# A study on Adobe Experience Manager Security

**Sivabalan N [1], Vandana C.P[2]**
Department of CSE
[1, 2]Assistant Professor, New Horizon College of Engineering, India,

***Abstract-*** *Adobe Experience Manager (AEM) is an intense web content management framework for building and overseeing complex, dynamic, multi-channel digital experiences—effortlessly and effectively. With Adobe Experience Manager, we can oversee ventures, work processes, resources, integrations, and social groups; build adaptive complex forms; and make websites and mobile applications. Built on the Java platform, it is powered by open source principles and cutting edge frameworks and technologies, including the Java Content Repository (JCR) API, and a strong and structured representational state transfer (REST) architecture. Clients can either deploy Adobe Experience Manager on-premises using their own network infrastructure or Adobe can host their deployment as a managed service. In this paper, some of the key security mechanisms available in AEM are studied.*

***Keywords***- Adobe Experience Manager (AEM), REST , JCR, Security

## I. INTRODUCTION

With the onset of digitalization, time and money are shifted online. The opportunity to engage customers and customer retention is challenging day by day. Users are exposed to diverse environments, creating greater challenges to business. They have to create their presence everywhere where the customers are and provide them a personalized experience. To meet this challenge to optimize customer experience to the peak through all the rapid channels and devices, industry is seeking for new technologies and processes. To win the market they need to be innovative, creative, dynamic and agile in all senses. However, the marking workflow for managing and publishing digital content online has not reached the heights. Personalized user targeting is not consistent. Websites and campaigns are launched successfully now a day, but the lack of an analytical tool to measure its impact and loop-holes is not in place.

Content Management Systems help to create, organize, manage, maintain web content in a multi-user environment. Users can add/remove the functionality as per their requirement which is the core of modularity. The adobe Experience Manager, a web content management and digital asset management suite is the solution to engage customer experiences in all diverse channels and devices , making the business presence everywhere and every time.

In section 2, a brief overview of the various security issues and solutions present in the market is reviewed; section 3 highlights the architecture of Adobe Experience manager and security solutions in section 4 followed by conclusion on the security issues.

## II. SECURITY ISSUES AND SOLUTIONS

Content Management Systems help to create, organize, manage, maintain web content in a multi-user environment. Users can add/remove the functionality as per their requirement which is the core of modularity. Most of the web content management systems are built on open –source platforms , making the system vulnerable since any one can study the system and exploit the same leading to security breach. Since these digital asset management systems are dealing with customer data, it may lead to huge data and financial losses, loss of reputation, trust and business relationships, customer loss in case of a security attack. Typical the security attacks are launched on core modules, configuration parameters.

Data Manipulation: This attack is typically initiated to compromise the data integrity by using SQL injections, exploiting database vulnerabilities.

Unauthorized data access and Phising: Confidential information is accessed via email or input dialogs and form fill-in.

Code execution: Inputs are not validated properly leading to malicious code execution. Also, remote files can be executed by attacker using scripts on remote web servers.

Local File Inclusion: Intruder requests a sensitive file in lieu of the file from the pristine request. Directory Traversal or Backtracking or Path Traversal forces an application to access a critical file located outside the root folder and to show the file content to the intruder, utilizing variables that contains relative or absolute file paths references.

Cross-Site Scripting (XSS): Attacker send scripts to client's browser in order to obtain credentials, deface web sites,

insert maleficent content or redirect users. This type of susceptibility appears as a result to an inopportunely validated code. Comment Spamming approach, the assailant posts desultory comments automatically in order to make his own site more visible for the search engines.

Utilization of some of the best security practices in CMS such as maintaining the CMS themes and plugins updated, customarily engendering backups to the website files and associated databases, expunging default admin username and utilizing vigorous passwords, ascertaining that accounts and files sanctions are congruously set or implementing SSL sessions.

## III. ADOBE EXPERIENCE MANAGER APPLICATION ARCHITECTURE

The Adobe Experience Manager arrangement incorporates the accompanying five (5) capabilities:

Experience Manager Sites — This is the place where user can create, manage, and deliver digital experiences across websites, mobile sites, and on-site screens to make them globally visible

Experience Manager Assets — Enables you to create, manage, and deliver images, video, and other content to virtually any screen or any device.

