Journal of Informatics and Vocational Education (JOIVE)
Vol.6, No.1, March 2023, pp. 25~32
ISSN: 2746-7813

Evaluation of Capture The Flag-Based Online Cyber Security Learning Media in Terms of Ethical Hacking and Gamification

Aji Nur Rohman[1], Puspanda Hatta[2], Cucuk Wawan Budiyanto[3]
[1,2,3] Department of Informatics Education, Sebelas Maret University

Article Info

Article history:

Revised Oct 17, 2022
Accepted March 1, 2023

Corresponding Author:

Aji Nur Rohman,
Departement of Informatics Education,
Sebelas Maret University,
Jl Ahmad Yani, no 200,
Pabelan, Kartasura, Surakarta,
Jawa Tengah, 57169, Indonesia.
Email:
ajinurofficial@student.uns.ac.id

ABSTRACT

This study intend to (1) determine the suitability of the components of online learning media for network and computer security to suitability with the ethical hacking process, (2)conduct a comprehensive review of cyber security learning media. This research is a qualitative research with a grounded theory research approach. The data sources of this study include Capture The Flag websites, ethical hacking aspects and gamification aspects. Sampling techniques are carried out using application search strategies based on certain keywords in accordance with the relevance of online applications of cyber security learning media. Data analysis in this study uses qualitative data analysis, as for data analysis techniques that are adjusted to the stages in the study (Perry, Lunde, and Chen 2016). The first thing that is done is to search for research data sources using predetermined keywords. Filtering is carried out on search results so that search results are unique and duplication does not occur. Filtering is carried out to find inappropriate online applications, then removed from the list. Scoring of data that is in accordance with the ethical hacking aspects and gamification aspects. Second, the obstacle experienced in the research process is that there are several obstacles that cannot be accessed due to closed access or developers who do not update the CTF-based cyber security website so that it cannot be run. Third, the maker or owner or developer of this CTF-based cyber security website needs to consider the gamification side in the creation and preparation of this CTF-based cyber security website. This is necessary to increase the interest of participants with the presence of gamification aspects that are implemented.

Keywords: Ethical Hacking, Gamifikasi, *Capture the Flag*

1. INTRODUCTION (10 PT)

With the increasing level of development of the internet, computer security is becoming the main concentration for a business and government. They hope to take advantage of the various advantages that the internet provides but they also worry about the possibility of being "hacked"[1]

Cyber security is an activity or treatment given to protect a system, network, and program from digital attacks. These cyber attacks are usually aimed at accessing, altering or destroying sensitive information and data, extorting money from users or disrupting business processes.

To protect sensitive data and information, a good security system is needed so that it is expected to protect these data and information. The thing that needs to be done to protect existing data and information is to install a computer network security system. This is because network security is a defense system used to protect threats from attacks from outside the network.

After the installation of the security system, security is not immediately guaranteed secure from outside attacks. To further strengthen the defense system, testing is needed to find out how strong the defense system is and if in the test there are loopholes that can still be entered, it can be repaired to improve the security of the system from threats outside the network.

Of course, special skills are needed to be used for testing network security systems, this can use ethical hacking skills how to hack the system yourself. Ethical hacking or also known as penetration test or white hat

hacking, using tools, tricks, and techniques commonly used by hackers, the difference is that ethical hacking is carried out legally with the consent of the target. The main purpose of ethical hacking is to look for system loopholes from the point of view of hackers so that security can be better [2].

The ethichal hacking ability is divided into 5 stages or blocks or sections [2], consisting of:

Reconnaissance, where hackers secretly search for information on the targeted system. Scanning and Enumeration, scanning itself is a common technique used by testers to find open doors of a system. While enumeration is the process of initial attack towards the target to get information from the target machine and actively stay connected. Gaining Access, from here hackers start trying to gain access into the system with the help of tools. Here hackers begin to search and try to get passwords from system machines [2]. Maintaining Access, after being able to enter the system machine, hackers have hacked not only on the system but also on the resources on the machine [2]. Clearing Tracks, after the hacker gets what he wants or has finished hacking then the next stage is to remove his existence from the system that has been hacked (Patil et al., 2018).Sudah ada materi-materi yang yang bisa dipelajari mengenai ethical hacking melalui buku dan video tutorial, dirasa masih belum cukup untuk mengingkatkan kemampuan ethical hacking.

