# DAFTAR ISTILAH

| Istilah | | Deskripsi | Halaman pertama kali digunakan |
|---|---|---|---|
| *Webserver* | : | Berfungsi sebagai jembatan antara pengguna (*client*) dan *server* tempat situs *web* atau aplikasi web di-host. | 2 |
| OWASP | : | *Open Web Application Security Project* (OWASP) adalah organisasi nirlaba yang fokus pada peningkatan keamanan perangkat lunak. | 3 |
| OWASP Top 10 | : | Sebuah proyek dari *Open Web Application Security Project* (OWASP) yang merangkum sepuluh risiko keamanan aplikasi *web* yang paling kritis. | 3 |
| *OWASP ZAP* | : | Sebuah alat atau tools yang bersifat *open source* untuk mendeteksi kerentanan keamanan aplikasi *web*. | 3 |
| XML | : | *Extensible Markup Language* (XML) adalah bahasa markup yang dirancang untuk menyimpan dan mengangkut data. | 3 |
| *Domain* | : | Nama domain yang digunakan untuk mengidentifikasi situs *web* atau aplikasi *web* di internet. | 5 |
| *Risk Rating* | : | Proses menilai dan mengkategorikan risiko berdasarkan tingkat keparahan dan kemungkinan terjadinya. | 9 |
| CSRF | : | *Cross-Site Request Forgery* (CSRF) adalah serangan keamanan pada aplikasi *web* yang memanfaatkan kepercayaan otentikasi yang dimiliki oleh pengguna yang sudah *login*. | 10 |
| CIA Triad | : | Model keamanan informasi yang terdiri dari tiga komponen utama: *Confidentiality* (Kerahasiaan), *Integrity* (Integritas), dan *Availability* (Ketersediaan). | 13 |
| *Likelihood* | : | Kemungkinan terjadinya atau probabilitas yang megacu pada seberapa besar kemungkinan terjadinya suatu risiko. | 18 |
| *Impact* | : | Dampak yang menunjukkan sejauh mana efek dari risiko jika ancaman tersebut terjadi. | 18 |
| *Threat Agent* | : | Entitas yang mungkin dapat merusak atau mengeksploitasi sistem, jaringan maupun data. | 18 |
| *Vulnerability* | : | Faktor kerentanan dapat mempengaruhi tingkat kesulitan seperti mudah atau tidaknya dalam menemukan dan memanfaatkan celah keamanan pada suatu aplikasi. | 18 |
| CVE | : | *Common Vulnerabilities and Exposures* (CVE) adalah sistem referensi publik yang | 19 |

| Istilah | | Deskripsi | Halaman pertama kali digunakan |
|---|---|---|---|
| | | menyediakan identifikasi standar untuk kerentanan keamanan yang diketahui di sistem perangkat lunak dan perangkat keras. | |
| *Technical Impact* | : | Faktor dari dampak ini dapat membantu dalam mengevaluasi seberapa besar dampak teknis yang kemungkinan akan terjadi pada saat kerentanan dieksploitasi. | 21 |
| *Business Impact* | : | Faktor dari dampak ini dapat membantu dalam mengevaluasi seberapa besar konsekuensi yang kemungkinan akan terjadi terhadap operasi bisnis, reputasi, dan kepatuhan pada saat kerentanan dieksploitasi. | 22 |
| *Proxy* | : | Sebuah *server* atau perangkat yang bertindak sebagai perantara antara pengguna dan sumber daya di internet atau jaringan. | 27 |
| *Exploit* | : | Metode yang memanfaatkan kerentanan atau kelemahan dalam suatu sistem untuk mendapatkan akses yang tidak sah atau menyebabkan perilaku yang tidak diinginkan pada sistem tersebut. | 28 |
| *Payload* | : | Bagian dari eksploitasi yang berisi kode atau data berbahaya yang dieksekusi oleh sistem target setelah eksploitasi berhasil. | 29 |
| *Parameter* | : | Variabel atau nilai yang digunakan untuk menguji kerentanan dan keamanan sistem secara menyeluruh. | 30 |
| DNS | : | *Domain Name System* (DNS) adalah sistem yang menerjemahkan nama domain yang mudah diingat menjadi alamat IP numerik yang digunakan oleh komputer untuk saling berkomunikasi di jaringan,termasuk internet. | 35 |
| *GET* | : | Metode *HTTP* yang digunakan untuk meminta data dari *server*. Data dikirimkan sebagai bagian dari *URL*. | 37 |
| *Brute-force* | : | Metode serangan yang mencoba semua kemungkinan kombinasi untuk menemukan kata sandi, kunci enkripsi, atau informasi sensitif lainnya. | 38 |
| *HTTP* | : | *HyperText Transfer Protocol* (HTTP) adalah protokol dasar yang digunakan untuk mengirim data antara klien (misalnya, *web browser*) dan *webserver*. | 41 |
| *Script* | : | Serangkaian instruksi atau kode yang ditulis dalam bahasa pemrograman tertentu yang dapat dijalankan oleh interpreter atau runtime | 41 |

