





Please support the OWASP mission to improve software security through open source initiatives and community education. [Donate Now!](#) X

 PROJECTS CHAPTERS EVENTS ABOUT Q  Store  Donate  Join

## OWASP Dependency-Check

Dependency-Check is a Software Composition Analysis (SCA) tool that attempts to detect publicly disclosed vulnerabilities contained within a project's dependencies. It does this by determining if there is a Common Platform Enumeration (CPE) identifier for a given dependency. If found, it will generate a report linking to the associated CVE entries.



### Introduction

The OWASP Top 10 2013 contains a new entry: A9-Using Components with Known Vulnerabilities. Dependency Check can currently be used to scan applications (and their dependent libraries) to identify any known vulnerable components.

The problem with using known vulnerable components was described very well in a paper by Jeff Williams and Arshan Dabirsiaghi titled, "[Unfortunate Reality of Insecure Libraries](#)". The gist of the paper is that we as a development community include third party libraries in our applications that contain well known published vulnerabilities (such as those at the [National Vulnerability Database](#)).


Dependency-check has a command line interface, a Maven plugin, an Ant task, and a Jenkins plugin. The core engine contains a series of analyzers that inspect the project dependencies, collect pieces of information about the dependencies (referred to as evidence within the tool). The evidence is then used to identify the [Common Platform Enumeration \(CPE\)](#) for the given dependency. If a CPE is identified, a listing of associated [Common Vulnerability and Exposure \(CVE\)](#) entries are listed in a report. Other 3rd party services and data sources such as the NPM Audit API, the OSS Index, RetireJS, and Bundler Audit are utilized for specific technologies.



Dependency-check automatically updates itself using the [NVD Data Feeds](#) hosted by NIST. "IMPORTANT NOTE:" The initial download of the data may take ten minutes or more. If you run the tool at least once every seven days, only a small JSON file needs to be downloaded to keep the local copy of the data current.


 Watch 179  Star 7,113

The OWASP® Foundation works to improve the security of software through its community-led open source software projects, hundreds of chapters worldwide, tens of thousands of members, and by hosting local and global conferences.

### Project Classification



 Builders  Defenders



## Downloads

Version 12.1.0

[Command Line](#)

[Ant Task](#)

[Maven Plugin](#)

[Gradle Plugin](#)


[Mac Homebrew:](#)

```
brew update && brew install dependency-check
```








[Other Plugins](#)

