BAB II
LANDASAN TEORI

2.1 Kajian Pustaka

Penelitian yang dilakukan oleh K. A. Kurniawan, A. Nugroho, dan D. Wulandari berjudul "Implementasi Penetration Testing Metode Black Box untuk Mengetahui Keamanan Website Pemerintahan" berfokus pada pengujian keamanan website pemerintah menggunakan metode *black box*. Hasil penelitian menunjukkan bahwa website yang diuji masih memiliki beberapa kerentanan, termasuk *Cross-Site Scripting* (XSS) dan celah keamanan pada konfigurasi server. Studi ini menyimpulkan bahwa pengujian penetrasi secara berkala sangat penting untuk mengidentifikasi dan memperbaiki kelemahan sebelum dieksploitasi oleh pihak yang tidak bertanggung jawab. Temuan ini menegaskan bahwa website layanan publik merupakan target yang rentan dan memerlukan perhatian keamanan secara proaktif[1].

Penelitian selanjutnya oleh F. Yusuf dengan judul "Metode Vulnerability Assessment dalam Mengetahui Kerentanan Sistem Website: Studi Kasus E-Gov" menerapkan metode penilaian kerentanan (*vulnerability assessment*) untuk mengidentifikasi celah keamanan pada sistem *e-government*. Penelitian ini berhasil memetakan sejumlah kerentanan, seperti kelemahan pada form input dan manajemen sesi pengguna. Peneliti menyimpulkan bahwa pendekatan *vulnerability assessment* merupakan langkah fundamental dalam siklus hidup pengembangan sistem yang aman, karena memungkinkan deteksi dini dan mitigasi risiko secara sistematis. Hasil studi ini memberikan kontribusi dalam penerapan metodologi standar untuk audit keamanan pada platform digital pemerintah[2].

Penelitian yang dilakukan oleh R. Anwar dan S. R. Putri melalui karya berjudul "Analisis SQL Injection pada Sistem Informasi Akademik Menggunakan Metode White Box Testing" mengkaji secara spesifik serangan *SQL Injection* pada sistem informasi akademik. Dengan menggunakan metode *white box*, peneliti menganalisis kode sumber aplikasi dan berhasil

menemukan baris-baris kode yang rentan terhadap injeksi *query* SQL. Studi ini menyimpulkan bahwa tanpa penerapan *prepared statements* atau validasi input yang ketat, aplikasi sangat berisiko terhadap manipulasi dan pencurian data dari database. Temuan ini menyoroti pentingnya praktik pengkodean yang aman (*secure coding*) sejak awal pengembangan[3].

Penelitian yang dilakukan oleh M. Ali, A. A. Gani, dan M. I. Zainal dalam artikel "Cybersecurity Threats and Countermeasures in Digital Government: A Systematic Literature Review" membahas secara komprehensif berbagai ancaman siber yang menargetkan sistem pemerintahan digital. Studi ini mengidentifikasi bahwa serangan seperti *phishing*, *malware*, *SQL Injection*, dan XSS merupakan ancaman yang paling umum. Hasil tinjauan literatur ini menyimpulkan bahwa strategi penanggulangan yang efektif harus mencakup kombinasi antara perlindungan teknis (seperti *firewall* dan enkripsi), kebijakan keamanan yang kuat, serta peningkatan kesadaran pengguna. Penelitian ini memberikan landasan teoritis mengenai lanskap ancaman siber di sektor publik[4].

Penelitian kelima oleh B. A. Latif, M. A. M. Isa, dan S. M. M. Shah berjudul "A Comparative Study on Web Application Vulnerabilities: SQL Injection and XSS" melakukan studi perbandingan mendalam terhadap dua jenis kerentanan aplikasi web yang paling umum: *SQL Injection* dan *Cross-Site Scripting* (XSS). Penelitian ini menguraikan mekanisme serangan, dampak, serta teknik mitigasi untuk kedua jenis kerentanan tersebut. Kesimpulan utama dari studi ini adalah bahwa meskipun keduanya merupakan serangan berbasis injeksi, cara pencegahannya memerlukan pendekatan yang berbeda, yaitu validasi input sisi server untuk SQLi dan *output encoding* sisi klien untuk XSS. Karya ini memberikan pemahaman teknis yang detail mengenai dua ancaman utama yang juga dianalisis dalam penelitian ini[5].

