kPoint

Videofy the enterprise.

kPoint Product Security Note

Table of Contents

ABOUT THIS DOCUMENT

Basic Details

Document File Name	kPoint Product Security Features
Version #	1.1
Release Date	01/12/2014
Author	Manish Sapariya
Document Owner	Chaitanya Bokil

Modification Summary

Version #	Created / Modified By	Modification Date	Modification Notes
1.0	Manish Sapariya/Amol Potnis	12/02/2012	First copy
1.1	Manish Sapariya	01/12/2014	Formatted as per standard template

Introduction

kPoint is an enterprise-grade online platform for creation, hosting and sharing of rich multimedia videos. Using any online collaboration and recording solution requires careful consideration of potential threats and resulting business risks. Business security needs that must typically be addressed adopting such solution include:

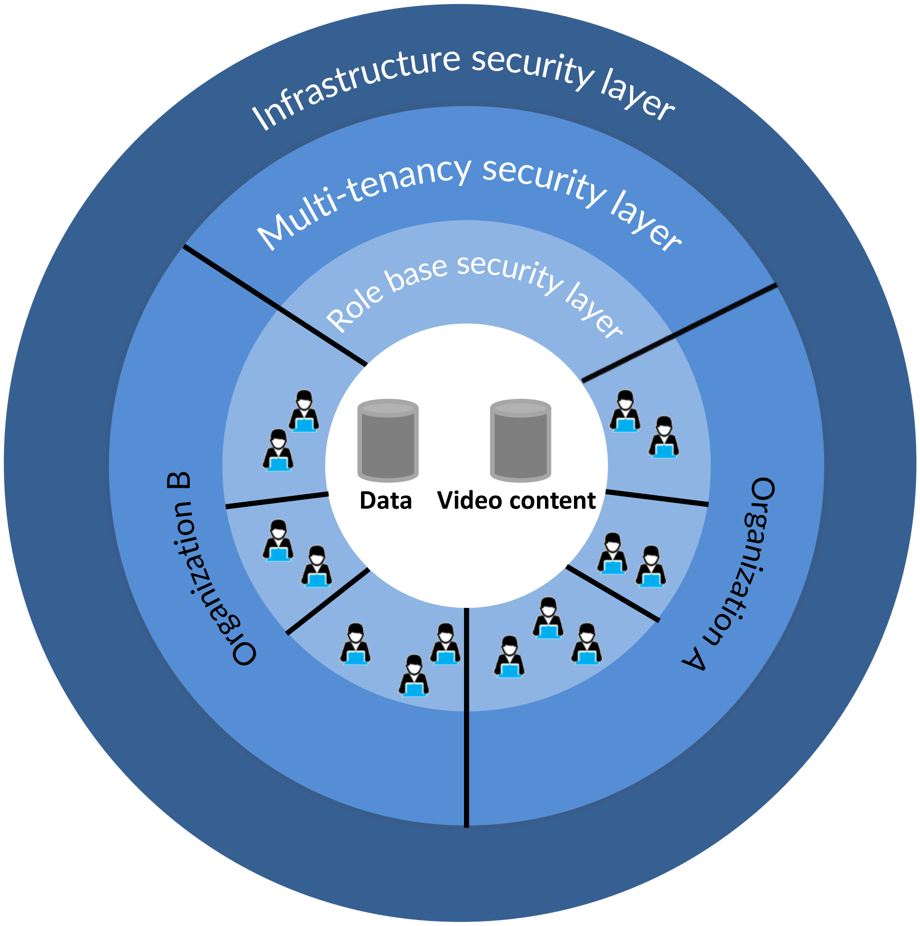
- Preventing unauthorized use of the service and its features.
- Protecting the privacy and integrity of confidential communication.
- Ensuring availability and reliability of the service itself.

Helping ensuring the confidentiality, integrity and availability of the customer data is of the utmost importance to kPoint, as is maintaining trust and confidence.

By incorporating security features and making them easy to use and administer, kPoint enables effective and safe online business collaboration and recording.