The textbooks used for cyber security learning are already very numerous and various such as CEH, CompTIA, Security+, Cisco Cyberops Course Materials, Linux Security, and others. In addition, material about cyber security can also be obtained or can be obtained in tutorial videos, for example on the UDEMY website, Netacad-InPurchase, Cybrary IT, and others.

In addition to the three learning media above, there is still one alternative solution that can be used to learn and practice cyber security and ethical hacking more freely and fun, namely using online applications for computer and network security learning media devoted to the capture the flag cyber security lesson ([3]. With the existence of cyber security online learning media applications Capture The Flag, it makes it easier to practice cyber security and ethics hacking because it can be accessed anywhere and does not require large costs with the condition of a good internat connection.

In addition, it is discussed in various fields in recent decades such as education, tourism, and services that discuss gamification [4]. According to Deterding[5], characteristics in a thing can be seen in the context of the game using gamification. Gamification itself can be defined as elements of game design in non-game situations to increase players' interest in carrying out complex tasks or achieving certain goals [6].

2. RESEARCH METHOD (10 PT)

In this study, the methodology carried out was based on research references that had been used previously by Rachel Perry, Britt Lunde, Katherine T. Chen [7] with the title An Evaluation of Contraception Mobile Applications for Providers of Family Planning Services. The methodology used is to search according to relevance with the research carried out.

In this study, a methodology with a qualitative approach was used, which has natural characteristics (natural setting) as a direct data source, descriptive, process is more important than the results, analysis in qualitative research tends to be carried out in inductive analysis and meaning is essential.

The research method carried out by the researcher is a reference from a study conducted by Rachel Perry, Britt Lunde, Katherine T. Chen [7]with the title An Evaluation of Contraception Mobile Applications for Providers of Family Planning Services.

Data

This research data is in the form of a collection of online applications related to the research theme, namely regarding the evaluation of capture the flag-based online cyber security learning media in terms of ethical hacking aspects and gamification aspects collected through observation with searches on google search engines, namely search engines that are quite good for now, the results of which are then selected based on keywords that are related and have relevance to elements of cyber security and ethical hacking. The definition of this data refers to research that has been carried out by Rachel Perry, Britt Lunde, Katherine T. Chen [7].