No.	Judul Penelitian Terdahulu	Kesimpulan Utama Penelitian Terdahulu	Perbedaan dengan Penelitian Saat Ini
1	Implementasi Penetration Testing Metode Black Box	Website pemerintah rentan terhadap serangan XSS dan	Penelitian ini berfokus pada objek spesifik yaitu website 'SAMBANG'

	untuk Mengetahui Keamanan Website Pemerintahan – Kurniawan et al. (2022)	miskonfigurasi server, sehingga perlu pengujian penetrasi rutin.	dan tidak hanya mengidentifikasi kerentanan, tetapi juga melakukan analisis risiko untuk memprioritaskan mitigasi.
2	Metode Vulnerability Assessment dalam Mengetahui Kerentanan Sistem Website: Studi Kasus E-Gov – Yusuf (2023)	Metode vulnerability assessment efektif untuk deteksi dini kelemahan pada form input dan manajemen sesi di sistem e-government.	Penelitian ini menggabungkan vulnerability assessment dengan kerangka kerja risiko dari OWASP dan NIST untuk memberikan rekomendasi yang lebih terstruktur dan berbobot.
3	Analisis SQL Injection pada Sistem Informasi Akademik Menggunakan Metode White Box Testing – Anwar & Putri (2024)	Praktik secure coding seperti penggunaan prepared statements sangat krusial untuk mencegah serangan SQL Injection pada sistem informasi.	Fokus penelitian ini lebih luas, mencakup berbagai jenis serangan (SQLi, XSS, CSRF, Brute Force) pada platform pemerintah, bukan hanya satu jenis serangan pada sistem akademik.
4	Cybersecurity Threats and Countermeasures in Digital Government: A Systematic Literature Review – Ali et al. (2023)	Ancaman umum pada sistem pemerintah digital meliputi SQLi dan XSS yang harus ditangani dengan kombinasi pendekatan teknis dan kebijakan.	Studi ini bersifat tinjauan literatur, sementara penelitian saat ini melakukan implementasi teknis berupa pengujian langsung pada sistem yang beroperasi (live system).
5	A Comparative Study on Web Application Vulnerabilities: SQL Injection and XSS – Latif et al. (2023)	Pencegahan SQL Injection dan XSS memerlukan teknik yang berbeda, yaitu validasi input di server (SQLi) dan encoding output di klien (XSS).	Penelitian ini menerapkan temuan-temuan teoritis tersebut dalam sebuah studi kasus praktis untuk memberikan rekomendasi mitigasi yang relevan bagi pengelola sistem.

2.2 Keamanan *Cyber*

Cyber crime merupakan bentuk kejahatan di dunia maya yang dilakukan individu maupun kelompok dengan cara menyerang sistem keamanan komputer maupun data yang tersimpan di dalamnya. Motif tindakan ini beragam, mulai dari sekadar kepuasan pribadi hingga tujuan yang merugikan aspek ekonomi maupun politik. Secara umum, Cybercrime adalah aktivitas yang melanggar hukum yang melibatkan komputer, perangkat digital, atau jaringan computer [1]. Contoh kasusnya meliputi rekayasa sosial, eksploitasi celah perangkat lunak, hingga serangan jaringan. Dengan kata lain, tindak kriminal ini menggunakan teknologi komputer sebagai sarana utama dalam melakukan kejahatan.

Keamanan siber atau *cyber security* merupakan upaya sistematis yang dilakukan untuk melindungi sistem informasi, jaringan, perangkat, serta data digital dari berbagai ancaman yang berpotensi merugikan, baik berupa serangan siber, penyalahgunaan, maupun akses ilegal [20]. Seiring dengan meningkatnya ketergantungan masyarakat terhadap teknologi informasi dan komunikasi, isu keamanan siber menjadi semakin krusial tidak hanya bagi individu, tetapi juga organisasi, perusahaan, hingga negara [18]. Dalam konteks ini, keamanan siber mencakup perlindungan terhadap tiga aspek utama, yaitu kerahasiaan (confidentiality) yang menjamin data hanya dapat diakses oleh pihak berwenang, integritas (integrity) yang memastikan data tetap utuh dan tidak dimanipulasi, serta ketersediaan (availability) yang menjamin sistem maupun informasi tetap dapat diakses ketika dibutuhkan.