High level security architecture

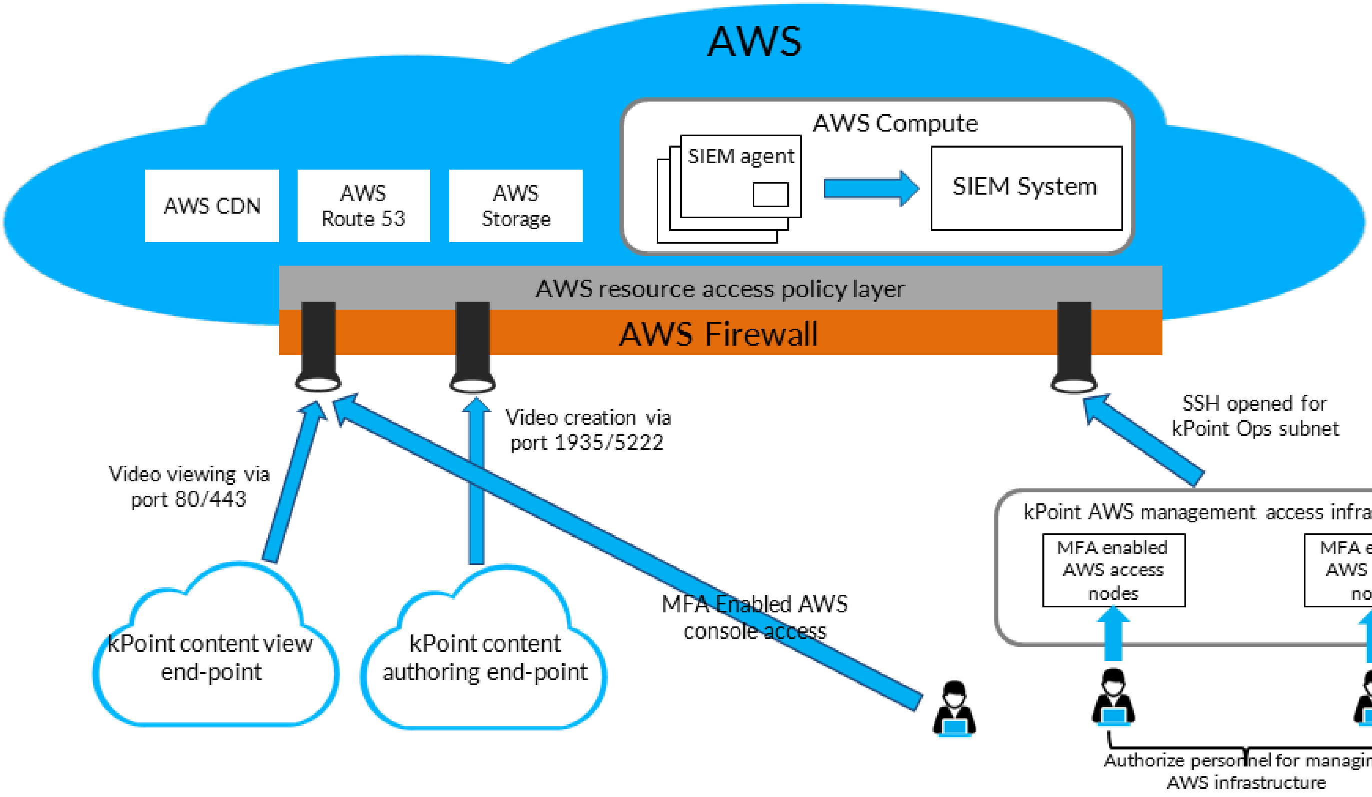
kPoint is a multi-tenancy architecture and below diagram depicts various security layers incorporated in the kPoint architecture to ensure security at various layers. We will discuss each of the layers in detail to depict that how various security controls are implemented in kPoint at each layer.



Infrastructure Security Layer

kPoint service is hosted on Amazon Web Services (AWS). The AWS cloud service ensures very high availability and accessibility of the kPoint service. kPoint's service architecture has been designed to make it work with cloud service (like AWS) and to make it robust and easily scalable by taking benefit of the facilities provided by the cloud service. For details of security implementation by AWS please refer to http://media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf

Following diagrams details out the various controls implemented at AWS and local infrastructure to protect the infrastructure hosted in the AWS cloud.


AWS
AWS Compute
SIEM agent
SIEM System
AWS CDN
AWS Route 53
AWS Storage
AWS resource access policy layer
AWS Firewall
Video creation via port 1935/5222
SSH opened for kPoint Ops subnet
Video viewing via port 80/443
kPoint AWS management access infrastructure
MFA enabled AWS access nodes
MFA enabled AWS access nodes
MFA Enabled AWS console access
kPoint content view end-point
kPoint content authoring end-point
Authorize personnel for managing AWS infrastructure

Public service access:

kPoint servers are firewall enabled. Only the ports necessary for kPoint service end points are opened. These open ports are : 80 (HTTP) and 443 (HTTPS) for content view end points, 935 (RTMP) and 5222 (XMPP) are content authoring endpoints. If the RTMP and XMPP ports are blocked at the user end, the traffic is tunneled over HTTP.