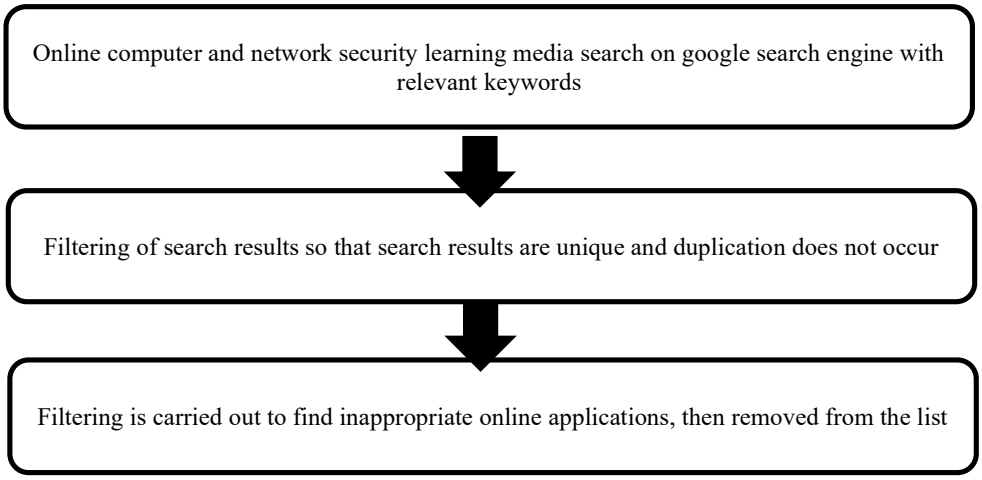
Data Sources

In collecting data sources, it is using diverse and relevant keywords in order to produce complete and valid data for research. In this study, the data source is the online applications of cyber security learning media. The process of collecting this data source refers to research that has been carried out by Rachel Perry, Britt Lunde, Katherine T. Chen [7]

The technique of taking research subjects in this study used an application search strategy based on certain keywords in accordance with the relevance of online applications of cyber security learning [7]. Here are the search keywords used by researchers in this study:

- *Virtual lab cyber security*
- *Cyber security capture the flag*
- *Capture the flag*
- Latihan *Capture The Flag*
- *Virtual lab cyber security for education*
- *Cyber security education*

To find out the data from the data collection sources in this study, it was carried out with the observation stage. Observation is observation through the activity of concentrating attention to an object.



Data Validity

There are several types of data validity tests in qualitative research, one of which is credibility (internal validity), which is used in this study. The test of data credibility or trust in the data of qualitative research results, among others, was carried out by [8]:

1. Extension of observation
   By extension of observations means the researcher returns to the field, makes observations, interviews again with data sources that have ever encountered as well as new ones. In addition, the extension of observations is also carried out during the evaluation stage, so that the resulting evaluation is valid, there is no mistake in giving a score on each aspect studied in cyber security learning media.
2. Increase perseverance
   Increasing perseverance means making more careful and continuous observations. This is done by researchers when summarizing existing search results. Researchers copy the search results from the browser to the word page first, then only then move them one by one according to their respective attributes to Excel so that the data can then be processed properly and easily.
3. Analysis of negative cases
   Negative cases are cases that do not correspond or differ from the results of the study up to a certain moment. This is intended to ensure that no data is mixed or confused with each other.
4. Using reference materials
   What is meant by reference material here is that there are supporters to prove the data that has been found by researchers.
5. Hold a member check
   Member check is the process of checking the data obtained by the researcher to the data provider. The purpose of member check is to find out how far the data obtained is in accordance with what is provided by the data provider.

Data Analysis Techniques

Data analysis in this study uses qualitative data analysis, as for data analysis techniques that are adjusted to the stages in the study[7], are:

1. Correlate cyber security learning media.
2. Description of the evaluation results.

Scoring

After completing the filtering stages and finding the appropriate media with research, the media scoring stage is carried out. In this study, the scoring used refers to: (1) the suitability of the media to the elements in the security audit, (2) conformity with the gamification aspects of a learning media. The scoring rule is 1=exists, 0=none.

3. RESULT (10 PT)

Observation and Filtering

In the first stage of this study, what was carried out was by observation according to what was described in figure 3.2. The observation made is to do a search with predetermined keywords on Google searches with the intention of making it easy to copy searches.

In the next stage, namely the filtering stage, there are several stages described in the previous figure 3.2. After finding data with observation based on keywords, 21 websites were found. The next stage is data filtering.

Stage 1 filtering

Filtering stage 1 is the stage of spending applications that are no longer accessible or no longer online. This is because there are several websites that apply virtual laboratories sometimes do not renew their website licenses so that these websites are no longer accessible. Like IO Netgarage where this website is no longer accessible for web terminals which is the main feature what to look for in this study. Out of a total of 21 websites found using relevant keywords, there are 5 websites that were excluded from this stage 1 filtering. What will be filtered phase 2 is 16 websites.

