Is Your Open Source LMS Open to Hackers?

http://dx.doi.org/10.3991/ijac.v8i1.4396

Joseph Fish
SmrrtPros Ltd, Hawthorne. NY, USA

***Abstract*—Here's the Top 5 Security and Open Source Questions You Should Ask Your LMS Vendor (and other SaaS vendors) RIGHT NOW....**

***Index Terms*—Open source, LMS, security, hackers**

With the recent publication of major security vulnerabilities related to Open Source based applications and server operating systems, along with major security breaches resulting in 10's of millions of consumer banking records being stolen via the web, you need to be more careful than ever in reviewing your vendors' security vulnerabilities. And for those Open Source Software as a Service (SaaS) solutions that collect and store Personally Identifiable Information (PII) on behalf of your clients and employees, including many installed LMS Open Source solutions, the increasing exposure warrants your immediate attention.

While getting more than its fair share of press about security issues this year, "Open Source" is not inherently less secure than other methods of application development. However, systems that utilize Open Source libraries can quickly become a target simply because of how far reaching the Open Source initiative has spread. As we have seen, when many use the same code libraries, one un-discovered flaw can end up effecting millions of web sites. And unfortunately, this has spread to Open Source LMS solutions, where vulnerabilities are beginning to surface.

As part of your organization's standard vendor due diligence, you must ask the right security questions, understand the ramifications and risks involved, make smart decisions and take the right remediation actions in order to safeguard your intellectual property, customer and client PII, to ensure you have mitigated any risks BEFORE you suffer a breach and data loss.

Here are 5 questions you should be asking your existing and potential SaaS LMS vendors:

1) Do you perform External Application and Network Penetration Tests?

This means the company has hired or obtained testing services to "attack" their website and network looking for exposed weaknesses in security. LMS vendors and other SaaS providers who are serious about security will have this performed at least quarterly, with additional testing completed against any updates to their systems. You should ask for the most recent report as well as requesting each new report be shared with you.

2) If Open Source is used in your LMS solution, how have you addressed the recent security flaws discovered?

Good software development calls for system and application hardening. It also calls for regular updates, patches, and modifications to stay "one step ahead" of risk. The vendor should have specifically addressed the Shellshock and Heartbleed vulnerabilities.

3) If you utilize eCommerce in your LMS, are you PCI compliant?

The Payment Card Industry Data Security Standards call for assessments and adherence to a rigid set of rules defining best practices to ensure the safety of data used for making online purchases. An LMS or other SaaS vendor should be able to deliver to you a signed Attestation of compliance, or in the case of larger organizations, a report from a qualified external assessor.

4) Where will my data be housed and who will have access to it?

It is important to understand where exactly your LMS data is stored. In today's Cloud environment, without asking, you may find out your data is stored in an insecure facility or in a part of the world you may not be confortable with. Additionally, you must understand who has access to the data outside the systems that use it. Solid organizational security procedures call for a separation and regulation of duties so that only "trusted" individuals have access to your data behind the scenes, strictly limited to only what they need to know and access.

5) Will our data be encrypted both in transit and at rest?

Note that even the best practices have gaps. Generally the biggest gap can be a "trusted" employee becoming untrusted. If your data is protected through encryption while moving (perhaps with HTTPS forced across the entire application), and encrypted at rest (while stored in the database), much of the value of the data is lost to the casual data thief.

While you may have asked some of these questions when originally vetting your LMS vendor, now is the time to ask again. As the Internet evolves, things change often. Ensuring that you are knowledgeable and remain concerned about your organization's data will help keep your vendors in line and above board.

AUTHOR

Joseph Fish is EVP, CTO at SmartPros Ltd. (joe@smartpros.com, 914-517-1171).

Submitted 21 January 2015. Published as resubmitted by the author 10 March 2015.