Call identifier: H2020-ICT-2016 - **Grant agreement no**: **732907**

Topic: ICT-18-2016 - Big data PPP: privacy-preserving big data technologies

Deliverable 9.4

Public Hacking Challenge Results Report

Due date of delivery: December 30th, 2019

Actual submission date: December 31th, 2019

Start of the project: 1st November 2016
Ending Date: 31st December 2019

Partner responsible for this deliverable: CNR

Version: 1.5

Document Classification

Title	Public Hacking Challenge Results Report
Deliverable	D9.4
Reporting Period	M36
Authors	Enrico Cambiaso (CNR), Ivan Vaccari (CNR), Elisabetta Punta (CNR), Maurizio Aiello (CNR)
Reviewers	Rudolf Mayer (SBA), Mirko De Maldé (Lynkeus)
Work Package	WP9
Security	Public
Nature	Report
Keyword(s)	Cyber-security; vulnerability assessment; penetration testing; hacking challenge.

Document History

Name	Remark	Version	Date
Ivan Vaccari (CNR)	First Version	1.0	December 3st, 2019
Enrico Cambiaso, Maurizio Aiello (CNR)	Revised version	1.1	December 6th, 2019
Enrico Cambiaso (CNR)	Revised version after internal review	1.2	December 23th, 2019
Rudolf Mayer (SBA)	Amendments and suggestions	1.3	December 23th, 2019
Enrico Cambiaso (CNR)	Revised version	1.4	December 23th, 2019
Mirko De Maldé (Lynkeus)	Final version	1.5	December 30th, 2019

List of Contributors

Name	Affiliation
Enrico Cambiaso	CNR
Ivan Vaccari	CNR
Elisabetta Punta	CNR
Maurizio Aiello	CNR
Rudolf Mayer	SBA
Mirko De Maldé	Lynkeus

Abstract

This report describes the public hacking challenge of the MHMD project, reporting organization information, participants enrolment and obtained results. The organized challenge aimed to allow ethical hackers the possibility of performing security and privacy tests on the developed platform, identifying potential vulnerabilities in the system and allow project partners to fix these vulnerabilities and make more secure and reliable the MHMD platform. As the platform will be potentially used to handle highly sensitive data, security and privacy testing activities are a very important and fundamental for the success of the project. Furthermore, in order to involve the participants more closely, public hacking challenge activities were carried out and a cash prize was associated on the basis of the vulnerabilities identified by the participants.

1 Adopted approach

The first phase was the decision of the type of competition and the prize. In agreement with the other project partners, it was decided to leave the online platform publicly available and accessible for a specific time period, giving ethical hackers full access to the functionalities of the system, and permission to run security tests, in order to perform all the appropriate security testing activities. In particular, the document reported in Appendix A, including information and instruction on how to join the challenge, along with sample videos describing the usage of the platform, were shared with the participants. The following activities were prohibited to the participants:

- Denial of service attack against each component of the system: not allowed in order to make the system unavailable for other participants
- Exploit vulnerabilities related to the `SpongyCastle` library included in the MHMD mobile app: not allowed since this is a known vulnerability already identified and evaluated by Digi.me as non-critical to the Digi.me SDK-s security and thus not fixed for the context of the challenge
- Inject out-of-the-scope malware/worms inside of the system: not allowed since it may interfere with the activities of other participants
- Target or exploit systems outside of the scope reported above: not allowed to protect external systems
- Directly target other participants to the challenge: not allowed to protect the other participants to the challenge

At the end of the penetration testing and privacy breaking activities, the ethical hackers had to deliver a report of all the activities and the related vulnerabilities identified.

After the selection of the competition, the consortium has decided for a prize of 5,000 Euro*, raised from other sources than from project funding*, assigned the participants based on the criticality of vulnerabilities discovered. Cash compensation is proportional to the criticality of the identified vulnerability.

During the challenge period support to participants has been provided, via a dedicated mailing group including both organizers and technical teams.

