KSADS-COMP

Application Security

Feb 2022

Contents

KSADS-COMP Process

Securing Applications – At Every Stage

Security should be embedded in every phase of application development to provide protection in its true sense. To accomplish this, we need to understand the complete lifecycle of application development and incorporate security best practices that connects with its individual stages.

Multi-faceted Approach

Any application development starts by gathering the requirement and perform analysis followed by design, code, testing, and deployment into production environment and finally provides ongoing maintenance support. To look at this lifecycle holistically, we need to incorporate security at strategic phases that will help identify gaps and vulnerabilities early on and also provide layered protection.

- Application design and development is where it all begins to materialize and provide shape to an application. It is important to adopt secure coding practice to build a secure application. Static code review will help achieve the objective of identifying and mitigating the vulnerabilities at code level.

- Application Testing phase needs adequate protection to the application. Our dynamic process provides the necessary information that helps the developer to make the security-related modifications while the application is being built.

- Application in production environment is what the world sees. Adding security at this phase is a must as it provides insight to the visibility that the attacker is likely to have.

- Run-time protection is the ongoing mechanism to safeguard the application from external attacks. It is imperative as any leakage of sensitive data leads to financial loss and negatively impacts brand value.

Application Security

KSADS Phase II application (KSADS-COMP) 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
- The clients' requirement driven business logic is programmed in a separate layer and this architecture helps to scale and maintain the application with less downtime.

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

Input validation

Input validation is performed to ensure only properly formed data is entering the workflow in an information system, preventing malformed data from persisting in the database and triggering malfunction of various downstream components. Input validations are applied on both syntactical and Semantic level.

Syntactic validation enforces correct syntax of structured fields (e.g., date).

Semantic validation enforces correctness of their values in the specific business context (e.g. start date is before end date, grades are within age limits etc.).

Authentication

Security and privacy have been of the utmost concern in the development of the application. KSADS-comp architecture includes authentication and authorization business logic layers.

The application's authentication process requires the combination of a username and password and on-demand two-factor authentication (2TFA) and to access the content. 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 is not directly be embedded in SQL statements; rather parameterized statements are used).

Authorization

KSADS-COMP authorization layer is constructed by taking the different user roles into consideration.
User Roles are permission sets that control access to areas and features within the KSADS-COMP environment. KSADS-COMP has super-admin, study-admin, admin, and client user roles for each site. Each user will have specified user roles thus allowing/ denying access to resources and data according to the configured policies. Unauthorized users cannot access features on the site for which they are not authorized to access. They also cannot assess the data from other sites.

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 Atlassian bitbucket 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 and Data Encryption

Password verification is a particularly important application for cryptographic hashing. Storing users' passwords in a plain-text document is a recipe for disaster; any hacker that manages to access the document would discover a treasure trove of unprotected passwords. That's why it's more secure to store the hash values of passwords instead. When a user enters a password, the hash value is calculated and then compared with the table. If it matches one of the saved hashes, it's a valid password and the user can be permitted access. KSADS-COMP uses the latest and most advanced Secure Hash Algorithm 256 (SHA-256).

Cryptography is used at a various level 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.

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.

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

Cloud Computing

Cloud computing provides a simple way to access servers, storage, databases and a broad set of application services over the Internet. A cloud services platform such as Amazon Web Services owns and maintains the network-connected hardware required for these application services

MFA

AWS Multi-Factor Authentication (MFA) is a simple best practice that adds an extra layer of protection on top of your username and password. With MFA enabled, when a user signs in to an AWS website, they will be prompted for their user name and password (the first factor—what they know), as well as for an authentication response from their AWS MFA device (the second factor—what they have). Taken together, these multiple factors provide increased security for your AWS account settings and resources.

IP Whitelisting

Only authorized admins from approved locations are allowed access to our secured servers.

Compliance

The IT infrastructure that AWS provides to its customers is designed and managed in alignment with best security practices and a variety of IT security standards. The following is a partial list of assurance programs with which AWS complies:

- SOC 1/ISAE 3402, SOC 2, SOC 3
- FISMA, DIACAP, and FedRAMP
- PCI DSS Level 1
- ISO 9001, ISO 27001, ISO 27017, ISO 27018

Penetration-Testing for GDPR

Web application security remains a major roadblock to universal acceptance of the Web for many kinds of online transactions, especially since the recent sharp increase in remotely exploitable vulnerabilities has been attributed to Web application bugs. In software engineering, software testing is an established and well-researched process for improving software quality. Recently, formal verification tools have also shown success in discovering vulnerabilities in C programs. In this chapter we shall discuss how to apply software testing and verification algorithms to Web applications and improve their security attributes. Two of the most common Web application vulnerabilities that are known to date are script injection, e.g., SQL injection, and cross-site scripting (XSS).

KSADS-COMP has undergone rigorous Penetration testing (pen-testing) or ethical hacking testing as required by the General Data Protection Regulation (GDPR) 2016/679 a regulation in EU law by a third-party vendor (https://www.dongit.nl/en) to find security vulnerabilities that an attacker could exploit.

The team used testing guidelines set by various ICT security branches as a foundation for its security assessment methodology. The following methodologies and comprehensive frameworks are used for assessment of network and web application security:

- Open Web Application Security Project (OWASP)
- Information System Security Assessment Framework (ISSAF)
- Open-Source Security Testing Methodology Manual (OSSTMM)
- Penetration Testing Execution Standard (PTES)
- National Institute of Standards and Technology Cybersecurity Framework (NIST)

The team tested the web application, network, firewall and the cloud server for vulnerabilities in many areas like brute-force attacks, SQL injections, cross-site scripting, social-engineering techniques etc., and we closed all reported issues and our security policy has been updated accordingly.

The Pen testing offers these following benefits

- Identify and Prioritize Risks
- Prevent Hackers from Infiltrating Systems
- Mature the Organization's Environment
- Avoid Costly Data Breaches and Loss of Business Operability
- Comply with Industry Standards and Regulations

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

Key Contacts

Joan Kaufman, PhD

KSADS-COMP co-developer

Kenneth Kobak, PhD

KSADS-COMP co-developer

Alison Deep, MCA

KSADS-COMP IT director

KSADS-COMP
LLC

KSADS-COMP

The gold standard in child and adolescent psychiatric diagnoses.

www.KSADS-COMP.com v1.2_02_12_22