Hak Cipta Dilindungi Undang-Undang
1. Dilarang memperbanyak atau mendistribusikan dokumen ini untuk tujuan komersial tanpa izin tertulis dari penulis atau pihak berwenang. Penggunaan untuk kepentingan akademik, penelitian, dan pendidikan diperbolehkan dengan mencantumkan sumber.
2. Penggunaan tanpa izin untuk kepentingan komersial atau pelanggaran hak cipta dapat dikenakan sanksi sesuai dengan UU Hak Cipta di Indonesia. Plagiarisme juga dilarang dan dapat dikenakan sanksi.
3. Universitas hanya berhak menyimpan dan mendistribusikan dokumen ini di repositori akademik, tanpa mengalihkan hak cipta penulis, sesuai dengan peraturan yang berlaku di Indonesia.
Universitas Islam Indragiri

BAB II

TINJAUAN LITERATUR

2.1 *Website*

Konsep *website* dapat dipahami melalui dua sudut pandang. Pertama, *website* dapat dipandang sebagai himpunan laman yang menyajikan informasi melalui beragam bentuk, misalnya tulisan, gambar, audio, ataupun animasi. Setiap laman dapat bersifat tetap maupun berubah secara dinamis, kemudian dihubungkan satu sama lain sehingga membentuk struktur situs yang terintegrasi [12]. Kedua, aplikasi web merupakan perangkat lunak yang dijalankan melalui *browser* sehingga pengguna tidak diwajibkan memasang aplikasi secara langsung pada perangkat. Pengoperasiannya memanfaatkan koneksi internet dan secara umum tidak terbatas pada satu sistem operasi tertentu, sehingga layanan dapat digunakan secara daring dari berbagai perangkat [13].

Secara teknis, sebuah *website* dibangun oleh sejumlah *file* yang saling berkaitan dan ditempatkan dalam suatu direktori. Berbagai komponen seperti dokumen halaman, gambar, CSS, audio, maupun *file* pendukung lainnya membentuk keseluruhan layanan *website*. Oleh sebab itu, pengelolaan komponen secara teratur diperlukan agar proses akses dan kinerja *website* dapat berlangsung secara optimal [14].

Berdasarkan kedua pengertian tersebut, *website* tidak hanya dapat dimaknai sebagai sekumpulan halaman penyaji informasi, tetapi juga sebagai struktur digital yang saling terhubung dan dapat bersifat statis ataupun dinamis. Sementara itu, aplikasi web memberikan layanan tanpa proses instalasi langsung karena pengguna cukup mengaksesnya menggunakan *browser* dengan dukungan jaringan internet

[13]. Dengan demikian, kedua konsep tersebut menggambarkan cara *website* serta aplikasi berbasis *browser* menyediakan informasi dan layanan kepada pengguna secara daring.

2.2 Sistem Informasi

Sistem informasi dalam suatu organisasi berfungsi menghubungkan proses pengolahan transaksi operasional dengan kebutuhan pengelolaan manajemen dan penyusunan strategi. Selain mendukung kegiatan internal organisasi, sistem tersebut juga dapat menghasilkan informasi maupun laporan yang diperlukan oleh pihak luar sesuai kebutuhan tertentu [15].

2.3 *Penetration Testing*

Secara legal, *penetration testing* dilakukan dengan mencoba mengeksplorasi kelemahan pada sistem komputer untuk mengetahui bagian yang memerlukan pengamanan lebih lanjut [16]. Apabila dilaksanakan dengan prosedur yang tepat, hasil pengujian dapat digunakan sebagai dasar penyusunan rekomendasi untuk menangani kelemahan maupun persoalan yang berhasil ditemukan [17].

Dalam pelaksanaannya, *penetration testing* terdiri atas serangkaian prosedur serta teknik evaluasi yang mensimulasikan pola serangan terhadap komputer maupun jaringan [18]. Melalui simulasi tersebut, titik lemah yang berpotensi menjadi jalur eksploitasi dapat diketahui sehingga tindakan penutupan atau perbaikan dapat dilakukan lebih awal. Dengan demikian, pendekatan ini digunakan sebagai salah satu tindakan preventif untuk menekan peluang terjadinya peretasan pada sistem [19].

Hak Cipta Dilindungi Undang-Undang
1. Dilarang memperbanyak atau mendistribusikan dokumen ini untuk tujuan komersial tanpa izin tertulis dari penulis atau pihak berwenang. Penggunaan untuk kepentingan akademik, penelitian, dan pendidikan diperbolehkan dengan mencantumkan sumber.
2. Penggunaan tanpa izin untuk kepentingan komersial atau pelanggaran hak cipta dapat dikenakan sanksi sesuai dengan UU Hak Cipta di Indonesia. Plagiarisme juga dilarang dan dapat dikenakan sanksi.
3. Universitas hanya berhak menyimpan dan mendistribusikan dokumen ini di repositori akademik, tanpa mengalihkan hak cipta penulis, sesuai dengan peraturan yang berlaku di Indonesia.
Universitas Islam Indragiri

2.4 OWASP

Open Web Application Security Project (OWASP) merupakan inisiatif bersifat *open source* yang berorientasi pada peningkatan perlindungan aplikasi perangkat lunak [20]. Organisasi ini menjalankan berbagai kegiatan untuk membantu identifikasi serta penanganan kelemahan pada aplikasi web. Standar OWASP memuat sejumlah tahapan dalam proses pemeriksaan keamanan *website*, antara lain Information Gathering, Configuration Management, *Secure* Transmission, Authentication, Session Management, Authorization, Cryptography, Data Validation, Denial of Service, dan Error Handling. Rangkaian tersebut dapat digunakan untuk menelusuri potensi celah kemudian menentukan tindakan penanganan sehingga perlindungan aplikasi web dapat diperkuat [21].