## DAY 2

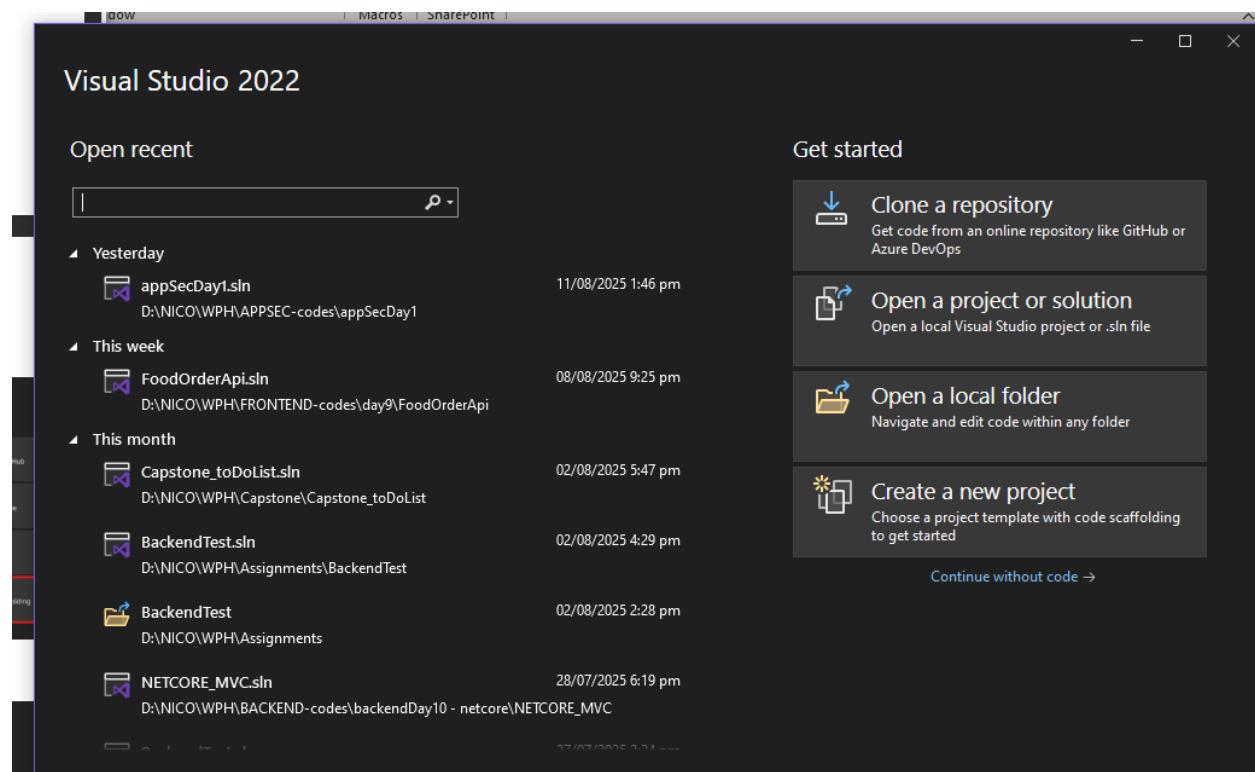
## STEP 3

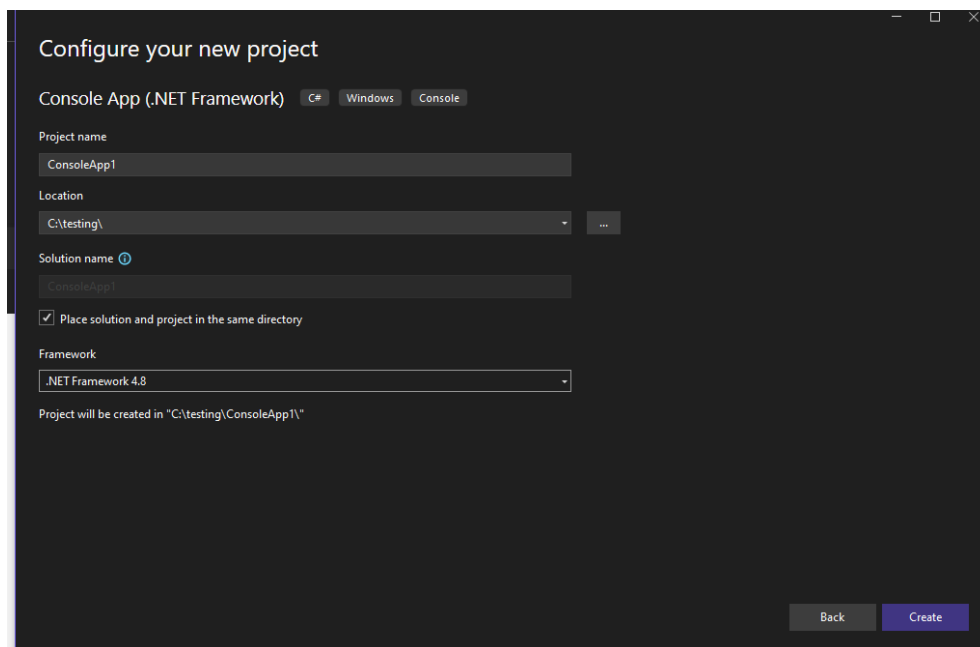
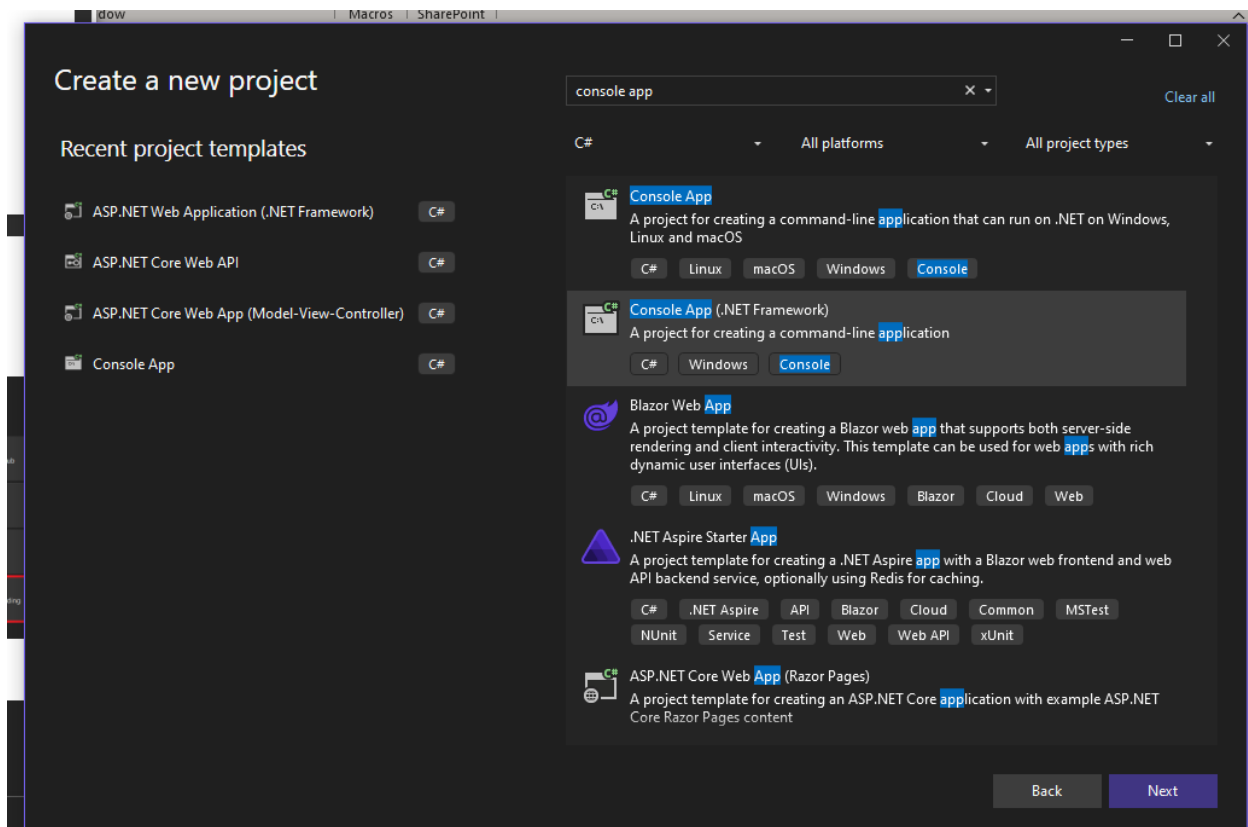
Name	Date modified	Type	Size
▼ Today (1)			
 dependency-check-12.1.0-release.zip	12/08/2025 11:30 am	WinRAR ZIP archive	36,147 KB
▼ Last month (2)			

## STEP 4

This PC > Local Disk (C:) > Users > Nicolas Family > Downloads > dependency-check >				
Name	Date modified	Type	Size	
 bin	16/02/2025 2:06 pm	File folder		
 lib	16/02/2025 2:06 pm	File folder		
 licenses	16/02/2025 2:06 pm	File folder		
 plugins	16/02/2025 2:06 pm	File folder		
 LICENSE.txt	16/02/2025 2:06 pm	Text Document	12 KB	
 NOTICE.txt	16/02/2025 2:06 pm	Text Document	1 KB	
 README.md	16/02/2025 2:06 pm	Markdown Source...	2 KB	

