



16 May 2023

In February 2023 Z-Labs was contracted by Dipolar Pty Ltd to conduct a penetration testing of the Web Survey Creator application. The scope of testing included all the functionality available to unauthenticated and authenticated users. To make sure that the whole attack surface was covered and all critical parts of the Web Survey Creator application were sufficiently tested to industry guidelines, the OWASP Application Security Verification Standard was followed. Specifically, the testing included but was not limited to following areas:

- 1) It was verified that **Authentication and Session Management** subsystems are securely implemented and can't be bypassed, and that session can't be hijacked.
- 2) In an effort to confirm correctness of **Authorization and Permissions** subsystems various tests were performed to make sure that it is not possible to escalate privileges or to access functionality and/or resources only available for higher privileged users.
- 3) **Malicious Input Handling**: all discovered endpoints were thoroughly tested against various forms of server-side content injection issues (SQL, XXE, LDAP, XML, etc.). Also testing for client-side content injection was performed (XSS, HTML injection, JS script inclusion, response splitting, etc.).
- 4) **Risky Functionality and Business Logic**: application-specific logic was tested to make sure that it can't be abused or circumvented.
- 5) **Cryptography** is used correctly and does not use insecure/obsolete protocols and crypto primitives.

Z-Labs acknowledges that all high and medium risk issues identified during the testing were properly mitigated by Dipolar which was confirmed during a separate retesting phase.

Sincerely,

Mariusz Ziulek  
Chief Executive Officer  
Z-Labs, Software Security Labs