| Istilah | | Deskripsi | Halaman pertama kali digunakan |
|---|---|---|---|
| | | environment untuk melakukan tugas atau fungsi tertentu secara otomatis. | |
| *APP_KEY* | : | Kunci enkripsi yang digunakan oleh aplikasi untuk berbagai tujuan keamanan, seperti enkripsi data dan pembuatan token. | 41 |
| *APP_DEBUG* | : | Pengaturan yang menentukan apakah aplikasi berjalan dalam *debug mode*. *Debug mode* biasanya digunakan selama pengembangan untuk memudahkan proses debugging dan pelacakan kesalahan. | 41 |
| *Cookie* | : | File yang disimpan oleh *web browser* di perangkat pengguna ketika mereka mengunjungi situs *web*. | 42 |
| *HTTPS* | : | *HyperText Transfer Protocol Secure* (HTTPS) adalah versi aman dari *HTTP* yang menggunakan SSL/TLS (*Secure Sockets Layer/Transport Layer Security*) untuk mengenkripsi data yang dikirim antara klien dan *server*. | 47 |
| *Port* | : | Angka 16-bit yang digunakan oleh protokol Transport Layer seperti *Transmission Control Protocol* (TCP) dan *User Datagram Protocol* (UDP) untuk membedakan antara berbagai aplikasi atau layanan yang berjalan pada satu *host* (komputer atau perangkat jaringan). | 47 |
| *POST* | : | Metode *HTTP* yang digunakan untuk mengirimkan data ke server untuk diproses. Data dikirimkan dalam badan (*body*) permintaan *HTTP*. | 68 |
| *Intercept* | : | Proses menangkap atau memantau data yang sedang dikirim atau diterima di suatu jaringan atau sistem. | 68 |
| *Endpoint* | : | *URL* yang digunakan oleh klien untuk berinteraksi dengan *server* melalui permintaan *HTTP*. | 74 |
| CSP | : | *Content Security Policy* (CSP) adalah sebuah mekanisme keamanan web yang dirancang untuk membantu mencegah berbagai jenis serangan seperti *Cross-Site Scripting* (XSS) dan data *injection*, yang dapat menyebabkan kerusakan pada aplikasi *web* dan pengguna. | 106 |
| *Reverse Shell* | : | Teknik yang sering digunakan dalam serangan keamanan siber di mana penyerang mengendalikan sebuah sistem dari jarak jauh | 117 |

| Istilah | | Deskripsi | Halaman pertama kali digunakan |
|---|---|---|---|
| | | dengan menghubungkan *shell* atau *command line* dari sistem target ke sistem penyerang. | |
| RHOST | : | *Remote Host* (RHOST) adalah alamat IP atau nama *host* dari sistem target yang berada di jaringan yang berbeda atau *remote*. | 118 |
| VHOST | : | *Virtual Host* (VHOST) adalah konsep dalam konfigurasi *webserver* yang memungkinkan satu *server* fisik untuk menghosting beberapa situs *web* atau aplikasi *web*. | 118 |
| LHOST | : | *Local Host* (LHOST) adalah alamat IP dari mesin lokal atau komputer yang digunakan untuk menerima koneksi balik. Dalam konteks pengujian penetrasi, ini biasanya adalah alamat IP dari komputer penyerang atau penguji yang akan menerima koneksi dari target. | 118 |
| LPORT | : | *Local Port* (LPort) adalah nomor *port* pada mesin lokal yang digunakan untuk mendengarkan atau menerima koneksi. | 118 |
| *Base64* | : | Metode encoding yang sering digunakan untuk mengubah data biner menjadi format teks yang dapat dengan mudah ditransmisikan melalui media yang hanya mendukung teks. | 129 |