HNG: Attack Surface Explorer Use Cases

Contents

[Style Guide 3](#_Toc199089815)

[Solution Management 3](#_Toc199089816)

[ASE Project 3](#_Toc199089817)

[Attack Profiles 3](#_Toc199089818)

[Snapshots 3](#_Toc199089819)

[Checklists 4](#_Toc199089820)

[Attack Surface 4](#_Toc199089821)

[Discovering 4](#_Toc199089822)

[Browsing 4](#_Toc199089823)

[Testing 5](#_Toc199089824)

[Qualifying Resources 5](#_Toc199089825)

[Managing VS Tasks 5](#_Toc199089826)

[Managing TFS Work Items 5](#_Toc199089827)

[Reporting & Dashboard 6](#_Toc199089828)

[Getting guidance 6](#_Toc199089829)

[TeamMentor 6](#_Toc199089830)

[Attack Surface Library 7](#_Toc199089831)

[ASE SDK 7](#_Toc199089832)

[Licensing and Product Support 8](#_Toc199089833)

[Installation 8](#_Toc199089834)

[Product Trial and Registration 8](#_Toc199089835)

[Getting Product Updates and News 8](#_Toc199089836)

[Getting Support 8](#_Toc199089837)

[Definitions 8](#_Toc199089838)

# Style Guide

* Text: Is used for indicating a Persona. Personas are defined separately in the Personas document.
* *Text*: Italicized words or phrases are used for product specific terms. These terms should be defined in the Glossary section of this document.
* Text: Grayed text indicates that the topic is being considered for expulsion.

# Solution Management

### ASE Project

* ASE User selects from ASE Profile types in the VS New Project Wizard to use with their application
* ASE User creates a new VS solution using selected ASE Profile Type
* ASE User adds new ASE Profile to existing *ASE Project*
* ASE User adds existing *ASE Profile* to existing *ASE Project*
* ASE User specifies an executable binary as Test Application in the New Profile Wizard.
* ASE User selects a Visual Studio Project from the current VS Solution as the Test Application in the New Profile Wizard.
* ASE User specifies a binary image or process ID which ASE should attach to in the New Profile Wizard.
* ASE User provides details about the *Test Application* using the New Profile Wizard
* ASE User provides details about remote machines and the remote agents are activated automatically
* ASE User views/changes *ASE Project* settings
* ASE User views/changes *ASE Profile* settings
* ASE User removes *ASE Profile* from *ASE Project*
* ASE User removes *ASE Project* from VS solution

### Attack Profiles

* Engineer creates new Attack Profile in ASE Project to discover the attack surface of the Test Application
* ASE User adds existing Attack Profile in ASE Project
* ASE User removes Attack Profile from ASE Project
* ASE User merges one or more Attack Profiles in order to get a cumulative idea about the attack surface of the components or features in question.

### Snapshots

* ASE User saves existing Attack Profile as a Snapshot to save the current attack surface data for future analysis and comparison.
* ASE User exports Snapshot to specified disk location to export the current attack surface data for sharing with other users via external means such as email.
* ASE User imports Snapshot into ASE Profile.

### Checklists

* RM answers questions in the Product Risk Assessment Checklist to attest that the Test Application meets common security principles.
* RM updates questions in the Product Risk Assessment Checklist to add to the list of security principles that the Test Application needs to adhere to.
* RM views related *TeamMentor* content for a specific question in the *Checklist* to better understand the reasons behind the question.
* RM exports *Product Risk Assessment Checklist* to specified disk location in selected format for sharing with other users via externals means such as email.
* RM imports *Product Risk Assessment Checklist* from specified disk location and overwrites existing *Checklist*.

# Attack Surface

### Discovering

* Engineer sets one ASE Profile as the Active profile, which will collect discovered information when the Test Application is launched.
* Engineer turns Discovery ON by toggling the Discovery button from the ASE Toolbar and launches the Test Application by pressing F5 in VS.
* Engineer launches a local *Test Application* from a specific *Attack Profile* in order to discover its attack surface.
* Engineer launches a remote *Test Application* from a specific *Attack Profile by utilizing the ASE Agent* in order to discover its attack surface.
* Engineer manually launches local *Test Application* and starts discovery by attaching an *Attack Profile*
* Engineer manually launches remote *Test Application* and starts discovery by attaching an *Attack Profile* via an *ASE Agent.*
* Engineer pauses\resumes discovery of attack surface from *Attack Profile* in order to control what features should be excluded from discovery.

