Farfalline
Security Assessment

Technical Report

Prepared for: Istituto Farfallino
Performed by: Alessandro Molari, Giacomo Mantani

Date: 8 Feb 2018

Contents

Introduction **3**

Assets involved 3

Context & Scope 3

Introduction

The following document was written as a reference for the security assessment done by Alessandro Molari, Giacomo Mantani towards Istituto Farfallino on 8 Feb 2018.

Assets involved

The following assets were involved during the testing activities:

- **www.farfalline.it**: Main website
- **www.join.farfalline.it**: Meeting section of the website

Context & Scope

This audit has been carried out at the request of Istituto Farfallino. Its goal was to evaluate the security of the assets under test, as described in section: Assets involved.

The team has done a **Black-Box Vulnerability Assessment** and **Penetration Test**. No prior knowledge of a company network is known except the endpoints mentioned above. In essence an example of this is when an external web based test is to be carried out and only the details of a website URL or IP address is supplied to the testing team. It would be their role to attempt to break into the company website or network. This would equate to an external attack carried out by a malicious hacker.

The study focuses on main **Web Vulnerabilities** as described in **OWASP Web Application Penetration Testing Methodology**.

In particular the following testing areas have been considered:

- Configuration and Deployment Management Testing
- Identity Management Testing
- Authentication Testing
- Authorization Testing
- Session Management Testing
- Input Validation Testing
- Error Handling Testing
- Cryptography Testing

- Business Logic Testing
- Client Side Testing