Experience Manager Mobile — Helps you to create and deliver mobile apps for customers and devices and then integrate these mobile apps into your overall marketing strategy.

Experience Manager Forms — helps you to make your own forms, documents, and their processes with paperless, high efficient, and automated. With Experience Manager Forms, you can convert complex transactions into simple, digital experiences on virtually any device.

Experience Manager Communities — Enables you create online community experiences, including forums, user created groups, learning resources materials, and other social features that are valuable to customers, employees, and your brand.

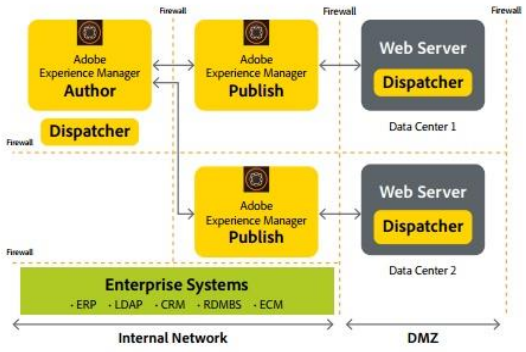


Figure 1: Adobe Experience Manager Application Architecture

## IV. ADOBE EXPERIENCE MANAGER APPLICATION SECURITY AND NETWORK ARCHITECTURE

**Adobe Experience Manager Data Flow**

Before content authors can create and publish content in AEM, web developers need to create the target website using Sightly, an open-source templating language for AEM. SightIy makes it easy on the component development process and allows HTML web developers to do programming that historically had to be done by Java/JSP developers. It also includes many built-in security controls.

**Sightly includes:**

- A server-side template language.
- Auto-escaping ensures secure output by avoiding cross-site scripting (XSS) vulnerabilities, a top security risk according to Open Web Application Security Project (OWASP)
- High end technology used on real-life projects to increase development efficiency.

Once the templates have been made, content authors can utilize the templates to submit content to the website.

Authors sign into the Adobe Experience Manager UI and upload content to the servers. The document security modules proactively shields and control data from burglary or abuse, regardless of where the information resides or travels—inside or outside the enterprise. With Adobe Experience Manager Forms Document Security, clients can make customized PDF archives and allow desktop or mobile users to access them via the website or web portal. Adobe Experience Manager encrypts files and applies standard and dynamic

policies that help maintain confidentiality and control use on fixed or mobile devices. In the event that the client has picked Adobe to host its deployment, all content is secured during upload over the Internet using S-HTTP. The content stays protected and private on the Adobe Experience Manager servers until publishes the content, enabling consumers of the website to access it.

**User Authentication for Adobe Experience Manager**

Commonly, clients coordinate Adobe Experience Manager into their existing enterprise identity management system. It supports legacy LDAP-compliant systems, SAML compliant systems, SSO systems, and social integration via OAuth. Custom integrations are additionally conceivable.

**LDAP Support**

Adobe Experience Manager can use existing Lightweight Directory Access Protocol (LDAP) executions, including Microsoft Active Directory, to authenticate user credentials. It also works with enhanced authentication server deployments, for example, synchronized, multi-server environments, to support massive scalability.

**SAML Support for Federated Identity Management**

Adobe Experience Manager is completely compatible with SAML (Security Assertion Markup Language) and can incorporate with any SAML-compliant federated identity provider. SAML gives a standard XML representation for specifying the exchange of secured information between a security system, such as an authentication authority, and an application that trusts the security system, and gives interoperable approaches to exchange and obtain it. In that capacity, SAML guarantees the security of identity information between business partners, keeping federated identity cross-domain transactions more secure. Adobe Experience Manager ships with a SAML verification handler that offers help for the SAML 2.0 Authentication Request Protocol including support for both Single Sign On and Single Log Out.

