EXTRACT from the Penetration Test on EspoCRM for Ukraine operation.

EXECUTIVE SUMMARY

As a result of the test, we have concluded that although the server itself is protected against external attacks through the https://ukrainecrm.ifrc.org web application, or other services, there are some security issues that might affect the web site's users. We must conclude that most of the findings found during the previously performed test were fixed, except the 2 low risk issues. **On top of the last assessment, we found a stored XXS, which received a Moderate risk rating.**

Any user can add a dashlet to their dashboard. Arbitrary JavaScript code can be inserted into the URL textbox at the Iframe dashlet option. After applying the URL, the server stores the inserted JavaScript code. Every time the user visits its dashboard, the code gets executed. This finding received a moderate risk-rating.

During the test we observed that the username details are captured in cookie. Username is identity of the end users of the application and used to uniquely identify the user. Setting up the username details in the cookie header is not the best practice. This finding received a low-risk rating.

Finally, the application is missing the "Content-Security-Policy", "Strict-Transport-Security", "X-Frame-Options" security headers and the "X-Content-Type" header. This finding received a low-risk rating.

Table of new findings:

Ref.	Finding	Risk rating
1.	Stored XXS at Iframe dashlet option	Moderate

Table of previous findings and its states:

Ref.	Finding	Risk rating	Current state
1.	Username details are captured in cookie attribute	Low	Not Fixed
2.	Missing security headers	Low	Not Fixed

GOAL OF THE TEST

The goal of the assessment is to test the security of The International Federation of Red Cross and Red Crescent Societies (hereinafter IFRC or Client) given web application, with gray-box approach. The penetration test imitates a real attack in a sense that we use the tools and techniques a real-world adversary would most probably use. Our assessment reveals the flaws that can be exploited to gain access to sensitive information, to elevate privileges or gain system level access to the infrastructure running the application.

This resulting document gives a high-level security overview of the target application and servers as well as detailed write-ups, possible impact, and recommended remediation steps for each finding.

SCOPE OF THE TEST

The scope of the test covers the web application https://ukrainecrm.ifrc.org/ with 10 different roles, its external infrastructure and other services found on the server.

TEST CIRCUMSTANCES

The tests were performed remotely from the Internet via our external gateways (IP addresses: 80.249.164.232 and 80.249.164.233).

TEST LIMITATIONS

During the assessment we did not experience any technical or other obstacle and could complete the tests successfully.

TEST LOCATION

We conducted the tests remotely from the Internet.

DURATION OF THE TEST

The tests were carried out between 12-09-2022 and 19-09-2022.

CLAUSE

During the security tests, we took due care and diligence and acted upon the authorization of the Client. The assessment only covers the testing – carried out according to those written in the related methodology description – of the IT systems and security requirements featured in the offer and agreement.

We would like to draw the attention of the Client to the fact that the test is a kind of snapshot which is suitable for the static evaluation of the status of the IT system and does not track the changes made after project termination (system changes, recently discovered attack methods, vulnerabilities). During the tests, it is not our responsibility to examine the functional conformity of the systems under the scope.

It is our responsibility to draw the attention of the Client to the risks, the dangers they bear and the applicable best-practices for the security improvement of the networks, systems and applications of the Client. Client's responsibility covers the evaluation of the identified risks in the light of their business goals, costs and profit and the existing controls.

Furthermore, the management of the identified risks and their reduction to an acceptable level is also the responsibility of the Client. Throughout this process, Client can decide whether this goal is achieved through the suggestions made by us or any other means.

We would like to note that due to the time dedicated to the security testing being limited, it is impossible to identify every vulnerability. A malicious attacker (or group) not limited in time and tools and with adequate financial resources could succeed in bypassing the security measures.