100 Web

Vulnerabilities List

Injection exploits vulnerabilities

- SQL Injection (SQLi)
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- Remote Code Execution (RCE)
- Command Injection
- XML Injection
- LDAP Injection
- XPath Injection
- HTML Injection
- Server-Side Includes (SSI) Injection
- OS Command Injection
- Blind SQL Injection
- Server-Side Template Injection (SSTI)

Broken Authentication and Session Management

- Session Fixation
- Brute Force Attack
- Session Hijacking
- Password Cracking
- Weak Password Storage
- Insecure Authentication
- Cookie Theft
- Credential Reuse

Sensitive Data Exposure:

- Inadequate Encryption
- Insecure Direct Object Reference (IDOR)
- Data Leakage
- Unencrypted Data Storage
- Missing Security Headers
- Insecurte File Handling

Security Misconfiguration

- Default Passwords
- Directory Listing
- Unprotected API Endpoints
- Open Ports and Services
- Improper Access Controls
- Information Disclosure
- Unpatched Software
- Misconfigured CORS (Cross-Origin Resource Sharing)
- HTTP Security Headers Misconfiguration

XSS-Related Vulnerabilities:

- XML External Entity (XXE) Injection
- XML Entity Expansion (XEE)
- XML Bomb

Broken Access Control:

- Inadequate Authorization
- Privilege Escalation
- Insecure Direct Object References
- Forceful Browsing
- Missing Function-Level Access Control

Insecure Deserialization:

- Remote Code Execution via Deserialization
- Data Tampering
- Object Injection

API Security Issues:

- Insecure API Endpoints
- API Key Exposure
- Lack of Rate Limiting
- Inadequate Input Validation

Insecure Communication:

- Man-in-the-Middle (MITM) Attack
- Insufficient Transport Layer Security
- Insecure SSL/TLS Configuration
- Insecure Communication Protocols

Client-Side Vulnerabilities:

- DOM-based XSS (Cross-Site Scripting)
- Insecure Cross-Origin Communication
- Browser Cache Poisoning
- Clickjacking
- HTML5 Security Issues

Denial of Service (DoS):

- Distributed Denial of Service (DoS)
- Application Layer DoS
- Resource Exhaustion
- Slowloris Attack
- XML Denial of Service

Other Web Vulnerabilities:

- Server-Side Request Forgery (SSRF)
- HTTP Parameter Pollution (HPP)
- Insecure Redirects and Forwards
- File Inclusion Vulnerabilities
- Security Header Bypass
- Clickjacking
- Inadequate Session Timeout
- Insufficient Logging and Monitoring
- Business Logic Vulnerabilities
- API Abuse

Mobile Web Vulnerabilities:

- Insecure Data Storage on Mobile Devices
- Insecure Data Transmission on Mobile Devices
- Insecure Mobile API Endpoints
- Mobile App Reverse Engineering

IoT Web Vulnerabilities:

- Insecure IoT Device Management
- Weak Authentication on IoT Devices
- IoT Device Vulnerabilities

Web of Things (WoT) Vulnerabilities:

- Unauthorized Access to Smart Homes
- IoT Data Privacy Issues

Authentication Bypass:

- Insecure "Remember Me" functionality
- CAPTCHA Bypass

Server-Side Request Forgery (SSRF)

- Blind SSRF
- Time-based Blind SSRF

Content Spoofing

- MIME Sniffing
- X-Content-Type-Options Bypass
- Content Security Policy (CSP) Bypass

Business Logic Flaws:

- Inconsistent Validation
- Race Conditions
- Order Processing Vulnerabilities
- Price Manipulation
- Account Enumeration
- User-Based Flaws

Zero-Day Vulnerabilities:

- Unknown Vulnerabilities
- Unpatched Vulnerabilities
- Dey-Zero Exploits

Explore our
CyberSecurity Courses

Ethical Hacking Training	Diploma in Cyber Security	Cyber Security Training
INR 15,000/-	INR 63,300/-	INR 23,599/-

Call Us
1800-123-500014

Registered Office
Kolkata, India

DN-36, Primarc Tower, Unit no-1103, College More, Salt Lake, Sec-5, Kolkata-700091

Corporate Office
Bangalore, India

Nomads Horizon, Building No. 2287, 14th A Main Road, HAL 2nd Stage, Indiranagar, Bangalore - 560008, Land Mark: Beside New Horizon School

Corporate Office
Hyderabad, India

Awfis Oyster Complex, 3rd Floor, Oyster Complex, Greenlands Road Somajiguda, Begumpet, Hyderabad, Telangana 500016

www.indiancybersecuritysolutions.com

info@indiancybersecuritysolutions.com