Stage 2 filtering

In filtering stage 2 is the stage of expenditure of applications that are not relevant to the discussion of research and or applications that are not related to research. In addition to those related to online media network security will be issued in this stage. Out of a total of 21 websites found using relevant keywords, there is 1 website that is not relevant to this research. Therefore, at filtering stage 2, 1 website is expelled. What will be filtered out phase 3 is 15 websites.

Stage 3 filtering

This 3rd stage of filtering is the last stage of filtering, namely the expenditure of websites that use third-party applications or devices when running it. Like for example PWNABLE. TW and w3Calls where this website cannot be directly run through the website but requires a supporting application, namely a virtual box to run Linux. Therefore, at the filtering stage 2, 2 websites were expelled.

Scoring

The next stage after carrying out the filtering stages is to score the selected data which will be analyzed on websites resulting from the filtering process with regard to online learning media network security.

INDEX	1	2	3	4	5	7	8
Title	PWNABLE .TW	W3Challs	RingZeroTeam CTF	GoogleCTF2019	Play Game EarlyHacker Catches the Bug	CTFLearn	PicoCTF
Alamat Website	https://pwnable.tw/	https://w3challs.com/	https://ringzer0ctf.com/	https://capturetheflag.withgoogle.com/	http://pwnable.kr/	https://ctflearn.com/	https://play.picoctf.org/
Aspek Penilaian							
Ethical Hacking | Reconnaissance							
1.Nama Domain	1	1	1	0	1	0	1
2.Google Hacking	0	0	0	0	0	0	0
3.Examining HTML	0	0	0	1	0	0	1
Ethical Hacking | Scanning							
1.Open Ports	0	1	1	0	1	0	1
2.Network Scan	0	0	0	0	0	0	0
Ethical Hacking | Gaining Tracks							
1.Dictionary Attack	0	0	0	0	0	0	0
2.Man in the middle	0	0	0	0	0	0	0
3.Phising	0	0	0	0	0	0	0
4.Password Guessing	0	0	0	0	0	0	0
5.Social Enginering	0	0	0	0	0	0	0
Ethical Hacking | Maintain Tracks							
1.Priviledge Escalation	0	0	0	0	0	0	0
Ethical Hacking | Clearing Tracks							
1.Clearing Logs	0	0	0	0	0	0	0
2.Maintain Logs	0	0	0	0	0	0	0
3.Removing Files	0	0	0	0	0	0	0
	1	2	2	1	2	0	3
Aspek Gamifikasi							
Dinamika							
Dinamika | Rintangan	1	1	1	1	1	1	1
Dinamika | Narasi	0	0	0	1	1	1	1
Dinamika | Progress	1	1	1	1	0	1	1
Dinamika | Hubungan	0	1	0	0	0	0	0
Mekanika							
Mekanika | Tantangan	1	1	1	1	1	1	1
Mekanika | Peluang	0	0	0	0	0	0	0
Mekanika | Kompetisi	0	0	0	0	0	0	0
Mekanika | Kerjasama	0	0	0	0	0	0	0
Mekanika | Umpan balik	0	0	0	0	0	0	1
Mekanika | Akuisisi Sumber Daya	0	0	0	0	0	0	0
Mekanika | Hadiah	0	1	0	0	0	0	0
Mekanika | Transaksi	0	0	0	0	0	0	0
Mekanika | Perubahan	0	0	0	0	0	0	0
Mekanika | Pernyataan Kemenangan	0	1	1	1	0	1	1
Komponen							
Komponen | Perolehan	0	1	1	0	0	0	1
Komponen | Avatar	0	0	0	0	0	0	0
Komponen | Lencana	0	1	0	0	0	1	0
Komponen | Perlawanan	0	0	0	0	0	0	0
Komponen | Koleksi	0	0	0	0	0	0	0
Komponen | Pertempuran atau Perang	0	0	0	0	0	0	0
Komponen | Pembukaan konten selanjutnya	0	0	0	1	0	0	0
Komponen | Pemberian hadiah	0	0	1	0	0	0	1
Komponen | Papan Prestasi	0	1	0	0	0	0	1
Komponen | Tingkat	0	0	0	0	0	0	0
Komponen | Poin	0	1	1	0	0	0	1
Komponen | Quest	0	1	1	1	1	0	1
Komponen | Grafik Sosial	0	0	0	0	0	1	1
Komponen | Tim	0	0	0	0	0	0	0
Komponen | Barang Virtual	0	0	0	0	0	0	0
	3	11	8	7	4	7	12