Mulyanto dkk. [22] menjelaskan bahwa Open Web Application Security Project (OWASP) merupakan organisasi nirlaba berskala internasional yang berada di bawah OWASP Foundation dan didirikan di Amerika Serikat pada 21 April 2004. Kegiatannya diarahkan pada peningkatan keamanan perangkat lunak dengan menyediakan dukungan bagi organisasi dalam proses pengembangan, pengadaan, pengoperasian, serta pemeliharaan aplikasi yang dapat dipercaya. Melalui misinya, OWASP mendorong tersedianya perangkat lunak yang lebih aman sehingga keputusan mengenai risiko keamanan dapat diambil secara lebih tepat oleh individu maupun organisasi.

2.5 OWASP ZAP

OWASP Zed Attack Proxy (ZAP) merupakan perangkat *penetration testing* bersumber terbuka yang dapat digunakan tanpa biaya dan dikembangkan di bawah Open Web Application Security Project (OWASP) [23]. Perangkat ini ditujukan

Hak Cipta Dilindungi Undang-Undang
1. Dilarang memperbanyak atau mendistribusikan dokumen ini untuk tujuan komersial tanpa izin tertulis dari penulis atau pihak berwenang. Penggunaan untuk kepentingan akademik, penelitian, dan pendidikan diperbolehkan dengan mencantumkan sumber.
2. Penggunaan tanpa izin untuk kepentingan komersial atau pelanggaran hak cipta dapat dikenakan sanksi sesuai dengan UU Hak Cipta di Indonesia. Plagiarisme juga dilarang dan dapat dikenakan sanksi.
3. Universitas hanya berhak menyimpan dan mendistribusikan dokumen ini di repositori akademik, tanpa mengalihkan hak cipta penulis, sesuai dengan peraturan yang berlaku di Indonesia.
Universitas Islam Indragiri

Hak Cipta Dilindungi Undang-Undang
1. Dilarang memperbanyak atau mendistribusikan dokumen ini untuk tujuan komersial tanpa izin tertulis dari penulis atau pihak berwenang. Penggunaan untuk kepentingan akademik, penelitian, dan pendidikan diperbolehkan dengan mencantumkan sumber.
2. Penggunaan tanpa izin untuk kepentingan komersial atau pelanggaran hak cipta dapat dikenakan sanksi sesuai dengan UU Hak Cipta di Indonesia. Plagiarisme juga dilarang dan dapat dikenakan sanksi.
3. Universitas hanya berhak menyimpan dan mendistribusikan dokumen ini di repositori akademik, tanpa mengalihkan hak cipta penulis, sesuai dengan peraturan yang berlaku di Indonesia.
Universitas Islam Indragiri

untuk pemeriksaan aplikasi berbasis web serta dirancang agar fleksibel dan mudah dikembangkan sesuai kebutuhan. Pada mekanisme kerjanya, ZAP dapat ditempatkan sebagai perantara antara *browser* penguji dan aplikasi yang diuji. Posisi tersebut memungkinkan lalu lintas pesan antara kedua sisi ditangkap serta diperiksa, bahkan isinya dapat dimodifikasi apabila diperlukan sebelum diteruskan kembali ke tujuan. ZAP dapat dijalankan sebagai aplikasi mandiri ataupun sebagai proses *daemon*. Dalam praktik uji penetrasi, fitur pemindaian otomatisnya banyak dimanfaatkan untuk menemukan potensi titik lemah pada aplikasi *website* [21].

Selain digunakan untuk proses pemindaian, OWASP ZAP dikembangkan sebagai salah satu proyek aktif di lingkungan OWASP. Karakter *open source* memungkinkan kode programnya diakses, digunakan, dipelajari, bahkan dikembangkan kembali oleh pengguna. Keterbukaan tersebut membuat komunitas dapat turut memberikan kontribusi terhadap pengembangan fungsi dan peningkatan kemampuan ZAP. Karena itu, perangkat ini banyak dimanfaatkan sebagai sarana untuk membantu mendeteksi sekaligus mengevaluasi kelemahan keamanan aplikasi web [24].



Gambar 2.1 Logo *Software* OWASP ZAP

Zed Attack Proxy (ZAP) termasuk perangkat uji penetrasi bersumber terbuka yang dapat digunakan secara gratis dan berada dalam pengelolaan The *Software* Security Project (SSP) [25]. Penggunaannya difokuskan pada pemeriksaan aplikasi berbasis web serta dirancang agar fleksibel dan memungkinkan pengembangan

fungsi tambahan. Dalam proses pengujian, ZAP bekerja sebagai perantara antara *browser* dan aplikasi web. Melalui posisi tersebut, pertukaran pesan dapat ditangkap, dianalisis, maupun disesuaikan apabila diperlukan sebelum data diteruskan menuju tujuan. Perangkat ini dapat dijalankan secara independen ataupun melalui proses *daemon*.



Gambar 2.2 Proses ZAP Tahap 1

Apabila lingkungan jaringan telah menggunakan layanan proxy lain, seperti yang umum diterapkan pada infrastruktur perusahaan, koneksi ZAP dapat diarahkan agar terlebih dahulu melalui proxy jaringan tersebut.



Gambar 2.3 Proses ZAP Tahap 2

ZAP dirancang agar dapat digunakan oleh kelompok pengguna dengan tingkat kemampuan yang beragam, mulai dari pengembang, pengguna yang baru mempelajari pengujian keamanan, hingga praktisi yang telah memiliki keahlian khusus. Aplikasi ini tersedia untuk berbagai sistem operasi utama dan juga dapat dijalankan melalui Docker sehingga pengguna tidak dibatasi oleh satu *platform* tertentu. Kemampuan ZAP dapat diperluas menggunakan beragam *add-on* yang tersedia melalui *ZAP Marketplace* dan dapat diakses dari aplikasi. Karakter *open source* memungkinkan struktur kode ZAP ditinjau secara terbuka sehingga cara setiap fungsi diterapkan dapat dipahami dengan lebih jelas. Pengguna maupun

Hak Cipta Dilindungi Undang-Undang
1. Dilarang memperbanyak atau mendistribusikan dokumen ini untuk tujuan komersial tanpa izin tertulis dari penulis atau pihak berwenang. Penggunaan untuk kepentingan akademik, penelitian, dan pendidikan diperbolehkan dengan mencantumkan sumber.
2. Penggunaan tanpa izin untuk kepentingan komersial atau pelanggaran hak cipta dapat dikenakan sanksi sesuai dengan UU Hak Cipta di Indonesia. Plagiarisme juga dilarang dan dapat dikenakan sanksi.
3. Universitas hanya berhak menyimpan dan mendistribusikan dokumen ini di repositori akademik, tanpa mengalihkan hak cipta penulis, sesuai dengan peraturan yang berlaku di Indonesia.
Universitas Islam Indragiri

pengembang dapat turut melakukan kontribusi, misalnya menangani bug, menambahkan kemampuan baru, mengajukan perubahan pada proyek, ataupun membuat *add-on* untuk kebutuhan tertentu.

