|  |  |  |  |
| --- | --- | --- | --- |
| **Issue** | Exposure of System Data to an Unauthorized Control Sphere | | |
| **Category** | Error Handling | | |
| **Weakness** | Exposing system data or debugging information helps an adversary learn about the system and form an attack plan | | |
| **Source** | **Line number** | **Description** | **Risk** |
| Verbat.AbbPricingTool.Authenrizeuser | *170,173* | The error messages generated on lines 170 and 173 contain stacktraces. If these are sent back to the user, they could provide an attacker with valuable information about the underlying system. Stacktraces should be reserved for a log and kept out of error messages that are sent back to the user. | *Low* |

|  |  |  |  |
| --- | --- | --- | --- |
| **Issue** | Missing Authentication for Critical Function | | |
| **Category** | Authorization | | |
| **Weakness** | The software does not perform any authentication for functionality that requires a provable user identity or consumes a significant amount of resources. | | |
| **Source** | **Line number** | **Description** | **Risk** |
| N/A | N/A | The application allows anyone to make a request for consolidated contact information related to a given employee ID. It is understood that this is the current choice of the design team; however this issue should be addressed if the application is ever used in a more open environment where not everyone that could make a request should have access to the contact information | Low |

|  |  |  |  |
| --- | --- | --- | --- |
| **Issue** | Improper Input Validation | | |
| **Category** | Data Validation | | |
| **Weakness** | The product does not validate or incorrectly validates input that can affect the control flow or data flow of a program. When software does not validate input properly, an attacker is able to craft the input in a form that is not expected by the rest of the application. This will lead to parts of the system receiving unintended input, which may result in altered control flow, arbitrary control of a resource, or arbitrary code execution | | |
| **Source** | **Line number** | **Description** | **Risk** |
| Verbat.AbbPricintTool.aggregator.validate | *294* | The userid that is obtained from the request string is never validated. Although this doesn't appear to be harmful in its current use, it is still advisable to perform some amount of rudimentary validation on the input. Data validation is the easiest way to prevent most security issues from occurring. | Low |

|  |  |  |  |
| --- | --- | --- | --- |
| **Issue** | Boxing/unboxing should be avoided | | |
| **Category** | Casting | | |
| **Weakness** |  | | |
| **Source** | **Line number** | **Description** | **Risk** |
| Verbat.AbbPricingTool.Logging.Logger.Log;  Verbat.AbbPricingTool.Common |  | Avoid boxing and unboxing operations instead use generics | Low |

|  |  |  |  |
| --- | --- | --- | --- |
| **Issue** | Non-static classes should be instantiated or turned to static | | |
| **Category** |  | | |
| **Weakness** | 23 matches | | |
| **Source** | **Line number** | **Description** | **Risk** |
| Verbat.AbbPricingTool.Common.MailSender |  | First it is important to investigate why the class is never instantiated. If the reason is \*the class hosts only static methods\* then the class can be safely declared as \*static\*. | Low |
| **Issue** | Avoid empty interfaces | | |
| **Category** |  | | |
| **Weakness** | The interface does not declare any members or implement two or more other interfaces. | | |
| **Source** | **Line number** | **Description** | **Risk** |
| Verbat.AbbPricingTool.DataAccess .IMotorRepository |  | If your design includes empty interfaces that types are expected to implement, you are probably using an interface as a marker or a way to identify a group of types. If this identification will occur at run time, the correct way to accomplish this is to use a custom attribute. Use the presence or absence of the attribute, or the properties of the attribute, to identify the target types. If the identification must occur at compile time, then it is acceptable to use an empty interface. | Low |

|  |  |  |  |
| --- | --- | --- | --- |
| **Issue** | Do not hide base class methods | | |
| **Category** | Abstraction | | |
| **Weakness** |  | | |
| **Source** | **Line number** | **Description** | **Risk** |
| Verbat.AbbPricingTool.DataAccess | 345 | get\_CorporateName(); Set\_CorporateName(String)   Remove or rename the method, or change the parameter signature so that the method does not hide the base method. | Major |