Scoring with description of ethical hacking aspect and gamification aspect

Indeks *Website Cyber Security*	1	2	Indeks *Website Cyber Security*	3	4
Nama Aplikasi	PWNABLE.TW	W3Challs	Nama Aplikasi	RingZeroTeam CTF	GoogleCTF2019
Alamat Website	https://pwnable.tw/	https://w3challs.com/	Alamat Website	https://ringzer0ctf.com/	https://capturetheflag.withgoogle.com/
Deskripsi penilaian Security Audit	aspek security audit yang ada sangat kurang, dilihat dari skor peolehan yang sangat kecil	Aspek ethical hacking yang terdapat dalam website ini masih sangat kurang, hanya terdapat beberapa saja yang di implementasikan	Deskripsi penilaian Security Audit	Dilihat dari perolehan skor, website CTF ini belum memberikan rintangan mengenai ethical hacking secara menyeluruh	Dilihat dari skor yang didapatkan, website CTF ini hanya memenuhi satu sub aspek dari ethical hacking saja, dan tidak mengimplementasikan sub-aspekyang lain
Deskripsi penilaian Gamifikasi	Aspek gamifikasi yang tercapai masih sangat sedikit, dan masih bisa ditambahkan dan ditingkatkan	Aspek gamifikasinya masih sangat minim, sehingga kurang menghasilkan rasa penasaran saat menjalankannya	Deskripsi penilaian Gamifikasi	Aspek gamifikasi yang diberikan sangat minim, yang ditonjolkan sebatas tantangan dan rintangan	Aspek gamifikasinya masih kurang memuaskan, aspek komponen hanya mendapatkan nilai 0,13
Security Audit| Reconnaissance |Domain Name	1	1	Security Audit| Reconnaissance |Domain Name	1	0
Security Audit| Reconnaissance | Google Hacking	0	0	Security Audit| Reconnaissance | Google Hacking	0	0
Security Audit| Reconnaissance | Examining HTML	0	0	Security Audit| Reconnaissance | Examining HTML	0	1
Security Audit| Scanning | Open Ports	0	1	Security Audit| Scanning | Open Ports	1	0
Security Audit| Scanning | Network Scan	0	0	Security Audit| Scanning | Network Scan	0	0
Security Audit| Gaining Access | Dictionary Attack	0	0	Security Audit| Gaining Access | Dictionary Attack	0	0
Security Audit| Gaining Access | MITM	0	0	Security Audit| Gaining Access | MITM	0	0
Security Audit| Gaining Access | Phising	0	0	Security Audit| Gaining Access | Phising	0	0
Security Audit| Gaining Access | Password Guessing	0	0	Security Audit| Gaining Access | Password Guessing	0	0
Security Audit| Gaining Access | Social Enginering	0	0	Security Audit| Gaining Access | Social Enginering	0	0
