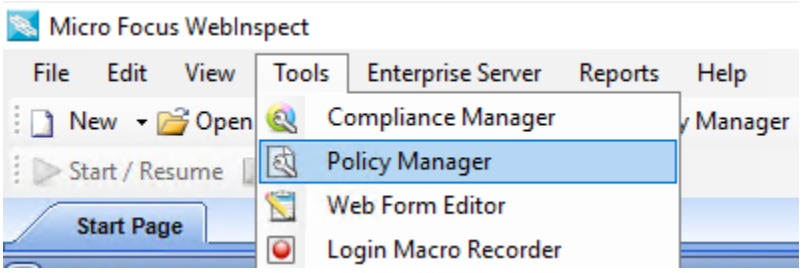
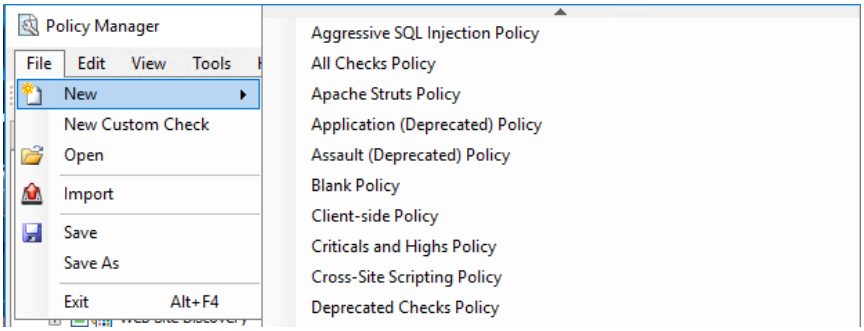
How to use Policy Manager Tool

Creating a custom check

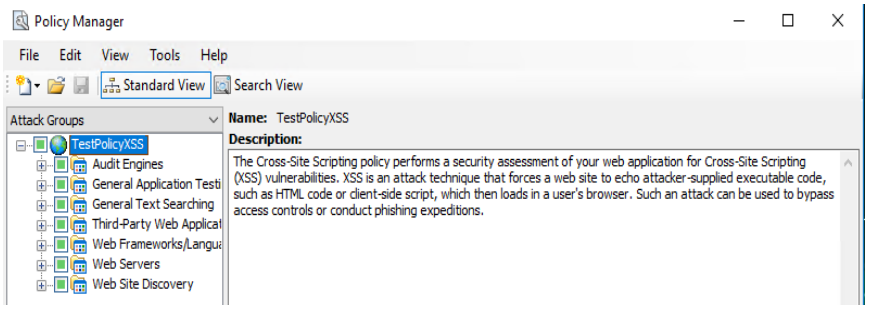
1. Firstly, you can use Policy Manager tool from WebInspect -> Tools -> Policy Manager. Or from Start Menu -> Fortify -> Policy Manager.



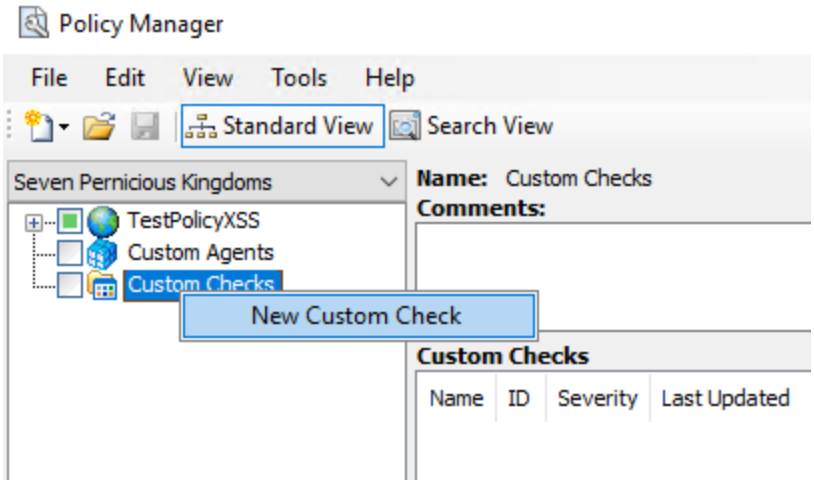
2. Open Policy Manager tool.
3. When you already have opened Policy Manager tool, you would need to create a new custom check.
4. So, it is required to have a custom policy created in your end.
5. If you do not have one created, you can create a new custom policy based on prepackaged policy, selecting File -> New (or clicking on New Policy Icon) and select the policy on which you will model a new one.

