ABC Dengan *Vulnerability Assessment*.	Muhammad Aziz 2021	Tujuan penelitian ini adalah untuk mengetahui kerentanan apa saja yang terdapat pada *website e-learning* yang dimiliki oleh Universitas ABC.	Aplikasi *E-Learning* dapat menggunakan *tool nessus*, hal ini dibuktikan dengan hasil *vulnerability scanning* menggunakan *tool nessus* yang dapat memberikan daftar kerentanan, penjelasan di setiap kerentanan, dampak dari kerentanan, serta rekomendasi untuk mengatasi kerentanan yang telah ditemukan.	Adanya implementasi atau perbaikan keamanan untuk aplikasi *web e-learning* milik universitas ABC.	Implementasi perbaikan sistem, pada jurnal ini dilakukan analisa kerentanan dan juga diberikan contoh bagaimana implementasi penguatan keamanan pada sistem *e-learning*.
4.	Methodology Based On The *NIST Cybersecurity Framework* As A Proposal For Cybersecurity Management In	Maurice Frayssinet Delgado, Doris Esenarro, Francisco Fernando Juárez Regalado, Mónica Díaz Reátegui 2021.	Penelitian ini bertujuan untuk mengusulkan penggunaan metodologi berbasis Kerangka Kerja *NIST* untuk manajemen keamanan *cyber* yang memadai di organisasi pemerintah dalam kerangka penyediaan layanan digital.	Sebagian besar organisasi pemerintah tidak memiliki keamanan *cyber* yang diformalkan, karena mereka tidak memiliki statistik insiden.	Dalam penelitian ini hanya sebatas analisa dan usulan terkait penggunaan *NIST Cybersecurity Framework*.	Perbedaan terletak pada penggunaan *Framework* dimana pada jurnal digunakan seluruh fungsi sebagai acuan sedangkan pada penelitian digunakan satu

Tabel 2.1 Matriks Literatur Review dan Posisi Penelitian						
No	Judul	Peneliti, Media Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
	Government Organization.					fungsi dengan penekanan pada setiap sub-babnya.
5.	Penerapan Kerangka Kerja *NIST Cybersecurity* Dan *CIS Controls* Sebagai Manajemen Risiko Keamanan Siber	Vicky Mahendra, Benfano Soewito 2023	Mengukur kematangan keamanan siber pada infrastruktur aplikasi sehingga dapat mengurangi kemungkinan terjadinya serangan siber.	Hasil penilaian kondisi saat ini pada aplikasi ditemukan terdapat kerentanan terhadap serangan siber *SQL Injection* dengan tingkat keparahan tinggi. Dikarenakan ditemukan kerentanan dengan tingkat keparahan tinggi, peneliti telah melakukan mitigasi dengan cara melakukan penambalan pada kode sumber pada aplikasi, sehingga setelah mitigasi, kerentanan tersebut menjadi tidak ditemukan.	-	Pada penelitian ini dilakukan analisa dan manajemen resiko terkait kerentanan pada aplikasi, pada penelitian ini juga dilakukan mitigasi terhadap kerentanan yang terdapat dalam aplikasi.
6.	Pengujian Keamanan Basis Data Sistem	Andria, Wahyu Ambar Ningrum, Iqbal Mubarok 2021.	Melakukan pengujian keamanan basisdata pada suatu sistem	Penelitian dilakukan untuk menguji keamanan basis data	Pada penelitian ini digunakan sistem informasi berbasis	Perbedaan terletak pada objek penelitian dimana

Tabel 2.1 Matriks Literatur Review dan Posisi Penelitian						
No	Judul	Peneliti, Media Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
	Informasi Berbasis *Web*.		informasi berbasis *web* dengan melakukan simulasi pada situs *web* yang memiliki celah kerentanan menggunakan media perangkat *Smartphone* bersistem operasi *Android* dengan bantuan aplikasi *Termux* yang didalamnya di *install tool SQLMap*, sehingga dengan ditemukan adanya celah kerentanan tersebut maka dapat dijadikan pedoman bagi pemilik atau pengelola *web* untuk dapat melakukan tindakan pengamanan secara tepat sebagai upaya preventif dalam mengamankan data dan aset digitalnya, sehingga resiko peretasan data oleh pihak yang tidak bertanggung jawab dapat diminimalisir dan dicegah sedini mungkin.	pada sistem informasi berbasis web dan membantu *administrator* atau pengelola *web* untuk dapat memeriksa adanya celah keamanan basis data yang dapat dieksploitasi oleh peretas.	*web* yang memang dirancang oleh *developer* untuk digunakan sebagai media belajar melakukan *penetration testing*.	digunakan sistem informasi berbasis *web* yang dibuat untuk belajar melakukan *penetration testing* sedangkan pada penelitian ini digunakan sistem informasi berbasis *web* yang dibuat untuk memenuhi kebutuhan pembelajaran.