Cobalt

CASE STUDY

PowerSchool Leverages Cobalt AI & LLM Pentesting to Secure Their Learning Assistant

PowerSchool Launches PowerBuddy, “Responsible AI for Everyone in Education”

THE CHALLENGE

PowerSchool created PowerBuddy, an AI assistant that delivers personalized insights, fosters engagement, and creates a supportive environment for every step of the educational journey. After developing PowerBuddy it became clear that the introduction of AI and LLMs in their software also introduced new attack vectors that extend well beyond traditional application security. PowerSchool’s product team recognized that security and safety would be a key requirement for a successful launch. Facing the challenge of safely and securely introducing AI-powered features into a suite of software used by millions of students worldwide, PowerSchool started their search for an offensive security provider to ensure PowerBuddy satisfied the concerns of students and educators and was safe to use.

THE SOLUTION

PowerSchool needed a partner with expertise in testing LLM applications. During their search, they focused on a list of requirements ranging from what type of methodology the pentesters followed to whether or not the pentesters could credibly execute real-world attack scenarios. This search led PowerSchool to Cobalt.

PowerSchool

ABOUT CUSTOMER

PowerSchool is a leading provider of cloud-based software for K-12 education in North America. Its mission is to empower educators, administrators, and families to ensure personalized education for every student journey. PowerSchool offers end-to-end product clouds that connect the central office to the classroom to the home with award-winning products including Schoology Learning and Naviance CCLR, so school districts can securely manage student data, enrollment, attendance, grades, instruction, assessments, human resources, talent, professional development, special education, data analytics and insights, communications, and college and career readiness. PowerSchool supports over 60 million students in more than 90 countries and over 18,000 customers, including more than 90 of the top 100 districts by student enrollment in the United States.

INDUSTRY

Software Development: EdTech

HEADQUARTERS

Folsom, CA, USA

SIZE

3000+ employees

COBALT SERVICES

AI & LLM Pentesting

BY THE NUMBERS

8 issues fixed, including preventing the generation of inappropriate content about human reproduction prompted by young students

“There is a lot of snake oil out there. We loved that Cobalt was the real thing and actually knew what they were talking about. They were the first pentesting solution that presented us with a clear methodology on AI and LLM applications.”

MISHKA MCCOWAN, CHIEF INFORMATION SECURITY OFFICER AT POWERSCHOOL

"There is a lot of snake oil out there. We loved that Cobalt was the real thing and actually knew what they were talking about. They were the first pentesting solution that presented us with a clear methodology on AI and LLM applications," says Mishka McCowan, Chief Information Security Officer at PowerSchool. Cobalt applied a comprehensive methodology for testing LLM applications, aligned with OWASP principles, combining manual assessments and advanced techniques to uncover vulnerabilities such as prompt injection, model denial of service, and sensitive information disclosure. The testers also evaluated application logic and security configurations to ensure robust protection, ensuring PowerBuddy was secure and user-friendly for its user base of students and teachers.

THE OUTCOME

Cobalt and PowerSchool together developed a plan to perform a comprehensive assessment of PowerBuddy in order to focus on both vulnerabilities and safety in alignment with the company's policies and expectations. During testing, Cobalt identified that a 5th grade student could generate inappropriate content by prompting PowerBuddy to change the topic from assigned schoolwork to human reproduction. PowerBuddy responded by providing detailed information about the human reproduction system along with YouTube videos on the topic. While not a traditional security vulnerability, this was deemed a critical issue due to the mature nature of the content that could be provided to a young student. PowerSchool updated PowerBuddy to address the issue and reorient students to appropriate topics.

In 2024, PowerSchool launched PowerBuddy to great fanfare at their user conference, EDGE. Completing comprehensive pentesting beforehand allowed PowerSchool to remediate vulnerabilities ahead of time and ensure that students were able to use PowerBuddy as intended. "This gave us the confidence to know our product was secure and allowed us to talk more about the features rather than answer security questions," says McCowan.

Looking ahead, PowerSchool is committed to regularly pentest new AI features with Cobalt. "AI security isn't a one and done process. Continuous testing is essential to stay ahead of evolving risks, and Cobalt's expertise makes them the ideal partner for this ongoing effort," concludes McCowan.

"AI security isn't a one and done process. Continuous testing is essential to stay ahead of evolving risks, and Cobalt's expertise makes them the ideal partner for this ongoing effort."

MISHKA MCCOWAN,
CHIEF INFORMATION SECURITY OFFICER AT POWERSCHOOL

To learn more about what Cobalt can do for your organization, visit www.cobalt.io/get-started