**Log Injection**

**Description1:** Writing invalidated user input to log files can allow an attacker to **forge log entries or inject malicious content into the logs**.

Log forging vulnerabilities occur when:

1. Data enters an application from an untrusted source.
2. The data is written to an application or system log file.

Applications typically use log files to store a history of events or transactions for later review, statistics gathering, or debugging. Depending on the nature of the application, the task of reviewing log files may be performed manually on an as-needed basis or automated with a tool that automatically culls logs for important events or trending information.

Interpretation of the log files may be hindered or misdirected if an attacker can supply data to the application that is subsequently logged verbatim. **In the most benign case, an attacker may be able to insert false entries into the log file** by providing the application with input that includes appropriate characters. If the log file is processed automatically, the attacker **can render the file unusable** by corrupting the format of the file or injecting unexpected characters. A subtler attack might involve **skewing the log file statistics**. Forged or otherwise, corrupted log files can be used to **cover an attacker's tracks or even to implicate another party in the commission of a malicious act**. In the worst case, **an attacker may inject code or other commands into the log file and take advantage of a vulnerability in the log processing utility**. [1]

**Description2:** This attack targets the log files of the target host. The attacker injects, manipulates or forges malicious log entries in the log file, allowing him to **mislead a log audit**, **cover traces of attack**, or perform other malicious actions. The target host is not properly controlling log access. As a result, tainted data is resulting in the log files leading to a **failure in accountability**, **non-repudiation** and **incident forensics capability**.

**Description 3:** Logging is one of the most common things that an application does. Logging is a very generic term that can mean lots of different things, from debug style logging for the developer, up to and including functioning as the system audit log. The 3 most common logging mechanisms I see in real world use are:

1. System output (System.out.println) [3]

2. 3rd party logging library (log4j, commons logging, slf4j, etc.)

3. DB Logging

attacker can forge entries in the application log which **reduces the value of the logs**, and **frustrates any forensic type activities**.

**Refrences**

**[1]** <https://www.owasp.org/index.php/Log_Injection>

**[2]** <https://capec.mitre.org/data/definitions/93.html>

**[3]** http://www.jtmelton.com/2010/09/21/preventing-log-forging-in-java/