System Information Leak Internal

An internal system information leak occurs when system data or debugging information is sent to a local file, log, or console. In System production environments, the debug and info logging messages are disabled.

# Preventing System Information Leak Internal

Write error messages with security in mind. In production environments, turn off detailed error information in favor of brief messages. Restrict the generation and storage of detailed output that can help administrators and programmers diagnose problems. Be careful, debugging traces can sometimes appear in non-obvious places (embedded in comments in the HTML for an error page, for example).

Even brief error messages that do not reveal stack traces or database dumps can potentially aid an attacker. For example, an "Access Denied" message can reveal that a file or user exists on the system.

In addition, in system, access to system logs are restricted to authorized users.

# Example

Try {

…

} catch (Exception e) {

e.printStackTrace();

}

Depending on the environment configuration, the call to printStackTrace will leak information internally. calls to getStackTrace are equally dangerous.

# References

<http://www.hpenterprisesecurity.com/vulncat/en/vulncat/dotnet/system_information_leak_internal.html>

<https://www.owasp.org/index.php/Information_Leakage>