**Password Management: Password in Configuration File Development Mitigation SOP**

Storing a plaintext password in a configuration file allows anyone who can read the file access to the password-protected resource. Developers sometimes believe that they cannot defend the application from someone who has access to the configuration, but this attitude makes an attacker's job easier. Good password management guidelines require that a password never be stored in plaintext.

**Defense Against Password Management: Password in Configuration File**

A password should never be stored in plaintext. Instead, the password should be entered by an administrator when the system starts. If that approach is impractical, a less secure but often adequate solution is to obfuscate the password and scatter the de-obfuscation material around the system so that an attacker has to obtain and correctly combine multiple system resources to decipher the password.

Some third-party products claim the ability to manage passwords in a more secure way. For example, WebSphere Application Server 4.x uses a simple XOR encryption algorithm for obfuscating values, but be skeptical about such facilities. WebSphere and other application servers offer outdated and relatively weak encryption mechanisms that are insufficient for security-sensitive environments. For a secure solution the only viable option is a proprietary one.

**Example**

Database.username = bob

Database.pass = hunter2

**References**

1. [HP Enterprise Security - Password Management: Password in Configuration File](http://www.hpenterprisesecurity.com/vulncat/en/vulncat/java/password_management_password_in_configuration_file.html)
2. [OWASP - Password Plaintext Storage](https://www.owasp.org/index.php/Password_Plaintext_Storage)