Farfalline
Security Assessment

Technical Report

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

Date: 8 Feb 2018

Contents

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 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

Strength of Test

The tests were executed in Safe Check. Doing so there is no possibilities to disrupt the services during the vulnerability scans. However, this safer approach entails some risk and a lower level of strength: not all exploit were tested nor DoS or DDoS attacks were performed. Instead, external attackers would try to break into the system without having to worry about what can be damaged.

Approach

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.

Threat

A threat is a potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. In this particular scenario we try to anticipate and overcome problems from malicious agents (both human and software) intentional or unintentional.

Information Gathering

Passive Intelligence

Active Intelligence

Corporate Intelligence

Personnel Intelligence