### Browsing

* ASE User views Attack Surface using the *Attack Tree View*
* ASE User views Attack Surface using the *Attack Map View*
* ASE User controls the visibility of resources by applying pre-set or new filters which hide or show information based on resource characteristics.
* ASE User searches for matching resources in the Attack Surface views by using a search box.
* ASE User selects items in the Attack Tree or Attack Map and views\updates their properties in the Properties Pane

### Testing

* ~~Engineer views applicable tests for selected resource in the Resource Popup View~~
* ~~Engineer views code sample associated with each applicable test which can be plugged into the Test Application code to create and remove Testpoints from within the Test Application.~~
* ~~Engineer creates a new Testpoint by selecting from a list of applicable tests presented in the Resource Popup View to see if that resource is vulnerable.~~
* ~~Engineer views list of Testpoints in Testpoints pane (similar to Breakpoints pane in VS) to get an overview of all the tests that exist in the current Attack Profile.~~
* ~~Engineer disables a Testpoint from the Testpoints pane~~
* ~~Engineer deletes a Testpoint from the Testpoints pane~~
* ~~Engineer creates notes for selected resource to save and share observed test results with other team members.~~
* ~~Tester views application crash dump and associates it with selected resources in order to set context for the Developer.~~
* ~~Developer views crash dump and analyzes problem in order to fix the reported problem.~~

### Ranking Resources

* ASE User chooses to completely *ignore* a specific resource in order to exclude it from analysis and decongest the views from unrelated resources.
* ASE User updates *Damage magnitude* for a specific resource
* ASE User updates *Exploitability magnitude* for a specific resource
* ASE User updates notes for a specific resource in order to communicate their opinion about the resource with other team members.

### Managing VS Tasks

* ASE User views Tasks associated with a specific resource to get an overview of the work required to be done.
* ASE User creates a Task for a specific resource
* ASE User modifies an existing Task for a specific resource
* ASE User deletes Task(s) for a specific resource

Managing TFS Work Items [only with TFS]

* ASE User views TFS Work Items associated with a specific resource
* ASE User creates TFS Work Item for a specific resource
* ASE User modifies existing TFS Work Item for a specific resource
* ASE User deletes TFS Work Item(s) for a specific resource
* ASE User creates a work-item from a warning thrown by ASE

### Reporting & Dashboard

* Engineer creates a *Live Report* from an existing Attack Profile to analyze the current state of the *Test Application*.
* RM creates a *Static Report* from an existing Attack Profile to analyze the state of the *Test Application*.
* RM creates a *Static Report* from an existing Snapshot to analyze a past state of the Test Application.
* RM creates a comparative *Static Report* for two or more Attack Profiles and/or Snapshots to compare between two or more states of the Test Application.
* ASE User exports a *Live Report* or *Static Report* to specified disk location in one of the Report Format Choices for sharing with other users via external means such as email.
* ASE User imports report from specified disk location to ASE Project.
* RM pushes an Attack Profile (which is converted to a snapshot) or a saved Snapshot to the *Dashboard* for comparison.
* RM selects from different views in the *Dashboard* to view product progress between different snapshots.

# Getting guidance

### TeamMentor

* ASE User without TM subscription receives free TM updates for 90 days from the day the license is activated.
* ASE User finds TM content helpful and decides to subscribe to TM at the end of the 90 day trial period.
* ASE User with TM subscription views latest TeamMentor content related to a resource via the *Resource Popup View* to learn about best practices for that type of resource.
* ASE User who did not subscribe to TM at the end of the 90 day trial, continues to view the last version of the article that was cached locally.
* ASE User views the Attack Surface Library checks associated with a TeamMentor item.

