DAFTAR ISTILAH

VAPT	: Metode yang digunakan untuk mengidentifikasi, mengevaluasi, dan menguji kerentanan keamanan pada suatu sistem, seperti website, untuk mengetahui potensi eksploitasi oleh pihak tidak bertanggung jawab.
IP	: Serangkaian angka unik yang digunakan untuk mengidentifikasi perangkat dalam jaringan komputer.
IT	: Teknologi yang digunakan untuk membuat, menyimpan, memproses, dan menyebarkan informasi, termasuk perangkat keras, perangkat lunak, jaringan, dan basis data.
OWASP ZAP	: *Aplikasi open-source dari OWASP yang digunakan untuk mendeteksi kerentanan pada aplikasi web secara otomatis maupun manual, seperti XSS dan SQL Injection.*
Acunetix	: *Alat pemindai keamanan otomatis untuk aplikasi web yang digunakan untuk menemukan celah keamanan seperti SQL Injection, XSS, serta kesalahan konfigurasi.*
BurpSuite	: Aplikasi yang digunakan dalam pengujian keamanan aplikasi web, terutama untuk eksploitasi manual dan analisis traffic HTTP
KaliLinux	: Distribusi sistem operasi Linux yang dirancang khusus untuk kebutuhan *penetration testing* dan keamanan informasi, berisi berbagai tools seperti Nmap, Nikto, dan Burp Suite.
NMAP	: Tools open-source yang digunakan untuk melakukan pemindaian jaringan dan mendeteksi port, layanan aktif, serta sistem operasi dari suatu host.

SQL Injection	: Serangan di mana penyerang menyisipkan perintah SQL berbahaya ke dalam input aplikasi untuk mendapatkan akses ke database.
XSS	: Serangan yang menyisipkan skrip berbahaya ke halaman web, yang kemudian dieksekusi oleh browser pengguna lain.
HTTP	: Informasi tambahan dalam komunikasi HTTP yang digunakan untuk mengatur perilaku browser, otentikasi, pengendalian cache, dan aspek keamanan.
CSRF	: Serangan yang memaksa pengguna yang telah login untuk menjalankan aksi tertentu tanpa persetujuan melalui permintaan palsu.