Daftar OWASP *Top Ten* adalah alat yang diakui secara luas untuk mengidentifikasi kerentanan dalam aplikasi web. Karena panduan keamanan khusus untuk *blockchain* saat ini masih kurang, memetakan kerangka kerja yang ada, seperti OWASP, ke dalam *blockchain* dapat membantu mengidentifikasi potensi kerentanan dalam sistem *blockchain*. Meskipun Daftar OWASP *Top Ten* dirancang untuk menggambarkan kerentanan yang dihadapi oleh pengembang aplikasi web, sembilan dari sepuluh kerentanan OWASP juga berlaku untuk sistem blockchain. Pengecualiannya adalah XML *External Entities* (XXE), yang tidak berlaku karena tidak adanya penggunaan XML dalam *blockchain* [26].

Ancaman keamanan terhadap aplikasi mobile semakin meningkat dengan pesat. Kelemahan dan cacat keamanan dalam aplikasi mobile memberikan peluang bagi peretas untuk masuk dan mengakses informasi sensitif. Analisis kebutuhan defensif harus menjadi bagian integral dari SDLC (*Software Development Life Cycle*) yang aman untuk *mobile*. Pengembang perlu mempertimbangkan kerahasiaan informasi dan integritas data, serta memverifikasi keamanan sejak awal siklus pengembangan daripada memperbaiki lubang keamanan setelah serangan dan kebocoran data terjadi. Menghilangkan kerentanan keamanan yang diketahui sejak awal akan membantu pengembang meningkatkan keamanan aplikasi dan mengurangi kemungkinan eksploitasi. Namun, banyak pengembang perangkat lunak kurang memiliki pengetahuan dan keterampilan keamanan yang diperlukan pada tahap pengembangan, sehingga pendidikan *Secure Mobile Software*

Hak Cipta Dilindungi Undang-Undang
1. Dilarang memperbanyak atau mendistribusikan dokumen ini untuk tujuan komersial tanpa izin tertulis dari penulis atau pihak berwenang. Penggunaan untuk kepentingan akademik, penelitian, dan pendidikan diperbolehkan dengan mencantumkan sumber.
2. Penggunaan tanpa izin untuk kepentingan komersial atau pelanggaran hak cipta dapat dikenakan sanksi sesuai dengan UU Hak Cipta di Indonesia. Plagiarisme juga dilarang dan dapat dikenakan sanksi.
3. Universitas hanya berhak menyimpan dan mendistribusikan dokumen ini di repositori akademik, tanpa mengalihkan hak cipta penulis, sesuai dengan peraturan yang berlaku di Indonesia.
Universitas Islam Indragiri

Hak Cipta Dilindungi Undang-Undang
1. Dilarang memperbanyak atau mendistribusikan dokumen ini untuk tujuan komersial tanpa izin tertulis dari penulis atau pihak berwenang. Penggunaan untuk kepentingan akademik, penelitian, dan pendidikan diperbolehkan dengan mencantumkan sumber.
2. Penggunaan tanpa izin untuk kepentingan komersial atau pelanggaran hak cipta dapat dikenakan sanksi sesuai dengan UU Hak Cipta di Indonesia. Plagiarisme juga dilarang dan dapat dikenakan sanksi.
3. Universitas hanya berhak menyimpan dan mendistribusikan dokumen ini di repositori akademik, tanpa mengalihkan hak cipta penulis, sesuai dengan peraturan yang berlaku di Indonesia.
Universitas Islam Indragiri

Development sangat diperlukan bagi insinyur perangkat lunak mobile. Dalam makalah ini, kami mengusulkan analisis kebutuhan keamanan yang dipandu berdasarkan rekomendasi risiko keamanan OWASP *Mobile Top Ten* untuk pengembangan perangkat lunak mobile Android dan keterkaitannya dengan kontrol pengembangan dalam SDLC. Membangun aplikasi yang aman dan kebal terhadap risiko OWASP *Mobile Top Ten* akan menjadi pendekatan yang efektif untuk memberikan pedoman keamanan mobile yang sangat berguna [27]. Adapun acaman yang dapat diidentifikasi oleh OWASP ZAP sebagai berikut:

1) *Injection*

Serangan injeksi dapat terjadi ketika aplikasi tidak melakukan validasi dan penyaringan input pengguna secara memadai, sehingga penyerang memiliki peluang untuk memasukkan perintah yang seharusnya tidak dijalankan oleh sistem. Pada kasus SQL, lemahnya proses validasi input dapat dimanfaatkan untuk melewati mekanisme autentikasi maupun mengeksekusi perintah tertentu pada basis data tanpa izin. Permasalahan serupa juga dapat muncul pada teknologi blockchain. Sebelum peluncuran mainnet EOS, peneliti dari Qihoo 360 menemukan kelemahan pada proses parsing smart contract EOS yang memungkinkan terjadinya penulisan buffer di luar batas [28]. Kerentanan tersebut berpotensi dimanfaatkan untuk mengganggu atau mengambil alih sistem melalui eksekusi smart contract berbahaya.

