ELEARNINGNEWS ARTICLE

Year 6 - number 227 Wednesday 7 december 2022

How to recognize a secure eLearning app

How do eLearning app developers defend our security? Let's learn how to spot the signs that an app is secure.

eLearning has grown in popularity because of its ability to address the growing demand for **faster, more focused and accessible training**. In addition, today's technologies allow anyone with an Internet connection to create a site or app to sell their courses. This explains why there has been a great evolution in the development of eLearning applications in recent years. As always, every aspect of technology comes with its own set of security threats.

Data security is also put to the test in eLearning applications. The repercussions of a data security breach could be problematic for learners whose rights are violated and devastating to the reputation of course providers. In this article we explore the behind-the-scenes of app development to understand how developers defend our security and to learn how to spot the signs that an app is secure.

Security measures to defend data

Every eLearning app developer should approach the issue of data security with the utmost care. Otherwise, the application will be vulnerable to attacks such as identity theft, online fraud, data tampering, and even loss of intellectual property. Therefore, the best strategy is to implement security measures to prevent data vulnerabilities from infiltrating eLearning apps. This article outlines some essential tips that can help protect eLearning apps from security threats.

1. Write secure code

The first crucial security measure that app developers should take is to write secure code. There is no doubt that app codes are vulnerable to several security flaws that often have devastating repercussions, such as reputational damage, exposure of sensitive user data, identity theft, and privacy breaches. To protect a code from these and many other security problems, it is always essential to follow secure code writing practices.
The most important security practice that every developer should adopt when writing code is to sign the code using a **code signing certificate**, called code signing certificates. This certificate is critical because it ensures that code is not corrupted or altered by malicious individuals as it moves between developer and user systems. If you have developed your own eLearning app remember that you need these certificates to protect the codes from being corrupted. Fortunately, there are various products online and you do not need to purchase an expensive one to ensure your security.

2. Assess and prevent server-related threats

An eLearning application developer must make sure to assess and prevent all server-related vulnerabilities. This should be done early in the application lifecycle. Server-related vulnerabilities open the door for malicious attackers to infiltrate the website and tamper with its contents. These vulnerabilities can be unsecured communications, malware and viruses, etc., all of which can pose threats to servers.

There are three methods that developers can use to prevent server-related security threats.

a. First, eLearning app developers should always adhere to **code security best practices**. A list of some of the control practices for secure data coding is given below:

- Secure password authentication
- Session management with full user details
- Access control and management with proper user verification
- File uploads must be specific to the context of the page
- Secure transmission with HTTPS

b. Second, developers should use an **automated scanner**. Automation is the best way to reduce the chances of human error. Carelessness can lead to the loss of sensitive data, and automation is like putting essential security processes on autopilot and eliminating any errors.

c. The purpose of automation is to encourage developers to fix bugs early in development, rather than performing a security audit at the end of the process. Therefore, it is always useful to perform a manual app **security risk assessment**. This helps distinguish app threats by ranking them according to their intensity and likelihood of occurrence.

3. Using SSL certificates

SSL certificates are cryptographic tools that take care of hiding data from unauthorized access. In simpler words, they are pieces of code that ensure the security of online communications. When a Web browser contacts your site, the SSL certificate enables an encrypted connection. This is not so different from sealing a letter in an envelope before sending it through the mail. Their use is not limited to this; they are also used as tools for securing websites as part of the migration from HTTP to HTTPS. The latter are considered more secure because they allow a site's information to be encrypted, so much so that Google uses HTTPS as a standard for sites featured on Google Chrome.
However, their scope is not limited to websites. SSL certificates also play a key role in app security. The lack of an SSL certificate, or even just the possibility that the certificate has not been properly verified, can invite many attackers to exploit your website. Without these tools, even inexperienced hackers have the ability to appropriate data and communications that take place on your website.

4. Use strong authentication for apps

The **Verizon Data Breach Investigation Report of 2021** reported some startling statistics: 81 percent of data breaches occur because of weak passwords. Attackers easily decode weak passwords to access private data. To prevent this from happening, eLearning app developers should establish a threshold that requires users to use only strong and unique passwords. Developers should also remember to **integrate authentication factors** into the user login process. Multi-factor authentication increases security because it requires users to use more than a single password to access the app.

Other useful practices for defending data

Protect e-mail from phishing attacks
Hackers attack not only through malware hidden in apps or sites, but also in a more direct way, for example by sending e-mails. This type of attack is very popular and unfortunately reaps so many victims that it has received its own name: **phishing**. Sending malware-infested e-mails has been the hallmark of hackers trying to wreak havoc in the IT world. Hackers can block student profiles, and to thwart these attacks, it is advisable to install S/MIME certificates.

Protect confidential documents
Another key issue for those doing eLearning is to prevent the manipulation and tampering of school certificates, such as diplomas, transcripts, etc. Fortunately, the pandemic has forced companies, individuals and the public administration to adopt a useful tool to ensure the protection of these types of documents. The **digital signature of documents** has provided the security of remote signing of documents and, when combined with the advantages of PKI, offers a high level of security in the exchange of school certificates, such as diplomas and transcripts. In fact, a digital signature cannot be forged unlike a hand-signed and scanned document. In addition, it has no expiration date and is valid forever.

Privacy rules in app-mobile stores

Despite the fact that the issue of data privacy and security is increasingly important to policy and users, the major tech giants do not seem to be taking promising steps to defend the security of our data.

The major players in app-mobile stores, namely the **Play Store and Apple Store**, are constantly adopting new data protection policies with the aim of providing their users with an effective security system. For example, Apple states that the controls performed on its store are so strict that it is able to intervene immediately if a suspicious case is detected. Despite this, reports came out in 2022 regarding the presence of **7 apps on Apple's store containing malware**. Apple promptly intervened by removing these apps (from the store, but not from devices), but the fact that they arrived on the store and were available for

download raises several questions about the security standards set by the tech giant. Google also does not seem to be taking steps to defend data. Some security rules on the Play Store have changed recently. Until July 2022, the app download page displayed a list, written by software created by Google, containing all the required permissions. In this way, the user could immediately guess the risks they were facing and assess the security of the application. Today, when you browse through apps or games on Google Play, you may notice that the list of permissions is no longer available. It seems that Google has decided that the new data security list is sufficient in this regard. Publishers who want to sell their apps on these stores are still required to provide data security information, as Google has made it mandatory. However, it is up to the publisher to compile this information and it is not explained to the end user how this information is controlled.

Conclusion

Given that the topic of privacy and the use of our data requires legal tools that are still being refined, and that companies do not always seem to make decisions in favor of end users, it is vital that end users protect themselves. Creating a secure eLearning application depends primarily on the skills and knowledge of the developers. However, it is also necessary for users to be aware of the risks involved in downloading an app without security certifications and to know the ways to best protect themselves from these risks.

Translated with www.DeepL.com/Translator