cyberflexx

Case Study

Situation

In mid-2023, BaseLinker, a leading provider of an all-in-one eCommerce management system, engaged our cybersecurity team to conduct a comprehensive web penetration testing (Web PenTest) of their platform. Despite having been tested multiple times in the past by other companies, BaseLinker sought a fresh perspective to identify and address any potential vulnerabilities that might have been overlooked, thereby enhancing the security posture of their system.

Challenge

With over 800 integrations, the challenge was substantial. From previous experience in the eCommerce sector, our team understands that securing such platforms from cyber threats can be more involved than in other sectors. The need to balance the liberal sharing of information with the requirement to protect valuable customer and business data calls for a nuanced and segmented approach to risk.

Organization · BaseLinker

Industry · eCommerce

Challenge · Conducting a thorough Web PenTest on a live production environment for a platform with over 800 integrations, ensuring the security of customer and business data.

Solution · Our cybersecurity team executed a comprehensive Web PenTest, identifying overlooked vulnerabilities and providing actionable recommendations for improvement.

Result · The security of BaseLinker's platform has been significantly improved, with previously omitted vulnerabilities addressed, enhancing the protection of its eCommerce operations.

Solution

Our cybersecurity team designed a comprehensive Web PenTest strategy, tailored to BaseLinker's unique needs. The testing process was thorough, covering all aspects of the platform, and was carried out on the live production environment to truly simulate a potential attacker's perspective.

The Web PenTest identified several areas for improvement that had been missed in previous tests conducted by other companies. These included vulnerabilities related to access control, potential disclosure of sensitive information, script migration, and potential privilege escalation. Specific vulnerabilities cannot be disclosed due to confidentiality, but each of these areas represented a potential risk that needed to be addressed.

Our team provided BaseLinker with a detailed report outlining these general areas of concern and offering actionable recommendations for enhancing their platform's security. The report also included potential countermeasures and best practices to prevent similar vulnerabilities in the future.

Result

Following the Web PenTest, BaseLinker took immediate action to address the identified vulnerabilities. The result is a platform that is significantly more secure, providing peace of mind for BaseLinker and its users. The successful project has further strengthened the trust between BaseLinker and its customers, demonstrating BaseLinker's commitment to maintaining the highest standards of security. The fact that our team was able to identify vulnerabilities that had been overlooked in previous tests conducted by other companies speaks to the excellence of our services.

Vulnerabilities by OWASP Category and Risk Level

	Low	Medium	High	Critical	
A1	0	0	3	1	Broken Access Control
A2	0	1	0	1	Cryptographic Failures
A4	2	0	2	0	Injection
A6	2	1	0	0	Security Misconfiguration
A7	2	1	0	0	Identification and Authentication Failures
A8	0	0	0	1	Software and Data Integrity Failures
A9	1	0	0	0	Security Design
A10	2	0	0	0	Security Logging and Monitoring Failures

WARSAW OFFICE
Cyberflex sp. z o.o.
Plac Bankowy 2
00-095 Warszawa

LET'S TALK

contact@cyberflexx.com
+48 571 341 471

cyberflexx