2) Kerentanan CSRF

Pada serangan *CSRF* (Cross-Site Request Forgery), mekanisme kepercayaan antara *browser* pengguna dan *website* dimanfaatkan oleh

Hak Cipta Dilindungi Undang-Undang
1. Dilarang memperbanyak atau mendistribusikan dokumen ini untuk tujuan komersial tanpa izin tertulis dari penulis atau pihak berwenang. Penggunaan untuk kepentingan akademik, penelitian, dan pendidikan diperbolehkan dengan mencantumkan sumber.
2. Penggunaan tanpa izin untuk kepentingan komersial atau pelanggaran hak cipta dapat dikenakan sanksi sesuai dengan UU Hak Cipta di Indonesia. Plagiarisme juga dilarang dan dapat dikenakan sanksi.
3. Universitas hanya berhak menyimpan dan mendistribusikan dokumen ini di repositori akademik, tanpa mengalihkan hak cipta penulis, sesuai dengan peraturan yang berlaku di Indonesia.
Universitas Islam Indragiri

penyerang untuk menjalankan tindakan tanpa persetujuan pengguna. Serangan dapat terjadi ketika seseorang masih berada dalam kondisi telah terautentikasi pada sebuah layanan, kemudian secara tidak sadar diarahkan untuk mengirimkan permintaan menuju sistem target. Sebagai contoh, pengguna yang sedang masuk ke media sosial, layanan perbankan, ataupun *platform e-commerce* dapat dipicu untuk mengirim permintaan *HTTP* tertentu yang telah disiapkan oleh penyerang. Kondisi tersebut memungkinkan suatu tindakan diproses menggunakan hak akses milik korban tanpa disadarinya [29].

3) Kerentanan otentikasi yang rusak

Kerentanan otentikasi yang rusak memungkinkan penyerang menyamar sebagai pengguna sah. Implementasi otentikasi yang benar sangat penting dalam sistem blockchain karena penggunaan kriptografi kunci publik menciptakan permukaan serangan yang besar. Contoh kasus terjadi pada cryptocurrency LISK, di mana desain yang kurang memperhatikan keamanan memungkinkan serangan pada otentikasi. Alamat pengguna dihasilkan dengan hashing kunci publik dan memotong hasilnya menjadi 64 bit, yang membuat alamat tidak langsung terikat dengan kunci publik dan rentan terhadap serangan. Alamat di LISK hanya terikat dengan kunci publik saat pengguna melakukan transaksi, sehingga banyak akun yang hanya menerima nilai tetap rentan terhadap serangan. Penyerang hanya perlu melakukan 2^{64} operasi pembuatan kunci untuk menemukan pasangan kunci privat/publik yang cocok dengan alamat tertentu, mengurangi kompleksitas dengan faktor M jika menargetkan salah

satu dari M alamat. Serangan ini cukup layak dilakukan dan beberapa akun rentan memegang jutaan dolar.

4) *Sensitive Data Exposure*

Sensitive data exposure adalah data berharga yang harus dijaga kerahasiaannya tidak terlindungi dengan baik. Teknologi blockchain rentan terhadap kerentanan ini karena kurangnya pemahaman tentang teknologinya. Blockchain bersifat tidak dapat diubah, artinya data yang disimpan tidak dapat dihapus tanpa kontrol dari semua node di jaringan. Kebanyakan blockchain juga bersifat publik, memungkinkan siapa saja untuk mengunduh dan menyimpan salinan lengkap data dalam buku besar.

Dalam jangka pendek, kombinasi ini membuat blockchain rentan terhadap upaya penambangan data. Banyak organisasi berspesialisasi dalam menambang blockchain untuk data publik yang dapat digabungkan menjadi informasi berguna yang dapat digunakan untuk penegakan hukum, spionase perusahaan, dan tujuan lainnya. Dalam jangka panjang, semua kriptografi dapat ditembus. Komputasi kuantum di masa depan akan memungkinkan dekripsi data yang disimpan di blockchain yang dienkripsi dengan algoritma enkripsi asimetris klasik. Jika data harus dirahasiakan selamanya, seperti data pribadi yang dilindungi oleh undang-undang privasi seperti GDPR atau HIPAA, data tersebut sebaiknya tidak pernah disimpan di blockchain publik, bahkan dalam format terenkripsi.

5) *XML External Entities (XXE)*

Kerentanan XXE muncul ketika parser XML mengizinkan pemrosesan referensi menuju entitas yang berada di luar dokumen utama. Kondisi

Hak Cipta Dilindungi Undang-Undang
1. Dilarang memperbanyak atau mendistribusikan dokumen ini untuk tujuan komersial tanpa izin tertulis dari penulis atau pihak berwenang. Penggunaan untuk kepentingan akademik, penelitian, dan pendidikan diperbolehkan dengan mencantumkan sumber.
2. Penggunaan tanpa izin untuk kepentingan komersial atau pelanggaran hak cipta dapat dikenakan sanksi sesuai dengan UU Hak Cipta di Indonesia. Plagiarisme juga dilarang dan dapat dikenakan sanksi.
3. Universitas hanya berhak menyimpan dan mendistribusikan dokumen ini di repositori akademik, tanpa mengalihkan hak cipta penulis, sesuai dengan peraturan yang berlaku di Indonesia.
Universitas Islam Indragiri

tersebut dapat membuka kemungkinan terbaca atau tereksposnya berkas internal yang bersifat sensitif pada server. Akan tetapi, ancaman semacam ini secara umum tidak relevan pada teknologi *blockchain* apabila sistem yang digunakan memang tidak memanfaatkan XML sebagai format pemrosesan data.

6) *SQL Injection*

SQL Injection merupakan teknik serangan yang mengeksploitasi kelemahan pengolahan masukan pada aplikasi yang berinteraksi dengan basis data melalui *SQL* (Structured Query Language). Ancaman muncul ketika data yang berasal dari pengguna diteruskan menuju basis data tanpa pemeriksaan maupun penyaringan yang memadai. Akibat kondisi tersebut, perintah *SQL* tambahan dapat disisipkan ke dalam kueri yang kemudian dijalankan oleh server basis data. Eksploitasi semacam ini dapat menimbulkan konsekuensi serius, mulai dari terbukanya informasi rahasia, pengambilan data tanpa izin, perubahan maupun penghapusan isi basis data, sampai kemungkinan diperolehnya kendali yang lebih luas terhadap server. Teknik yang digunakan dapat memanfaatkan karakter khusus, komentar *SQL*, maupun manipulasi sintaks untuk mengubah alur logika kueri yang semestinya dijalankan [30].