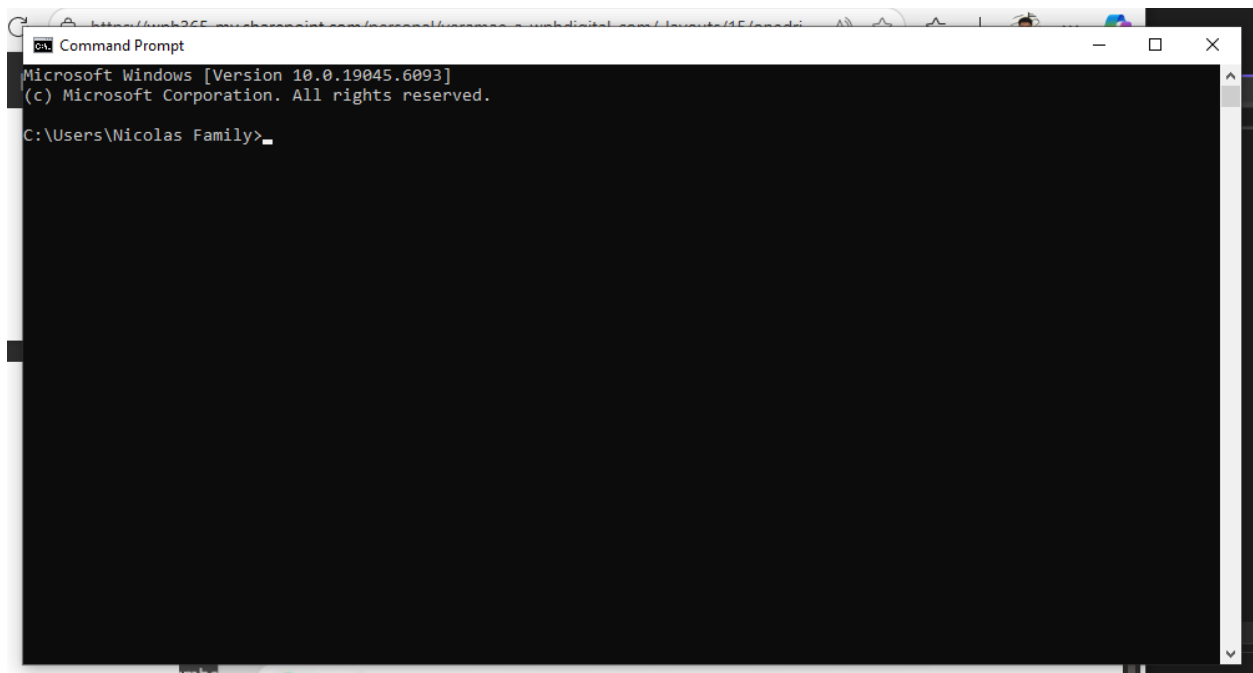
## STEP 5





## DAY 2

## STEP 8



## STEP 9

```
C:\testing>dir
Volume in drive C has no label.
Volume Serial Number is 0C09-C8B1

Directory of C:\testing

12/08/2025  12:10 pm    <DIR>          .
12/08/2025  12:10 pm    <DIR>          ..
12/08/2025  12:11 pm    <DIR>          ConsoleApp1
                0 File(s)                0 bytes
                3 Dir(s)  231,671,939,072 bytes free

C:\testing>cd ConsoleApp1
C:\testing\ConsoleApp1>_
```