Ancaman terhadap keamanan siber hadir dalam berbagai bentuk, mulai dari serangan *malware*, *phishing*, *ransomware*, serangan *Distributed Denial of Service* (DDoS), pencurian data pribadi, hingga praktik spionase digital . Ancaman tersebut berkembang pesat seiring dengan kemajuan teknologi digital yang semakin kompleks [19]. Untuk mengantisipasi hal tersebut, diperlukan penerapan strategi yang komprehensif, seperti penggunaan sistem keamanan berlapis, penyusunan kebijakan keamanan informasi, peningkatan kesadaran pengguna melalui edukasi, penerapan enkripsi data, serta pemantauan dan audit sistem secara berkala [17]. Dengan demikian,

keamanan siber tidak hanya dipandang sebagai persoalan teknis, melainkan juga terkait erat dengan manajemen risiko, kepatuhan terhadap regulasi, serta perilaku pengguna dalam menjaga keamanan data dan informasi di ruang digital.

Keamanan siber, juga dikenal sebagai "keamanan siber", merupakan rangkaian tindakan dan prosedur pengamanan yang dimaksudkan untuk melindungi dari serangan, ancaman, maupun gangguan yang disebabkan oleh komponen yang ada di ruang siber [2]. Ruang siber sendiri adalah media maya tempat terjadinya komunikasi, yang mencakup perangkat keras, perangkat lunak, serta jaringan komputer. Keamanan siber dapat pula dimaknai sebagai mekanisme perlindungan terhadap kerahasiaan, integritas, dan ketersediaan informasi [10]. Mekanisme tersebut berfungsi sebagai pertahanan dari serangan di dunia maya atau cyber attack. Peran utama keamanan siber meliputi identifikasi, perbaikan, dan mitigasi risiko terhadap ancaman (*cyber threat*) maupun serangan (*cyber attack*) [4]. Istilah ini memiliki cakupan luas, mulai dari konteks bisnis hingga komputasi perangkat bergerak, dengan kategori utama seperti keamanan jaringan, keamanan informasi, serta edukasi bagi pengguna akhir [8].

Ketahanan siber (*cyber resilience*) merupakan kemampuan suatu sistem dalam mempersiapkan diri, menyerap dampak, memulihkan, serta menyesuaikan dengan efek merugikan yang ditimbulkan, khususnya akibat serangan siber (Linkov & Kott, 2019). Dengan kata lain, ketahanan siber dapat diartikan sebagai kapasitas untuk tetap menghasilkan kinerja atau layanan yang diharapkan meskipun menghadapi insiden siber yang merugika [4].

Istilah *cybersecurity* dan keamanan informasi (*information security*) kerap digunakan secara bergantian, meskipun sebenarnya *cybersecurity* merupakan bagian dari keamanan informasi. Secara lebih spesifik, *cybersecurity* didefinisikan sebagai upaya perlindungan aset informasi dari berbagai ancaman terhadap data yang diproses, disimpan, maupun ditransmisikan melalui sistem informasi berbasis internet [7].

Cybersecurity mencakup semua yang melindungi perusahaan dan individu dari serangan yang disengaja, pelanggaran dan insiden serta konsekuensi. Dalam prakteknya, *cybersecurity* terutama menunjukkan jenis jenis serangan, pelanggaran atau insiden yang ditargetkan, terlalu canggih dan sulit untuk mendeteksi atau mengelola *cybersecurity*. Bidang yang jauh lebih besar dari serangan oportunistik dan kejahatan biasanya dapat ditangani dengan menggunakan strategi dan tool sederhana namun efektif. Akibatnya, fokus *cybersecurity* adalah pada apa yang dikenal sebagai *Advanced Persistent Threats* (APTs). [7].