7) *Broken Access Control*

Broken access control berbeda dengan broken *authentication* di mana penyerang berpura-pura menjadi pengguna yang tidak sah, *broken access control* memungkinkan pengguna jahat mengakses fungsi yang dilindungi secara tidak sah. Mekanisme kontrol akses yang buruk adalah salah satu

Hak Cipta Dilindungi Undang-Undang
1. Dilarang memperbanyak atau mendistribusikan dokumen ini untuk tujuan komersial tanpa izin tertulis dari penulis atau pihak berwenang. Penggunaan untuk kepentingan akademik, penelitian, dan pendidikan diperbolehkan dengan mencantumkan sumber.
2. Penggunaan tanpa izin untuk kepentingan komersial atau pelanggaran hak cipta dapat dikenakan sanksi sesuai dengan UU Hak Cipta di Indonesia. Plagiarisme juga dilarang dan dapat dikenakan sanksi.
3. Universitas hanya berhak menyimpan dan mendistribusikan dokumen ini di repositori akademik, tanpa mengalihkan hak cipta penulis, sesuai dengan peraturan yang berlaku di Indonesia.
Universitas Islam Indragiri

kerentanan utama dalam *smart contract Ethereum*. Contoh nyata adalah dompet multi-tanda tangan berbasis *smart contract Parity* yang dieksploitasi dua kali karena kerentanan kontrol akses. Pada serangan pertama, penyerang mengambil alih kontrak dompet Parity dan menguras dana. Pada serangan kedua, fungsi serupa dalam kontrak perpustakaan yang digunakan oleh semua dompet Parity diserang, diambil alih, dan dihancurkan, membuat semua dompet Parity tidak dapat digunakan dan menyebabkan sekitar 1% dari seluruh Ether hilang selamanya.

2.6 Keamanan *Website*

Perlindungan terhadap sebuah situs merupakan unsur penting yang harus menjadi perhatian baik bagi pengelola maupun pengguna. Dalam praktiknya, aspek visual dan penyajian konten sering memperoleh perhatian lebih besar daripada perlindungan sistem. Padahal, kelemahan pengamanan dapat menyebabkan konsekuensi yang jauh lebih serius, seperti akses tanpa izin terhadap informasi penting maupun perubahan tampilan situs oleh pihak yang tidak mempunyai kewenangan. Pengamanan *website* pada dasarnya mencakup upaya menjaga perangkat, aplikasi, jaringan, dan informasi agar tidak mudah diakses, diubah, maupun disalahgunakan oleh pihak yang tidak sah. Oleh sebab itu, tanggung jawab terhadap perlindungan sistem tidak hanya berada pada administrator, tetapi juga berkaitan dengan perilaku setiap pengguna yang berinteraksi dengan layanan tersebut [22].

Editya dan Mulyati [31] menjelaskan bahwa perlindungan informasi merupakan bagian penting dalam lingkungan internet. Internet tersusun atas berbagai perangkat dan jaringan yang saling berkomunikasi. Semakin banyak pihak

Hak Cipta Dilindungi Undang-Undang
1. Dilarang memperbanyak atau mendistribusikan dokumen ini untuk tujuan komersial tanpa izin tertulis dari penulis atau pihak berwenang. Penggunaan untuk kepentingan akademik, penelitian, dan pendidikan diperbolehkan dengan mencantumkan sumber.
2. Penggunaan tanpa izin untuk kepentingan komersial atau pelanggaran hak cipta dapat dikenakan sanksi sesuai dengan UU Hak Cipta di Indonesia. Plagiarisme juga dilarang dan dapat dikenakan sanksi.
3. Universitas hanya berhak menyimpan dan mendistribusikan dokumen ini di repositori akademik, tanpa mengalihkan hak cipta penulis, sesuai dengan peraturan yang berlaku di Indonesia.
Universitas Islam Indragiri

yang terhubung, semakin besar pula kebutuhan untuk menjaga data yang dipertukarkan agar tidak mudah diakses, dimanipulasi, maupun dimanfaatkan secara tidak semestinya. Karena itu, pengamanan informasi pada lingkungan internet merupakan kebutuhan yang tidak dapat dikesampingkan.

2.7 Keamanan Siber (*Cybersecurity*)

Pada lingkungan digital modern, keamanan siber mempunyai fungsi strategis dalam mempertahankan infrastruktur, sistem, serta informasi dari berbagai ancaman. Salah satu perannya ialah mencegah data pribadi maupun informasi bernilai tinggi diperoleh oleh pihak yang tidak memiliki kewenangan. Selain itu, mekanisme keamanan juga diperlukan untuk mempertahankan keaslian informasi serta memastikan layanan tetap tersedia bagi pengguna yang memiliki hak akses. Penerapan keamanan siber turut mendukung terciptanya rasa percaya pada aktivitas digital, menekan potensi malware, dan membantu menjaga sistem strategis seperti infrastruktur energi maupun keuangan. Upaya tersebut juga berkontribusi terhadap pemenuhan ketentuan perlindungan data, pencegahan penyalahgunaan identitas, serta pembentukan budaya sadar keamanan di lingkungan organisasi. Dengan demikian, cybersecurity menjadi komponen penting dalam mempertahankan keandalan sistem informasi seiring berkembangnya teknologi [32].