## DAY 2

## STEP 10

```
C:\>cd testing

C:\testing>cd ConsoleApp1

C:\testing\ConsoleApp1>C:\dependency-check\bin\dependency-check.bat --nvdApiKey YOUR_KEY_HERE -s .
^CTerminate batch job (Y/N)? y

C:\testing\ConsoleApp1>C:\dependency-check\bin\dependency-check.bat --nvdApiKey e3ac20fc-a782-436b-ab08-73171ac8336a -s
[INFO] Checking for updates
[INFO] NVD API has 304,869 records in this update
[INFO] Downloaded 10,000/304,869 (3%)
[INFO] Downloaded 20,000/304,869 (7%)
[INFO] Downloaded 30,000/304,869 (10%)
[INFO] Downloaded 40,000/304,869 (13%)
[INFO] Downloaded 50,000/304,869 (16%)
```

```
[INFO] Completed processing batch 150/153 (98%) in 815ms
[INFO] Completed processing batch 151/153 (99%) in 512ms
[INFO] Completed processing batch 152/153 (99%) in 896ms
[INFO] Completed processing batch 153/153 (100%) in 236ms
[INFO] Updating CISA Known Exploited Vulnerability list: https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json
[INFO] Begin database defrag
[INFO] End database defrag (11742 ms)
[INFO] Check for updates complete (3313908 ms)
[INFO]

Dependency-Check is an open source tool performing a best effort analysis of 3rd party dependencies; false positives and false negatives may exist in the analysis performed by the tool. Use of the tool and the reporting provided constitutes acceptance for use on an AS IS condition, and there are NO warranties, implied or otherwise, with regard to the analysis or its use. Any use of the tool and the reporting provided is at the user's risk. In no event shall the copyright holder or OWASP be held liable for any damages whatsoever arising out of or in connection with the use of this tool, the analysis performed, or the resulting report.

About ODC: https://jeremylong.github.io/DependencyCheck/general/internals.html
False Positives: https://jeremylong.github.io/DependencyCheck/general/suppression.html

~f40 Sponsor: https://github.com/sponsors/jeremylong

[INFO] Analysis Started
[INFO] Finished File Name Analyzer (0 seconds)
[INFO] Finished MSBuild Project Analyzer (0 seconds)
[INFO] Finished Dependency Merging Analyzer (0 seconds)
[INFO] Finished Hint Analyzer (0 seconds)
[INFO] Finished Version Filter Analyzer (0 seconds)
Aug 12, 2025 5:58:10 PM org.apache.lucene.store.MemorySegmentIndexInputProvider <init>
INFO: Using MemorySegmentIndexInput with Java 21 or later; to disable start with -Dorg.apache.lucene.store.MMapDirectory.enableMemorySegments=false
Aug 12, 2025 5:58:10 PM org.apache.lucene.internal.vectorization.VectorizationProvider <lookup>
WARNING: You are running with Java 23 or later. To make full use of the Vector API, please update Apache Lucene.
[INFO] Created CPE Index (3 seconds)
[INFO] Finished CPE Analyzer (2 seconds)
[INFO] Finished False Positive Analyzer (0 seconds)
[INFO] Finished NVD CVE Analyzer (0 seconds)
[WARN] Unable to determine Package-URL identifiers for 1 dependencies
[INFO] Finished Sonatype OSS Index Analyzer (0 seconds)
[INFO] Finished Vulnerability Suppression Analyzer (0 seconds)
[INFO] Finished Known Exploited Vulnerability Analyzer (0 seconds)
[INFO] Finished Dependency Bundling Analyzer (0 seconds)
[INFO] Finished Unused Suppression Rule Analyzer (0 seconds)
[INFO] Analysis Complete (4 seconds)
[INFO] Writing HTML report to: C:\testing\ConsoleApp1\dependency-check-report.html
```

The screenshot displays the web interface of the Dependency-Check tool. At the top, there's a navigation bar with links like "How to read the report", "Suppressing false positives", and "Getting Help: github issues". Below this, the "Project:" section shows "ConsoleApp1.csproj". The "Scan Information" section provides details about the scan, including the version (12.1.8), the report generation time (Tue, 12 Aug 2025 17:58:14 +0000), and the number of dependencies scanned (11 unique), vulnerable dependencies (1), and vulnerabilities found (1). The "Summary" section includes a link to "Showing Vulnerable Dependencies (click to show all)". Below this, a table displays the vulnerable dependencies:

Dependency	Vulnerability IDs	Package	Highest Severity	CVE Count	Confidence	Evidence Count
ConsoleApp1.csproj	org.apache.commons:commons-lang3:3.12.0	MEDIUM	1	High	4	

The "Dependencies (vulnerable)" section shows a detailed view of the vulnerable dependency, "ConsoleApp1.csproj". It includes the file path, MD5, SHA1, and SHA256 hashes. Below this, there are sections for "Evidence" and "Identifiers".

