At the OWASP Project Summit, active participants and community members decided on a vulnerability view, with up to two (2) forward looking vulnerability classes, with ordering defined partially by quantitative data, and partially by qualitative surveys.

**Industry Ranked Survey**

For the survey, we collected the vulnerability categories that had been previously identified as being “on the cusp” or were mentioned in feedback to 2017 RC1 on the Top 10 mailing list. We put them into a ranked survey and asked respondents to rank the top four vulnerabilities that they felt should be included in the OWASP Top 10 2017. The survey was open from Aug 2 – Sep 18, 2017. 516 responses were collected and the vulnerabilities were ranked.

|  |  |  |
| --- | --- | --- |
| ***Rank*** | ***Survey Vulnerability Categories*** | **Score** |
| 1 | Exposure of Private Information ('Privacy Violation') [CWE-359] | 748 |
| 2 | Cryptographic Failures [CWE-310/311/312/326/327] | 584 |
| 3 | Deserialization of Untrusted Data [CWE-502] | 514 |
| 4 | Authorization Bypass Through User-Controlled Key (IDOR & Path Traversal) [CWE-639] | 493 |
| 5 | Insufficient Logging and Monitoring [CWE-223 / CWE-778] | 440 |

Exposure of private information is clearly the highest-ranking vulnerability, but fits very easily as additional an emphasis into the existing Sensitive Data Exposure. Cryptographic Failures can also fit within Sensitive Data Exposure. Deserialization was ranked at number three, so it was added to the Top 10 as A8:2017. The fourth ranked User Controlled Key is included in the Authorization category; it is good to see it rank highly on the survey, as there is not much data relating to authorization vulnerabilities. The number five ranked category in the survey is Insufficient Logging and Monitoring, which we also believe is a good fit for the Top 10 list. We have moved to a point where applications need to be able to define what may be an attack and generate appropriate log messages and alerts.

**Public Data Call**

Traditionally, the data collected and analyzed was more along the lines of frequency data; how many vulnerabilities found in tested applications. As is well known, tools traditionally report all instances found of a vulnerability and humans traditionally report a single finding with a number of examples. This makes it very difficult to aggregate the two styles of reporting in a comparable manner.

For 2017, the incidence rate was calculated by how many applications in a given data set had one or more of a specific vulnerability type. The data from many larger contributors was provided in two views: The first was the traditional frequency style of counting every instance found of a vulnerability, the second was the count of applications that each vulnerability was found in (one or more time). While not perfect, this reasonably allows us to compare the data from Human Assisted Tools and Tool Assisted Humans. The raw data and analysis work will be provided in GitHub. We intend to expand on this with additional structure for 2020 (or earlier).

We received 40+ submissions in the call for data, as many were from the original data call that was focused on frequency, we were able to use data from 23 contributors covering ~114k applications. We used a one year block of time where possible and identified by the contributor. The majority of applications are unique, though we acknowledge the likelihood of some repeat applications between the yearly data from Veracode. The 23 datasets used were either identified as tool assisted human testing or specifically provided incidence rate from human assisted tools. Anomalies in the selected data of 100%+ incidence were adjusted down to 100% max. To calculate the incidence rate, we calculated the percentage of the total applications there were found to contain each vulnerability type. The ranking of incidence was used for the prevalence calculation in the overall risk for ranking the Top 10.