

```
cve_scanner.py X
VulnerabilityScanner > cve_scanner.py > ...
142 def main() -> None:
143     version = input("Enter version (optional, press enter to skip): ").strip()
146
147     if not product:
148         print("Product name is required.")
149         sys.exit(1)
150
151     keyword = product if not version else f"{product} {version}"
...
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS
• PS D:\Cyber Security Tools\VulnerabilityScanner> python cve_scanner.py
=== Advanced CVE Vulnerability Scanner (Demo) ===
Enter product name (e.g., apache, openssl, nginx): windows
Enter version (optional, press Enter to skip): 10

Filter by minimum severity:
1) CRITICAL
2) HIGH
3) MEDIUM
4) LOW
5) No filter (show all)
Choose option (1-5): 3

• [+] Searching NVD for: 'windows 10'
[+] Minimum severity filter: MEDIUM

[+] Showing 1 CVEs (after filtering):

CVE: CVE-2005-0772
Severity: HIGH (score: 7.5)
Summary: VERITAS Backup Exec 9...
Reference: http://secunia.com/advisories/15789
-----
• PS D:\Cyber Security Tools\VulnerabilityScanner>
```

```
cve_scanner.py X
VulnerabilityScanner > cve_scanner.py > ...
142 def main() -> None:
143     version = input("Enter version (optional, press enter to skip): ").strip()
146
147     if not product:
148         print("Product name is required.")
149         sys.exit(1)
150
151     keyword = product if not version else f"{product} {version}"
...
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS
• PS D:\Cyber Security Tools\VulnerabilityScanner> python cve_scanner.py
=== Advanced CVE Vulnerability Scanner (Demo) ===
Enter product name (e.g., apache, openssl, nginx): apache
Enter version (optional, press Enter to skip):

Filter by minimum severity:
1) CRITICAL
2) HIGH
3) MEDIUM
4) LOW
5) No filter (show all)
Choose option (1-5): 1

• [+] Searching NVD for: 'apache'
[+] Minimum severity filter: CRITICAL

[+] Showing 1 CVEs (after filtering):

CVE: CVE-2001-0766
Severity: CRITICAL (score: 9.8)
Summary: Apache on MacOS X Client 10...
Reference: http://archives.neohapsis.com/archives/bugtraq/2001-06/0090.html
-----
• PS D:\Cyber Security Tools\VulnerabilityScanner>
```

```
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS
PS D:\Cyber Security Tools\VulnerabilityScanner> python cve_scanner.py
=== Advanced CVE Vulnerability Scanner (Demo) ===
Enter product name (e.g., apache, openssl, nginx): openssl
Enter version (optional, press Enter to skip):

Filter by minimum severity:
1) CRITICAL
2) HIGH
3) MEDIUM
4) LOW
5) No filter (show all)
Choose option (1-5): 2

[+] Searching NVD for: 'openssl'
[+] Minimum severity filter: HIGH

[+] Showing 4 CVEs (after filtering):

CVE: CVE-2003-0545
Severity: CRITICAL (score: 9.8)
Summary: Double free vulnerability in OpenSSL 0...
Reference: http://secunia.com/advisories/22249
-----
CVE: CVE-2004-0079
Severity: HIGH (score: 7.5)
Summary: The do_change_cipher_spec function in OpenSSL 0...
Reference: ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-04:05.openssl.asc
-----
CVE: CVE-2005-2946
Severity: HIGH (score: 7.5)
Summary: The default configuration on OpenSSL before 0...
Reference: http://www.cits.rub.de/MD5Collisions/
-----
CVE: CVE-2008-0166
Severity: HIGH (score: 7.5)
Summary: OpenSSL 0...
Reference: http://metasploit.com/users/hdm/tools/debian-openssl/
-----
PS D:\Cyber Security Tools\VulnerabilityScanner>
```

```
cve_scanner.py X
VulnerabilityScanner > cve_scanner.py > ...
142 def main() -> None:
143     version = input('Enter version (optional, press Enter to skip): ').strip()
146
147     if not product:
148         print('Please enter a product name.')
149         return
150
151     # Search for CVEs
152     search_results = search_nvd(product, version, severity_filter)
153
154     # Display results
155     display_results(search_results)
156
157 if __name__ == '__main__':
158     main()
159
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS
PS D:\Cyber Security Tools\VulnerabilityScanner> python cve_scanner.py
=== Advanced CVE Vulnerability Scanner (Demo) ===
Enter product name (e.g., apache, openssl, nginx): mysql
Enter version (optional, press Enter to skip):

Filter by minimum severity:
1) CRITICAL
2) HIGH
3) MEDIUM
4) LOW
5) No filter (show all)
Choose option (1-5): 5

[+] Searching NVD for: 'mysql'
[+] Minimum severity filter: UNKNOWN

[+] Showing 60 CVEs (after filtering):

CVE: CVE-1999-1188
Severity: UNKNOWN (score: 4.6)
Summary: mysql in MySQL 3...
Reference: http://marc.info/?l=bugtraq&m=91479159617803&w=2
-----
CVE: CVE-1999-0652
Severity: Not scored in NVD (no CVSS data)
Summary: Rejected reason: DO NOT USE THIS CANDIDATE NUMBER...
-----
CVE: CVE-2000-0045
Severity: UNKNOWN (score: 6.4)
Summary: MySQL allows local users to modify passwords for arbitrary MySQL users via the GRANT privilege...
Reference: http://www.securityfocus.com/bid/926
```

cve_scanner.py X

VulnerabilityScanner > cve_scanner.py > ...

```
142 def main() -> None:
143     version = input("Enter version (optional, press Enter to skip): ").strip()
146
147     if not product:
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS

PS D:\Cyber Security Tools\VulnerabilityScanner> python cve_scanner.py

```
-----
CVE: CVE-2005-0799
Severity: UNKNOWN (score: 5.0)
Summary: MySQL 4...
Reference: http://bugs.mysql.com/bug.php?id=9148
-----
CVE: CVE-2005-0004
Severity: UNKNOWN (score: 4.6)
Summary: The mysqlaccess script in MySQL 4...
Reference: http://distro.conectiva.com.br/atualizacoes/?id=a&anuncio=000947
-----
CVE: CVE-2005-0081
Severity: UNKNOWN (score: 5.0)
Summary: MySQL MaxDB 7...
Reference: http://www.iddefense.com/application/poi/display?id=187&type=vulnerabilities
-----
CVE: CVE-2005-0082
Severity: UNKNOWN (score: 5.0)
Summary: The sapdbwa_GetUserData function in MySQL MaxDB 7...
Reference: http://www.iddefense.com/application/poi/display?id=187&type=vulnerabilities
-----
CVE: CVE-2005-0684
Severity: UNKNOWN (score: 10.0)
Summary: Multiple buffer overflows in the web tool for MySQL MaxDB before 7...
Reference: http://dev.mysql.com/doc/maxdb/changes/changes_7.5.00.26.html#WebDAV
-----
CVE: CVE-2005-1274
Severity: UNKNOWN (score: 10.0)
Summary: Stack-based buffer overflow in the getIfHeader function in the WebDAV functionality in MySQL MaxDB before 7...
Reference: http://www.iddefense.com/application/poi/display?id=236&type=vulnerabilities
-----
PS D:\Cyber Security Tools\VulnerabilityScanner> 
```