Also, dissemination activities publicized the challenge on the project website, social networks and via email, in order to attract ethical hackers. For this reason, a special section (see Figure 1), was created on the MHMD project website, allowing interested participants to register a dedicated newsletter and subsequently receive information on the public hacking challenge.

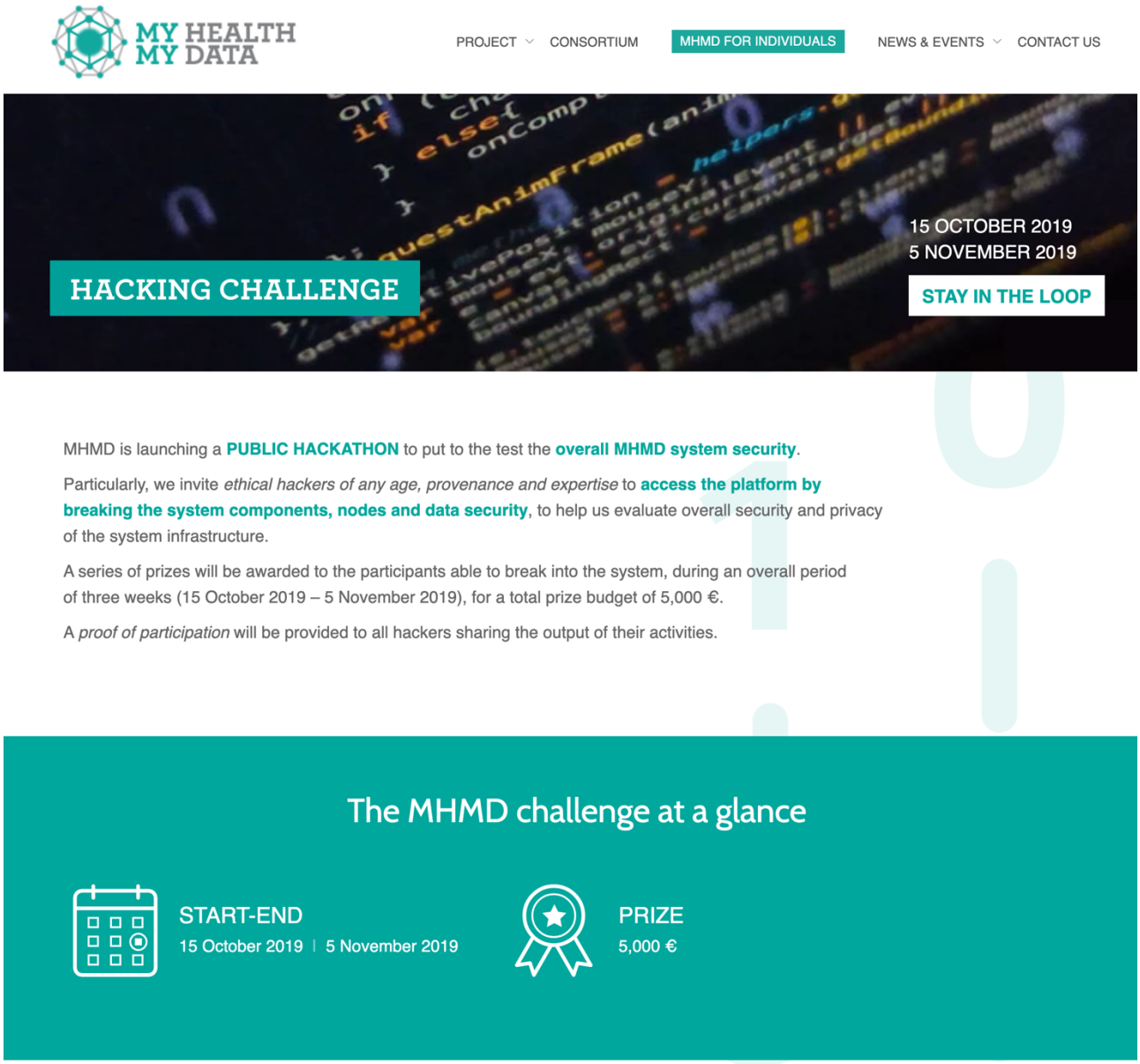

Figure 1 - Public hacking challenge portal

2 Enrolled participants

During the development of the task the expected timeline shifted due to development and technical reasons. In particular, the initial timeline expected to start the challenge in April 2019 and to last 3 months, as agreed within the consortium. The beginning of the challenge was then however first postponed to July 1st, 2019. The challenge was in this renewed timeline expected to last until end of August 2019. Advertisement of the challenge with consequent enrollment of the participants was referring to this expected timeline. This date, due to delays in finalizing the MHMD system to be tested, shifted further back, to finally start the challenge in October 2019, and to last around a month. During the challenge, due to technical and scalability reasons, the number of concurrent participants had to be limited to 2. All the subscribers were contacted in batches, in answer to their interest, to inform them of the shift. After such contact, 2 participants, kept anonymous in this report, to respect their privacy, fully participated in the public hacking challenge. The small number is

due to a delay in the development of the platform and to the shift in time period from the summer/low-load period to the after-summer one. In addition, the scope of the challenge being broad, with possibility to test a large amount of aspects (e.g. network vulnerabilities, privacy breaking, system flows), representing a (supposed) high effort expected from the participants, the challenge was not easily to complete in the given timeframe. Nevertheless, dedicated telephone conferences were done, introducing the system to the 2 hacking teams , asking for the sign of an NDA document, and describing the input provided and expected outputs.

3 Results

3.1 User 1 output

Report of the Public Hacking Challenge	MHMD-H2020-ICT-2016 (732907)

MY HEALTH MY DATA