**SSO Authentication Handler**

Adobe Experience Manager incorporates a SSO Authentication Handler service for associations that don't execute LDAP or SAML however need to make federated identity for their users. This service confirms the authentication results provided by the trusted authenticator. Single Sign On (SSO) permits a client to access multiple systems after providing authentication credentials ,such as a user name and password once. A different framework (known as the trusted authenticator) performs the authentication and provides Adobe Experience Manager with the user identity, usually in the form of an HTTP header. The SSO Authentication Handler can be utilized as concert with LDAP, if necessary, or as part of a larger integration with bespoke identity management systems.

**Social Integration via OAuth**

The Social Login feature of Adobe Experience Manager empowers organizations to give a social login choice on owned digital properties and then personalize the user experience based on profile data. Marketers can also combine social profile information with data from additional sources, such as a customer relationship management system or a website profile, to create a unique view of the customer.

Adobe Experience Manager includes in built support for Social Login using Facebook and Twitter. This integration can be extended on a project basis to include many other providers that has the OAuth standard. OAuth defines an enhanced framework for securing application access to protected resources, such as the identity attributes of a specific user. It permits an application that desires information to send an API query to a resource server hosting the desired information. The server can then confirm that the client in actuality sent the message.

**Adobe Experience Manager Hosting**

When a customer decides to have Adobe host its Adobe Experience Manager deployment as a managed service, every components are hosted on Amazon Web Services (AWS), including Amazon Elastic Compute Cloud (Amazon EC2) and Amazon Simple Storage Service (Amazon S3), in the United States, EU, and Asia Pacific. Amazon EC2 is a web service that provides resizable compute capacity in the cloud, making web-scale computing easier. Amazon S3 is a highly redundant data storage infrastructure for storing and retrieving any amount of data, at any time, from anywhere. The AWS platform provides services in accordance with industry-standard practices and undergoes regular industry-recognized certifications and audits.

**Adobe Risk & Vulnerability Management**

Adobe endeavors to guarantee that our risk and vulnerability management, incident response, mitigation, and resolution process is nimble and accurate. We ceaselessly screen the threat landscape, share knowledge with security specialists around the globe, swiftly resolve incidents when they occur, and feed this information back to our development teams to help accomplish the most elevated amounts of security for all Adobe products and services

**Adobe Secure Product Development**

Likewise with other key Adobe product and service organizations, the Adobe Experience Manager organization utilizes the Adobe Software Product Lifecycle (SPLC) handle. A thorough arrangement of a few hundred particular security exercises spreading over software development practices, processes, and tools, the Adobe SPLC is integrated into multiple stages of the product lifecycle, from design and development to quality assurance, testing, and deployment.ASSET security researchers provide specific SPLC guidance for each key product or service based on an assessment of potential security issues. Complemented by continuous community engagement, the Adobe SPLC evolves to stay current as changes occur in technology, security practices, and the threat landscape.

## V. CONCLUSION

The proactive approach to security and stringent procedures described in this paper help protect the security of the Adobe Experience Manager environment and confidential data. Adobe, take the security of digital experience very seriously and it continuously monitor the evolving threat landscape to try to stay ahead of malicious activities and help ensure the security of customers' data.

## REFERENCES

[1] Trends.builtwith.com. (2016). CMS technologies Web Usage Statistics. [online] Available at: http://trends.builtwith.com/cms [Accessed 31 Jan. 2016].

[2] "Security Issues in Most Popular Content Management Systems" ,Cosmin A. Con˙u, Eduard C. Popovici, Octavian Fratu, Mădălina G. Berceanu, COMM 2016 International Conference Proceedings

[3] Thomas , stdahl, "Security Issues with Content Management Systems (CMSs) on the Cloud", 2011 [5] IMPERVA, 2015 Web Application Attack Report (WAAR) 6th edition, 2015.

[4] CMS Report, C. (2015). CMS Security 2015: Top 5 Security Tools for WordPress, Drupal, and Joomla | CMS Report. [online] Cmsreport.com. Available at: https://cmsreport.com/articles/cms-security-2015-top-5-security-tools-wordpress-drupal-and-joomla-13696 [Accessed 31 Jan. 2016].

[5] Issues List. (2016). Joomla! Issue Tracker - CMS. [online] Available at: https://issues.joomla.org [Accessed 2 Feb. 2016].