Meskipun *cyber resilience* dan *cyber security* tampak mirip, keduanya memiliki fokus yang berbeda. Perbedaan keduanya dapat dilihat sebagai berikut [8].

No	Aspek	Keamanan Siber	Ketahanan Siber
1	Objektif	Lindungi sistem dan teknologi informasi	Memastikan keberlanjutan bisnis
2	Rencana	Aman dari kegagalan	Aman untuk gagal
3	Pendekatan	Terapkan kemanan dari luar	Bangun keamanan dari dalam
4	Arsitektur	Perlindungan berlapis tunggal	Perlindungan multi lapis
5	Cakupan	Atomistik satu organisasi	Holistik, jaringan organisasi

Tabel 2. 1 Karakteristik Siber dan Ketahanan Siber

2.3 SQL Injection

SQL Injection adalah serangan yang dilakukan untuk mendapatkan akses atau memanipulasi data di database dengan cara menyisipkan sintak berbahaya ke dalam query SQL melalui input data tanpa filter dari klien ke aplikasi. Setiap kali permintaan dikirim dari klien, sistem akan membuat query berdasarkan input pengguna untuk berkomunikasi dengan database. Oleh karena itu, sangat penting untuk menyaring input pengguna sebelum dieksekusi oleh aplikasi.

Sudah menjadi rahasia umum bahwa itu adalah tanggung jawab pengembang aplikasi untuk menyaring dan menvalidasi input yang masuk ke sistem, namun karena kelalaian atau ketidaktahuan pengembang, mereka sering meninggalkan ruang bagi penyerang untuk menggunakan serangan SQL Injection. Oleh karena itu, perlu adanya proses pengamanan tambahan untuk memastikan sistem terlindungi dari serangan *SQL Injection*.

SQL Injection adalah teknik serangan yang dilakukan dengan menyisipkan kode berbahaya ke dalam string yang kemudian dieksekusi oleh database server [5]. Serangan ini memanfaatkan celah pada aplikasi web, biasanya melalui form input atau Uniform Resource Locator (URL), untuk menjalankan query SQL tambahan dengan tujuan memperoleh informasi dari basis data. Adapun 3 jenis dari SQL Injection yaitu: [11].

1. *Union-Based SQL Injection*

   Jenis SQL Injection ini merupakan salah satu yang paling sering digunakan. Menurut Baloch (2015: 343), serangan ini memanfaatkan perintah UNION, yaitu penggabungan dua perintah SELECT, untuk mengekstrak informasi dari basis data. Contoh serangan dapat dilihat pada perintah berikut: http://localhost/index.php?support=yes' and 1=0 UNION all select 1,2,3,4--± Kode tersebut menyisipkan query tambahan yang memungkinkan penyerang menampilkan informasi dari kolom dalam basis data. Bagian "1=0" berfungsi menonaktifkan eksekusi query di sisi kiri UNION, sementara "all select 1,2,3,4--±" digunakan untuk menampilkan data dari kolom basis data. Dengan demikian, penggunaan UNION memberi celah bagi penyerang untuk menambahkan query tambahan ke dalam aplikasi.

2. *Error-Based SQL Injection*

   Jenis SQL Injection ini termasuk yang paling sederhana untuk digunakan. Teknik ini bekerja dengan cara menyisipkan perintah SQL pada input, sehingga *database* memberikan respon berupa pesan error yang ditampilkan langsung pada halaman web [13]. Dari pesan error tersebut, penyerang dapat memperoleh informasi terkait database.

Contoh serangan adalah: http://www.example.com/product.aspx?Id=7 and @@version=1--. Pada kasus ini, penyisipan query "and @@version=1--" memungkinkan penyerang mengetahui jenis database maupun sistem operasi yang digunakan.

3. Blind SQL Injection

Teknik ini umumnya diterapkan ketika *error-based SQL injection* tidak berhasil karena situs web telah dikonfigurasi untuk tidak menampilkan pesan error. *Blind SQL Injection* merupakan metode di mana penyerang memperoleh data dengan mengajukan pertanyaan "benar atau salah" kepada database [13]. Dalam teknik ini, informasi mengenai database didapatkan melalui analisis respon dari website, bukan dari pesan error. Proses injeksi dilakukan secara berulang hingga penyerang memperoleh data yang dibutuhkan [10]. Oleh sebab itu, *blind SQL injection* termasuk salah satu jenis serangan SQL Injection yang paling kompleks. Misalnya, seorang penyerang dapat menggunakan teknik ini untuk mengetahui versi MySQL yang digunakan.