Name:___ __Eleni_____ Surname: ___Trouva_____

Profession: ___Senior Engineer_____ Email: ___eleni.trouva@intrasoft-intl.com__

I hereby declare that any vulnerability related to the system will not be released to third parties.
I also accept the unquestionable judgement of the hacking challenge committee.

Date: ___15/11/2019_____ Sign: _____Eleni Trouva_____

Identified vulnerabilities:

#	Discovery date	Affected component	Adopted tools	Remediations
1	11/11/2019	UI server	robtext, knock.py	Consider moving the service to dedicated servers as sibling domains exist (see output details in the notes section).
2	11/11/2019	Catalogue	robtext, knock.py	Consider moving the service to dedicated servers as sibling domains are too many (see output details in the notes section).
3	11/11/2019	UI server	dirb	.htaccess files should be protected from all external access (see output details in the notes section).

1

3.2 User 2 output

Report of the Public Hacking Challenge	MHMD-H2020-ICT-2016 (732907)

MY HEALTH MY DATA

Name: [redacted] Surname: [redacted]

Profession: [redacted] Email: [redacted]

I hereby declare that any vulnerability related to the system will not be released to third parties.
I also accept the unquestionable judgement of the hacking challenge committee.

Date: 16th November 2019 Sign: [redacted]

Identified vulnerabilities:

#	Discovery date	Affected component	Adopted tools	Remediations
1	12/11/2019	MHMD PORTAL	BURP SCANNER WITH PROXY	BANNER GRABBING VULNERABICITY for catalogue checkout
2	12/11/2019	CATALOGUE	BURP SCANNER	BANNER GRABBING VULN. at GetView JSON
3	12/11/2019	CATALOGUE	BURP SCANNER WITH PROXY	Access token always the same for all accounts.

Notes:

I was only able to scan the MHMD Portal for vulnerabilities due to limited time and little documentation regarding the Blockchain access. I have found the web app running at mhmd-demo.hwcomms.com to be secure and resistant to my attacks. I was only able to find low-risk vulnerabilities.

1

3.3 Output analysis

At the end of the public challenge, the project security team elaborated the participants' reports and assigned a level of criticality and severity to the vulnerabilities found. The vulnerabilities and their results are shown in Table 1, where the assigned severity is considered as the “minimum value” between the impact and the probability.