Hosted infrastructure access:

Access to servers in AWS infrastructure is configured via SSH. The SSH access is restricted only from a designated end points at the kPoint office. The SSH access is further protected by keys and two factor authentication password/tokens. The SSH access is restricted only to authorized admin users. Any need based access is strictly provided by the authorized personnel upon approval by the VP of Technical Operations or above.

Hosted infrastructure hardening:

The servers deployed in the AWS cloud are hardened as per the server hardening best practices to ensure the server security.

Vulnerability assessment

kPoint is assessed for security flaws that lead to various vulnerabilities which could be exploited for credential theft, online account compromise, identity theft, sensitive information leakage, general system failure, etc., as part of its installation process. kPoint is tested against well-known vulnerabilities published by OWASP (The Open Web Application Security Project). The OWASP Top Ten, as it is referred to, represents a broad consensus about what the most critical web application security flaws. Please refer to the annexure for brief information about the OWASP Top 10 vulnerabilities. Automatic and manual techniques are used to complete this assessment with the help of following industry standard open source and free tools:

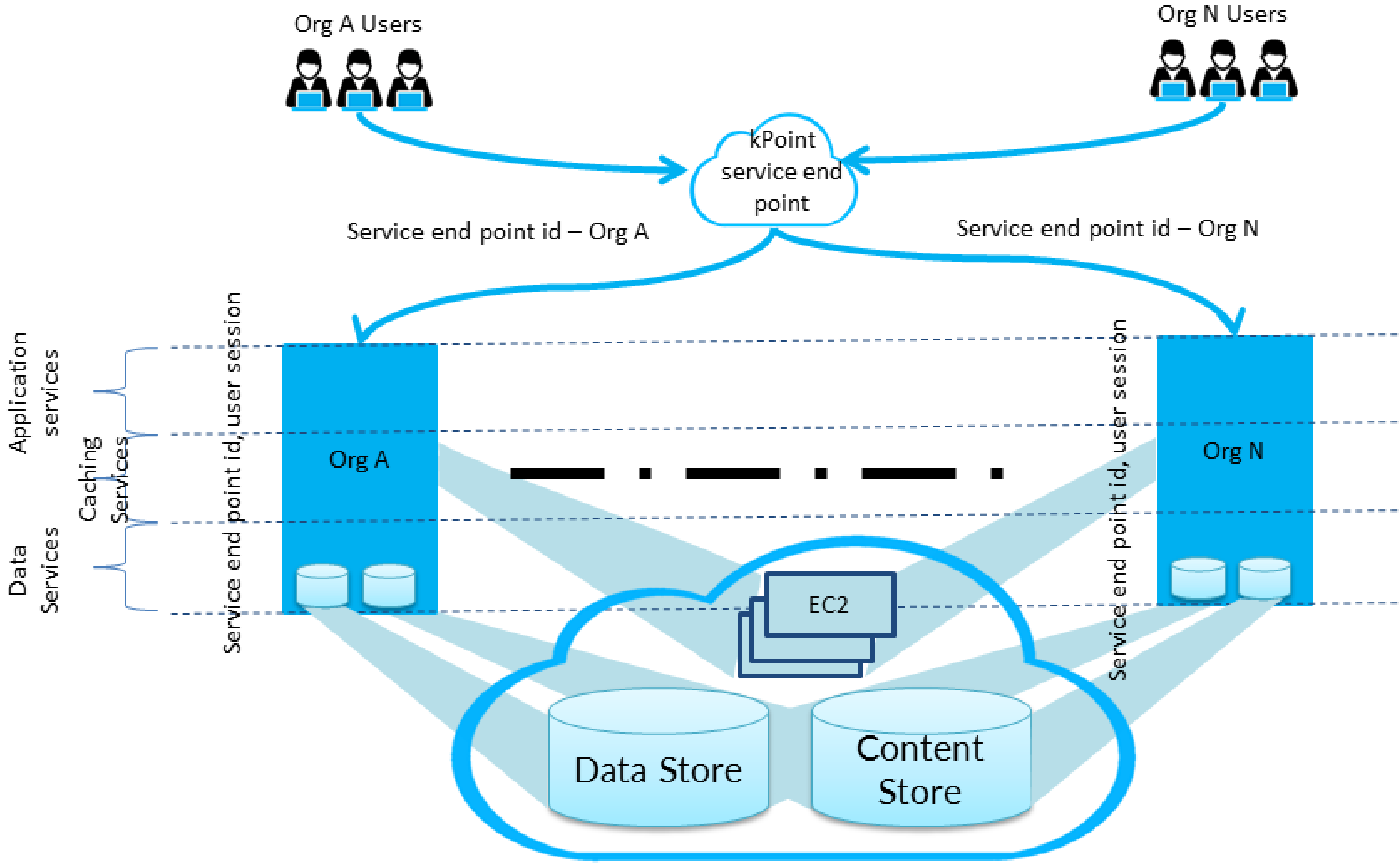
- Paros/Zapproxy : Web application security assessment tool (http://www.parosproxy.org/)
- Ratproxy : Passive web application security assessment tool (http://code.google.com/p/ratproxy/)
- Scrawlr : SQL Injector and Crawler by HP (https://h30406.www3.hp.com/campaigns/2008/wwcampaign/1-57C4K/index.php)
- Nmap : Utility for network exploration and security auditing (http://nmap.org)
- SSLDigger : Tool to assess the strength of SSL servers by testing the ciphers supported(http://www.mcafee.com/in/downloads/free-tools/ssldigger.aspx)

