Success Story:

ControlScan Penetration Testing Reinforces Differentiation of QuickSilk's CMS Platform

Incidents of cyber theft are growing exponentially as bad actors hack websites looking to steal financial data and other sensitive information. Cyber criminals execute unauthorized code, launch malicious attacks, vandalize websites and generally disrupt a website owner's online presence. These attacks can significantly damage a company's brand and reputation, as well as inflict real financial damage and liability.

Software-as-a-Service (SaaS) company QuickSilk offers a secure content management system (CMS) that enables enterprise grade website management, without sacrificing ease-of-use and affordability. The secure technologies and processes behind the QuickSilk CMS are one of its greatest customer benefits, given the frequency and magnitude of today's website security threats and the fact that leading open source CMS providers have failed to make security a priority.

The Challenge: Proving Out a Security-First Business Model

From the very beginning, QuickSilk has considered data security integral to a properly functioning website. After all, its clients are putting their information out there for the world to see, so they need to be able to trust that they and their site visitors can securely interact with their website. Furthermore, QuickSilk must ensure that its nascent CMS platform, in which the company has already invested more than 90 person years of development, doesn't have inherent security risks that make it an easy target for cybercriminals.

"We built the QuickSilk CMS from the ground up, incorporating a multi-layered security architecture," said Garry Brownrigg, QuickSilk CEO and Founder. "Security risk is the open source CMS community's Achilles heel, so we worked to proactively address that risk throughout the process, while maintaining the ease-of-use and affordability of our platform."

The biggest concern, however, has been whether prospective clients and investors would accept the company's security-specific value proposition. Would the company be able to gain traction in the marketplace without external validation of its security-related claims?

> "Security Risk is the open source CMS community's Achilles heel, so we worked to proactively address that risk throughout the process..." ~ Gary Brownrigg, QuickSilk

The Solution: Independently Conducted Security Penetration Testing

QuickSilk needed a comprehensive, third-party review that would prove out the confidence it had in its CMS platform's security. Brownrigg had already been talking with various companies—including ControlScan—about PCI compliance assessments, so the topic of penetration testing was a natural progression.

"Our ControlScan contact took the time to understand our business, worked to develop a relationship based on our needs and timing, and pulled in consulting team resources to ensure everyone was in alignment," said Brownrigg. "The other vendors we spoke with treated us as nothing more than a number. Relationships matter!"

Penetration tests are conducted by highly credentialed ethical hackers. Leveraging their expertise and a bevy of tools, these information security experts seek out and exploit security vulnerabilities to see just how broad and deep they can reach into the network or application. When the test concludes, the client receives a report that details the security vulnerabilities that were discovered and their level of severity.

The Engagement: Testing, Reporting and Re-Testing

QuickSilk opted for External Penetration Testing of its Internet-facing web SaaS application. As part of its ControlScan engagement, QuickSilk would undergo two tests in total: 1) An initial test to discover all vulnerabilities within the agreed-upon scope, and 2) A remediation test to ensure that QuickSilk had effectively remedied the higher-risk vulnerabilities found during the initial test.

Upon completion of the initial test, ControlScan provided QuickSilk with a detailed report, reviewing the technical findings with them and recommending that they take a prioritized approach to remediation. The good news was that the QuickSilk environment had no critical vulnerabilities and only three high-level vulnerabilities, which were immediately remediated.

"According to our testers, QuickSilk did a great job with security best practices such as username and password complexity restrictions and requirements," said Marc Punzirudu, Vice President of Security Consulting Services, ControlScan. "Other areas they excelled in included output encoding and configuration management for their web server."

The Result: Confidence in a Strong Security Posture

The ControlScan penetration testing engagement reinforced QuickSilk's confidence that overall, they are on a secure path with their product development efforts. At the same time, it provided visibility into specific areas of the CMS that allowed the company to further strengthen its platform.

"Penetration tests make use of the latest methods and tools for exploiting a network or an application's vulnerabilities, so they're ideal for finding issues internal developers may have overlooked," said Punzirudu. "It's important to undergo these point-in-time security tests on a regular basis, because the security threat landscape isn't static and neither, of course, is the everyday business environment."

"Helping clients maintain a strong security posture is a sustainable differentiator for QuickSilk," said Brownrigg. "It's a position we will continue to reinforce through our own development efforts and in conjunction with multi-faceted, point-in-time security assessments."

About ControlScan

ControlScan managed security and compliance solutions help secure IT networks and protect payment card data. Partner with us for easy, cost-effective access to the expertise, technologies and services that keep cyber criminals and data thieves at bay. We've got your back with highly-credentialed cybersecurity and compliance experts, 24/7 managed detection and response, advanced endpoint protection, managed UTM firewall, ASV vulnerability scanning, PCI Qualified Security Assessments, security penetration testing, HIPAA assessments and much more.