Gambar 2. 1 *False result* hasil dari *Blind SQL Injection*

Sumber: Buku Ethical Hacking and Penetration Testing Guide, p.358

Query berikut: "http://localhost/index.php?support=yes' AND SUBSTRING (version (),1,1)=4;--+" digunakan untuk memverifikasi apakah MySQL yang digunakan merupakan versi 4. Hasil pengujian menunjukkan false result, sehingga dapat disimpulkan bahwa versi yang digunakan bukanlah versi 4.

Sebaliknya, saat dijalankan query: "http://localhost/index.php?support=yes' AND SUBSTRING(version (),1,1)=5;--+", website memberikan output sesuai tampilan pada gambar, yang mengindikasikan bahwa database menggunakan MySQL versi 5.

Gambar 2. 2 *True result* hasil dari *Blind SQL Injection*

Sumber: Buku Ethical Hacking and Penetration Testing Guide, p.358

Output yang diperoleh menunjukkan true result, yang berarti MySQL yang digunakan adalah versi 5. Dengan demikian, meskipun prosesnya lebih kompleks, penyerang tetap mampu memperoleh informasi terkait database tanpa bergantung pada pesan error.

2.4 *Cross-Site Scripting* (XSS)

Cross Site Scripting (XSS) merupakan salah satu bentuk *code injection attack* yang memanfaatkan celah pada sisi klien maupun server [2]. Serangan ini dilakukan dengan cara menyisipkan kode HTML atau skrip klien lainnya ke dalam sebuah situs atau form input. Karena dijalankan seolah berasal dari sumber terpercaya, skrip berbahaya tersebut dapat mengakses informasi pada browser, seperti *cookies*, token sesi, maupun data sensitif lainnya. Lebih jauh, skrip ini bahkan mampu memodifikasi ulang konten HTML pada halaman web [15]. Dampak dari serangan ini antara lain memungkinkan penyerang melewati mekanisme keamanan di sisi klien, memperoleh data sensitif, maupun menyisipkan aplikasi berbahaya. Beberapa karakteristik URL yang rentan terhadap XSS dapat diidentifikasi meliputi:

1. Memiliki url yang panjang

2. Memiliki tag script seperti: <script>
3. Memiliki karakter special seperti: ['<','>','%',')','(',']','[','\'"]
4. Memiliki tag html seperti: Cookie, session, onclick, onload dll.
5. Memiliki karakter yang berulang seperti: //,< >,%%,''

Gambar 2. 3 *A high-level viewing of typical XSS attack*

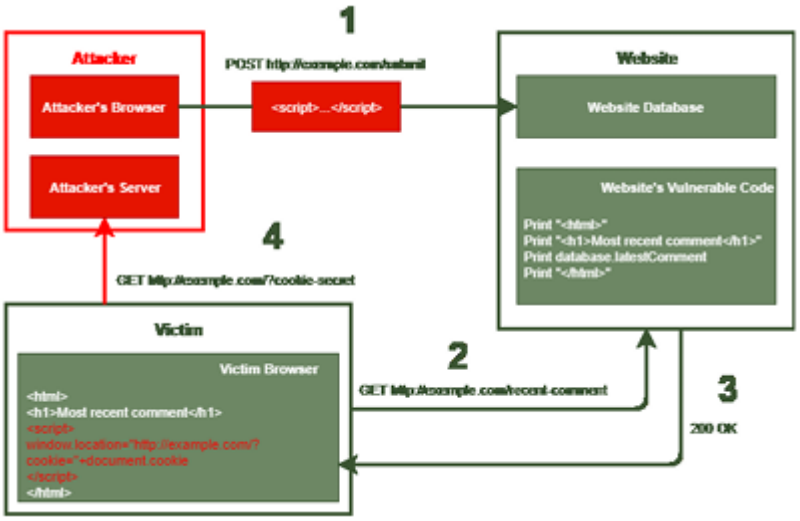
Tipe XSS dibagi menjadi jenis:

