cwe_map.py

```
CWE_TITLES = {
    "CWE-79": "Cross-Site Scripting",
    "CWE-89": "SQL Injection",
    "CWE-20": "Improper Input Validation",
    "CWE-22": "Path Traversal",
    "CWE-119": "Buffer Overflow",
    "CWE-200": "Information Exposure",
    "CWE-287": "Improper Authentication",
    "CWE-120": "Buffer Copy without Checking Size",
    "CWE-264": "Permissions, Privileges, and Access Controls",
    "CWE-193": "Off-by-one Error",
    "CWE-19": "Data Processing Errors",
    "CWE-178": "Improper Handling of Case Sensitivity",
    "CWE-17": "Code",
    "CWE-276": "Incorrect Default Permissions",
    "CWE-255": "Credentials Management",
    "CWE-327": "Use of a Broken or Risky Cryptographic Algorithm",
    "CWE-307": "Improper Restriction of Excessive Authentication Attempts",
    "CWE-384": "Session Fixation",
    "CWE-88": "Argument Injection or Modification",
    "CWE-78": "OS Command Injection",
    "CWE-59": "Improper Link Resolution Before File Access",
    "CWE-94": "Code Injection",
    "NVD-CWE-Other": "Other/Unclassified",
    "NVD-CWE-noinfo": "Unclassified",
    "Unclassified": "Unknown"
}
def cwe_title(cwe):
    return CWE_TITLES.get(cwe, cwe if cwe else "Not specified")
```