

FTC PrivacyCon Submission

Abstract

Patterns of Security Flaws in Ed-Tech Applications, and the Risks They Pose to Student Privacy

Tony Porterfield, Independent Security Researcher
tony@edtechinfosec.org

Disclosure

The security flaws described in this presentation are the result of my ongoing efforts to assess security practices of ed-tech applications, and have all been disclosed to the applications' operators, with sufficient time to address the issues. Many of them have been publicly disclosed in news articles or on the edtechinfosec.org blog. Some of the examples will be drawn from my talk "Web App Security Testing for Everyone" presented at O'Reilly Fluent Conference in April 2015. See the references section for links to news reports and the Fluent Conference.

This presentation will not identify the web applications that the examples are drawn from. The focus of the presentation is to identify common patterns of ed-tech security flaws and the risks they pose to student privacy.

Overview

The widespread and increasing adoption of educational technology has led to a proliferation of educational web and mobile applications, offered by companies ranging from major corporations to start-ups.

Though ed-tech applications bring many benefits to students, educators and parents, I have observed that many of these applications have security flaws that expose the student personal and academic information held by the applications to unauthorized access. A set of common vulnerabilities has emerged. Some are general security problems found in many types of apps and others are more unique to educational applications. My methods for testing involve end-user security tests and checks that can be done with a personal computer and free software tools. A document describing many of these is available at:

<http://edtechinfosec.org/2015/02/08/a-starting-point-a-web-app-security-test-plan-for-end-users/>

This presentation will describe these common vulnerabilities in terms accessible to a general audience, and how they can be used in exploits against educational apps and the data they protect.

Details

The presentation will describe common ed-tech security vulnerabilities, with illustrative examples, in terms accessible to a general audience. As mentioned in the Disclosure section, this presentation will not identify the web applications that the examples are drawn from. The focus of the presentation is to identify common patterns of ed-tech security flaws and the risks they pose to student privacy.

Specific vulnerability types will include:

- Missing or flawed Transport Layer Security
- Enumeration of student numeric IDs and numeric class IDs
- Enumeration of student or parent “Access Codes”
- Web-facing APIs with missing authentication checks
- Rostering functions with missing authentication checks
- Lack of brute-force protections
- Information leakage - sending more information than needed to the client
- Sensitive information in URLs
- Missing cache controls

In security circles, the term “remote attack” describes a situation where an adversary is able to exploit a vulnerability without access to a user’s credentials or the messages that the user’s computer sends across the network. An example of this type of attack is if an intruder can craft a URL with a numeric userid and retrieve the user’s profile information without being logged in. Over the course of my work, I have found remote attack vulnerabilities enabling unauthorized access to the following types of information about, or access to, my own children through apps used at their schools.

- full name
- gender
- date of birth
- in-class behavior records
- reading level and progress assessments
- math skill and progress assessments
- in-class test and quiz scores
- report cards
- ability to send private message to a student through an app
- voice recordings
- usernames (some with passwords)
- password hashes
- school lunch assistance status
- name and address of school,
- teacher and class roster affiliations
- classmate names
- class photos with students labeled by name
- parent email address
- home phone number

During the course of the presentation I will map these types of information and access to students to the vulnerabilities that enabled the unauthorized access.

Conclusions

Though ed-tech applications can be very beneficial to students, educators, and parents, care must be taken to protect the enormous amount of personal information that they collectively hold about our students. Many ed-tech applications have security flaws that are the result of not following well-known best practices, and expose students to potential privacy breaches through unauthorized access. Uniformly addressing the common problems that have known defenses will lead to a significant reduction of our students' collective privacy risk.

References

Edtechinfosec: EdTech security blog:
<http://www.edtechinfosec.org>

O'Reilly Fluent Conference "Web App Security Testing for Everyone"
<http://fluentconf.com/javascript-html-2015/public/schedule/detail/39518>

"Data Security is a Classroom Worry, Too" (NYTimes)
<http://www.nytimes.com/2013/06/23/business/data-security-is-a-classroom-worry-too.html>

"Uncovering Security Flaws in Digital Education Products for Schoolchildren" (NYTimes)
<http://www.nytimes.com/2015/02/09/technology/uncovering-security-flaws-in-digital-education-products-for-schoolchildren.html>

"Data Security Gaps in an Industry Student Privacy Pledge" (NYTimes)
<http://bits.blogs.nytimes.com/2015/02/11/data-security-gaps-in-an-industry-student-privacy-pledge/>

"Digital Learning Companies Falling Short of Student Privacy Pledge" (NYTimes)
<http://bits.blogs.nytimes.com/2015/03/05/digital-learning-companies-falling-short-of-student-privacy-pledge/>

"Why Student Data Security Matters" (Edsurge)
<https://www.edsurge.com/news/2015-03-23-why-student-data-security-matters>