Participant	Vuln. #	Affected component	Adopted tools	Remediations	Impact	Probab.	Assigned Severity
USER 1	1	UI server	robtext, knock.py	Consider moving the service to dedicated servers as sibling domains exist.	Medium	Low	Low
USER 1	2	Catalogue	robtext, knock.py	Consider moving the service to dedicated servers as sibling domains are too many.	Medium	Low	Low
USER 1	3	UI server	dirb	.htaccess files should be protected from all external access.	Medium	High	Medium
USER 2	1	MHMD portal	Burp scanner with proxy	Banner grabbing vulnerability for catalogue checkout.	High	Medium	Medium
USER 2	2	Catalogue	Burp scanner	Banner grabbing vulnerability at getview json.	High	Medium	Medium
USER 2	3	Catalogue	Burp scanner with proxy	Access token always the same for all the accounts.	High	High	High

Table 1 - Results of the hacking challenge

The identified vulnerabilities were analyzed and processed by the platform development team and then addressed further elevating the platform’s security level.

4 Conclusions

In this deliverable, we have reported details on the organization of the public hacking challenge of the MHMD project, aimed to allow ethical hackers the possibility to run security and privacy tests against the implemented system. We have described the approach that we have followed and the enrolment activities we have accomplished. Due to the shift of the beginning of the challenge, a limited number of participants joined the event. Nevertheless, the issues identified are considered highly relevant for the platform development. In virtue of this, they were analysed and processed by the development team and addressed them to make the system more secure.

Appendix A – Guidelines for the participants of the public hacking challenge

In the following, we report the document shared with the participants to the public hacking challenge.

Call identifier: H2020-ICT-2016 - **Grant agreement no**: **732907**

Topic: ICT-18-2016 - Big data PPP: privacy-preserving big data technologies

Guidelines for the participants of the Public Hacking Challenge

Start of the project: 1st November 2016
Ending Date: 31st October 2019

Partners responsible for this document: CNR, SBA

Version: 3.4

Document Classification: Public

Title	**Guidelines for the participants of the Public Hacking Challenge**
Authors	Enrico Cambiaso, Ivan Vaccari, Rudolf Mayer
Work Package	9
Nature	Public

Document History

Name	**Remark**	**Version**	**Date**
CNR	First Version	1.0	Sept 20th, 2019
CNR, SBA	Second Version	2.0	Sept 23th, 2019
CNR	Third.4 Version	3.4	Oct 15th, 2019

List of Contributors

Name	**Affiliation**
Ivan Vaccari	CNR
Enrico Cambiaso	CNR
Rudolf Mayer	SBA

5 General information

5.1 The MHMD project (LYNKEUS)

MHMD is EU-funded project currently developing the first **open biomedical information network centred on the connection between individuals, healthcare organisations, research centres and industries**, where de-identified clinical datasets and individual data on private clouds can be shared among diverse constituencies through a blockchain-based and smart contracts-mediated transaction system, in exchange for value, for the benefit of medical care, research and innovation. The network implements trust-based and value-based relationships and strict protection of data owners' identity, privacy and preferences. Strong, multi-tier **de-identification and encryption solutions** are in place to secure and de-associate data from subjects' identities, and private **blockchain ledger and smart contracts** controls data transactions and manages consent from individual users and supports direct data access requests. Meanwhile **personal data accounts (PDA)**, i.e., individual clouds managed by mobile device, allow setting and managing articulated and dynamic consent according to personal preferences. In this way, **patients** are allowed to take control over the use of their data and will be able to fully leverage the value of their clinical information for personal use. **Researchers in public or private centers**, on the other side, will have a new wealth of biomedical records available for their work. Through a dedicated **data catalogue** featuring high-level descriptive statistics on encrypted data, they will be able to browse and evaluate all available sources, pick the one of interest, request it and finally downloading the anonymized version of it. In the background registered data are in the meanwhile profiled and classified based on their sensitivity, informational and economic value, and data curation and harmonisation tools, encryption and de-identification technologies are applied for their protection. **Advanced AI and knowledge discovery applications** such as deep learning, medical annotation retrieval engines and patient-specific models for physiological prediction can now also be applied to the discovery of new drugs and devices and to the personalization of treatments. The ultimate frontier of the project is the creation of **a true information marketplace** governed by peer-to-peer relationships, where a constant flux of lawful data exchanges in exchange for services will be fuelling European economy, giving a new boost to scientific research, technological advancement and clinical innovation.