Security Audit| Maintain Access | Priveliedge Escalataion	0	0	Security Audit| Maintain Access | Priveliedge Escalataion	0	0
Security Audit| Clearing Tracks | Clearing Logs	0	0	Security Audit| Clearing Tracks | Clearing Logs	0	0
Security Audit| Clearing Tracks | Modifyign Logs	0	0	Security Audit| Clearing Tracks | Modifyign Logs	0	0
Security Audit| Clearing Tracks | Removing files	0	0	Security Audit| Clearing Tracks | Removing files	0	0
Dinamika | Rintangan	1	1	Dinamika | Rintangan	1	1
Dinamika | Narasi	0	0	Dinamika | Narasi	0	1
Dinamika | Progress	1	1	Dinamika | Progress	1	1
Dinamika | Hubungan	0	1	Dinamika | Hubungan	0	0
Mekanika | Tantangan	1	1	Mekanika | Tantangan	1	1
Mekanika | Peluang	0	0	Mekanika | Peluang	0	0
Mekanika | Kompetisi	0	0	Mekanika | Kompetisi	0	0
Mekanika | Kerjasama	0	0	Mekanika | Kerjasama	0	0
Mekanika | Umpanbalik	0	0	Mekanika | Umpanbalik	0	0
Mekanika | Akuisisi Sumber Daya	0	0	Mekanika | Akuisisi Sumber Daya	0	0
Mekanika | Hadiah	0	1	Mekanika | Hadiah	0	0
Mekanika | Transaksi	0	0	Mekanika | Transaksi	0	0
Mekanika | Perubahan	0	0	Mekanika | Perubahan	0	0
Mekanika | Pernyataan Kemenangan	0	1	Mekanika | Pernyataan Kemenangan	1	1
Komponen | Perolehan	0	1	Komponen | Perolehan	1	0
Komponen | Avatar	0	0	Komponen | Avatar	0	0
Komponen | Lencana	0	1	Komponen | Lencana	0	0
Komponen | Perlawanan	0	0	Komponen | Perlawanan	0	0
Komponen | Koleksi	0	0	Komponen | Koleksi	0	0
Komponen | Pertempuran atau perang	0	0	Komponen | Pertempuran atau perang	0	0
Komponen | Pembukaan Konten selanjutnya	0	0	Komponen | Pembukaan Konten selanjutnya	0	1
Komponen | Pemberian Hadiah	0	0	Komponen | Pemberian Hadiah	1	0
Komponen | Papan Prestasi	0	1	Komponen | Papan Prestasi	0	0
Komponen | Tingkat	0	0	Komponen | Tingkat	0	0
Komponen | Poin	0	1	Komponen | Poin	1	0
Komponen | Quest	0	1	Komponen | Quest	1	1
Komponen | Grafik Sosial	0	0	Komponen | Grafik Sosial	0	0
Komponen | Tim	0	0	Komponen | Tim	0	0
Komponen | Barang Virtual	0	0	Komponen | Barang Virtual	0	0
Total Reconaissance	1	1	Total Reconaissance	1	1
Total Scanning	0	1	Total Scanning	1	0
Total Gaining Access	0	0	Total Gaining Access	0	0
Total Maintain Access	0	0	Total Maintain Access	0	0
Total Clearing Tracks	0	0	Total Clearing Tracks	0	0
Total Dinamika	2	3	Total Dinamika	2	3
Total Mekanika	1	3	Total Mekanika	2	2
Total Komponen	0	5	Total Komponen	4	2

