HNG: Attack Surface Explorer Requirements List

This document has been retired and will no longer be maintained.

please look at requirements in tfs

|  |  |  |
| --- | --- | --- |
| User Requirements | | links |
| **UR001** | ASE should not fail to identify any security related resources that are used by the Test Application | [TK003](#_TK003) |
| **UR002** | ASE should identify only those resources that are directly used by the Test Application |  |
| **UR002.1** | ASE should not identify those resources that are accessed indirectly by the OS | [TK005](#_TK005) |
| **UR003** | ASE should assist the user in understanding the security implications of identified resources |  |
| **UR003.1** | ASE will ship with a base set of TeamMentor guidance |  |
| **UR004** | ASE should automatically identify potentially dangerous behavior |  |
| **UR004.1** | ASE will ship with a base set of ASL checks |  |
| **UR005** | Users should be able to create custom rules for identifying potential security problems |  |
| **UR005.1** | ASL checks should be customizable |  |
| **UR006** | Users should be capable of sharing custom rules between projects and teams |  |
| **UR006.1** | ASL checks should be importable\exportable |  |
| **UR007** | Users should be able to discover attack surfaces of both local and remote applications and services |  |
| **UR008** | Users should be able to take snapshots of the Test Application’s attack surface so that the progress of an application and be tracked and compared |  |
| **UR009** | Each identified resource should be marked with a threat level (vulnerability prioritization) so that it can be investigated | [BS011](#_BS011) |
| **UR009.1** | ASE should try to automatically mark the threat level of identified resources | [TK004](#_TK004) |
| **UR009.2** | Users should be able to manually mark and override the threat level of resources |  |
| **UR010** | Users should be able to view the attack surface of the Test Application over a period of time in a central dashboard |  |
| **UR011** | ASE should provide reporting features with multiple views to and customizable levels of detail |  |
| **UR011.1** | Reports should be exportable in formats such as HTML and Serialized XML |  |
| **UR012** | ASE should be capable of mapping the attack surface of more than one application/service simultaneously |  |
| **UR013** | ASE should inform the user about best practices via a checklist that the user can follow |  |
| **UR014** | ASE should enable users to share notes about identified resources |  |
| **UR015** | ASE should integrate with the user’s bug reporting system and enable smooth work item creation |  |
| **UR016** | Users should be able to include their custom DLLs into ASE’s interception library |  |
| **UR017** | ASE should provide helpful documentation on all its features |  |
| **UR018** | ASE should provide free written or video demonstrations of how to use the product |  |
| **UR019** | ASE should explain each calculated metric in order to explain to the user what the numbers mean |  |

|  |  |  |
| --- | --- | --- |
| Business Requirements | | links |
| **BS001** | Licensing enforcement need not be draconian but license keys should be centrally tracked and strict install counts not immediately enforced unless the copies exceeds a reasonable number or that encoded in the key itself. |  |
| **BS002** | License keys should bind to a specific machine using CPU serial# / MAC Address or a similar common attribute |  |
| **BS003** | License keys should be version aware |  |
| **BS004** | ASE should provide a try and buy model where a user can evaluate the product free of charge for 15 days |  |
| **BS005** | Registered product can be unregistered if the user desires OR un-installation of product should remove stored licensing information |  |
| **BS006** | ASE should have a built in bug reporting system |  |
| **BS006.1** | Users should be able to report bugs manually by following a link from the ASE shell |  |
| **BS006.2** | Upon an internal failure, ASE should offer the user an option to send an automated error report to the company |  |
| **BS007** | ASE should have an online community where users can share plugins and discuss the product |  |
| **BS008** | ASE should integrate with VS2005+ if it is installed on the user’s computer |  |
| **BS008.1** | ASE should install as a standalone VS Shell if the user does not have VS2005 or above installed on their computer |  |
| **BS009** | Users should be able to email HNG support and receive a response within 24 hours. |  |
| **BS010** | Users who purchase support should be able to call HNG support and if a technical response is required it should take no longer than 24 hours. |  |
| **BS011** | ASE should use industry accepted terminology and scales for vulnerability prioritization | [UR009](#_UR009) |
|  |  |  |

|  |  |  |
| --- | --- | --- |
| Technical Requirements | | links |
| **TK001** | ASE should support 32-bit and 64-bit versions of the following OS’s and all their service packs - Windows 2000, Windows XP, Windows Vista, Win2K3, Windows Server 2008 |  |
| **TK002** | ASE should support all versions of the .NET Framework |  |
| **TK002.1** | ASE will ship with support for .NET Framework version 3.5 |  |
| **TK002.2** | ASE updates should be available for download within 3 weeks of a new .NET Framework release |  |
| **TK003** | Discovery should use *entry-point and exit-point methodology* to determine whether a resource will have a security impact or not. | [UR001](#_UR001) |
| **TK004** | Discovery should use *the damage potential - effort ratio* methodology to automatically assign default threat levels to resources | [UR009.1](#_UR009.1) |
| **TK005** | ASE will use the HEAT-NG engine with the re-entrance option turned OFF in order to discover only those resources which are accessed directly by the Test Application | [UR002.1](#_UR002.1) |
|  |  |  |

|  |  |  |
| --- | --- | --- |
| Standards Requirements | | links |
| **ST001** | ASE should secure all remote communication with the Agent using strong encryption |  |
| **ST002** | ASE should secure all automatic product updates and downloads using digital signatures |  |
| **ST003** | ASE should use industry-wide security terminology as much as possible throughout the product and its documentation |  |
| **ST004** | ASE should warn users about the possible security implications of importing and installing ASE plugins from the ASE community or another location on the internet. |  |
|  |  |  |