Secara umum, cybersecurity diarahkan untuk mempertahankan sistem digital beserta informasi di dalamnya dari tindakan yang dapat mengakibatkan kerusakan, kehilangan, pencurian, maupun gangguan operasional. Beberapa sasaran tersebut antara lain:

Hak Cipta Dilindungi Undang-Undang
1. Dilarang memperbanyak atau mendistribusikan dokumen ini untuk tujuan komersial tanpa izin tertulis dari penulis atau pihak berwenang. Penggunaan untuk kepentingan akademik, penelitian, dan pendidikan diperbolehkan dengan mencantumkan sumber.
2. Penggunaan tanpa izin untuk kepentingan komersial atau pelanggaran hak cipta dapat dikenakan sanksi sesuai dengan UU Hak Cipta di Indonesia. Plagiarisme juga dilarang dan dapat dikenakan sanksi.
3. Universitas hanya berhak menyimpan dan mendistribusikan dokumen ini di repositori akademik, tanpa mengalihkan hak cipta penulis, sesuai dengan peraturan yang berlaku di Indonesia.
Universitas Islam Indragiri

1. Perlindungan Data Sensitif: Membatasi pihak yang tidak memiliki otorisasi agar tidak dapat memperoleh data bernilai tinggi, termasuk identitas personal, informasi finansial, maupun informasi internal perusahaan.
2. Mempertahankan Integritas Data: Menjamin agar isi informasi tetap autentik dan tidak mengalami perubahan, manipulasi, maupun modifikasi yang dilakukan tanpa kewenangan.
3. Menjamin Ketersediaan Layanan: Memastikan bahwa sistem dan layanan digital tersedia untuk pengguna yang berhak dan tidak terganggu oleh serangan atau gangguan.
4. Meningkatkan Kepercayaan: Memberikan kepercayaan kepada pengguna dalam melakukan transaksi online dan interaksi digital lainnya dengan aman dan terpercaya.
5. Mencegah Ancaman Malware: Melakukan deteksi, pencegahan, serta penanganan perangkat lunak berbahaya yang berpotensi mengganggu sistem ataupun memperoleh informasi penting secara ilegal.
6. Menjaga Infrastruktur Kritis: Mempertahankan layanan strategis seperti energi, sektor finansial, serta pelayanan publik agar tetap beroperasi dan tidak mudah terganggu oleh aktivitas siber yang merugikan.
7. Pematuhan Regulasi: Menjamin aktivitas organisasi tetap sesuai dengan ketentuan hukum dan regulasi yang mengatur perlindungan informasi serta privasi pengguna.
8. Meningkatkan Kesadaran Keamanan: Memberikan edukasi kepada pegawai maupun pengguna mengenai perilaku digital yang aman sehingga kemungkinan terjadinya insiden siber dapat ditekan.

Hak Cipta Dilindungi Undang-Undang
1. Dilarang memperbanyak atau mendistribusikan dokumen ini untuk tujuan komersial tanpa izin tertulis dari penulis atau pihak berwenang. Penggunaan untuk kepentingan akademik, penelitian, dan pendidikan diperbolehkan dengan mencantumkan sumber.
2. Penggunaan tanpa izin untuk kepentingan komersial atau pelanggaran hak cipta dapat dikenakan sanksi sesuai dengan UU Hak Cipta di Indonesia. Plagiarisme juga dilarang dan dapat dikenakan sanksi.
3. Universitas hanya berhak menyimpan dan mendistribusikan dokumen ini di repositori akademik, tanpa mengalihkan hak cipta penulis, sesuai dengan peraturan yang berlaku di Indonesia.
Universitas Islam Indragiri

Hak Cipta Dilindungi Undang-Undang
1. Dilarang memperbanyak atau mendistribusikan dokumen ini untuk tujuan komersial tanpa izin tertulis dari penulis atau pihak berwenang. Penggunaan untuk kepentingan akademik, penelitian, dan pendidikan diperbolehkan dengan mencantumkan sumber.
2. Penggunaan tanpa izin untuk kepentingan komersial atau pelanggaran hak cipta dapat dikenakan sanksi sesuai dengan UU Hak Cipta di Indonesia. Plagiarisme juga dilarang dan dapat dikenakan sanksi.
3. Universitas hanya berhak menyimpan dan mendistribusikan dokumen ini di repositori akademik, tanpa mengalihkan hak cipta penulis, sesuai dengan peraturan yang berlaku di Indonesia.
Universitas Islam Indragiri

9. Perlindungan Reputasi dan Efisiensi Operasional: Mengurangi dampak serangan siber untuk menjaga reputasi bisnis, efisiensi operasional, dan kelangsungan operasi organisasi.
10. Mengamankan Jaringan dan IoT: Menjaga keamanan jaringan komputer dan perangkat In*ternet of Things* (IoT) dari serangan dan eksploitasi yang dapat merusak atau mencuri data.

2.8 Penelitian Terdahulu

Tabel 2.1 Perbandingan Penelitian Terdahulu

Peneliti	Hasil Penelitian	Komentar
Yum Thurfah Afifa Rosaliah, Jayanta Jayanta, Bayu Hananto (2021)	Kajian tersebut berhasil mengungkap sejumlah kelemahan pada sistem, terutama yang berkaitan dengan *Broken Authentication*, *Sensitive Data Exposure*, serta *Security Misconfiguration*. Temuan itu memperlihatkan masih adanya permasalahan pada mekanisme autentikasi, pengamanan informasi sensitif, dan konfigurasi sistem. Selain itu, indikasi *Clickjacking* juga ditemukan sehingga menunjukkan adanya titik lemah lain yang masih membutuhkan penanganan.	Evaluasi hanya dilakukan melalui OWASP ZAP tanpa menghadirkan perangkat atau pendekatan *penetration testing* lain sebagai pembanding. Akibatnya, cakupan temuan belum tentu mampu menggambarkan seluruh kemungkinan kelemahan yang terdapat pada sistem.
Bahrun Ghozali, Kusrini Kusrini, Sudarmawan Sudarmawan (2019)	Penilaian dilakukan berdasarkan kombinasi nilai *Likelihood* dan *Impact* sehingga diperoleh tiga kategori, yaitu *high*, *medium*, dan *low*. Pengelompokan	Pengujian masih bergantung pada OWASP ZAP tanpa dibandingkan dengan teknik *penetration testing* lainnya. Kondisi tersebut menyebabkan potensi