System monitoring:

All kPoint servers are enabled for 24x7 security and availability monitoring. All terminal logins to the server are logged. Internal systems are extensively instrumented to monitor key operational metrics. SIEM tool (OSSIM) is enabled on kPoint servers which automatically filters all logs and raises alerts in the form of email for all suspicious activities. Nagios framework is used to continuously monitor system health in terms of CPU usage, disk i/o, disk space and availability of internal critical services. For all critical observations, alerts are raised in the form of emails. Such alerts are seen on daily basis by the kPoint administrators and appropriate actions are taken.

Multi-Tenancy Security Layer

Following diagrams details out the multi-tenancy architecture of kPoint and how separation of tenant data access is implemented.



kPoint is a multi-tenanted service, which implements security at various layers of services whenever user requests the access to data. As the user request is received at the kPoint service end point multiplexer, a tuple is identified, based on user authentication and authorization, which consists of service end point id and the user session. All services at allow the access to the data requested by users only if it passes the authorization checks against the user session.

Role based security

kPoint Role-Privilege matrix:

kPoint implements role-based access control (RBAC) for protecting the content from un-authorized access and to control access to various product features, which provides access to potentially confidential data. Every kPoint user is assigned one of several application–defined roles. kPoint user interface provides intuitive controls and status indicators that facilitate productive and secure access to all the content. Control and privileges available to each user depend on the currently assigned role to that user.

kPoint Role	Privileges
Viewer	• View videos • Search for videos on kPoint portal • Search within videos • Add comments to videos • Add private or public bookmarks to videos (only for videos where the creator has allowed bookmarks from viewers) • Add private or public questions to videos (only for videos where the creator has allowed questions from viewers) • Edit or delete their own bookmarks and questions • Rate videos • Share videos (over email or social media) • Browse and view playlists • View FAQ and Help videos
Creator	• All viewer rights • Upload content to kPoint for video creation • Create videos (using narrate slides OR capture screen OR Create rich media mash up OR Import existing video OR import YouTube video) • Edit their videos • Publish their videos • Change video settings (including view options) • Add, edit, delete bookmarks for their videos • Respond to questions posted on their videos • Change video ownership for their videos (to another creator) • Add transcripts to their videos • View video analytics • Embed videos in other portals • Create playlists • Share playlists • Schedule and host kPoint Meetings
Reviewer **(Optional Role)**	• All “Creator” rights • Rights to approve or reject videos for publishing This is an optional role which can be enabled for enterprises that wish to have the videos created by “Creators” reviewed by an approving authority before they are published. Can be enabled if the enterprise wishes to implement such a review mechanism. When this role is enabled, the “Creators” have an added step of sending the videos for review to a “Reviewer” from the designated list, who then approves or

