Finding ID	Severity	Title	Description	Justification
V-222400	High	Validity periods must be verified on all application messages using WS-Security or SAML assertions.	When using WS-Security in SOAP messages, the application should check the validity of the time stamps with creation and expiration times. Time stamps that are not validated may lead to a replay...	Time stamps are used to sort, validity is determined by the whitelist. This is for quick catagorization and keeping alerts lightweight.
V-222404	High	The application must use both the NotBefore and NotOnOrAfter elements or OneTimeUse element when using the Conditions element in a SAML assertion.	SAML is a standard for exchanging authentication and authorization data between security domains. SAML uses security tokens containing assertions to pass information about a principal (usually an...	No forced authentification
V-222612	High	The application must not be vulnerable to overflow attacks.	A buffer overflow occurs when a program exceeds the amount of data allocated to a buffer. The buffer is a sequential section of memory and when the data is written outside the memory bounds, the...	Resets alert list every two minutes, but no formal limit. This is to prevent overflow over some time.
V-222578	High	The application must destroy the session ID value and/or cookie on logoff or browser close.	Many web development frameworks such as PHP, .NET, and ASP include their own mechanisms for session management. Whenever possible it is recommended to utilize the provided session management...	No system authentication.

V-222430	High	The application must execute without excessive account permissions.	Applications are often designed to utilize a user account. The account represents a means to control application permissions and access to OS resources, application resources or both. When the...	No authentication is required to utilize the program.
V-222432	High	The application must enforce the limit of three consecutive invalid logon attempts by a user during a 15 minute time period.	By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute forcing, is reduced. Limits are imposed by locking the...	No system authentication.
V-222577	High	The application must not expose session IDs.	Authenticity protection provides protection against man-in-the-middle attacks/session hijacking and the insertion of false information into sessions. Application communication sessions are...	No system authentication.
V-222609	High	The application must not be subject to input handling vulnerabilities.	A common application vulnerability is unpredictable behavior due to improper input validation. This requirement guards against adverse or unintended system behavior caused by invalid inputs, where...	Imputs are limited to certain choices, including buttons and prompts. This limits the unintended or improper behavior during use.

V-222608	High	The application must not be vulnerable to XML-oriented attacks.	Extensible Markup Language (XML) is widely employed in web technology and applications like web services (SOAP, REST, and WSDL) and is also used for configuration files. XML vulnerability examples...	Application is not subjected to XML injection as all database transit is done only from PCAP file network traffic to the SQL database
V-222602	High	The application must protect from Cross-Site Scripting (XSS) vulnerabilities.	XSS attacks are essentially code injection attacks against the various language interpreters contained within the browser. XSS can be executed via HTML, JavaScript, VBScript, ActiveX; essentially...	Application is protected from XSS as it runs from a local host
V-222601	High	The application must not store sensitive information in hidden fields.	Hidden fields allow developers to process application data without having to display it on the screen. Using hidden fields to pass data in forms is a common practice among web applications and by...	Application does not store any information in hidden fields
V-222607	High	The application must not be vulnerable to SQL Injection.	SQL Injection is a code injection attack against database applications. Malicious SQL statements are inserted into an application data entry field where they are submitted to the database and...	SQL information is stored directly from PCAP files and transited to database

V-222604	High	The application must protect from command injection.	A command injection attack is an attack on a vulnerable application where improperly validated input is passed to a command shell setup in the application. The result is the ability of an attacker...	Application is not run from user commands
V-222403	High	The application must use the NotOnOrAfter condition when using the SubjectConfirmation element in a SAML assertion.	SAML is a standard for exchanging authentication and authorization data between security domains. SAML uses security tokens containing assertions to pass information about a principal (usually an...	Not applicable
V-222585	High	The application must fail to a secure state if system initialization fails, shutdown fails, or aborts fail.	Failure to a known safe state helps prevent systems from failing to a state that may cause loss of data or unauthorized access to system resources. Applications or systems that fail suddenly and...	Not applicable
V-222550	High	The application, when utilizing PKI-based authentication, must validate certificates by constructing a certification path (which includes status information) to an accepted trust anchor.	Without path validation, an informed trust decision by the relying party cannot be made when presented with any certificate not already explicitly trusted. A trust anchor is an authoritative...	No forced authorization of system