Important notice on the status of the platform for the hacking teams: being an EU-funded project, the current platform is to be considered an alpha prototype meant to provide a proof-of-concept of the usage of different technologies (blockchain, SMPC, anonymisation/pseudonymisation tools, homomorphic encryption, metadata catalogue, etc) for enabling secure sharing of data, data lifecycle management, permission/consent rule enforcement, and data analytics. In such a context, the intended outcome of the hacking challenge is to provide an external assessment of the security of the overall platform and its components, including the communication between different modules.

It is important to keep in mind that some extra features included as "placeholders" in the user interfaces (both mobile and web-based) are not fully deployed, as they are not directly included in the scope of the project but are rather to be intended as potential elements for future development of the platform. At the same time, being not in production mode, but rather developed in a research environment, the performances of the system might vary depending on the number of users, the kind of queries performed, and other factors. For all these reasons, the hacking teams might experience sub-optimal user experience and/or issues and delays in completing the full workflow. To minimise potential issues of this sort, we provided full guidance

for going through the workflow (demo available at: XXX), also indicating queries, keywords, user accounts, etc., to provide the smoother user experience possible while testing the security level of the overall platform.

5.2 Organization contacts

Contacts related to challenge organization are reported in the following ones[1]:

- Enrico Cambiaso: enrico.cambiaso@ieiit.cnr.it
- Rudolf Mayer: rmayer@sba-research.org
- Ivan Vaccari: ivan.vaccari@ieiit.cnr.it

6 Accounts retrieval

In this section we report details on the actions needed to the participants to the challenge in order to retrieve the accounts needed to interact with the MHMD platform. Participants have to send an email to mhmd-challenge@ge.ieiit.cnr.it, with subject "`MHMD – Hacking Challenge – Accounts creation`". As a response, two separate accounts will be provided, referring to hospital and research administrator users, respectively.

Please note that the email address used to access the system may be visible to all the other participants to the challenge. Because of this, temporary email addresses can be adopted.

[1] For any communication, also send the message by adding mhmd-challenge@ge.ieiit.cnr.it in cc to the message.

7 Entry points

By referring to the permission to attack documents, the entry points to test are reported on the following[2].

Component	Base URL	IP address
UI server	https://mhmd-test.hwcomms.com	35.246.50.144
Mobile application MHMD	https://drive.google.com/file/d/1h1g8K_G5rOZa_B4pY5CbxvG3PU6o2Noa/view?usp=sharing	N/A
Catalogue	https://mhmd-central-catalogue.gnubila.fr/catalogue/search/	195.176.241.199
SMPC	dl056.madgik.di.uoa.gr	88.197.53.56
	dl057.madgik.di.uoa.gr	88.197.53.57
	dl058.madgik.di.uoa.gr	88.197.53.58
Blockchain system	http://mhmd1.gnubila.fr:1111 http://185.34.140.227:1111 http://185.34.140.229:1111	185.34.140.215 185.34.140.227 185.34.140.229

In case technical information or malfunctioning of the targeted components, it is possible to contact direct contacts via email mhmd-public-hacking@hwcomms.com and mirko.koscina@be-ys.com, cc mhmd-challenge@ge.ieiit.cnr.it.

API documentation for the UI server is available at https://mhmd-test.hwcomms.com/mhmd/docs/index.html . This also provides details about any pre-existing known issues, and specifies which APIs are in scope for the hacking challenge.