	rejects the videos based on the enterprises' content publishing criteria.
Site Administrator	• All creator rights • Manage (add, modify, delete) users on the kPoint portal • Manage (add, modify, delete) groups on the kPoint portal • Manage videos • View and export (as CSV) admin summary reports for the kPoint portal
Host	The Host has complete control of a meeting and the ability to grant and revoke various privileges for other participants. Host privileges include: • Ability to start and end the meetings. • Ability to see the complete list of participants and their current status in a meeting. • Ability to make any participant Presenter (including self) in a meeting. • Ability to dismiss any participant from the meeting.
Speaker	Speaker privileges include all host-privileges EXCEPT the ability to end meetings. Thus Speaker becomes the next level of authority in the absence of the Host.
Presenter	A Presenter is the user who actively presents content or his/her own desktop in the meeting. Only one participant at a time within a meeting may be granted the Presenter role. Presenter privileges include • Ability to share documents, audio/video clips, whiteboards, desktop with other participants in the meeting. • Ability to grant/revoke remote keyboard/mouse control to another participant, which facilitates efficient communication through desktop sharing. • Ability to chat with all participants. • Ability to post multi-choice questions to all participants. • Ability to conduct polls. • Ability to insert bookmarks to generate richer video out of this session.
Participant	Users with basic Participant role have the following privileges: • Ability to join any meeting which they are authorized to join • In a meeting: ○ Ability to view all shared documents, audio/video clips and whiteboards, desktop. ○ Ability to chat with other participants. ○ Ability to ask queries. ○ Ability to answer the multi-choice questions posted by the Presenter. ○ Ability to respond to the polls conducted by the Presenter. ○ Ability to remote control the Presenter's mouse and keyboard, if allowed to do so. ○ Ability to leave the session at any time. ○ Ability to see the participants list and their current status. • Ability to view authorized videos and interact with them

Account and session authentication management

Web site account login

To access a user-account on kPoint web site, users must supply a valid login and corresponding password. Login credentials are transferred to the kPoint server using HTTPS protocol. Passwords stored in the service database are encrypted and checked using a cryptographically secured verifier that is highly resilient to offline dictionary attacks. The passwords will require to conform to the minimum password requirements of kPoint.

These are

1. Password must be minimum 8 character long
2. Password can be max 32 character long
3. Password should have at least 1 special character
4. Password should have at least 1 numeric character
5. Password should have at least 1 upper case character
6. Password should have at least 1 lower case character

kPoint application allows 5 invalid consecutive password entry. On the sixth attempt the user account will be locked. User will have to connect with kPoint support team to unlock the account.

Session information disclosures

The information describing scheduled kPoint session is only available to the Host and the invited participants. Session descriptions are displayed only after the users have successfully authenticated and then only to those users who are authorized to view it.

Unique session tokens

Access to live session and video streaming is managed using unique and time limited session tokens. Server generates a unique token for each user attempt to access each live session or video. The server maintains mapping of the token to the user and asset.

Thus server makes sure that the session gets appropriate privileges. The tokens, in themselves, do not contain resource, user or privilege information and thus cannot be manipulated to gain unauthorized access. Time limited nature of the token ensures that they cannot be used to perform replay attack

Firewall and proxy compatibility

kPoint includes built-in proxy detection and connection management logic that avoids the need for complex network (re)configuration and maximizes user productivity. Firewalls and proxies already present in your network generally do not need any special configuration to enable use of kPoint tools. Compatibility of working with existing network/security infrastructure enables enterprise customers of kPoint, enables to exercise existing security control at their end.

Note: Some application firewalls disable multimedia traffic completely which that can impact kPoint sessions.

Endpoint client software

kPoint client endpoint software is a completely browser-based tool and directly served from kPoint server when you connect to the server. Normally the browser is all that the user needs to participate in a kPoint session. However, if the user wants to share his/her desktop, a digitally signed browser plugin is downloaded to the user's computer. As the plugin is digitally signed, the user gets protected from inadvertently installing a Trojan or other malware posing as kPoint software. Strict quality control and configuration management procedures are followed by kPoint during development and deployment to ensure software safety. The endpoint software exposes no externally available network interfaces and cannot be used by malware or viruses to exploit or infect remote systems. This protects other desktops participating in a session from being infected by a compromised host used by another attendee.

Data Backup policy

Data backup consists of daily, weekly and monthly backup. It consists of local as well as remote backup. Overall it assures a backup availability for the data of last 6 months. kPoint service can be resumed from the backup data within 24 hours of the failure detection. This backup is taken using Amazon EBS and S3. The security of backup data is taken care by Amazon's security procedures (http://media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf).