**Dependencies (vulnerable)**

**ConsoleApp1.csproj**

File Path: C:\testing\ConsoleApp1\ConsoleApp1.csproj  
MD5: d9c3a3c52b5a959e753c2572718108a  
SHA1: 9a6c2ee18b3110d4462c8acc1e9f43b0d098a5  
SHA256: 29f585c40171c29e404402a130499ad9535080bea15e73e3ec773bc1f5fe

**Evidence**

**Identifiers**

- cve-2.3.a.console\_project\_page.1 (Confidence: High) [suppress]
- cve-2.3.a.console\_project\_console.1 (Confidence: High) [suppress]

**Published Vulnerabilities**

**CVE-2014-12970** [suppress]

A vulnerability has been found in yanhaven console and classified as problematic. Affected by this vulnerability is the function get\_zone\_hosts/availability/zonesTable of the file openstack\_dashboard/boards/admin/aggregates/tables.py. The manipulation leads to cross site scripting. The attack can be launched remotely. The patch is named ba908ae805959485783eb234cc4ea95017472b. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-217651.

CVE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

CVSSv3:

- Base Score: MEDIUM (5.1)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/L/A:NE:2/B:RC/RMAVA

CVSSv2:

- Base Score: MEDIUM (4.0)
- Vector: AV:N/AC:L/Au:S/C:N/I:P/A:N

References:

- #ff54a3a-2127-422b-91ae-364da2691108 - PATCH
- #ff54a3a-2127-422b-91ae-364da2691108 - THIRD PARTY ADVISORY
- #ff54a3a-2127-422b-91ae-364da2691108 - THIRD PARTY ADVISORY
- crak@vuln0.com - [V] [2]
- crak@vuln0.com - THIRD PARTY ADVISORY
- crak@vuln0.com - THIRD PARTY ADVISORY

Vulnerable Software & Versions:

- cve-2.3.a.console\_project\_console.1 versions up to (excluding) 2014-08-19

This report contains data retrieved from the [National Vulnerability Database](#).  
This report may contain data retrieved from the [CVE-2014-12970](#) Logos Vulnerability Catalog.  
This report may contain data retrieved from the [Exploit-DB](#) Database (via NPM Audit API).  
This report may contain data retrieved from [SecWiki](#).  
This report may contain data retrieved from the [Exploit-DB](#) Database.

## RELFECTION

I executed the Dependency-Check scan from the command line by navigating to my project folder using the `cd` command and running the `dependency-check.bat` script located in the `C:\dependency-check\bin` directory. Initially, I tried running the scan without an NVD API key, but the update process was extremely slow because it was downloading a large number of records with long pauses in between. I decided to stop the process, register my email with the NVD, and obtain an API key to speed up the database update. After some research, I learned how to pass the key as a parameter using the `--nvdApiKey` flag in the command. Once I restarted the scan with the API key, the download progressed steadily in increments of 10,000 records, which was much faster than before. The scan generated a report in the same directory as my project, listing detected vulnerabilities along with their severity and the files or dependencies where they were found. From reviewing the report, I noticed specific vulnerabilities tied to outdated libraries, which could potentially be addressed by upgrading dependencies to newer, patched versions or replacing them with secure alternatives. One of the main challenges I faced was understanding the update process and why it was slow without a key, but through trial, error, and research, I learned the importance of using the NVD API key for efficiency and the value of keeping the vulnerability database up to date before scanning.