**Privacy Violation: Heap Inspection Development Mitigation SOP**

Privacy violation vulnerabilities occur when private information, such as passwords or social security numbers, are mishandled and compromises the user’s privacy. Privacy violations occur when private user information enters the program or when the data is written to an external location, such as the console, filesystem or network.

Privacy violation in the form of the heap inspection vulnerability specifically occurs when sensitive data is stored in a String object, making it impossible to reliably purge the data from memory. Sensitive data stored in memory can be leaked if it is stored in a managed String object because they are not pinned, allowing the garbage collector to relocate those objects and leave copies in memory.

**Defense Against Privacy Violation: Heap Inspection**

Private information exposure should be limited and should be cleared when it is no longer in use. Unless access is required, access to private data should not be granted to applications, processes or employees. Private data should be encrypted if it needs to be stored. If storage in necessary, sensitive data should be stored in byte arrays or characters, instead of immutable objects like Strings, so they can be programmatically cleared.

**Example**

private JPasswordField pf;

final char[] password = pf.getPassword();

String passwordAsString = new String(password);

**Explanation**

This code converts a password from a character array to a String.

**Recommendation**

The password is never cleared from the array once it is used, the code below shows how to handle the password:

private JPasswordField pf;

final char[] password = pf.getPassword();

… // use the password

Arrays.fill(password, ‘’); //erases the password from the array

**References**

1. [HP Enterprise Security – Privacy Violation](http://www.hpenterprisesecurity.com/vulncat/en/vulncat/sql/privacy_violation.html)
2. [HP Enterprise Security – Privacy Violation: Heap Inspection](http://www.hpenterprisesecurity.com/vulncat/en/vulncat/sql/privacy_violation.html)