4.

.

5. CONCLUSION

Ethical Hacking

Of all these CTF-based Cyber Security websites, the CTF-based Cyber Security website that gets a score higher than the overall fulfillment score is 7 websites. And those that have not met the score of obtaining scores are as many as 2 websites.

Based on the data obtained from the research that has been carried out, there are aspects that can be met with the highest score of 10 out of 14, namely the Domain Name aspect, while there are aspects that do not get a score at all or these aspects are not contained in every CTF-based Cyber Security website that is used as the object of research. These aspects are Network Scan, all aspects of Gaining Tracks, and Maintain Track.

Ethical hacking should be practiced. Ethical hacking requires knowledge of networking and cyber security. Ethical hacking is a method that if done correctly can be used to understand the weaknesses of a network.

Gamification

Of all CTF-based Cyber Security websites, websites that get a score of more than the gamification score score are as many as 3 websites (This can be said that the website has met more than equal to the score value of the gamification aspect) and those that have not met the acquisition score are as many as 10 websites.

Based on the data, in terms of gamification aspects, the aspect that is most fulfilled is the Obstacle aspect. This aspect gets a fulfillment score of 14 out of 14 (100% of the total website there are aspects assessed). As opposed to that, there are several aspects of not getting a score at all or the score of the fulfillment score is 0 (all websites that are used as research objects, there are no aspects that are assessed), including aspects of Opportunities, Cooperation, Resource Acquisition, Transactions, Changes, Avatars, Resistance, Collections, Battles, Teams, and Virtual Goods. From the discussion above, it reflects that in this CTF-based cyber security website, almost all of them have implemented the Obstacles aspect based on the score of the fulfillment score which reached 14 out of 14. In this CTF-based cyber security website that is used as an object, obstacles are created with participants given questions or obstacles related to CTF-based cyber security that are in accordance with the ethical hacking aspects of course. Where the obstacles given have increased difficulty, participants are given obstacles by looking for flags that are more difficult than before and with a somewhat different method, so that the participant's ability to progess in line with the increased obstacles. Where the progress and results from the previous will be used also to go to the next obstacle. In the level aspect, this CTF-based cyber security website adds levels of obstacles when participants look for these flags, where with the addition of this level, it adds to the progress of participants in understanding CTF-based cyber security based on ethical hacking.

The suitability of the content of the cyber security online learning media with the aspects of ethical hacking is still very low with the total score of each aspect still far from the score. The most fulfilled aspect is the Obstacles with the total score obtained is 13 out of 13.

The results of the evaluation of CTF-based cyber security online learning media on conformity with the ethical hacking and gamification process are that there are many CTF-based cyber security online learning media websites that have not included gamification aspects that can be seen from the total gamification score which is small from the total fulfillment score should be.

ACKNOWLEDGEMENTS

I am especially grateful for Mr. Puspanda Hatta and Mr. Cucuk for constructive criticism and advice of my article.

REFERENCES

[1] C. C. Palmer, “Ethical hacking,” *IBM Syst. J.*, vol. 40, no. 3, pp. 769–780, 2001, doi: 10.1147/sj.403.0769.

[2] S. Patil, A. Jangra, M. Bhale, A. Raina, and P. Kulkarni, “Ethical hacking: The need for cyber security,” *IEEE Int. Conf. Power, Control. Signals Instrum. Eng. ICPCSI 2017*, pp. 1602–1606, 2018, doi: 10.1109/ICPCSI.2017.8391982.

[3] V. Švábenský, P. Čeleda, J. Vykopal, and S. Brišáková, “Cybersecurity knowledge and skills taught in capture the flag challenges,” *Comput. Secur.*, vol. 102, 2021, doi: 10.1016/j.cose.2020.102154.

[4] Elidjen, D. Hidayat, and E. Abdurachman, “The Roles of Gamification, Knowledge Creation, and Entrepreneurial Orientation towards Firm Performance,” *Artif. Intell. Agric.*, 2022, doi: 10.1016/j.ijis.2022.07.002.

[5] D. Dixon, E. Lawley, S. Deterding, S. Björk, and L. E. Nacke, “Designing Gamification: Creating

Gameful and Playful Experiences," *Conf. Hum. Factors Comput. Syst. - Proc.*, vol. 2013-April, pp. 3263–3266, 2013, doi: 10.1145/2468356.2479662.

[6] R. Patricio, A. C. Moreira, and F. Zurlo, "Gamification in innovation teams," *Int. J. Innov. Stud.*, vol. 6, pp. 156–168, 2022, doi: 10.1016/j.ijis.2022.05.003.

[7] R. Perry, B. Lunde, and K. T. Chen, "An evaluation of contraception mobile applications for providers of family planning services," *Contraception*, vol. 93, no. 6, pp. 539–544, 2016, doi: 10.1016/j.contraception.2016.01.005.

[8] D. Ary, L. C. J. Jacobs, C. Sorensen, and A. Razavich, *Introduction to Research in Education*. 2010.