Appendix : Glossary

1. Risk Rating

Severity	Description
High	The vulnerabilities under high rating are considered to be of highest risk level. Such vulnerability should be handled with highest priority. Under specific conditions, these vulnerabilities can potentially make the system unusable and lead to serious security breaches.
Medium	Though the threat is not critical at the moment, it has the potential to become a High risk threat in the future under certain circumstances if not mitigated. Medium risk vulnerabilities require significant mitigation to lower the impact of the threat.
Low	The information found is useful to the attacker, but is not a threat in itself. Existing security controls are likely to be adequate or the risk is acceptable, but over the period this may give rise to more serious problems.
Info	The data revealed is an additional piece of information and there are no serious security implications related to it. Items listed here are not vulnerabilities, but are indicators of overall application development security practices.

Risk Rating		Impact		
		High	Medium	Low
Likelihood	High	High	High	Medium
	Medium	High	Medium	Low
	Low	Medium	Low	Info

2. Vulnerability Title

The vulnerability title is a short one line description of the vulnerability discovered.

3. OWASP Reference

The OWASP reference is a standardized list of vulnerability types. This aims to identify each vulnerability type with a unique reference id, which may be used to access more information regarding the vulnerability.

4. Abstract

The section describes the severity of a potential attack based on successful exploitation of the vulnerability.

5. Vulnerability Description

The description gives the overview of flaw or bug that caused the vulnerability. This is a brief explanation of the vulnerability with examples.

6. Instance(s)

The section highlights vulnerabilities exist in Application scanned by plugin.

7. Recommendation

This section provides solutions or workarounds to mitigate the risk arising from this vulnerability.

8. Severity

The severity describes the risk level of the vulnerability.

9. Privacy Risk

Risk scoring of an application is based on the data obtained during risk analysis of application. Based on the data collected during the scan, the risk score is assigned to each risk and finally arrived at the overall score. The scan looks at the possible risks that an application can possess.

10. App Risk

This section rates the application based on the vulnerabilities and instances detected. A application is rated on a scale of 100 wherein the app with score in range 0 - 30 is under Low risk, 30 - 50 is under Medium risk, 50 and above is under High risk.

11. CVSS

The Common vulnerability scoring system CVSS is a NIST standard for assessing the severity of security vulnerabilities. The CVSS score establishes a measure of how much concern a vulnerability warrants, compared to other vulnerabilities. The score is arrived at considering various vectors and applying standard formulaes. The scores range from 0 to 10. Vulnerabilities with a base score in the range 7.0-10.0 are High, those in the range 4.0-6.9 as Medium, and 0-3.9 as Low.

Reference

www.first.org/cvss/cvss-guide

12. Compliance

An app must comply with privacy and data protection laws, regulations, and policies designed to protect confidential information, such as PCI DSS, NIST, HIPAA. This section provides an overview on which compliance has been violated by the app.

PCI Reference

https://www.pcisecuritystandards.org/index.php

HIPPA Reference

http://www.hhs.gov/ocr/privacy/

NIST Reference

http://csrc.nist.gov/publications/PubsSPs.html

Document Reference

https://www.google.co.in/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&ved=0CC0QFjAD&url=https%3A%2F%2Fcloudsecurityalliance.org%2Fguidance%2FCSA-ccm-v1.00.xlsx&ei=I6vhU82yEpK8uqSMzoDgCQ&usg=AFQjCNH50ajXlFyJ_Q5KMCyU16tlDJSYeg&bvm=bv.72197243,d.c2E