|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CWE/SANS Top 25** | | | **Releases** | | |
| **Insecure Interaction between Components** | | | **2009** | **2010** | **2011** |
|  | 89 | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')[[1]](#footnote-1) | ✓ | 2 | 1 |
|  | 78 | Improper Sanitization of Special Elements used in OS Command (‘OS Command Injection’) | ✓ | 9 | 2 |
|  | 79 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')[[2]](#footnote-2) | ✓ | 1 | 4 |
|  | 319 | Cleartext Transmission of Sensitive Information | ✓ | 10 | 8 |
|  | 434 | Unrestricted Upload of File with Dangerous Type | 🗶 | 8 | 9 |
|  | 352 | Cross-Site Request Forgery (CSRF) | ✓ | 4 | 12 |
|  | 601 | URL Redirection to an Untrusted Site (‘Open Redirect’) | 🗶 | 23 | 22 |
|  | 20 | Improper Input Validation | ✓ | x | x |
|  | 116 | Improper Encoding or Escaping of Output | ✓ | x | x |
|  | 362 | Concurrent Execution using Shared Resource with Improper Synchronization (‘Race Condition’)[[3]](#footnote-3) | ✓ | 25 | x |
|  | 209 | Information Exposure Through an Error Message[[4]](#footnote-4) | ✓ | 16 | x |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CWE/SANS Top 25** | | | **Releases** | | |
| **Risky Resource Management** | | | **2009** | **2010** | **2011** |
|  | 120 | Buffer Copy without Checking Size of Input (‘Classic Buffer Overflow’) | 🗶 | 3 | 3 |
|  | 119 | Improper Restriction of Operations within the Bounds of a Memory Buffer[[5]](#footnote-5) | ✓ | 3/18 | 3/20 |
|  | 22 | Improper Limitation of a Pathname to a Restricted Directory (‘Path Traversal’) | 🗶 | 7 | 13 |
|  | 494 | Download of Code without Integrity Check | ✓ | 20 | 14 |
|  | 829 | Inclusion of Functionality from Untrusted Control Sphere | 🗶 | x | 16 |
|  | 98 | Improper Control of Filename for Include/Require Statement in PHP Program (‘PHP File Inclusion’) | 🗶 | 15 | 16 |
|  | 676 | Use of Potentially Dangerous Function | 🗶 | 🗶 | 18 |
|  | 131 | Incorrect Calculation of Buffer Size | 🗶 | 18 | 20 |
|  | 134 | Uncontrolled Format String | 🗶 | 🗶 | 23 |
|  | 190 | Integer Overflow or Wraparound | 🗶 | 17 | 24 |
|  | 805 | Buffer Access with Incorrect Length Value | 🗶 | 12 | 🗶 |
|  | 754 | Improper Check for Unusual or Exceptional Conditions | 🗶 | 15 | 🗶 |
|  | 129 | Improper Validation of Array Index | 🗶 | 14 | 🗶 |
|  | 770 | Allocation of Resources without Limits or Throttling | 🗶 | 22 | 🗶 |
|  | 642 | External Control of Critical State Data | ✓ | 🗶 | 🗶 |
|  | 73 | External Control of File Name of Path | ✓ | 🗶 | 🗶 |
|  | 426 | Untrusted Search Path | ✓ | 🗶 | 🗶 |
|  | 94 | Improper Control of Generation of Code (‘Code Injection’)[[6]](#footnote-6) | ✓ | 🗶 | 🗶 |
|  | 404 | Improper Resource Shutdown or Release | ✓ | 🗶 | 🗶 |
|  | 665 | Improper Initialization | ✓ | 🗶 | 🗶 |
|  | 682 | Incorrect Calculation | ✓ | 🗶 | 🗶 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CWE/SANS Top 25** | | | **Releases** | | |
| **Porous Defences** | | | **2009** | **2010** | **2011** |
|  | 306 | Missing Authentication for Critical Function | 🗶 | 19 | 5 |
|  | 862 | Missing Authorization | 🗶 | 5 | 6 |
|  | 285 | Improper Authorization[[7]](#footnote-7) | ✓ | 5 | 6/15 |
|  | 798 | Use of Hard-coded Credentials | 🗶 | 11 | 7 |
|  | 259 | Hard Coded Password | ✓ | 11 | 7 |
|  | 311 | Missing Encryption of Sensitive Data | 🗶 | 10 | 8 |
|  | 807 | Reliance on Untrusted Inputs in a Security Decision | 🗶 | 6 | 10 |
|  | 250 | Execution with Unnecessary Privileges | ✓ | 🗶 | 11 |
|  | 863 | Incorrect Authorization | 🗶 | 5 | 15 |
|  | 732 | Incorrect Permission Assignment for Critical Resource | ✓ | 21 | 17 |
|  | 327 | Use of Broken or Risky Cryptographic Algorithm | ✓ | 24 | 19 |
|  | 307 | Improper Restriction of Excessive Authentication Attempts | 🗶 | 🗶 | 21 |
|  | 759 | Use of One-Way Hash without Salt | 🗶 | 🗶 | 25 |
|  | 602 | Client-Side Enforcement of Server-Side Security | ✓ | 🗶 | 🗶 |
|  | 330 | Use of Insufficiently Random Values | ✓ | 🗶 | 🗶 |

1. Renamed from “Failure to Preserve SQL Query Structure ('SQL Injection')” on 21st June 2010. [↑](#footnote-ref-1)
2. Renamed from “Failure to Preserve Web Page Structure (‘Cross Site Scripting’)” on 21st June 2010. [↑](#footnote-ref-2)
3. Renamed from “Race Condition” on 13th December 2010. [↑](#footnote-ref-3)
4. Renamed from “Error Message Information Leak” on 1st December 2009. [↑](#footnote-ref-4)
5. Renamed from “Failure to Constrain Operations within the Bounds of Memory Buffer” on 13th December 2010. [↑](#footnote-ref-5)
6. Renamed from “Failure to Control Generation of Code (‘Code Injection’)” on 29th March 2011. [↑](#footnote-ref-6)
7. Renamed from “Improper Access Control (Authorization)” on 29th March 2011. [↑](#footnote-ref-7)