Approve assuming permissions check

Script approval provides three options: Approve, Deny, and "Approve assuming permissions check." While the purpose of the first two are self-evident, the third requires some additional understanding of what internal data scripts are able to access and how permissions checks inside of Jenkins function.

Consider a script which accesses the method `hudson.model.AbstractItem.getParent()`, which by itself is harmless and will return an object containing either the folder or root item which contains the currently executing Pipeline or Job. Following that method invocation, executing `hudson.model.ItemGroup.getItems()`, which will list items in the folder or root item, requires the `Job/Read` permission.

This could mean that approving the `hudson.model.ItemGroup.getItems()` method signature would allow a script to bypass built-in permissions checks.

Instead, it is usually more desirable to click **Approve assuming permissions check** which will cause the Script Approval engine to allow the method signature assuming the user running the script has the permissions to execute the method, such as the `Job/Read` permission in this example.