

OSI Model – Security Short Card

Layer 7 – Application • HTTP, DNS, SMTP, RDP • Vulns: SQLi, XSS, CSRF, traversal • Controls: WAF, MFA, patching

Layer 6 – Presentation • Encoding, TLS • Vulns: Weak crypto, bad certificate validation • Controls: TLS1.2/1.3, strong ciphers

Layer 5 – Session • Sessions, tokens • Vulns: Hijacking, fixation • Controls: Secure cookies, short tokens

Layer 4 – Transport • TCP/UDP Ports • Vulns: SYN flood, UDP amplification • Controls: FW rules, rate limit, IDS/IPS

Layer 3 – Network • IP, routing • Vulns: IP spoofing, ICMP attacks • Controls: ACLs, anti-spoofing

Layer 2 – Data Link • MAC, switching • Vulns: ARP poisoning, VLAN hop • Controls: DAI, port security

Layer 1 – Physical • Hardware, cables • Vulns: Tampering, jamming • Controls: CCTV, locks