<WRWeb 19.1 Reading File ***>

This Teen Hacker Found Bugs in School Software That Exposed Millions of Records

A few years ago, Bill Demirkapi started poking around software used by his school and countless others. What he found wasn't pretty

Elle Aon / Shutterstock.com

By Andy Greenberg
Wired

A few short decades ago, the archetypal hacker was a bored teenager breaking into his school's network to change grades, à la Ferris Bueller. So today, when cybersecurity has become the domain of state-sponsored spy agencies and multibillion-dollar companies, it may be refreshing to know that the high school hacker lives on—as do the glaring vulnerabilities in school software.

At the Defcon hacker conference in Las Vegas today, 18-year-old Bill Demirkapi presented his findings from three years of after-school hacking that began when he was a high school freshman. Demirkapi poked around the web interfaces of two common pieces of software, sold by tech firms Blackboard and Follett and used by his own school. In both cases, he found serious bugs that would allow a hacker to gain deep access to student data. In Blackboard's case in particular, Demirkapi found 5 million vulnerable records for students and teachers, including student grades, immunization records, cafeteria balance, schedules, cryptographically hashed passwords, and photos.

Demirkapi points out that if he, then a bored 16-year-old motivated only by his own curiosity, could so easily access these corporate databases, his story doesn't reflect well on the broader security of the companies holding millions of students' personal information."The access I had was pretty much anything the school had," Demirkapi says. "The state of cybersecurity in education

software is really bad, and not enough people are paying attention to it."

5,000 Schools, 5 Million Records

Demirkapi found a series of common web bugs in Blackboard's Community Engagement software and Follett's Student Information System, including so-called SQL-injection and cross-site-scripting vulnerabilities. For Blackboard, those bugs ultimately allowed access to a database that contained 24 categories of data, everything from phone numbers to discipline records, bus routes, and attendance records—though not every school seemed to store data in every field. Only 34,000 of the records included immunization history, for instance. More than 5,000 schools appeared to be included in the data, with roughly 5 million individual records in total, including students, teachers, and other staff.

In Follett's software, Demirkapi says he found bugs that would have given a hacker access to student data like grade point average, special education status, number of suspensions, and passwords. Unlike in Blackboard's software, those passwords were stored unencrypted, in fully readable form. By the time Demirkapi had gained that level of access to Follett's software, however, he was two years into his hacking escapades and slightly better informed about legal dangers like the Computer Fraud and Abuse Act, which forbids gaining unauthorized access to a company's network. So while he says he checked the data about himself and a friend who gave him permission, to verify that the bugs led to access, he didn't explore further or enumerate the total number of vulnerable records, as he had with Blackboard. "I was a little stupider in the 10th grade," he says of his earlier explorations.

When WIRED reached out to Blackboard and Follett, Follett's senior vice president of technology George Gatsis expressed his thanks to Demirkapi for helping the company identify its bugs, which he says were fixed by July of 2018. "We were happy to work with Bill and grateful he was wiling to work through those things with us," Gatsis says. But Gatsis also claimed that even with the security flaws he exploited, Demirkapi could never have accessed Follett data other than his own. Demirkapi counters that he "100 percent had access to other people’s data," and says he even showed Follett's engineers the password of the friend who had let him access his information.

Blackboard also thanked Demirkapi, but argued that based on its analysis no one else had accessed those records through the vulnerability he exposed. "We commend Bill Demirkapi for bringing these vulnerabilities to our attention and for striving to be part of a solution to improve our products' security and protect our client’s personal information," reads a statement from a Blackboard spokesperson. "We have addressed several issues that were brought to our attention by Mr. Demirkapi and have no indication that these vulnerabilities were exploited or that any clients’ personal information was accessed by Mr. Demirkapi or any other unauthorized party.

Advanced Persistent Teen

Demirkapi says he started digging up the two companies' security flaws out of a combination of teenage boredom and an ambition to learn more about cybersecurity and web-based hacking. "I have a passion to, I guess, break things," Demirkapi says. "I really wanted to learn about web application testing, so I thought, well, how cool would it be to test on my own school’s grading system?"

Demirkapi notes that, unlike Ferris Bueller, he never actually tried to change students' grades. which would have required a deeper level of access to Blackboard's network. He did, in a separate incident, exploit flaws in a

college admission software to change his admission status to "accepted" in the database of Worcester Polytechnic Institute, a college he had applied to. A spokesperson for the college said that change alone wouldn't have been enough to admit him.

After Demirkapi began to find bugs in Blackboard and Follett's software, he says he struggled to get the companies to take him seriously. In the winter of 2016, he initially tried to contact Follett by asking his school's director of technology to contact the company on his behalf. But as Demirkapi remembers it, she told him the company had dismissed his concerns. He says he later sent messages himself to Blackboard and Follett via email and Follette's contact page. Blackboard initially thanked him for his note and said it would investigate, but didn't follow up. Follett ignored him altogether.

So a few months later, Demirkapi took a more typical approach for a juvenile hacker. Among Follett's bugs, he found that could add a "group resource" to his school's account, a file that would be available to all users and, more importantly for Demirkapi, that would trigger a push notification with the resource's name to everyone in his school district who had Follett's Aspen app installed. Demirkapi sent a message reading "Hello from Bill Demirkapi :)" out to thousands of parents, teachers, and students.

That stunt got him suspended from school for two days. "It was really immature of me to do that, but I didn’t know any other way to get in touch with a company that wasn’t open to contact," Demirkapi says.

If It Weren't for That Meddling Kid

Over the course 2018, after Demirkapi enlisted the help of his school district's director of technology and Carnegie Mellon's CERT Coordination Center, he says the companies finally began to listen. With Blackboard, whose sensitive data he had accessed in the process of testing the software's security, he worked out a contract that stated the company wouldn't sue him, and in return he'd keep the company's vulnerabilities secret until they were fixed—after refusing an initial draft in which Blackboard tried to prevent him from telling anyone even after the patches went through.

Even now that both companies have fixed the software flaws Demirkapi found, he says that his work should worry anyone who cares about the security of student data. "It doesn't seem like there's any interest in this from the security field, because the incentives just aren't very high," he says, pointing out that neither Blackboard nor Follett has a bug bounty program for rewarding security researchers who find and their vulnerabilities. "These companies say they're secure, that they do audits, but don't take the necessary steps to protect themselves from threats."

Some months after his Blackboard vulnerability disclosures, Demirkapi noticed that Blackboard had posted a job opening for a new chief information security officer. Demirkapi jokes that he briefly considered applying. Instead, he's going to try college.