V-222522	High	The application must uniquely identify and authenticate organizational users (or processes acting on behalf of organizational users).	To assure accountability and prevent unauthenticated access, organizational users must be identified and authenticated to prevent potential misuse and compromise of the system. Organizational...	No system authentication in use.
V-222554	High	The application must not display passwords/PINs as clear text.	To prevent the compromise of authentication information such as passwords during the authentication process, the feedback from the information system must not provide any information that would...	No use of password for application
V-222596	High	The application must protect the confidentiality and integrity of transmitted information.	Without protection of the transmitted information, confidentiality and integrity may be compromised since unprotected communications can be intercepted and either read or altered. This...	Alert encryption is implemented in transit (sending/receiving).
V-222399	High	Messages protected with WS_Security must use time stamps with creation and expiration times.	The lack of time stamps could lead to the eventual replay of the message, leaving the application susceptible to replay events which may result in an immediate loss of confidentiality.	Not applicable

V-222658	High	All products must be supported by the vendor or the development team.	Unsupported commercial and government developed software products should not be used because fixes to newly identified bugs will not be implemented by the vendor or development team. The lack of...	Application is supported on open source product
V-222659	High	The application must be decommissioned when maintenance or support is no longer available.	Unsupported software products should not be used because fixes to newly identified bugs will not be implemented by the vendor or development team. The lack of security updates can result in...	Application will undergo decommision when maintenance is no longer available
V-222551	High	The application, when using PKI-based authentication, must enforce authorized access to the corresponding private key.	If the private key is discovered, an attacker can use the key to authenticate as an authorized user and gain access to the network infrastructure. The cornerstone of the PKI is the private key...	No forced authorization of system
V-222620	High	Application web servers must be on a separate network segment from the application and database servers if it is a tiered application operating in the DoD DMZ.	A tiered application usually consists of 3 tiers, the web layer (presentation tier), the application layer (application logic tier), and the database layer (data storage tier). Using one system...	Application is seperate from database and runs on local host

V-222536	High	The application must enforce a minimum 15-character password length.	The shorter the password, the lower the number of possible combinations that need to be tested before the password is compromised. Use of passwords for application authentication is intended only...	No use of password for application
V-222643	High	The application must have the capability to mark sensitive/classified output when required.	Failure to properly mark output could result in a disclosure of sensitive or classified data which is an immediate loss in confidentiality.	Application does mark highest threat level of intrusion
V-222542	High	The application must only store cryptographic representations of passwords.	Use of passwords for application authentication is intended only for limited situations and should not be used as a replacement for two-factor CAC-enabled authentication. Examples of situations...	No use of password for application
V-222543	High	The application must transmit only cryptographically-protected passwords.	Use of passwords for application authentication is intended only for limited situations and should not be used as a replacement for two-factor CAC-enabled authentication. Examples of situations...	No passwords in system
V-222425	High	The application must enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., networks, web servers, and web...	No forced authorization of system

V-222642	High	The application must not contain embedded authentication data.	Authentication data stored in code could potentially be read and used by anonymous users to gain access to a backend database or application servers. This could lead to compromise of application data.	Not applicable, as this application does not contain any embedded authentication data.
V-222662	High	Default passwords must be changed.	Default passwords can easily be compromised by attackers allowing immediate access to the applications.	Yes, passwords must be changed regularly to avoid compromization.
V-222555	High	The application must use mechanisms meeting the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.	A cryptographic module is a hardware or software device or component that performs cryptographic operations securely within a physical or logical boundary, using a hardware, software or hybrid...	Yes, this ensures legal compliance, enhances security, promotes interoperability, boosts market credibility, future-proofs the application, and aids in effective risk management.