# Password Management Hardcoded Password Developer SOP

It is never a good idea to hardcode a password. Not only does hardcoding a password allow all of the project's developers to view the password, it also makes fixing the problem extremely difficult. Once the code is in production, the password cannot be changed without patching the software. If the account protected by the password is compromised, the owners of the system will be forced to choose between security and availability.

# Hardcoded Password Prevention

Passwords should never be hardcoded and should generally be obfuscated and managed in an external source. Storing passwords in plaintext anywhere on the web site allows anyone with sufficient permissions to read and potentially misuse the password. For JavaScript calls that require passwords, it is better to prompt the user for the password at connection time.

# Example

The following code uses a hardcoded password to connect to an API

obj = new XMLHttpRequest();

obj.open(‘GET’, ‘/users.jsp?id=’+form.id.value,’true’,’BOB’,’Hunter2’);

The code will work properly, but anyone who views the source code of the web page can view the password.

# References

<https://www.owasp.org/index.php/Password_Management:_Hardcoded_Password>

<http://www.hpenterprisesecurity.com/vulncat/en/vulncat/javascript/password_management_hardcoded_password.html>