### **Attack Surface Library**

* ASE User views the *Attack Surface Library* checks that were performed on the selected resource and the result of those checks via the *Resource Popup View*.
* ASE User views the warnings set by the *Attack Surface Library* due to failed checks via the *Warnings Pane*.
* ASE User chooses to always ignore a certain warning and enters a reason for ignoring that warning.
* ASE User adds a custom note associated with a certain warning for that attack profile.
* ASE User views the complete list of checks for their Test Application via a page which is displayed after the user double-clicks on the *Attack Surface Library* node under the Attack Profile node in the solution explorer.
* ASE User adds/edits/enables/disables checks on a Attack Profile via a page which is displayed after the user double-clicks on the *Attack Surface Library* node under the Attack Profile in the solution explorer.
* ASE User exports a single or multiple customized checks into an XML file so that it can be imported into other projects and solutions by others.
* ASE User goes from check to (local or TM) guidance associated with the check.

# ASE SDK

* Developer starts discovery from within the *Test Application* by making calls to ASE SDK and associating a new or existing profile to use for saving the discovery information.
* Developer pauses\resumes\stops discovery from within the *Test Application* by making calls to ASE SDK.
* Tester starts discovery from a *Test Harness* by making calls to ASE SDK and associating a new or existing profile and Test Application for discovering and saving information.
* Tester pauses\resumes\stops discovery from a *Test Harness* by making calls to ASE SDK.
* Builder starts discovery from a *BVT Harness* by making calls to ASE SDK and associating a new or existing profile and Test Application for discovering and saving information.
* Builder pauses\resumes\stops discovery from a *BVT Harness* by making calls to ASE SDK in order to skip discovery of certain parts of the Test Application.
* Builder generates a static report of the Attack Profile being discovered from a *BVT Harness* by making calls to ASE SDK.
* Builder generates a snapshot of the Attack Profile being discovered from a *BVT Harness* by making calls to the ASE SDK.
* Builder pushes an Attack Profile or Snapshot to an existing Dashboard from a *BVT Harness* by making calls to the ASE SDK.

# Licensing and Product Support

### Installation

* ASE User installs product on a Windows machine with Visual Studio version 2005 or earlier
* ASE User installs product on a Windows machine with Visual Studio version 2008
* ASE User installs product on a Windows machine with Visual Studio version 2005 or earlier and Visual Studio 2008
* ASE User installs product on a Windows machine with no Visual Studio versions

### Product Trial and Registration

* ASE User runs ASE in trial mode to evaluate the product
* ASE User enters registration information to disable the time-trial limitation
* ASE User de-registers product from terminal so that the license can be used on another terminal.

### Getting Product Updates and News

* ASE User checks for available product updates
* ASE User views details of available product updates
* ASE User downloads and installs specific or all available product updates
* ASE User subscribes for product news in email
* ASE User choose to unsubscribe from receiving product news in email

### Getting Support

* ASE User sends email to support staff to report a problem
* ASE User views support information to phone support staff to report a problem or get assistance with using the product
* ASE User visits support forum on the web to check for solutions to problems, discuss features, and download plugins.

# Definitions

ASE Agent – A component that can be run on a remote machine for attack surface discovery of remote applications.

Application Questionnaire Wizard – This wizard will appear once the user starts creating an ASE Project. The wizard will collect application information by asking the user specific questions. Information bits will include but will not be limited to ASE Profile Type, application name, path, command line parameters, deployment scenario etc. Information collected in this Wizard will be viewable and editable via the VS Project Properties view and Profile Properties.

ASE Profile types – When creating a new ASE Project, users will be able to select a specific profile type depending on the type of application they are testing. This will help us create Checklists and also organize views best suited for that type of application. Some example Profile Types are: Standalone Windows Application, Client Application, Server Application and Windows Services.

ASE Project – Is a VS Project type which contains one or more than one of the following artifacts Attack Profiles, Dashboards, Reports.

Attack Profile – Is a node in the ASE Project and contains one Attack Tree, one Attack Map, one Product Assessment Checklist and one or more Snapshots.

Attack Surface Library – This is HNG’s database of known security issues associated with specific resource types and the way they are used. It is essentially a database of checks that are performed on the Test Application. The users of ASE will be able to add their own checks to this database and will also be able to share custom checks with other users and the online community via XML files.

Report Format Choices – When saving reports to disk, the user will be given a choice of file format. File format being current considered are HTML, DOC and XML.

Resource Popup View *–* This view will be an enlarged popup (?) which will help the user interact with that resource, set tests on it and view related guidance.