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.
- 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.

	▲
Noticy Manager	Aggressive SQL Injection Policy
File Edit View Tools H	All Checks Policy
🎦 New 🕨	Apache Struts Policy
New Custom Check	Application (Deprecated) Policy
🚰 Open	Assault (Deprecated) Policy
M Import	Blank Policy
· · · · · · · · · · · · · · · · · · ·	Client-side Policy
🚽 Save	Criticals and Highs Policy
Save As	Cross-Site Scripting Policy
Exit Alt+F4	Deprecated Checks Policy

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:

截 Policy Manager	
File Edit View Tools Help	•
🎦 🚽 📑 📕 🚠 Standard View 🔯	Search View
Seven Pernicious Kingdoms ~	Name: Custom Checks Comments:
Custom Agents	
New Custom C	heck
	Custom Checks
	Name ID Severity Last Updated
Wizard	? ×
Attack Type Select a type of attack to create.	
 Directory Enumeration File Extension Addition File Extension Replacement Keyword Search Parameter Injection Simple Attack Site Search 	Description Simple Attacks are attacks that are sent once for every server scanned.
	< Back Next > Cancel

- 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.

Wizard					?	\times
Signature Input the attack data to send.						
Attack - Ex. /admin/ /admin/ Signature Search for:	in	Resp	onse	~	Insert	×
[< Ba	ick	Next >	>	Ca	incel

- 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.

Wizard ? X	
Signature Input the attack data to send.	\$
Attack - Ex. /admin/	
Signature Search for: in Response v v Insert	
[STATUSCODE]200	
< Back Next > Cancel	

- 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.

_	_								
Report inf Fill out t	formation he report info	ormation and s	set the	vulnerability sever	ity.				
Summary	Implication	Execution	Fix	Reference Info					
Chock Tw	DOI Mulman	- Little -		Couosita I	A second to second				
Check Ty	pe: Vulnera	ability	~	Severity:	1edium		~		
Check Ty	pe: Vulner	ability		Severity:	1edium Finish	Car	~ icel		
Eheck Typ en	pe: Vulnera	ability		< Back	1edium Finish	Car	~		
Check Type en } Policy Man	pe: Vulnera	ability		< Back	1edium Finish	Car	rcel		:
Eheck Type en) Policy Man ile Edit	pe: Vulnera	Help		< Back	4edium ≓inish	Car	cel		
en) Policy Man ile Edit) T 🔐 🛃	pe: Vulnera nager View Tools ਿਜ਼ੋਰ Standard V	Help	/iew	< Back	1edium Finish	Car	cel		
en Policy Man ile Edit Prei I	pe: Vulnera nager View Tools :로그 Standard V s Kingdoms	Help Tiew 🖾 Search V	/iew Fype:	< Back Firectory Enumeration	¶edium ≂inish	Car	ncel	_	
en Policy Man ile Edit Ven Pernicious	pe: Vulnera nager View Tools standard V s Kingdoms PolicyXSS pm Agents	Help iew 🖾 Search V ✓ Attack T Check T	/iew Type: U	Severity:	1edium Finish	Car	cel		
en Policy Man ile Edit Ven Pernicious	pe: Vulnera nager View Tools 도급 Standard V s Kingdoms PolicyXSS com Agents com Agents	Help Tiew 🖾 Search V V Attack 1 Check Tr Severity	√iew Type: □ ype: ↓ y: ►	Severity:	1edium Finish	Car	v Incel		
en Policy Man ile Edit ✓ ☞ ☞ 및 ven Pernicious ····································	pe: Vulnera nager View Tools I Standard V s Kingdoms PolicyXSS som Agents som Checks New Custom Check	Help iew 🖾 Search V V Attack T Severity Attack:	View Type: D ype: V y: M	Severity:	finish	Car			
en Policy Man ile Edit Ven Pernicious Image Custr Image Custr Image Custr Image Custr Image Custr Image Custr	pe: Vulner; hager View Tools (류코 Standard V s Kingdoms PolicyXSS com Agents com Checks New Custom Check	Help Tiew 🖾 Search V Attack T Severity Attack: Signature	/iew Fype: D ype: V y: M fre: D	Severity:	fedium Finish	Car	× cel		

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