Peneliti	Hasil Penelitian	Komentar
	tersebut dapat dimanfaatkan pengelola maupun pengembang untuk menentukan prioritas tindakan pencegahan dan penanganan. Temuan ini juga memberikan kontribusi terhadap proses pengelolaan risiko pada sistem informasi penting di lingkungan pemerintahan.	ancaman di luar cakupan alat yang digunakan belum dapat dievaluasi secara menyeluruh.
Hery Sofyan, dkk (2023)	Pemindaian menghasilkan sepuluh temuan yang terdiri atas satu kerentanan kategori tinggi, tiga kategori menengah, serta enam kategori rendah. Berdasarkan komposisi tersebut, kondisi kerentanan *website* secara umum diklasifikasikan berada pada kategori menengah.	Analisis hanya memanfaatkan OWASP ZAP sebagai satu-satunya perangkat evaluasi tanpa pengujian pembanding menggunakan pendekatan lain. Akibatnya, kemungkinan kelemahan yang tidak terjangkau oleh OWASP ZAP belum dapat diketahui secara optimal.
Fahmi Fachri, Abdul Fadlil, Imam Riadi (2021)	Evaluasi terhadap *web server* Sistem Informasi Akademik perguruan tinggi menemukan empat kelemahan berkategori tinggi, empat berkategori menengah, dan dua berkategori rendah. Salah satu temuan menunjukkan adanya port terbuka yang dapat menjadi jalur bagi pihak tidak berwenang untuk memperoleh akses. Simulasi serangan bahkan mampu memperoleh *username* serta *password*. Hasil tersebut mengindikasikan perlunya penguatan perlindungan pada	Kajian tersebut hanya menggunakan *SQL* Lite dan tidak menyertakan metode *penetration testing* lain sebagai pembanding. Oleh karena itu, ancaman yang berada di luar kemampuan pendekatan tersebut belum dapat dipetakan secara menyeluruh.

Hak Cipta Dilindungi Undang-Undang
1. Dilarang memperbanyak atau mendistribusikan dokumen ini untuk tujuan komersial tanpa izin tertulis dari penulis atau pihak berwenang. Penggunaan untuk kepentingan akademik, penelitian, dan pendidikan diperbolehkan dengan mencantumkan sumber.
2. Penggunaan tanpa izin untuk kepentingan komersial atau pelanggaran hak cipta dapat dikenakan sanksi sesuai dengan UU Hak Cipta di Indonesia. Plagiarisme juga dilarang dan dapat dikenakan sanksi.
3. Universitas hanya berhak menyimpan dan mendistribusikan dokumen ini di repositori akademik, tanpa mengalihkan hak cipta penulis, sesuai dengan peraturan yang berlaku di Indonesia.
Universitas Islam Indragiri

Hak Cipta Dilindungi Undang-Undang
1. Dilarang memperbanyak atau mendistribusikan dokumen ini untuk tujuan komersial tanpa izin tertulis dari penulis atau pihak berwenang. Penggunaan untuk kepentingan akademik, penelitian, dan pendidikan diperbolehkan dengan mencantumkan sumber.
2. Penggunaan tanpa izin untuk kepentingan komersial atau pelanggaran hak cipta dapat dikenakan sanksi sesuai dengan UU Hak Cipta di Indonesia. Plagiarisme juga dilarang dan dapat dikenakan sanksi.
3. Universitas hanya berhak menyimpan dan mendistribusikan dokumen ini di repositori akademik, tanpa mengalihkan hak cipta penulis, sesuai dengan peraturan yang berlaku di Indonesia.
Universitas Islam Indragiri

Peneliti	Hasil Penelitian	Komentar
	web server dan dapat dijadikan dasar dalam merancang tindakan korektif.	
Sabrina Asiah Febriani, Abdul Muni, Bayu Riyanto, Muhammad Jalil, Chrismondari (2024)	Pemindaian pada SIAKAD CLOUD menghasilkan 18 temuan, terdiri atas 14 kelemahan pada kategori sedang sampai rendah dan empat temuan informasional. Setelah proses identifikasi dilakukan, sejumlah tindakan perbaikan disarankan. Walaupun tingkat kerentanannya relatif rendah, administrator tetap dianjurkan melakukan penguatan agar sistem lebih siap menghadapi ancaman dengan tingkat dampak yang lebih besar.	Evaluasi hanya menggunakan satu pendekatan tanpa dikombinasikan dengan alat lain seperti OWASP ZAP maupun Nmap. Keterbatasan tersebut berpotensi membuat ancaman yang lebih spesifik atau kompleks tidak terdeteksi sehingga rekomendasi penanganannya belum sepenuhnya menyeluruh.
Syarif Hidayatulloh, Desky Saptadiaji (2021)	Proses pemindaian pada *website* Universitas ARS menghasilkan 13 temuan. Satu di antaranya dikategorikan sebagai ancaman tingkat sedang, sedangkan dua belas lainnya berada pada tingkat rendah. Berdasarkan evaluasi keseluruhan, perlindungan *website* dinilai berada pada kondisi sangat baik. Sistem juga dinyatakan mampu memenuhi tiga prinsip utama keamanan informasi, yaitu confidentiality, integrity, dan availability, dengan dukungan *web server* serta	Analisis hanya didasarkan pada keluaran perangkat pemindai tanpa dilanjutkan melalui uji manual ataupun simulasi serangan secara langsung. Pendekatan tersebut dapat membatasi pengkajian terhadap kelemahan kategori sedang dan memungkinkan ancaman lain yang tidak terdeteksi alat pemindai tetap terlewat.

Peneliti	Hasil Penelitian	Komentar
	perangkat lunak akademik yang dinilai aman.	
Yunanri W, Yuliadi, Fahri Hamdani, Yasinta Bella Fitriana, dan Nabil Oper (2023)	Pengujian menunjukkan bahwa *website* Universitas Teknologi Sumbawa tetap mampu mempertahankan akses ketika diberikan simulasi *DDoS* menggunakan *Low Orbit Ion Cannon* (LOIC). Intensitas pengiriman dinaikkan mulai 500, 1.000, 5.000 hingga 10.000 paket. Walaupun terjadi penurunan kecepatan layanan, situs masih dapat diakses. Sebagai tindak lanjut, penggunaan *blacklist* IP serta *firewall* direkomendasikan untuk memperkuat perlindungan menghadapi *DDoS* pada masa berikutnya.	Evaluasi hanya memanfaatkan LOIC sebagai alat simulasi. Penggunaan perangkat pembanding seperti HOIC atau S*low*loris dapat memberikan sudut pandang yang lebih luas mengenai ketahanan sistem. Selain itu, efektivitas penerapan *blacklist* IP maupun *firewall* belum diuji secara langsung sehingga kemampuan solusi tersebut terhadap skenario serangan yang lebih kompleks belum dapat dipastikan.
Betta Wahyu Retna Mulya, Avinanta Tarigan (2018)	Kelemahan dalam jaringan komputer dapat dimanfaatkan oleh pihak tidak sah sehingga berdampak terhadap kerahasiaan, keutuhan, maupun ketersediaan layanan. Untuk menentukan urutan penanganannya, kajian tersebut memadukan metode *CVSS* dan *FMEA*. Hasil evaluasi menetapkan prioritas mitigasi pada server singa, kemudian server sierra, dino, dan leopard dengan rentang kerentanan 40-60%. Kombinasi kedua	Pendekatan *CVSS* dan *FMEA* memberikan dasar penentuan prioritas yang cukup luas. Namun, efektivitasnya belum dibandingkan dengan metode penilaian risiko lain seperti *OCTAVE* maupun *FAIR*. Penjelasan mengenai penerapan mitigasi pada masing-masing server juga masih terbatas sehingga keberhasilan solusi yang direkomendasikan belum dapat dievaluasi secara mendalam.