1. *Reflected XSS*

Reflected XSS merupakan jenis XSS yang paling umum sekaligus paling mudah dieksploitasi oleh penyerang. Teknik ini biasanya melibatkan rekayasa sosial, di mana pengguna diarahkan untuk mengklik URL yang telah disisipi kode berbahaya. Melalui cara tersebut, penyerang dapat mencuri cookie pengguna dan menggunakannya untuk membajak sesi pengguna. Upaya mitigasi yang dapat dilakukan adalah dengan melakukan validasi terhadap setiap input sebelum menampilkan data yang berasal dari pengguna [14]. Prinsip pentingnya adalah tidak mempercayai data apa pun yang dikirimkan oleh pengguna.

Pada serangan dengan jenis reflected XSS, script jahat akan disisipkan pada url yang menjadi target oleh penyerang seperti url berikut ini.

"(http://www.audiusa.com/search?query=<script>alert('XSS POSED')</script)"



Gambar 2. 4 *The XSS attack process*

2. *Stored XSS*

Stored XSS relatif jarang ditemukan, namun memiliki dampak serangan yang lebih luas. Serangan ini dapat memengaruhi seluruh pengguna ketika data berbahaya yang dimasukkan ditampilkan kembali [7]. Contoh kasus biasanya terjadi pada *message board*, buku tamu, atau layanan serupa, di mana penyerang menyisipkan kode HTML maupun skrip berbahaya pada unggahan mereka, seperti melalui URL berikut.

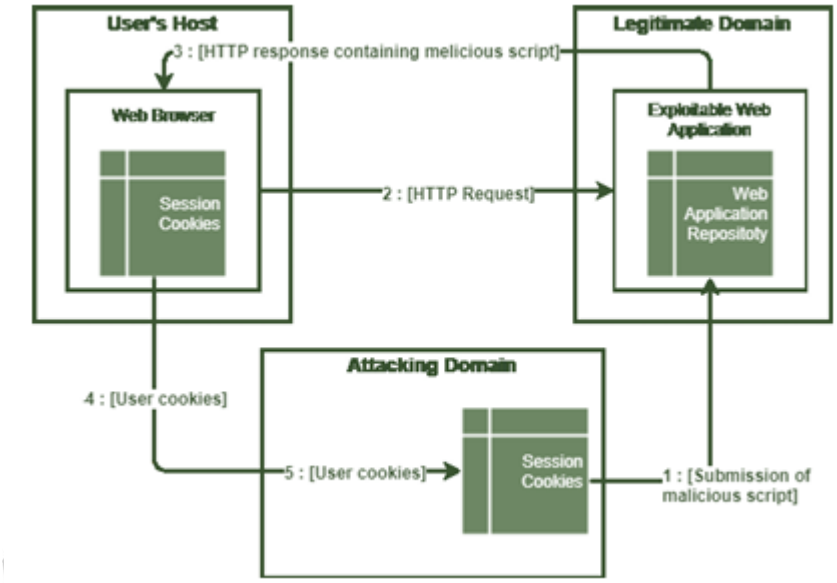
“<script type=”text/javascript”>alert(document.cookie);</script>”

Berdasarkan contoh serangan di atas merupakan serangan yang di lakukan dengan meletakkan script tersebut terhadap sebuah form inputan seperti comment, jika form tersebut di submit maka akan muncul alert dan akan bersifat permanent karna script tersebut tersimpan ke dalam database. Langkah-langkah serangan melalui store XSS[9]:

A. Penyerang memasukkan skrip jahat pada web yang memiliki kelemahan
B. Ketika pengguna mengirim HTTP *request,* maka skrip jahat yang berada di halaman tersebut ikut terkirim.
C. Skrip jahat tersebut berhasil dikirim pengguna melalui HTTP *response*.

D. Ketika skrip dijalankan pada browser makan akan otomatis mengirimkan *cookies* ke penyerang.

E. *Cookies* yang di curi disimpan di domain penyerang.



Gambar 2. 5 *The Store XSS attack*