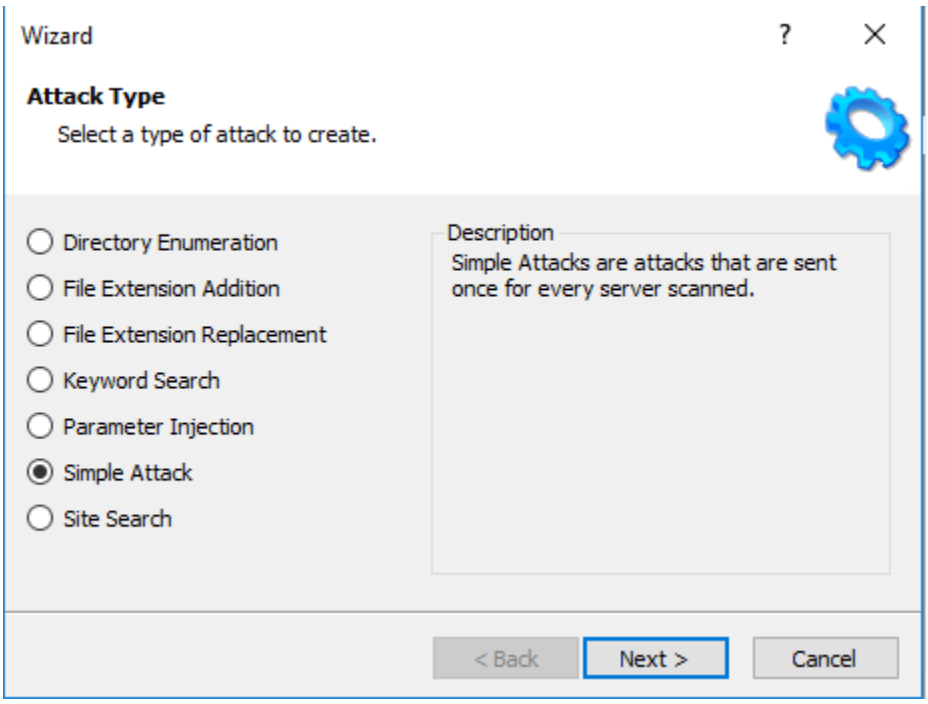


6. For example, we take Cross-site Scripting Policy and create a new custom policy.



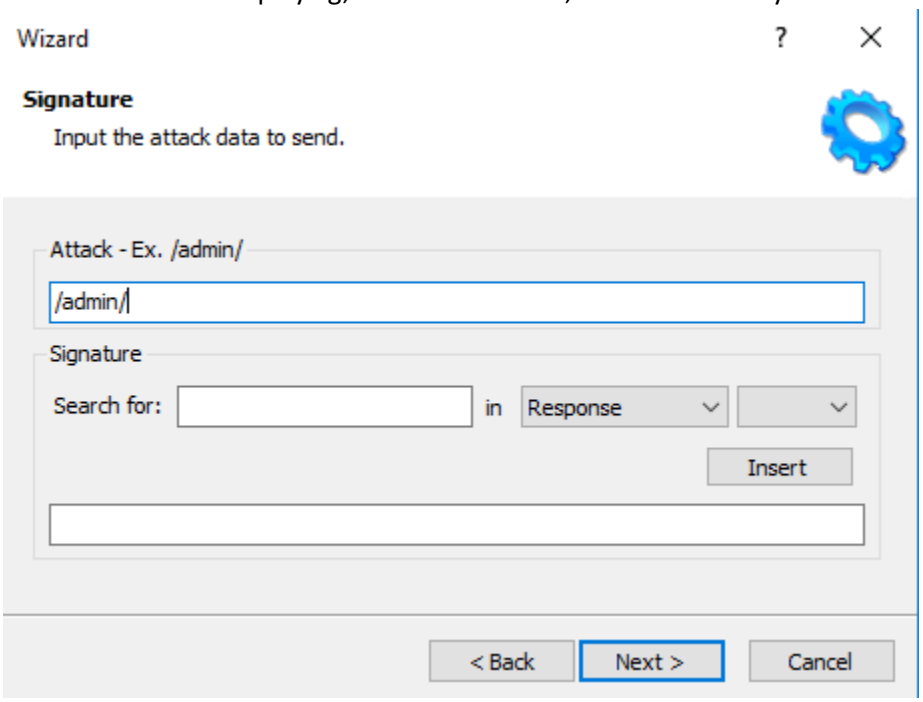
7. Make Sure the Standard View is selected, with attack groups listed in the left pane, as we can see in the image above.
8. Then right-click on Custom Checks and select New Custom Checks from shortcut menu. Custom Check wizard appears as follows:



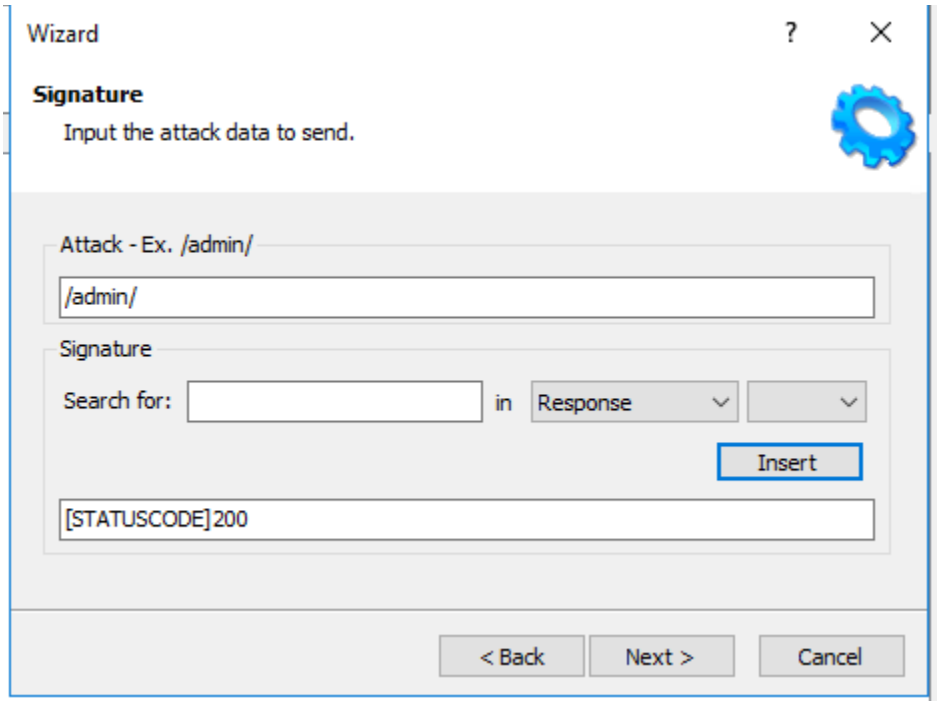


9. Select one of the attack types shown in the image above. So, each attack type has a description on right pane, so you can review for selecting the appropriated attack type for your custom check.
10. Then click Next when you have selected required Attack Type.

