# Weakness over time

## RQ1: Overall what type of weaknesses are predominant?

### Results

The following CWE IDs top the list of all weaknesses overall:

* 119-Improper Restriction of Operations within the Bounds of a Memory Buffer
* 79-Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
* 264-Permissions
* 89-Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
* 20-Improper Input Validation
* 399-Resource Management Errors
* 200-Information Exposure
* 310-Cryptographic Issues
* 94-Improper Control of Generation of Code ('Code Injection')
* 22-Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

The Least frequent 10:

|  |  |
| --- | --- |
| **id** | **frequency** |
| 17-Code | 157 |
| 254-Security Features | 150 |
| 19-Data Handling | 96 |
| 77-Improper Neutralization of Special Elements used in a Command ('Command Injection') | 56 |
| 345-Insufficient Verification of Data Authenticity | 20 |
| 74-Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') | 19 |
| 18-Source Code | 5 |
| 199-Information Management Errors | 2 |
| 21-Pathname Traversal and Equivalence Errors | 2 |
| 361-Time and State | 1 |

See allTimeWeaknesses.csv

### Methods

Extract CWE-ID, pushlished\_time from completeTable.csv Count the times of appearance of each CWE-ID

## RQ2: If you divide the time period of reporting weaknesses in 4 bins, whether the weaknesses trends change over time?

### Results

There are four bins: 1996 - 2001, 2002 - 2006, 2007 - 2011, 2012 - 2016

The most frequent ids for each bin is listed in the following table:

|  |  |  |  |
| --- | --- | --- | --- |
| 1996 to 2001 | 2002 to 2006 | 2007 to 2011 | 2012 to 2016 |
| 119-Improper Restriction of Operations within the Bounds of a Memory Buffer | 119-Improper Restriction of Operations within the Bounds of a Memory Buffer | 89-Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 119-Improper Restriction of Operations within the Bounds of a Memory Buffer |
| 20-Improper Input Validation | 94-Improper Control of Generation of Code ('Code Injection') | 79-Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 79-Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') |
| 264-Permissions | 79-Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 119-Improper Restriction of Operations within the Bounds of a Memory Buffer | 264-Permissions |
| 16-Configuration | 89-Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 264-Permissions | 20-Improper Input Validation |
| 94-Improper Control of Generation of Code ('Code Injection') | 264-Permissions | 20-Improper Input Validation | 310-Cryptographic Issues |
| 200-Information Exposure | 20-Improper Input Validation | 94-Improper Control of Generation of Code ('Code Injection') | 200-Information Exposure |
| 310-Cryptographic Issues | 399-Resource Management Errors | 399-Resource Management Errors | 399-Resource Management Errors |
| 59-Improper Link Resolution Before File Access ('Link Following') | 200-Information Exposure | 22-Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 89-Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') |
| 255-Credentials Management | 22-Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 200-Information Exposure | 352-Cross-Site Request Forgery (CSRF) |
| 287-Improper Authentication | 189-Numeric Errors | 189-Numeric Errors | 22-Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') |
| **Least 10** |  |  |
| 94-Improper Control of Generation of Code ('Code Injection') | 189-Numeric Errors | 310-Cryptographic Issues | 19-Data Handling |
| 200-Information Exposure | 287-Improper Authentication | 59-Improper Link Resolution Before File Access ('Link Following') | 16-Configuration |
| 310-Cryptographic Issues | 255-Credentials Management | 255-Credentials Management | 77-Improper Neutralization of Special Elements used in a Command ('Command Injection') |
| 59-Improper Link Resolution Before File Access ('Link Following') | 16-Configuration | 16-Configuration | 134-Uncontrolled Format String |
| 255-Credentials Management | 134-Uncontrolled Format String | 362-Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 345-Insufficient Verification of Data Authenticity |
| 287-Improper Authentication | 310-Cryptographic Issues | 134-Uncontrolled Format String | 74-Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') |
| 22-Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 59-Improper Link Resolution Before File Access ('Link Following') | 78-Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 18-Source Code |
| 362-Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 362-Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 19-Data Handling | 199-Information Management Errors |
| 79-Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 78-Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 254-Security Features | 21-Pathname Traversal and Equivalence Errors |
| 399-Resource Management Errors | 352-Cross-Site Request Forgery (CSRF) | 17-Code | 361-Time and State |

See 4\_Bin\_Weaknesses.csv

### Methods

Extract CWE-ID, pushlished\_time from completeTable.csv Sort the list by time, divide the list into four sub-list according to the bins Count the times of appearance of each CWE-ID in each list

## RQ3: What are some weaknesses that are consistently present over time, but might not be dominant?

### Results

Surprisingly there are only three IDs that appear in all time periods:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Frequencies in | 1996 - 2001 | 2002 -2006 | 2007 -2011 | 2012 -2016 |
| 119-Improper Restriction of Operations within the Bounds of a Memory Buffer | 15 | 334 | 2757 | 3487 |
| 264-Permissions | 10 | 151 | 1735 | 2581 |
| 399-Resource Management Errors | 1 | 121 | 1266 | 1260 |

See overtimeconsistent.csv

### Methods

Use the four lists from RQ2, find the intersection (in terms of id) of all lists, and the remains are the CWEs that appear in all periods