For the individual workflow, you need to download the Digi.me app and from Google Play (MHMD app will prompt for this at the appropriate time), then tap: I have a library and connect with the following details:

- Dropbox email: developers.demo@digi.me
- Dropbox password: `cademo`
- digi.me library password: `demo`

Keywords to be used:

[2] In case different entry points are provided, comparing the main document and permission to attack documents, please only refer to permission to attack documents.

In order to make sure that the studies are correctly completed, we selected specific keywords to be used on the catalogue:

- Regular study: “England” or “Scotland”
- For the second level anonymization: “Obesity”

For SMPC: any keyword (“Scotland” makes it faster) – the SMPC process can take up to 1 hour to provide a result, which will be made available through email (not through the user interface)Latency:

- Normal studies can take up to 15 minutes to get the response, which is provided directly on the User Interface (the study will change from “Pending” to “Ready to be downloaded)
- SMPC studies can take up to 1 hour to be completed, and the response is provided via email, with a link for downloading the results.

7.1 Forbidden activities

In order to test the security of the platform, the following actions are not allowed:

- Denial of service attack against each component of the system
- Exploit vulnerabilities related to the SpongyCastle library included in the MHMD mobile app
- Inject out-of-the-scope malware/worms inside of the system
- Target or exploit systems outside of the scope reported above
- Directly target other participants to the challenge
- Re-identification attack (all data are synthetic)

Any exploitation of related vulnerabilities will be considered as an illicit activity.

8 Output format

Expected output have to be sent via email within November 6th EOB to the mhmd-challenge@ge.ieiit.cnr.it email address. The subject “`MHMD - Hacking Challenge - Submission`” has to be used. A document including the following page has to be attached to the email. The structure of the document is reported in the following page[3], including a table with the following columns:

- **#**: a sequential number (used for internal reference)
- **Discovery date**: the date you discovered the vulnerability
- **Affected component**: the involved component, URL, IP address, etc.
- **Adopted tools**: the operating systems, tools, configuration and environments you used for the discovery, useful in order to reproduce the tests
- **Remediations**: suggestions to fix the identified vulnerability

An additional **Notes** section is available, to include any relevant note, such as information on how to reproduce the tests (external links to videos or other details are welcome).

[3] A Microsoft Word copy of the document can be requested to mhmd-challenge@ge.ieiit.cnr.it.

Any further documentation related to the identified vulnerabilities is welcome.

Name:_____ Surname: _____

Profession: _____ Email: _____

I hereby declare that any vulnerability related to the system will not be released to third parties.
I also accept the unquestionable judgement of the hacking challenge committee.

Date: _____ Sign: _____

Identified vulnerabilities:

#	Discovery date	Affected component	Adopted tools	Remediations

Notes:

_____
_____
_____
_____
_____
_____
_____
_____
_____

9 Submissions evaluation

9.1 Evaluation committee

Evaluation will be accomplished by the following evaluation committee:

- Enrico Cambiaso (Consiglio Nazionale delle Ricerche)
- Ivan Vaccari (Consiglio Nazionale delle Ricerche)
- Rudolf Mayer (SBA Research)
- Mirko De Maldé (Lynkeus)
- Mirko Kocina (Almerys)
- Daniel Essafi (SystemLoco)

By participating to the hacking challenge, participants accept the unquestionable judgement of the evaluation committee. Access to judgement data will not be granted to the participants to the challenge.

9.2 Evaluation metrics

Evaluations will be based on aspects like the following ones:

1. impact of the executed attack on the targeted system and its users
2. reproducibility of the attack (related to explaination on how to reproduce the attack)
3. novelty of the attack (e.g. well-known vs 0-day)
4. requirements of the attack (in terms of costs, software, hardware, etc.)

9.3 Submission requirements

Following submissions will not be considered:

- submission received outside of the expected deadline
- submissions not including the output form reported in Section 8, properly filled in
- submissions filled in languages different from English
- submissions sent through methods different by email, if not requested differently by the evaluation committee

10 Permission to attack documents

Within the end of the hacking challenge, the consortium will provide signed documents by the involved parties, for proving permission to attack the MHMD components.