**CWE and Risk Analysis:**

Below CWE’s related to logs are analyzed as part of the activity log misuse case.

[CWE-532](https://cwe.mitre.org/data/definitions/532.html): **Insertion of Sensitive Information into Log File**

<< https://cwe.mitre.org/data/definitions/532.html>>

Information in the log file can give valuable guidance to an attacker. Different log files can be used for different stages and can unconsciously report sensitive data. For example, server logs can give information on the full path, names, and system information, and sometimes usernames and passwords. This type of weakness is like CWE-538 Insertion of sensitive information into an externally accessible file or directory. CVE-2017-9615 and CVE-2018-19999036 are the related vulnerabilities resulting from this weakness. CAPEC-215 holds more information on attack patterns.

[CWE-117](https://cwe.mitre.org/data/definitions/117.html): **Improper output neutralization for Logs**

<< https://cwe.mitre.org/data/definitions/117.html>>

This can allow an attacker to forge log entries or inject malicious content into logs. This happens when data enters an application from an untrusted source or when data is written to an application or system log file. This type of weakness is related to CWE-116(Improper Encoding or Escaping of Output) and can lead to CWE-93(Improper Neutralization of CRLF sequences-CRLF Injection). We can see these related vulnerabilities in [CVE-2006-4624](http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4624). Related attack patterns show [CAPEC-268](http://capec.mitre.org/data/definitions/268.html)(audit log manipulation) [CAPEC-81](http://capec.mitre.org/data/definitions/81.html)(weblogs tampering) and CAPEC-93(Log Injection-Tampering-Forging).

CWE-778: **Insufficient Logging**

<< https://cwe.mitre.org/data/definitions/778.html>>

This type of issue occurs when software either does not record the event or omits important details about the event when logging it. If security-critical events such as failed login attempts are not logged properly, this can make malicious behavior more difficult to detect and can hinder analysis. This weakness is related to CWE-223 omission of security-relevant Information. This type of weakness can lead to CVE\_2008-4315, CVE-2008-1203 vulnerabilities.