KSADS-COMP
LLC

KSADS-COMP Security

APPLICATION SECURITY

KSADS Phase II application was developed using Microsoft's ASP.NET 4.0 framework and a Microsoft SQL Server 2016 database. These technologies have proven to be extremely stable, reliable, and secure. Several aspects of the ASP.NET framework promote reliability and security of the application.

- Code stability and reusability through extensive use of fully tested program libraries (class files)
- Code encapsulation through object-oriented programming. Use of independently tested and verified code objects minimizes system-wide issues
- Separation of programming logic (code-behind classes) from page design for easier identification and resolution of issues
- A separate "Data Access" layer of code responsible for interacting with the database.
- Data is hidden and cannot be accessed by external functions

Security and privacy have been of the utmost concern in the development of the application. The application requires the combination of a username and password in order to access the material. Data security within the SQL Server database is ensured through two levels of authentication, one at the SQL Server level, and a second at the database level. The application is also designed to defend against security attacks such as SQL injection (e.g., user input are not directly be embedded in SQL statements; rather parameterized statements are used). The application is hosted on a Web server maintained by a firm that specializes in Web hosting, ensuring that all software and hardware security is current. A secured socket layer (SSL) is also be deployed which provides the following benefits.

Secured Socket Layer

The primary reason why SSL is used is to keep sensitive information sent across the Internet encrypted so that only the intended recipient can understand it. This is important because the information you send on the Internet is passed from computer to computer to get to the destination server. Any computer in between you and the server can see the information if it is not encrypted with an SSL certificate. When an SSL certificate is used, the information becomes unreadable to everyone except for the server you are sending the information to. This protects it from hackers and identity thieves.

In addition to encryption, a proper SSL certificate also provides authentication. This means you can be sure that you are sending information to the right server and not to a criminal's server. Why is this important? The nature of the Internet means that your customers will often be sending information through several computers. Any of these computers could pretend to be your website and trick your users into sending them personal information. It is only possible to avoid this by using a proper Public Key Infrastructure (PKI), and getting an SSL Certificate from a trusted SSL provider.

The SSL Protect phishing emails as well. A phishing email is an email sent by a criminal who tries to impersonate your website.

A **firewall** is also installed on the application server since any computer networks may be vulnerable to many threats along many avenues of attack, including:

- Social engineering, wherein someone tries to gain access through social means (pretending to be a legitimate system user or administrator, tricking people into revealing secrets, etc.)
- War dialing, wherein someone uses computer software and a modem to search for desktop computers equipped with modems that answer, providing a potential path into a corporate network
- Denial-of-service attacks, including all types of attacks intended to overwhelm a computer or a network in such a way that legitimate users of the computer or network cannot use it
- Protocol-based attacks, which take advantage of known (or unknown) weaknesses in network services
- Host attacks, which attack vulnerabilities in particular computer operating systems or in how the system is set up and administered
- Password guessing
- Eavesdropping of all sorts, including stealing e-mail messages, files, passwords, and other information over a network connection by listening in on the connection.

The architecture and process used to develop the application is structured to keep the application secured using the following mechanisms:-

Input validation

Every input is validated using business logics for validity and authenticity making the application secured and error free.

Authentication

Using username and passwords validations are various levels and layers.

Authorization is deciding whether a user is allowed to perform an action

Each user using the web application and the database will have specified user roles thus allowing/ denying access to resources and data according to the configured policies

Configuration management (CM) is a process for establishing and maintaining consistency of a product's performance, functional and physical attributes with its requirements, design and operational information throughout its life.

We are using Microsoft Team Foundation Server for CM.

Session Management is a server side method of managing the state of an application i.e. all the web applications' state related info are stored on server side. The benefit of having this technique is that since we are keeping all the state related information on server, the request and response becomes lightweight. Also, the chances of someone intercepting or changing this data are also reduced.

Cryptography

Cryptography is used at a various levels since it provides the following benefits

· **Confidentiality**. To ensure data remains private. Confidentiality is usually achieved using encryption. Encryption algorithms (that use encryption keys) are used to convert plain text into cipher text and the equivalent decryption algorithm is used to convert the cipher text back to plain text. Symmetric encryption algorithms use the same key for encryption and decryption, while asymmetric algorithms use a public/private key pair.

· **Data integrity**. To ensure data is protected from accidental or deliberate (malicious) modification. Integrity is usually provided by message authentication codes or hashes. A hash value is a fixed length numeric value derived from a sequence of data. Hash values are used to verify the integrity of data sent through insecure channels. The hash value of received data is compared to the hash value of the data as it was sent to determine if the data was altered.

· **Authentication**. To assure that data originates from a particular party. Digital certificates are used to provide authentication. Digital signatures are usually applied to hash values as these are significantly smaller than the source data that they represent.

Parameter Manipulation

Query string is used to the minimum and all input parameters are validated that come from form fields, query strings and HTTP headers.
Session state is used instead of View state.
Cookies are not used.

Exception Management

The application was built using state of the art technologies and the proven process methodologies to ensure that all issues are identified and closed, however any unknown bugs and issues will be handled making the site user friendly and secured using Microsoft Exception handling classes.

SERVER SECURITY

The KSADS-COMP is hosted on an Amazon Web Service (AWS) server. Cloud security at AWS is the highest priority. The infrastructure is designed to meet the requirements of the most security-sensitive organizations.

AWS Security Platform is built on:

- Infrastructure Security
- DDoS Mitigation
- Data Encryption
- Inventory and Configuration
- Monitoring and Logging
- Identity and Access Control
- Penetration Testing

With regards to Server Level security (infrastructure and encryption):
Infrastructure Security:

AWS provides several security capabilities and services to increase privacy and control network access. These include:

- Network firewalls built into Amazon VPC, and web application firewall capabilities in AWS WAF let you create private networks, and control access to your instances and applications
- Customer-controlled encryption in transit with TLS across all services
- Connectivity options that enable private, or dedicated, connections from your office or on-premises environment
- Automatic encryption of all traffic on the AWS global and regional networks between AWS secured facilities

Data Encryption:

AWS offers the ability to add an additional layer of security to your data at rest in the cloud, providing scalable and efficient encryption features. This includes:

- Data encryption capabilities available in AWS storage and database services, such as EBS, S3, Glacier, Oracle RDS, SQL Server RDS, and Redshift
- Flexible key management options, including AWS Key Management Service, allowing you to choose whether to have AWS manage the encryption keys or enable you to keep complete control over your keys
- Encrypted message queues for the transmission of sensitive data using server-side encryption (SSE) for Amazon SQS
- Dedicated, hardware-based cryptographic key storage using AWS CloudHSM, allowing you to satisfy compliance requirements

All data flowing across the AWS global network that interconnects AWS datacenters and regions is automatically encrypted at the physical layer before it leaves our secured facilities. Additional encryption layers exist as well; for example, all VPC cross-region peering traffic, and customer or service-to-service TLS connections.

In addition, AWS provides APIs to integrate encryption and data protection with any of the services developed or deployed in an AWS environment.

For more information on the other AWS Security Platform security measures please visit this link: https://aws.amazon.com/security/