Hak Cipta Dilindungi Undang-Undang
1. Dilarang memperbanyak atau mendistribusikan dokumen ini untuk tujuan komersial tanpa izin tertulis dari penulis atau pihak berwenang. Penggunaan untuk kepentingan akademik, penelitian, dan pendidikan diperbolehkan dengan mencantumkan sumber.
2. Penggunaan tanpa izin untuk kepentingan komersial atau pelanggaran hak cipta dapat dikenakan sanksi sesuai dengan UU Hak Cipta di Indonesia. Plagiarisme juga dilarang dan dapat dikenakan sanksi.
3. Universitas hanya berhak menyimpan dan mendistribusikan dokumen ini di repositori akademik, tanpa mengalihkan hak cipta penulis, sesuai dengan peraturan yang berlaku di Indonesia.
Universitas Islam Indragiri

Hak Cipta Dilindungi Undang-Undang
1. Dilarang memperbanyak atau mendistribusikan dokumen ini untuk tujuan komersial tanpa izin tertulis dari penulis atau pihak berwenang. Penggunaan untuk kepentingan akademik, penelitian, dan pendidikan diperbolehkan dengan mencantumkan sumber.
2. Penggunaan tanpa izin untuk kepentingan komersial atau pelanggaran hak cipta dapat dikenakan sanksi sesuai dengan UU Hak Cipta di Indonesia. Plagiarisme juga dilarang dan dapat dikenakan sanksi.
3. Universitas hanya berhak menyimpan dan mendistribusikan dokumen ini di repositori akademik, tanpa mengalihkan hak cipta penulis, sesuai dengan peraturan yang berlaku di Indonesia.
Universitas Islam Indragiri

Peneliti	Hasil Penelitian	Komentar
	metode dinilai mampu membantu penyusunan peringkat penanganan berdasarkan konsekuensi setiap kelemahan.	
Wahyudin, Heri Kuswara, Resti, Sopiyan Dalis (2024)	Pemeriksaan pada sakupos.com menghasilkan sepuluh temuan keamanan setelah evaluasi dilakukan menggunakan OWASP ZAP. Komposisinya terdiri atas tujuh temuan berkategori *Medium*, dua berkategori *Low*, serta satu berkategori *Informational*. Selain melakukan identifikasi, kajian tersebut juga menyusun tindakan penanganan berdasarkan karakteristik kelemahan yang terdeteksi. Hasilnya memperlihatkan bahwa proses *vulnerability assessment* memiliki peranan penting dalam memperkuat perlindungan situs dan mengurangi peluang terjadinya insiden siber.	OWASP ZAP digunakan sebagai satu-satunya alat tanpa pembandingan melalui perangkat lain seperti Burp Suite ataupun Nessus. Karena itu, cakupan deteksi dan konfirmasi temuan masih dapat diperluas. Selain itu, rekomendasi yang dihasilkan belum diuji implementasinya sehingga tingkat efektivitasnya dalam menurunkan risiko belum dapat dipastikan.
Christian Alderi Jeffta Soeweh, dkk (2022)	Kajian tersebut menekankan pentingnya tindakan pencegahan melalui proses penilaian kerentanan berbasis OWASP Top 10. Berdasarkan laporan BSSN tahun 2021, peningkatan aktivitas serangan terhadap lingkungan perguruan tinggi menunjukkan bahwa institusi seperti FMIPA UNSRAT	Pembahasan terutama terpusat pada evaluasi kerentanan melalui OWASP Top 10 dan belum dilengkapi pendekatan lain seperti *penetration testing* atau *monitoring* berkelanjutan. Selain itu, rekomendasi keamanan yang disusun belum diuji penerapannya sehingga tingkat

Peneliti	Hasil Penelitian	Komentar
	perlu memperkuat perlindungan siber terhadap sistem serta aset informasi strategis. Sejumlah saran pengamanan kemudian diberikan untuk membantu memperkuat *website* FMIPA UNSRAT dan menekan potensi gangguan terhadap informasi penting institusi.	keberhasilannya belum dapat diverifikasi. Penambahan analisis risiko maupun pembandingan dengan kasus serupa dapat memperluas kontribusi kajian tersebut.

Hak Cipta Dilindungi Undang-Undang
1. Dilarang memperbanyak atau mendistribusikan dokumen ini untuk tujuan komersial tanpa izin tertulis dari penulis atau pihak berwenang. Penggunaan untuk kepentingan akademik, penelitian, dan pendidikan diperbolehkan dengan mencantumkan sumber.
2. Penggunaan tanpa izin untuk kepentingan komersial atau pelanggaran hak cipta dapat dikenakan sanksi sesuai dengan UU Hak Cipta di Indonesia. Plagiarisme juga dilarang dan dapat dikenakan sanksi.
3. Universitas hanya berhak menyimpan dan mendistribusikan dokumen ini di repositori akademik, tanpa mengalihkan hak cipta penulis, sesuai dengan peraturan yang berlaku di Indonesia.
Universitas Islam Indragiri