



To

January 12th, 2017

Idomoo

Subject: Web Application System Penetration Test

1. Avnet has been requested by Idomoo to conduct a penetration test of the Idomoo's **web application system** for the purpose of evaluating the quality of its information security level and identifying the main risks that exist in the Idomoo's web application system and address them so as to minimize the chances of information leaks and/or damage to the systems and business.
2. The penetration test was carried out during December 2016 and has been performed according to **OWASP** testing guide and Avnet's methodology, and included investigation of application weaknesses and vulnerabilities in the code, such as SQL injection, sensitive information leakage, session hijacking, logic flaws, authentication bypassing, defacement attempts, and more.
3. The penetration test has been performed through a series of predefined **entry points** given by Idomoo:
 - Personalized videos management website – pv.idomoo.com (including Landing Page)
 - API for video generation – [REDACTED]
 - SFTP – [REDACTED]
4. The conclusive statement of the **preliminary** penetration test which was conducted on the Idomoo's web application system is that its security level at that point in time is **unsatisfactory** and demands urgent mitigation of a high level exposure found.



5. Following the preliminary test results, a **retest** has been performed, which focused on testing the findings from the preliminary test and the changes made by Idomoo in regard to those findings. The retest took place on January 2017 and its results showed that all exposures were **remediated** and do not exist anymore.

Sincerely yours,

Boris Iskovsky

Project Manager

Roni Bachar

VP Cyber Technologies

**Avnet Information
Security Ltd.**