**1. [Encryption Techniques]**

**Definition:** Involves methods used to convert information into a secure, unreadable format to protect confidentiality. This includes encryption algorithms, encoding schemes, and cryptographic protocols.

**2. [Permission Management]**

**Definition:** Focuses on controlling access to resources through authentication and authorization mechanisms, including user identity verification and token-based access control.

**[Network Security]**

**Definition:** Concerns the protection of data during transmission over networks, including secure communication protocols and verification tools such as digital certificates.

**4. [Data Security]**

**Definition:** Involves measures to protect data at rest and during usage, ensuring confidentiality, integrity, and authenticity through secure storage and digital signatures.

**5. [Software Vulnerability]**

**Definition:** Relates to weaknesses or flaws in software that can be exploited, such as memory issues, injection attacks, race conditions, and security bugs.

**6. [Secure Development]**

**Definition:** Focuses on building software with security in mind, including secure coding practices, safe use of libraries, secure configurations, and handling vulnerability reports in development platforms.

**Category\_keywords**

"Encryption Techniques": ["encrypt", "decrypt", "AES", "RSA", "cipher", "encoding"],

"Permission Management": ["token", "authentication", "authorization", "access", "login"],

"Network Security": ["SSL", "TLS", "certificate", "https", "network attack"],

"Data Security": ["password", "storage", "integrity", "signature", "data breach"],

"Software Vulnerability": ["buffer overflow", "SQL injection", "race condition", "bug", "CVE"],

"Secure Development": ["secure coding", "config", "library", "patch", "report"]

}