On-Premise security

Background checks:

All the employees and contractors of the kPoint undergo a comprehensive background checks to asses for any criminal record, education qualification and previous employment verification. The access to the Amazon infrastructure is given only to kPoint employees.

Security Training

All kPoint employees go through basic security awareness training periodically. All the development/test/operations teams go through advanced security best practices for development and deployment.

Processes, Audits, Reviews

Monthly review of current security measures:

A dedicated team reviews current security measures on a daily/weekly basis. Observed problems and possible security threats are analyzed. Status of earlier decided actions items is checked and appropriate new actions are scheduled for subsequent releases/patches.

Privacy Policy

kPoint is committed to completely respect our customers privacy. A copy of our privacy policy is available online on www.kpoint.com

Annexure

Security standards compliance

kPoint is compliant with following industry standards for cryptography algorithms and security protocols:

- The TLS/SSL Protocol, Version 1.0 IETF RFC 2246
- RSA, PKCD #1
- MD5. IETF RFC 1321
- HTTPS

The Company Environment

kPoint leverages various aspects of its control environment in the delivery of its services. The collective control environment encompasses management and employee efforts to establish and maintain an environment that supports effectiveness of its service delivery.

- Executive and senior leadership play important roles in establishing the Company's tone and core values at the top.
- Every employee is provided with the Company's Code of Business Conduct and Ethics, which sets guiding principles.
- Roles and responsibilities are assigned appropriately to provide adequate staffing, efficiency of operations of segregation of duties.
- Authority and appropriate lines of reporting for key personnel has been established.
- The Company's strict hiring policy verifies education, previous employment and criminal checks of the applicant.
- Every new employee goes through an induction process to get familiarize with needed tools, processes, systems, policies and procedures.

Safeguards

Information Security	There is a clear information security policy that is communicated throughout the organization to the users.
Employee Lifecycle	Employee users' accounts (on internal/external systems/services) are added/modified/deleted in a timely manner to reduce the risk of unauthorized/inappropriate access.
Data security	Unauthorized access to internal/customer data is appropriately restricted.
Physical security	Physical access to the Company's office, internal network, machines and documents is restricted to authorized personnel.

Configuration Management

Any configuration changes to existing kPoint service infrastructure are authorized, logged, tested, approved and documented. Any updates to the kPoint service are done in such a manner that in the vast majority of cases they will not impact the customers and their use of the service. kPoint communicates with customers over email and phone when service use is likely to be adversely affected.

Software:

All changes to the customer impacting services are thoroughly reviewed, tested, approved and well communicated. The goal is to permit no unintended service disruptions and to maintain the integrity of the service to the customers. Changes deployed to the production environments are:

- Reviewed: Peer review of the technical aspect of this change.
- Tested: To confirm that it will behave as expected and not adversely impact the functionality and the performance.
- Approved: To provide appropriate oversight and understanding of the business impact.

OWASP Top 10 vulnerabilities in brief

All kPoint servers are assessed against following top 10 vulnerabilities.

A1-Injection	Injection flaws, such as SQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing unauthorized data.
A2-Cross Site Scripting (XSS)	XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation and escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
A3-Broken Authentication and Session Management	Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, session tokens, or exploit other implementation flaws to assume other users' identities.
A4-Insecure Direct Object References	A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.
A5-Cross Site Request Forgery (CSRF)	A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim.

A6-Security Misconfiguration	Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. All these settings should be defined, implemented, and maintained as many are not shipped with secure defaults. This includes keeping all software up to date, including all code libraries used by the application.
A7-Insecure Cryptographic Storage	Many web applications do not properly protect sensitive data, such as credit cards, SSNs, and authentication credentials, with appropriate encryption or hashing. Attackers may steal or modify such weakly protected data to conduct identity theft, credit card fraud, or other crimes.
A8-Failure to Restrict URL Access	Many web applications check URL access rights before rendering protected links and buttons. However, applications need to perform similar access control checks each time these pages are accessed, or attackers will be able to forge URLs to access these hidden pages anyway.
A9-Insufficient Transport Layer Protection	Applications frequently fail to authenticate, encrypt, and protect the confidentiality and integrity of sensitive network traffic. When they do, they sometimes support weak algorithms, use expired or invalid certificates, or do not use them correctly.
A10-Unvalidated Redirects and Forwards	Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.