11. A new window is displaying, so in Attack field, enter the data you want to use for the attack.



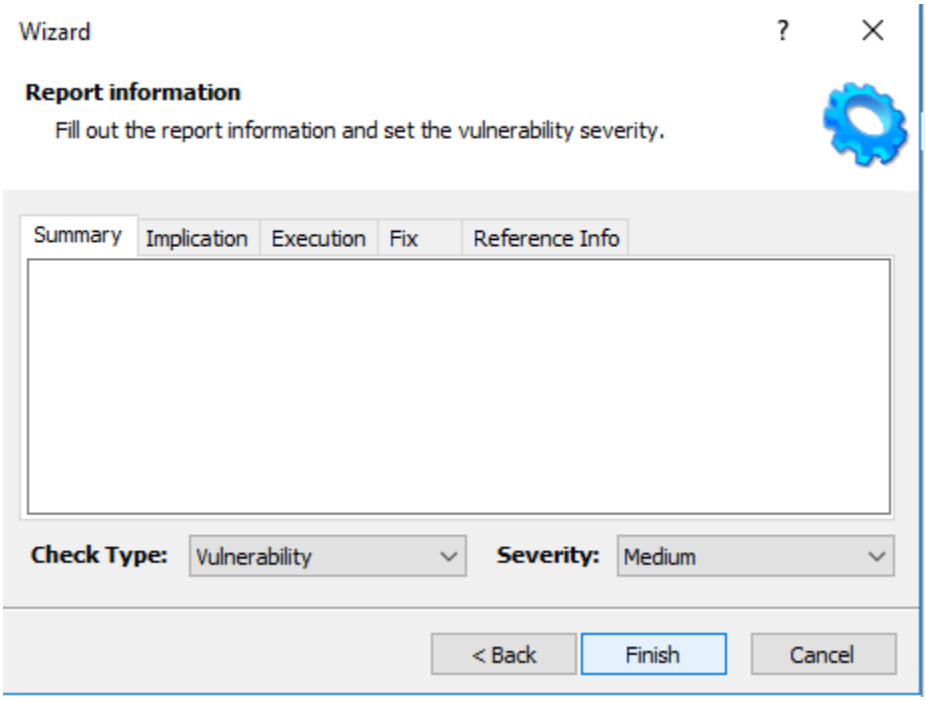
12. So, in our example, we type /login/ for directory enumeration, thus, the check will search for a directory named "admin" by appending the attack string (/admin/) to the target URL or IP address.
13. On Signature, you must specify a signature for the check, which is simply a regular expression. When WebInspect searches for HTTP response and find the text described by the signature, it will flag the session as vulnerability. Our example will check for Status Code 200.



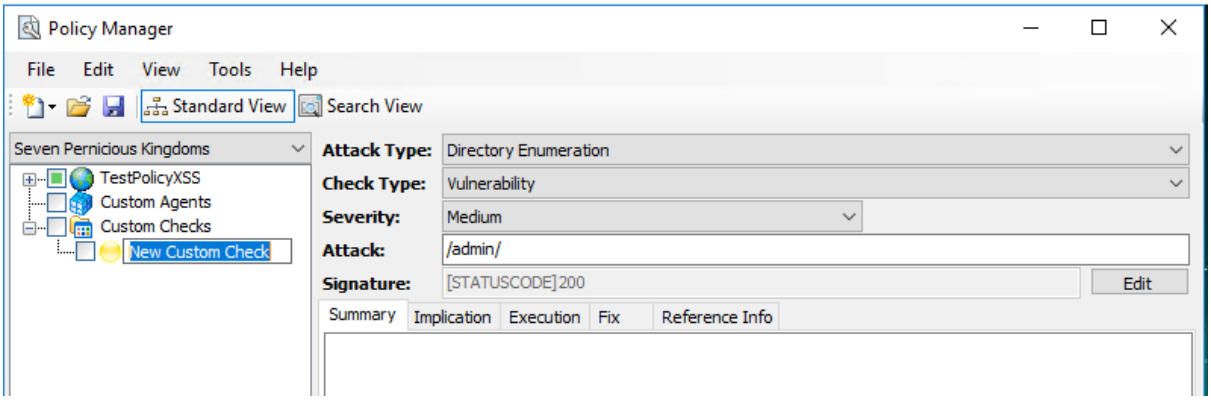
14. On Report information panel, click each tab and enter the text that will appear in the description.
    a. Select an entry form Check Type list.

b. Select a severity level from Severity list.

15. Cick on Finish. Then change the default name “New Custom Check” to reflect the purpose of the check.



Then



With these steps we can create a custom check for a specific vulnerability.