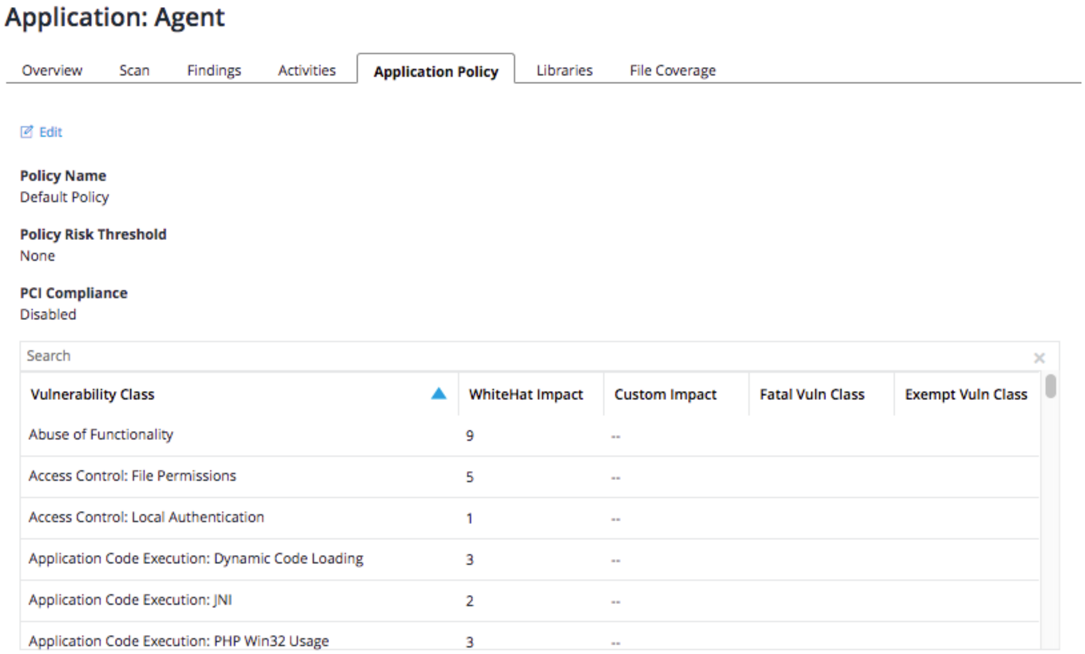
Adding or Editing an Application Policy

Application policies determine what sorts of vulnerabilities at what levels of severity will cause an application to fail its scan.

From the Application Overview page, select the Application Policy sub-tab.

This will bring up the Application Policy screen.



Application: Agent

Policy Name
Default Policy

Policy Risk Threshold
None

PCI Compliance
Disabled

Vulnerability Class	WhiteHat Impact	Custom Impact	Fatal Vuln Class	Exempt Vuln Class
Abuse of Functionality	9	--		
Access Control: File Permissions	5	--		
Access Control: Local Authentication	1	--		
Application Code Execution: Dynamic Code Loading	3	--		
Application Code Execution: JNI	2	--		
Application Code Execution: PHP Win32 Usage	3	--		

As you can see, from this screen you can create a new policy or edit an existing policy.

Editing a Policy

To edit a policy, choose "Edit." From here you can change the policy name, risk threshold, or mandatory PCI compliance (enabled or disabled), or set a custom impact for any listed vulnerability class. When you are done, click "Apply" to apply the policy to this asset, and then click "Save."

Adding a Policy

To add a policy, click on "New Policy." You will be asked to assign a name to your policy, set the risk threshold, and if desired to set a custom impact for a given vulnerability class or classes.

Once you have made those selections, you must choose "Apply" to apply this policy to this application, and "Save" to save the policy.

PCI Compliance

If you choose, you may enable PCI Compliance for a policy; if you do this, then any vulnerability that would cause the application to fail PCI compliance will cause the assessment to note a failure for that vulnerability.

Risk Threshold

The risk threshold at which vulnerabilities will fail the application must be set to none, critical, high, medium, low, or note. (see OWASP for more information on these levels.) The risk threshold is set accross the policy as a whole.

Custom Impact

For each vulnerability class, you may set a custom impact, declare that the vulnerability class is fatal (that is, the application must fail if this vulnerability class is present), or exempt the vulnerability class (that is, the application will not fail regardless of the presence of this class of vulnerability. Note that if you set a policy to "PCI Compliant," you will not be able to exempt any vulnerability class that is included in the PCI requirements.

For information on additional approaches to customizing your vulnerability ratings, please see Customizing Your Vulnerability Results.